

March 7, 2024

Cybersecurity Primer 3.0

TECHNOLOGY/ANALYTICS, DATA, SECURITY, AND
INFRASTRUCTURE SOFTWARE

SUMMARY

This report presents our comprehensive examination of the security market, analyzing trends from a thematic, technological, and vendor perspective. We believe rising technological complexity (cloud, microservices, containers, AI/GAI), evolving work norms (WFA), a complicated threat landscape, and evolving regulatory frameworks/pressures, are forcing enterprises and IT professionals to prioritize their cybersecurity posture. In turn, vendors are innovating (AI/ML/GAI, automation), evolving their business models (subscriptions/SaaS), and shifting to platforms (critical market share driver). We see solid security spending growth (\$185.4B 2023 TAM, 11.6%E CAGR) highlighting its mission-critical role. Within our group, our top picks are CrowdStrike ("best-of-platform" positioning), CyberArk (PAM leadership, Access/Secrets adoption), and Zscaler (leading SSE vendor). While acknowledging a still tough (but improving) macro backdrop, we expect demand for these vendors to remain resilient and outperform. In this update, we've added overviews for GAI security, enterprise browsers, SSCS, ASPM, DSPM, fraud detection, passwordless authentication, secrets management, and identity verification.

KEY POINTS

- **Landscape trends.** We highlight three developments that have a material impact to the cybersecurity industry. First, the pace/scope of ransomware attacks continues to increase, becoming more disruptive and costly to manage/remediate. Second, the emergence of GAI enables attackers to fine-tune/scale automated social engineering attacks, expanding an already complicated attack surface. Last, new regulations (SEC rules, White House Zero Trust executive order) are forcing execs/IT professionals to prioritize their security posture and spending.
- **Adapting to change.** Security vendors are evolving to address the threats by: (1) implementing AI/ML/GAI and automation to address the scale of modern security needs, improve threat discovery, streamline alerts, and accelerate response and remediation; (2) introducing broadly capable security platforms to better contextualize available data, tightly integrate tools, simplify security operations management, and ease staffing shortages; and (3) offering managed security services to ensure comprehensive enterprise security.
- **Large TAM, solid growth.** The overall security TAM is substantial, totaling \$185.4B in 2023 with an 11.6% 2023-27E CAGR despite recent macro headwinds. We view this as a testament to the diversity and resiliency of the demand catalysts in place, and the central nature and long-term importance of cybersecurity. Cloud security (\$5.6B, 23.2%E CAGR), data privacy (\$1.4B, 18.9%E CAGR), and endpoint security (\$28.2, 14.5%E CAGR) represent the fastest growing segments.
- **Top picks—CRWD, CYBR, ZS.** Our positive stance on CrowdStrike reflects its "best-of-platform" positioning and expansion into high-growth markets, including Threat Protection and Cloud Security. For CyberArk, we're positive on its evolution into an end-to-end identity security vendor, seeing a large opportunity with its workforce identity, secrets management, and endpoint privilege modules. And for Zscaler, we're positive on its SSE/SASE positioning, expanding product offerings, and evolving GTM efforts.
- **Emerging vendors.** Private vendors, such as 1Password, Aqua Security, Arctic Wolf, Armis, Axonius, BigID, Cato Networks, Claroty, Illumio, JumpCloud, Keyfactor, Netskope, OneTrust, Orca, RecordedFuture, Snyk, Sysdig, Versa Networks, and Wiz, are disrupting the security landscape. These innovators are leveraging cloud-native security platforms and AI/GAI to address challenges in their respective areas. We expect them to outpace market growth.

For analyst certification and important disclosures, see the Disclosure Appendix.

Ittai Kidron
212-667-6292
Ittai.Kidron@opco.com

Harshil Thakkar
212-667-6299
Harshil.Thakkar@opco.com

Param Singh, CFA
212-667-7683
param.singh@opco.com

George Iwanyc
415-399-5748
George.Iwanyc@opco.com

Disseminated: March 7, 2024 07:03 EST; Produced: March 7, 2024 07:03 EST

Table of contents

SECURITY MARKET PRIMER: EXECUTIVE SUMMARY	5
KEY TRENDS	6
GROWING ATTACK SURFACE, SOPHISTICATION, AND COST OF CYBER ATTACKS	6
SHORTAGE OF QUALIFIED SECURITY PROFESSIONALS	10
LABOR SHORTFALL = CATALYST FOR CHANGE ACROSS THE SECURITY MARKET	11
IMPACT OF GENERATIVE AI ON CYBERSECURITY	13
MARKET CONSOLIDATION AND THE EMERGENCE OF SECURITY PLATFORMS	17
SECURITY MARKET OPPORTUNITY & VENDOR MAP	20
NETWORK SECURITY	27
NETWORK FIREWALLS	27
NETWORK ACCESS CONTROL (NAC)	30
CLOUD ACCESS SECURITY BROKER (CASB)	31
ZERO TRUST NETWORK ACCESS (ZTNA)	33
SECURE WEB GATEWAY (SWG)	36
SOFTWARE-DEFINED WIDE AREA NETWORKING (SD-WAN)	37
SECURITY SERVICE EDGE (SSE)/SECURE ACCESS SERVICE EDGE (SASE)	39
MICRO-SEGMENTATION	41
ENTERPRISE BROWSERS	42
NETWORK SECURITY MARKET VENDOR OVERVIEW	44
CLOUD WORKLOAD SECURITY	50
CLOUD WORKLOAD PROTECTION PLATFORMS (CWPP)	51
CLOUD SECURITY POSTURE MANAGEMENT (CSPM)	53
CLOUD WORKLOAD SECURITY MARKET VENDOR OVERVIEW	55
APPLICATION SECURITY	56
APPLICATION SECURITY TESTING (AST)	61
SOFTWARE COMPOSITION ANALYSIS (SCA)	63
SOFTWARE SUPPLY CHAIN SECURITY (SSCS)	65
STATIC APPLICATION SECURITY TESTING (SAST)	67
DYNAMIC APPLICATION SECURITY TESTING (DAST)	68
INTERACTIVE APPLICATION SECURITY TESTING (IAST)	69
APPLICATION SECURITY POSTURE MANAGEMENT (ASPM)	70
APPLICATION RUNTIME SECURITY (ARS)	71
RUNTIME APPLICATION SELF-PROTECTION (RASP)	73
WEB APPLICATION FIREWALL (WAF)	74

CONTAINER SECURITY	76
API SECURITY	81
APPLICATION SECURITY MARKET EVOLUTION	85
CLOUD-NATIVE APPLICATION PROTECTION PLATFORMS (CNAPP)	88
APPLICATION SECURITY MARKET VENDOR OVERVIEW	91
DATA SECURITY	94
DATA SECURITY POSTURE MANAGEMENT (DSPM)	94
DATA LOSS PREVENTION (DLP)	96
DATA PRIVACY AND RISK MANAGEMENT	97
DATA DISCOVERY	104
RIGHTS, CONSENT, AND PREFERENCE	104
DATA PRIVACY, COMPLIANCE, AND GOVERNANCE VENDOR OVERVIEW	107
IDENTITY & ACCESS MANAGEMENT	109
ACCESS MANAGEMENT (AM)	111
FRAUD DETECTION	116
PASSWORDLESS AUTHENTICATION	117
IDENTITY GOVERNANCE & ADMINISTRATION (IGA)	119
PRIVILEGED ACCESS MANAGEMENT (PAM)	121
CLOUD INFRASTRUCTURE ENTITLEMENT MANAGEMENT (CIEM)	124
SECRETS MANAGEMENT	127
IDENTITY VERIFICATION	129
CONVERGENCE OF IDENTITY SECURITY CAPABILITIES AND OFFERINGS	129
IDENTITY & ACCESS MANAGEMENT MARKET VENDOR OVERVIEW	130
EMAIL SECURITY	137
EMAIL SECURITY MARKET VENDOR OVERVIEW	139
ENDPOINT SECURITY	140
ENDPOINT PROTECTION PLATFORMS (EPP)/ENDPOINT DETECTION & RESPONSE (EDR)	140
EXTENDED DETECTION & RESPONSE (XDR)	142
IDENTITY THREAT DETECTION & RESPONSE (ITDR)	145
MANAGED DETECTION & RESPONSE (MDR)	146
ENDPOINT SECURITY MARKET VENDOR OVERVIEW	148
SECURITY OPERATIONS	152
THREAT INTELLIGENCE (TI)	152
ATTACK SURFACE MANAGEMENT (ASM)	153
VULNERABILITY MANAGEMENT (VM)	156
SIEM AND SOAR	158

SIEM vs. XDR _____	160
SECURITY OPERATIONS MARKET VENDOR OVERVIEW _____	161
BLOCKCHAIN & CRYPTO SECURITY _____	165
BLOCKCHAIN BACKGROUND _____	165
THE BLOCKCHAIN ECOSYSTEM _____	169
BLOCKCHAIN SECURITY THREAT VECTORS _____	172
VENDOR HIGHLIGHTS _____	178
GLOSSARY OF ACRONYMS _____	179

Security Market Primer: Executive Summary

“When one door closes, another window opens.”— Julie Andrews. This undeniable truth is inevitable when describing the current state of the security market, which is trying to keep up with a complex threat landscape and the escalating sophistication of cyberattacks and their consequences. This challenge reflects a reality where security efforts must run shoulder-to-shoulder with business operations in constant motion, assuming threats are never fully addressed. Enterprises are embracing digital transformation, adapting to new work models (mobility and work from anywhere), prioritizing customer engagement (virtual and self-service), and adjusting to evolving regulatory demands (regulation, data sovereignty, etc.). The rapid technological shifts (cloud, SaaS, microservices, containers, etc.) complicate the security framework further, add to the threat landscape, and dramatically expand the attack surface (more users, devices, and use cases), opening new windows of opportunity for attackers. Coupled with budget constraints, organizations are struggling to strike a balance between cost and efficacy.

Today, more than ever, IT professionals must rethink their operational readiness, infrastructure and application development requirements, IT spending priorities, and how to best adapt to dynamic regulatory, macro, and geopolitical environments. An integral part of this adaptation is an escalating need to reinforce security readiness and reevaluate security investments and architectures to determine how best to protect infrastructure, data, workflows, and intellectual property.

This report comprehensively examines the security market, analyzing key trends from an environment, technical, and vendor perspective. Overall, our main observations of the all-encompassing security market are:

- The pace and sophistication of cybersecurity attacks continue to increase, and the associated business disruption and financial and reputational costs have worsened in 2023. Regulatory pressures are also rising, forcing C-suite and board-level conversations and accountability around cybersecurity posture.
- The technical complexity of securing the enterprise has never been more challenging as the attack surface expands outside the perimeter to remote and mobile devices, cloud infrastructure, and cloud-native and SaaS applications.
- AI/ML (including Generative AI) based automation is increasingly implemented within security tools to address the scale of modern security, improve threat discovery, streamline alert filtering, and accelerate response and remediation.
- Security platforms continue to gain traction as enterprises look to simplify security operations management and control their overall IT and security spending amidst a tepid macro landscape.
- Managed security services are increasingly critical to ensuring comprehensive security, especially for small and mid-sized businesses.
- The chronic shortage of trained security professionals has increased the intensity of the above trends.

With these trends in mind, we see risks and opportunities for cybersecurity vendors. Specifically, we expect vendors to (1) complete their transition to the cloud and embrace as-a-Service models; (2) complement their offerings with managed services, where it makes sense, to address opportunities in the mid/down market; (3) aggressively expand into adjacent market segments, shifting from a product-focused to a platform-focused model; and (4) enhance their product suite with AI/ML/GAI capabilities.

A large market with durable growth. We expect spending on security solutions to continue at a healthy pace. Based on Gartner’s market research, the overall security TAM is substantial, expected to total \$185.4 billion in 2023 and to grow at an 11.6% CAGR through 2027 to \$287.0 billion. This TAM aggregates market opportunities across application, cloud, data, endpoint, identity, and infrastructure security. Cloud security (\$5.6 billion with a 23.2% CAGR) and data privacy (\$1.4 billion with an 18.9% CAGR) reflect the most rapidly growing opportunities. In comparison, endpoint & SOC security (\$28.2 billion

with a 14.5% CAGR), infrastructure security (\$20.2 billion with an 11.3% CAGR), and identity security (\$16.1 billion with an 11.6% CAGR) are the largest markets based on absolute spending levels. We view the security market as a comparatively resilient IT spending area due to its mission-critical importance to operational readiness, although it is not immune and is sensitive to macroeconomic cycles. Nonetheless, the variety of sub-segments growing at healthy levels and at scale is a testament to the market's importance, the diversity and gravity of the demand catalysts, and the central nature of security to enterprise success.

Selective within our security coverage. Overall, we favor vendors with growing exposure to the fastest-demand areas within the market that have managed to evolve their portfolios into complete platforms. And while generally positive on all of the vendors in our security group, we highlight Zscaler, CyberArk, and CrowdStrike as our top picks.

We view Zscaler as the leading SSE vendor and a key beneficiary of the shift from traditional perimeter-based network security to zero-trust architectures, with incremental tailwinds from growing regulatory scrutiny (SEC; Zero-Trust Executive Order). In addition to strength in its core ZIA product, the company has significant upsell opportunities with ZPA, ZDX, and Data Protection, and sees sustained momentum over the next 2-3 years with new products such as Risk360, Branch Connector, and ITDR. In early 2024, Zscaler rebranded and repackaged its branch connector and ZIA/ZPA capabilities as a complete SASE offering. We believe that as Zscaler expands its GTM efforts (SIs/VARs), it can attain deeper large account penetration, mid-market logo growth, and margin expansion.

We're bullish on CyberArk and believe the company has successfully evolved from a pure-play PAM vendor to an identity security platform. It has seen strong traction for its endpoint privilege, secrets management, and access management solutions, and we expect this momentum to continue as customers prioritize spending for identity security. CyberArk was one the first vendors to offer a platform that includes PAM and AM, and we believe it is positioned to win customers looking to consolidate their identity security architecture into a single platform.

Our positive stance on CrowdStrike reflects our view that it: (1) has successfully evolved into a "best-of-platform" security vendor, an attractive option for customers looking to consolidate their security stack; (2) has significantly expanded its TAM into nascent (but fast-growing) markets such as Identity Threat Protection and Cloud Security; (3) can replicate its playbook and execution in driving quick adoption of new products (ASPM, Falcon for IT, Charlotte AI); and (4) can build a comprehensive Zero Trust platform that covers endpoint, data, and identity security.

Private companies are disrupting and driving change. A range of private companies addressing various parts of the security market is advancing many of the trends we highlight in this report. And with a large and fast-evolving security TAM, we see opportunities for these and other emerging security vendors to succeed and play a disruptive role in their domains. Several private companies have already emerged as market disruptors in the following security segments:

- **Identity and Access Management Security**—1Password, JumpCloud, Keyfactor.
- **Application and Cloud Security**—Aqua Security, Snyk, Orca Security, Sysdig, Wiz.
- **Security Operations**—Arctic Wolf, Claroty, Armis, Axonius, RecordedFuture.
- **Network Security**—Cato Networks, Illumio, Netskope, Versa Networks.
- **Data Security**—BigID, OneTrust.

Key Trends

Growing Attack Surface, Sophistication, and Cost of Cyber Attacks

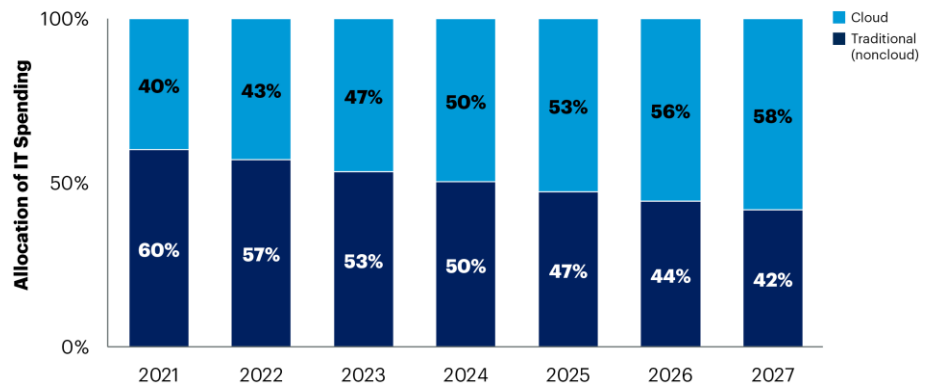
The pace and sophistication of cybersecurity attacks continue to increase, and the associated business disruption has worsened. This escalation reflects a fast-evolving landscape where the: (1) attack surface is expanding outside the perimeter to remote and mobile devices, cloud infrastructure, and SaaS applications; (2) security tools that address

modern-day cloud-native applications incorporating microservices, containers, and functions have yet to mature; (3) number of bad actors and volume of attacks continue to increase across multiple threat paths (ransomware, malware, phishing, malicious inside activity, etc.); (4) monetary impact of breaches continues to climb as the criticality and sensitivity of the data exposed, the reputational damage of a breach, and the magnitude of business disruption rises; (5) growing global geopolitical tensions (Russia-Ukraine, Middle East) add risks; (6) use of Generative AI in social engineering attacks is expanding; and (7) regulatory frameworks and disclosures adopted (SEC requirements, White House executive order on zero-trust) are requiring significant investment. Below, we review these drivers in more detail.

We start with the scope of securing an enterprise that has extended well beyond its perimeter. The workday paradigm has changed (remote work, work anywhere), the applications we engage with have evolved (cloud-native and SaaS), and remote connectivity has become ubiquitous (cellular and Wi-Fi). Despite a return-to-office push, many enterprises have embraced remote access and flexible work schedules to improve employee productivity and efficiency. As a result, CIOs have had to: (1) adapt to a bring-your-own-device (BYOD) mindset to save cost and appeal to workers; (2) look for ways to improve user experience and application/workflow speed to improve satisfaction and productivity; (3) incorporate applications that empower users with limited IT involvement; and (4) endure the realities of self-service shadow IT (use of free, open-source software, independent and unsupervised use of SaaS applications, etc.). The outcome is an explosion in the number/diversity of devices, endpoints, and connections that need to be secured, which makes for an expanding attack surface.

The shifting infrastructure landscape incorporating on-premise, hybrid, and multi-cloud resources has also complicated the security environment. The operational complexity of keeping a consistent framework (protocols, compliance, configuration, etc.) across domains is compounded as infrastructure scales. This is especially true in cloud environments where states change quickly, and scale and diversity are ever-growing. Ultimately, as infrastructure expands, so do the attack surface and security gaps, making their management difficult (too many alerts, false positives, uninvestigated alerts, compromised credentials, etc.). Companies earlier in their cloud migration are also often overly reliant on the native controls from cloud service providers, yielding misconfigurations and excess privileges that leave them vulnerable to breaches. Many enterprise stakeholders initially have overconfidence in built-in cloud security controls and move forward with their cloud initiatives before considering and implementing a proper security framework.

Exhibit 1: Cloud Share of IT Spending Continues to Grow



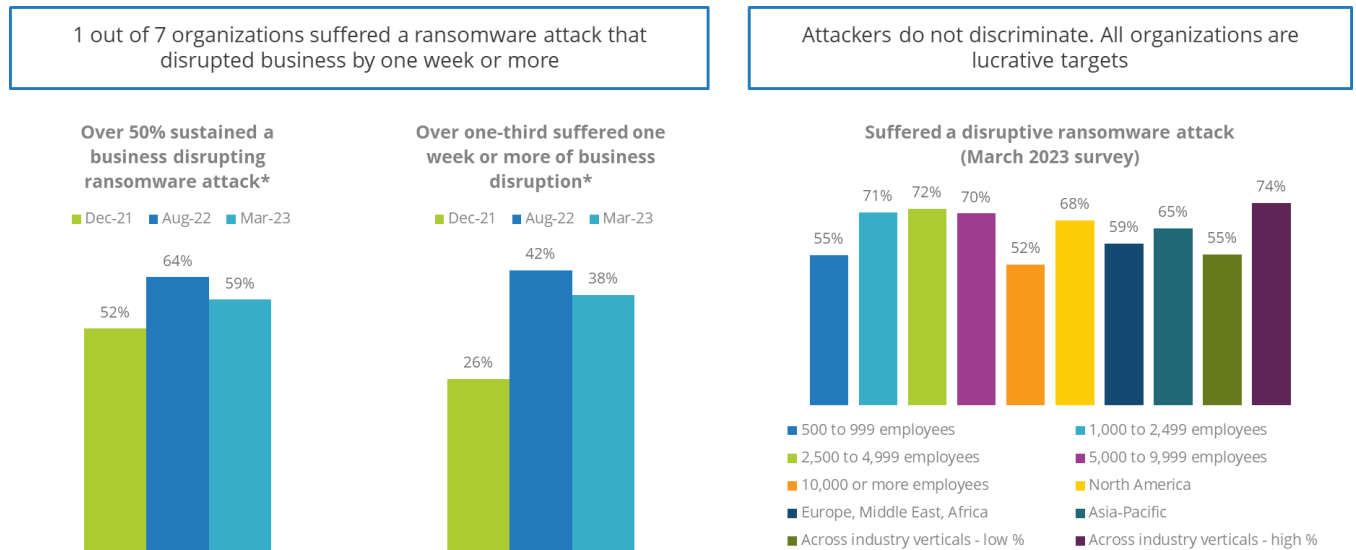
Source: Gartner

Evolving and growing infrastructure environments aren't the only cloud-related security challenges. Application scale, delivery, and complexity also grow as new cloud-native architectures leveraging containers, microservices, and serverless and cloud-native application development and delivery take hold. While these new foundational building blocks accelerate application development and deployment, they introduce many connections and dependencies between internal and third-party elements. And given the ephemeral nature of these tools, traditional agent-based security controls are often

ineffective. The result is a difficult-to-secure fragmented environment where many factors must come together cohesively. Attackers have responded and have capitalized on the added complexity, driving a rise in new zero-day attacks. The reality is that, while the security tools addressing containers, microservices, and cloud-native delivery have evolved, they are still not well integrated and lack feature sets and controls.

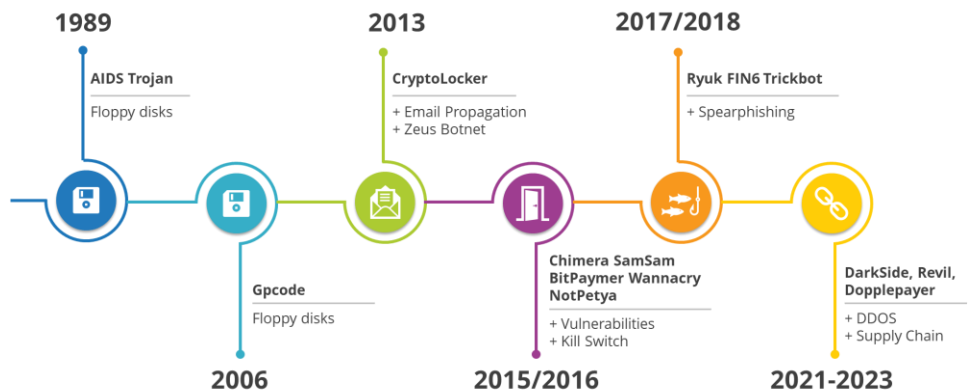
The rise of Generative AI (GAI) adds another wrinkle and has enabled attackers to fine-tune and scale automated social engineering attacks. With GAI, attackers can automatically comb social media to identify relevant personas to imitate and, with natural language processing capabilities, craft highly personalized phishing attacks. GAI deepfakes also pose a risk, as attackers can impersonate key executives and privileged individuals to manipulate unsuspecting employees. While GAI benefits organizations, enabling greater automation and improved productivity, it also enhances the capabilities of threat actors. We discuss GAI in greater detail later in the note.

Exhibit 2: Ransomware Attacks Becoming More Disruptive



Source: IDC Market Analysis Perspective Worldwide Endpoint Security (June 2023)

Exhibit 3: History of Cyber Attacks Becoming Progressively More Targeted



Source: IDC (Ransomware Winter 2023)

Lastly, expanding regulations and government mandates are pushing executives to re-examine their cyber security posture and actively address potential threats and exposures. In that regard, two recent government mandates have increased the urgency of implementing robust cybersecurity standards. The first was the US Securities and Exchange Commission (SEC), which published new rules requiring public companies to report on their cyber posture, systems, and material cybersecurity incidents within four business days via an 8-K filing. They must also outline their processes for identifying and

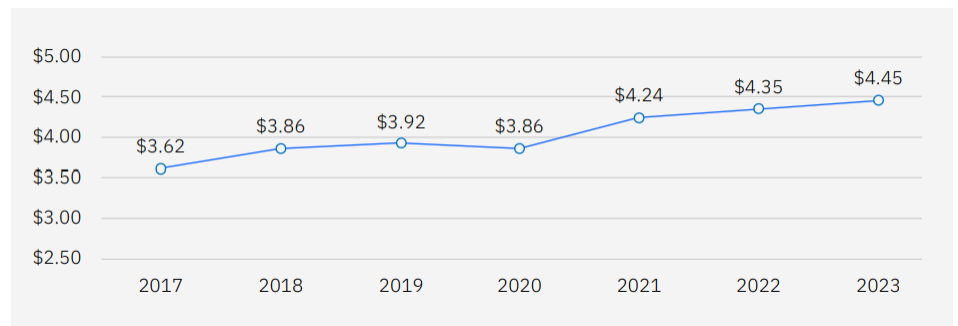
managing risks from potential cybersecurity threats in their annual 10-K filing. The second is Biden’s White House executive order, which requires US federal and civilian agencies to implement zero-trust cybersecurity principles with a heightened focus on critical infrastructure control systems by September 2025. We expect government scrutiny and mandates to increase in future years.

The negative operational consequences of cybersecurity attacks continue to be felt across enterprises of all sizes and can result in substantial business disruption, data loss, and high costs. To put the cost impact in perspective, IBM reported in its annual *Cost of a Data Breach Report 2023* that the average cost of a data breach increased 2.3% YoY to an all-time high of \$4.45 million and that it took on average 277 days to identify and contain a breach. And the longer it took to discover and contain a breach, the more costly its impact was. On average, a breach that takes longer than 200 days costs \$4.95 million, while breaches that take less than 200 days cost only \$3.93 million.

The type of breach also impacts its cost, with ransomware breaches incredibly destructive at an average of \$5.13 million, not including the ransom itself. This reflects a 13% increase from \$4.62 million in 2022. This is a significant issue as ransomware attacks are rising (up 95% from 2022) and are more common (~25% of attacks). Attackers are increasingly focusing on cloud data stores, which accounted for 27% of breaches in 2023, compared to 18% targeting on-premises stores. Cloud breaches are significantly more costly for organizations, with an average cost of \$4.57 million versus an average cost of \$3.99 million for an on-premises breach.

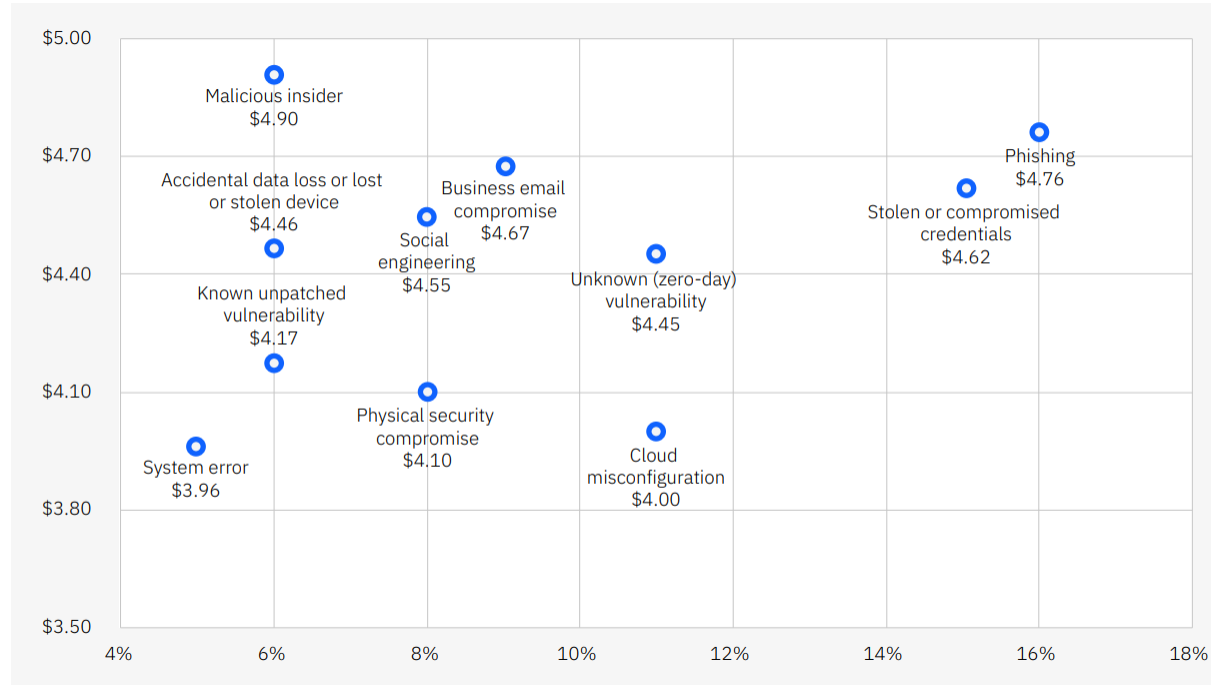
The MGM data breach in 2023 is an example of the high cost of a data breach. In September, MGM was the victim of a social engineering attack that enabled hackers to access internal systems, holding MGM up for ransom and effectively shutting down multiple properties in Las Vegas. The disruption cost MGM \$100M in lost revenue while it worked to regain control and bring systems back online. Beyond the financial impact of disrupting operations, several companies have had to pay fines and settlements for breaches that involved sensitive customer data. Equifax was ordered to pay ~\$700M for its 2017 data breach, and T-Mobile agreed to a \$350M settlement for its 2021 data breach.

Exhibit 4: Average Total Cost of a Data Breach (in US\$ Millions)



Source: IBM Security (Cost of a Data Breach Report 2023)

Exhibit 5: Average Total Cost and Frequency of Data Breaches by Initial Attack Vector (in US\$ Millions)*



Source: IBM Security (Cost of a Data Breach Report 2023)

* The X-axis reflects the percentage mix of the initial breach attack vector

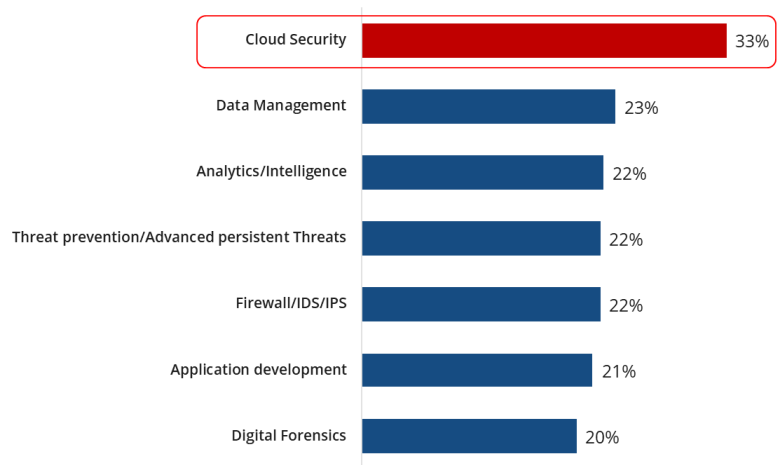
Shortage of Qualified Security Professionals

One of the first steps in implementing an effective security posture is building a team to plan, execute, and maintain it. Unfortunately, staffing remains challenging for many companies due to an acute shortage of security professionals, which is exacerbated by the fast-changing threat landscape, growing complexity in IT systems (on-premise, cloud, SaaS, mobile, etc.), and the ongoing need to keep pace with the rapid evolution and innovation in security tools addressing the changing threat landscape.

Several industry studies have attempted to put the shortfall in perspective. The (ISC)², an IT security professional trade association, reported in its *2023 Cybersecurity Workforce Study* that there were ~1.5M cybersecurity professionals estimated to be working in the US (an increase of +11.3% year-over-year) and 5.4M cybersecurity professionals worldwide (an increase of +8.7% year-over-year). However, the growth in cybersecurity professionals continues to fall short of demand, with the study estimating the global cybersecurity workforce gap increasing +12.6% year-over-year, with the US cybersecurity workforce shortage now over 482K (an increase of +17.6% year-over-year). Studies by CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE) and The Computing Technology Industry Association (CompTIA), have also reported troublesome shortfalls in talent. CyberSeek noted a US cybersecurity workforce of 1.1M and a need for an additional ~572K professionals.

Even organizations that have invested in cybersecurity talent have experienced a significant gap as they try to keep up with an ever-changing threat landscape and fast-paced digital transformation activity. An IDC survey from August 2022 noted that almost half of organizations surveyed reported a skills gap, with nearly a third reporting a need for skilled cloud security professionals. We expect this gap to remain in place as the rate of cloud adoption remains high and as organizations struggle to hire personnel with qualified skills, a still nascent security domain.

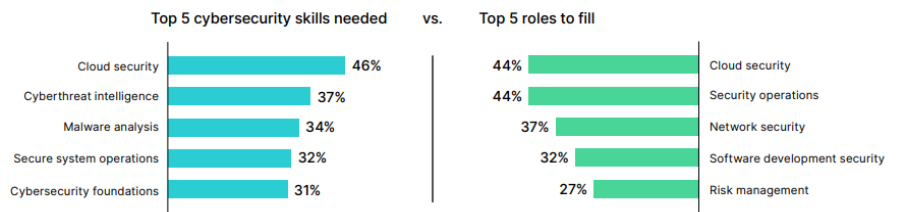
Exhibit 6: Top 7 Most Needed Skills by Security Domains



Source: IDC (Cybersecurity Outlook 2023)

Findings from Fortinet’s 2023 Cybersecurity Skills Gap report also underlined the shortage of cybersecurity professionals. In the report, 68% of respondents (out of 1,855) indicated additional risks due to a cybersecurity skills shortage, with 56% struggling to recruit professionals and 54% struggling to retain existing employees. From a domain perspective, the report highlighted cloud security and security operations as the most challenging roles to fill. Additionally, respondents highlighted growing involvement from the Board of Directors, with 93% of respondents indicating their boards raising questions about organizational cybersecurity posture. Given the increasing costs of breaches, we expect cybersecurity to remain a top governance priority.

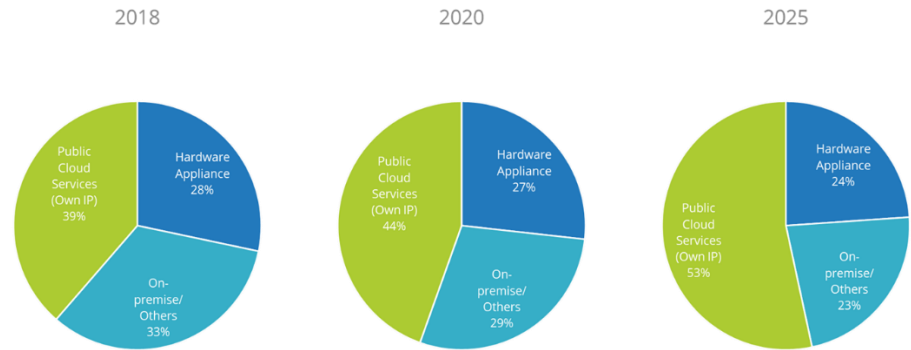
Exhibit 7: Cloud Security and Security Operations Remain a Priority



Source: Fortinet 2023 Cybersecurity Skills Gap Global Research Report (1,855 survey respondents)

Labor Shortfall = Catalyst for Change across the Security Market

The shortfall in trained security professionals and budget challenges are positives for security software vendors as enterprises seek technology solutions to fill gaps and increase security staff effectiveness. We believe the shortage of skilled security professionals is forcing enterprises to: (1) look for automation and AI to improve threat discovery, simplify alert filtering, and accelerate response and remediation; (2) grow the use of third-party security services, such as managed detection and response (MDR) services to complement and extend in-house security resources; and (3) increase the adoption of broadly capable security platforms that can simplify, streamline, and consolidate security operations management. This is favorable for cloud-native security tools that can eliminate operational overhead from an infrastructure and maintenance perspective, improve ease of use, and offer greater platform flexibility and scalability.

Exhibit 8: Changing Complexion of Security

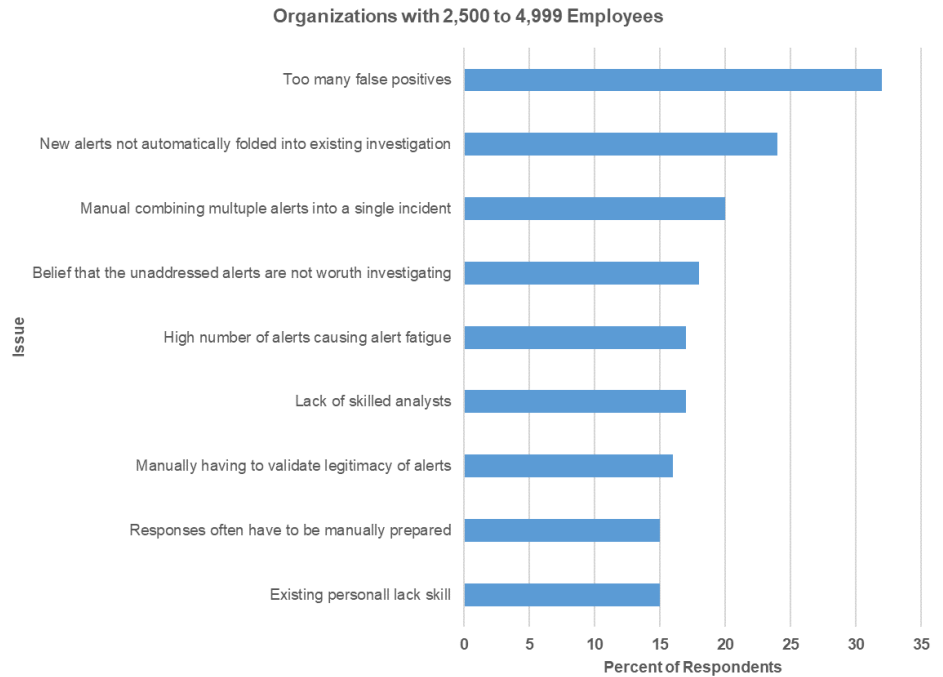
Source: IDC (Cybersecurity Megatrends 2022) IDC Semiannual Security Products Tracker (2H 2020)

AI and automation are critical to establishing efficient security workflows and implementing threat discovery, alert filtering, response, and remediation. They are also effective in lowering the financial cost of a data breach. While security vendors have incorporated AI-driven observation and decision-making for years, the rise of Generative AI has unlocked new opportunities. Most leading vendors have leveraged Generative AI to develop Security Assistants (examples include Charlotte AI from CrowdStrike and AI Assistant from Splunk) that enable users to automate repetitive tasks and queries with natural language. These new solutions offer an opportunity to reduce the skills shortages in operating complex SOC tools (like EDR, XDR, and SIEM) and alleviate pressure on overburdened SOC teams.

Another outcome of the shortage in skilled labor is the growing use of third-party security services, such as MDR services from independent service providers or EDR vendors. These services complement on-premise security operations with a remotely staffed 24/7/365 managed security operations center (SOC). They address a broad spectrum of needs, from passive monitoring and alerting (a “second set of eyes”) through more active alert triage, analytics, and threat hunting/mitigation, to assisting with the management of the security stack, performing contextualized data analysis, and remediating and responding to events on behalf of the customer.

Several MDR vendors provide services to manage the customer’s security toolset, while others bring their proprietary technology stack to replace or complement the customer’s existing capabilities. An IDC survey highlighted MDR as a top 3 spending priority for organizations, with almost 25% of respondents indicating their MDR solution will see an increase in funding. Consequently, many security vendors have introduced managed service elements into their portfolios. We believe this will become more important as threat levels escalate and evolve and vendors look to serve small and mid-sized businesses.

Exhibit 9: A High Alert Volume Can Lead to Ineffective Response



Source: IDC (Cybersecurity Megatrends 2022)

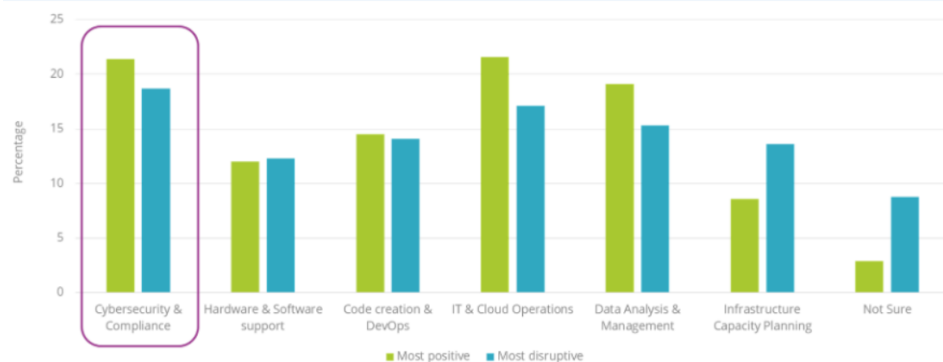
Lastly, the labor shortage is motivating CISOs to reduce the number of security tools and systems deployed by adopting broad security platforms to simplify and streamline overall security operations management. Following the “best-of-breed” boom in 2020-2021, organizations struggled to find professionals with knowledge of multiple security tools and interfaces. The challenging macro conditions in 2022 and 2023 exacerbated this issue and are driving organizations to consolidate spending to security platforms, elevating the strategic importance of vendors with broad product portfolios that have shown an ability to deeply integrate capabilities across security domains. Vendors establishing a top-of-the-stack position in the security layer, bringing all security-related telemetry into a single view, are in a strong competitive position. In the long term, tool consolidation will drive vendor consolidation as critical mass builds with a few leaders. We discuss this in more detail in the market consolidation section.

Impact of Generative AI on Cybersecurity

The advent of Generative AI (GAI) has had a dual impact on the cybersecurity industry. On the one hand, it enhanced existing security tools and capabilities, helped address the technical talent shortage, and created new revenue opportunities for security vendors. On the other hand, it opened up a new and broader attack surface for threat actors to exploit, created more sophisticated malware and phishing attacks, and increased autonomous attacks. This view is broadly reflected in IDC’s Future Enterprise Resiliency & Spending survey, which estimates that GAI will be the most positive and disruptive to the cybersecurity and compliance verticals.

Exhibit 10: Generative AI Most Impactful Across Cybersecurity

Thinking about the organization in which you work, in which IT area do you think generative AI will have the most positive impact in the next 18 months? Where will it have the most disruptive impact?



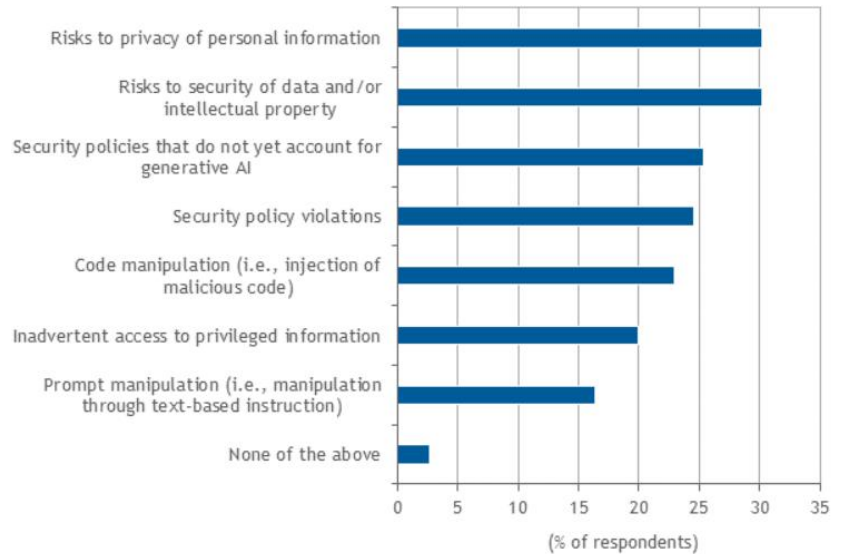
Source: IDC

We see multiple benefits to implementing GAI across the security software landscape. First and more near term, by introducing GAI-enabled co-pilot or workbench-like capabilities, the technical knowledge bar needed to operate security solutions drops, and security playbooks and activities can be automated. This can address the skilled labor shortage in the industry and improve the productivity of security personnel evaluating and troubleshooting security breaches in real time. CrowdStrike's Charlotte AI is an example of a GAI-based co-pilot that facilitates the usage and adoption of CrowdStrike cybersecurity product modules by automating manual tasks and personalizing the platform for security analysts. We expect all security vendors to introduce co-pilot-like capabilities in the near future.

Second, while still early in its development, we believe GAI could offer competitive differentiation in the long term to vendors that incorporate GAI/LLMs deeper into their decision and automation engine, which can drive better security outcomes. Such an implementation would require significant investment and fine-tuning to reduce hallucinations, but if well-executed, we believe it can substantially improve detection and response. In support, Gartner estimates that by 2025, 50% of all threat intelligence will be correlated against existing events by GAI and deliver new insights.

Finally, we expect security vendors to raise prices as GAI features and capabilities are gradually incorporated into existing tools, creating incremental revenue opportunities. Our *"Inaugural Oppenheimer Gen AI CTO Survey"* showed that 90% of customers would pay up to 30% more for AI-embedded products and that 88% plan to implement GAI on multiple vendors. Overall, we expect revenue upside from GAI features and capabilities to become more noticeable in 2025 after a broader set of customers adopts the capabilities throughout 2024. Although we're optimistic about the impact of GAI, adoption is still in its early stages. So far, AI enhancements to security offerings have predominantly focused on detecting abnormal signals missed by traditional threat detection techniques (tools across SIEM, NDR, EDR, CDR, XDR, etc.). The use of purpose-built LLMs has yet to see broad implementation.

Now to the dark side. The use of LLMs and GAI models in enterprise applications opens up new risk and attack vectors. First, it turns novice threat actors or "script kiddies" into a more formidable adversary by providing them with co-pilot-type attack scripts. Second, it allows for the creation of highly sophisticated attacks, such as social engineering attacks (e.g., phishing), that can more accurately mimic humans and GAI-based bots and malware (e.g., BlackMamba). Third, using LLMs and GAI expands the API and data attack surface, given the continuous interaction of multiple entities with the underlying model. Finally, while not a cybersecurity risk, GAI presents specific issues with hallucinations and faulty results that must be mitigated.

Exhibit 11: Security and Privacy Concerns with GenAI

Source: Gartner

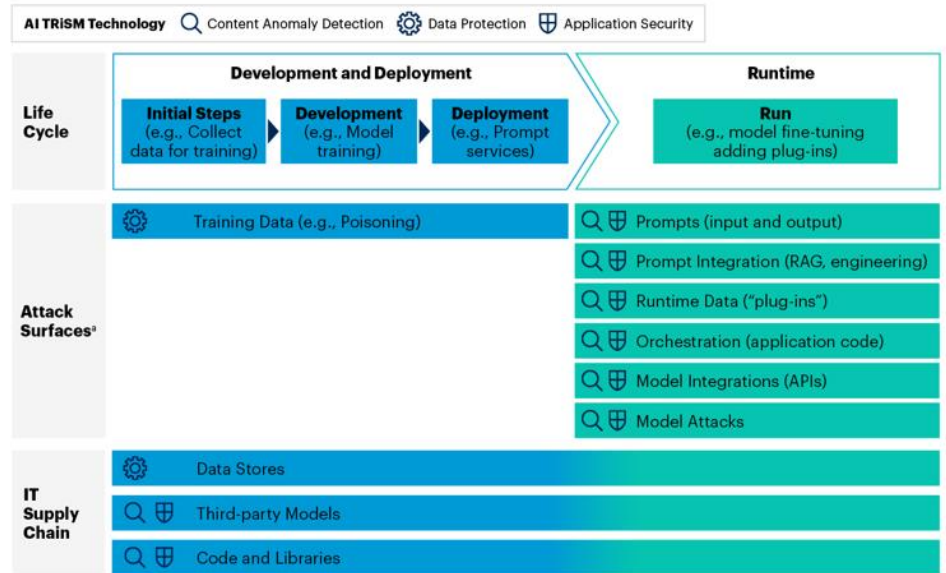
The risks mentioned above are derived from implementing GAI and LLMs as attack instruments by bad actors. But it's important to note that risks exist in the models and how they are trained, constructed, and operated. Vendors that have developed GAI/LLM models like OpenAI are exposed to bad data and privacy concerns during the model training phase. In addition, threat actors could attack the underlying model or manipulate the model during the inferencing phase to deliver either proprietary or confidential results. Lastly, some GAI/LLM providers don't offer users the ability to look "inside" the model and address inherent biases and risks the users want to neutralize or mitigate.

We broadly categorized these risks above into three categories – (1) content generation, (2) data protection, and (3) application vulnerabilities. These risks could require additional tools or enhanced functionality to address attack surface gaps that may emerge while creating, training, managing/operating, or inferencing GAI models. Below, we review the risks related to these three areas.

- Content anomaly detection** – Includes input and output data risks for GAI models. In the input phase, data submitted to the GAI model can be compromised if sent to unsecure environments. Additionally, unauthorized or malicious use contradicting data policies can create a GAI-specific input risk. Currently, inputs are in the form of an interactive prompt. Still, they may soon evolve to include API calls and other automated inputs, making enforcement of policies more complex to implement. On the output side, risks include presenting factual errors or hallucinations and transmitting confidential, copyrighted, or unwanted enterprise data.
- Data protection** – Enterprise GAI models are trained on company-specific data or interact with proprietary databases (tuned models, small language models, etc.) to deliver appropriate and relevant outcomes. This opens up GAI models and supporting infrastructure to potential proprietary or confidential data leakage. Poor data privacy and governance enforcement in hosted environments present another risk within the GAI ecosystem and have potential compliance and governance implications.
- GAI application security** presents additional attack surface risk unique to LLMs. These include adversarial prompting attacks such as "hijacking" as well as prompt injection attacks, vector database breaches, and threat actors' access to model states and parameters.

Exhibit 12: Generative AI Attack Surface Across Lifecycle

Generative AI Attack Surfaces Across the AI Life Cycle

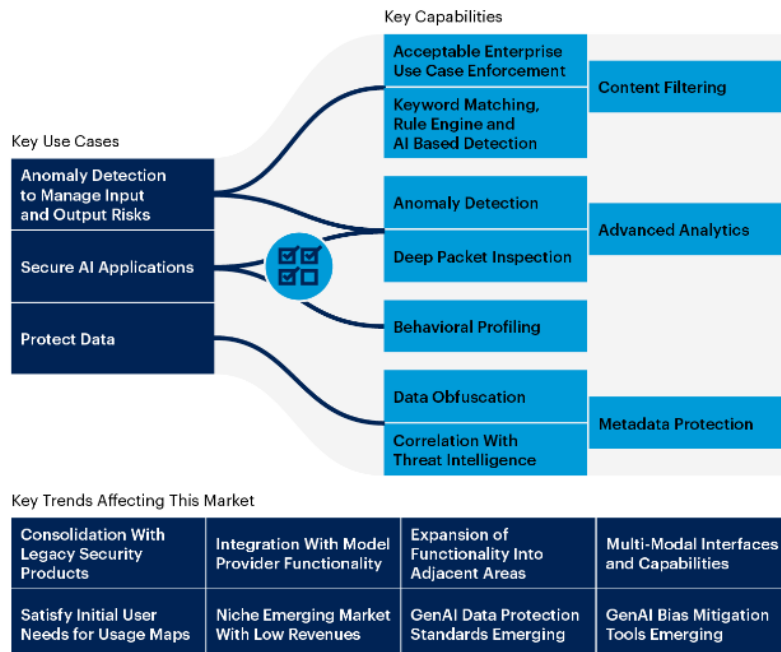


Source: Gartner

We believe the commercial use of GAI requires a much more robust security framework than is currently in place. At the first step of evolution, we expect existing security tools to expand their capabilities to address GAI and LLM-related risks and threats. Next, we believe such existing tools would be complemented in the longer term by purpose-built GAI and LLM tools that more natively address the expanded attack surface area. Eventually, we expect various tools to merge to form a comprehensive security platform.

Exhibit 13: Generative AI on Trust, Risk, and Security

Generative AI on Trust, Risk and Security (TRiSM) Overview



Source: Gartner

Some enhanced functionality content anomaly detection security tools would offer include content analysis, keyword matching, rule-based engagement, and case enforcement, delivering content filtering and advanced analytics. For data protection, we view data obfuscation and correlation with threat intelligence as crucial capabilities that can be used for metadata protection. Lastly, in addition to the GAI dashboard functionality currently provided by SIEM vendors, more capabilities around anomaly detection, deep packet inspection, and behavioral analysis during the GAI and LLM interaction are needed to deliver advanced analytics for GAI models and usage.

The AI security market is in its early stages of development with limited revenue generation and is highly fragmented. Nonetheless, the emergence of GAI in 2023 has accelerated the adoption of AI capabilities and features, and we expect the related security tools, including GAI technology embedded within legacy security products, to expand functional security areas and deliver multi-modal capabilities as we progress through 2024-2025. Over time, GAI capabilities will be embedded in security offerings and not exist as a separate category.

Market Consolidation and the Emergence of Security Platforms

The growing interest in broadly capable security platforms doesn't only reflect labor shortages and the need to streamline security operations. The strategic value of platforms rises with growing infrastructure (on-premise, cloud, etc.) and application architecture (microservices, containers, etc.) complexity; product sprawl and tool interoperability challenges; evolving cybersecurity threats that exploit security gaps; and the need to simplify security management and ease of use through a single coherent UI. As these forces impact product roadmaps, we expect cybersecurity vendors to better integrate and broaden their toolsets into comprehensive security platforms, evolve their product delivery into the cloud, simplify deployment and management, and pair their software tools with managed services to ease operational pressure points.

Exhibit 14: Benefits of Pursuing Consolidation

Primary Benefits for Pursuing Consolidation

Multiple Responses Allowed



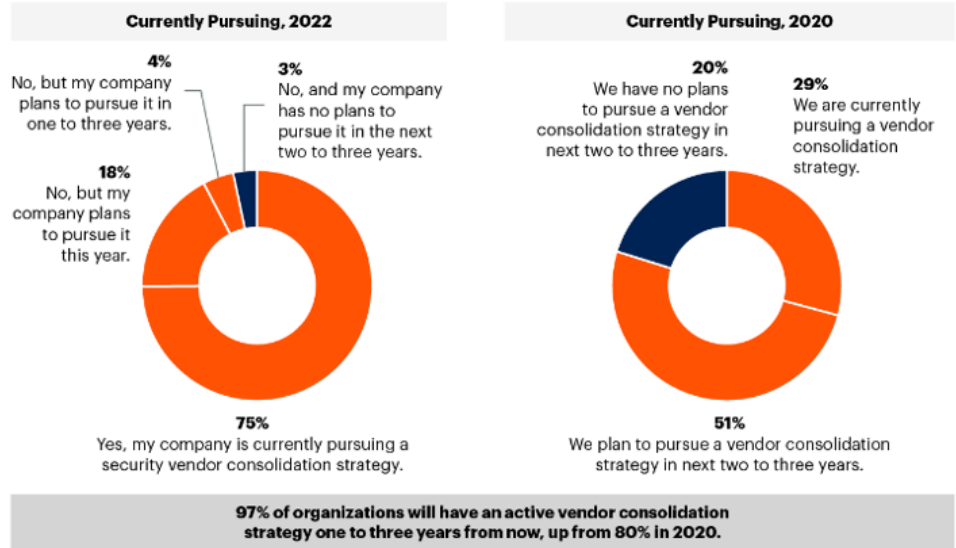
Source: Gartner

Gartner's research found that 97% of organizations are either consolidating security vendors or products or plan to do so over the next one to three years. Some vendors have already aggressively built comprehensive security "platforms" augmented by security analytics and incident response capabilities. However, deep and foundational integration and automation must be achieved to gain real, sustainable benefits from a platform approach. As a result, we expect the consolidation to take time to deliver genuinely integrated platforms capable of addressing different domains across the security

toolchain. In particular, we see integration as critical in key security sub-segments such as network and cloud security, identity and access management, and application security. And for security operations and threat detection and prevention efforts, we expect a capable security-focused AI overlay to provide a top-level management layer.

Exhibit 15: Enterprises Already Pursuing Consolidation

Organizations Pursuing a Vendor Consolidation Strategy



Source: Gartner

Our thoughts on how market consolidation and platform development could progress across the main security markets are as follows:

Network Security. The rise of remote work has redefined the network perimeter, rendering traditional security approaches centered on the data center insufficient to secure enterprise networks. In this new environment, organizations have turned to software-defined, cloud-delivered solutions like ZTNA, CASB, and SWG to address the challenge of enabling and scaling secure remote work access to internal enterprise applications, SaaS applications, and the Internet. This shift has challenged security teams operationally, led to agent bloat, and complicated the management of multiple cloud-based solutions and, in turn, has led to the emergence of a Security Service Edge (SSE) platform, which consolidates ZTNA, CASB, SWG, RBI, and FWaaS into a single cloud-delivered solution for secure access to the cloud, applications, and Internet. SSE offers tighter integration, and fewer consoles and locations where data is decrypted, inspected, and encrypted again.

SSE is also at the heart of a broader networking and security convergence. In recent years, organizations have overhauled their branch office networking architecture, moving away from expensive MPLS connections, which backhaul traffic from branches to centralized data centers, to a more software-defined architecture. The growing use of SaaS applications in remote offices has rendered MPLS transport expensive and highlighted SD-WAN as a more cost-effective way to route traffic directly to the Internet. In the near future, we expect independent adoption of cloud-based SSE and SD-WAN networking. In the long term, we expect their convergence into a single Secure Access Server Edge (SASE) model as long hardware refresh cycles are better aligned with security refresh cycles and as networking and security teams in large organizations come closer together. SD-WAN is most commonly deployed via a managed service in international markets, contributing to a slow adoption of a single-vendor SASE. That said, we expect organizations to make near-term adjustments, such as overhauling their network architecture by phasing out legacy hardware in favor of cloud-based solutions and consolidating onto SSE platforms at renewal points, gradually shifting to SASE.

Application Security. The application security market has evolved with the shift to agile CI/CD development (i.e., a move toward DevSecOps) and the rising use of cloud-based

infrastructure and cloud-native applications. Modern vendors increasingly take a holistic approach to application security, addressing as many application lifecycle domains as possible to protect the application at its development, deployment, and runtime life cycle. This has gradually pushed application security testing (AST) and application runtime security (ARS) tools closer to providing more comprehensive security coverage.

In particular, we expect (1) AST and ARS vendors to add Container and IaC scanning tools across application development and runtime, given the shift to cloud-native apps; (2) AST vendors to broaden their solution set to provide a comprehensive development toolset (SCA, SAST, DAST, IAST, MAST, API vulnerability assessment, fuzzing, etc.) and add complementary application runtime tools (RASP); (3) the emergence of ASPM, which acts as an orchestration, monitoring, analytics, and management layer on top of the AST and ARS tools; (4) traditional network security vendors to expand into application security runtime tools such as WAF and Container/IaC/serverless runtime scanning; and (5) the consolidation of AST and ARS capabilities for cloud-native applications into broader cloud security platforms for a comprehensive CNAPP solution.

Cloud Protection. As enterprises accelerate their migration to the cloud and adopt cloud-native applications, they require a more dynamic approach to security suitable for containers and microservices. Cloud Workload Protection Platforms (CWPPs) combine traditional security capabilities (malware scanning, extended detection, and response, behavioral monitoring, network firewalling, configuration management, etc.) with new approaches (network segmentation, file integrity monitoring, container scanning and monitoring, and serverless support) to protect cloud-native workloads at runtime. Cloud Security Posture Management (CSPM) tools complement CWPP and leverage APIs to scan, monitor, and remediate configuration vulnerabilities in cloud environments, validating conformity to compliance and regulatory mandates. We expect these tools to converge into a complete platform for managing and securing applications in the cloud.

CWPP and CSPM are also integral to the broader shift to Cloud-Native Application Protection Platforms (CNAPP). The unique architectural characteristics of cloud-native applications (microservices, containers, etc.) and the fragmented security toolchain make them difficult and expensive to secure and prone to misconfiguration and mistakes. CNAPP provides persistent security from application development to runtime. It combines CWPP and CSPM tools (focused on runtime environments), application security tools (focused on application development) such as SAST, DAST, SCA, container repository scanning, and IaC scanning, as well as other cloud and application security functionality such as KSPM, API security, and CIEM. This unified approach delivers a continuous end-to-end application security framework. The shift to CNAPP will take years. Yet, it has already pushed cloud and application security vendors to broaden their offerings to deliver end-to-end security for the entire cloud-native application development and runtime lifecycle.

Identity and Access Management. Securing workforce identity has become a priority for organizations as the global workforce moves to work from anywhere, and the transition to the cloud blurs traditional security perimeter lines. Identity vendors have evolved their offerings to include dynamic capabilities such as multi-factor authentication (MFA), single sign-on (SSO) for SaaS applications, and more sophisticated session management controls, but more is ahead.

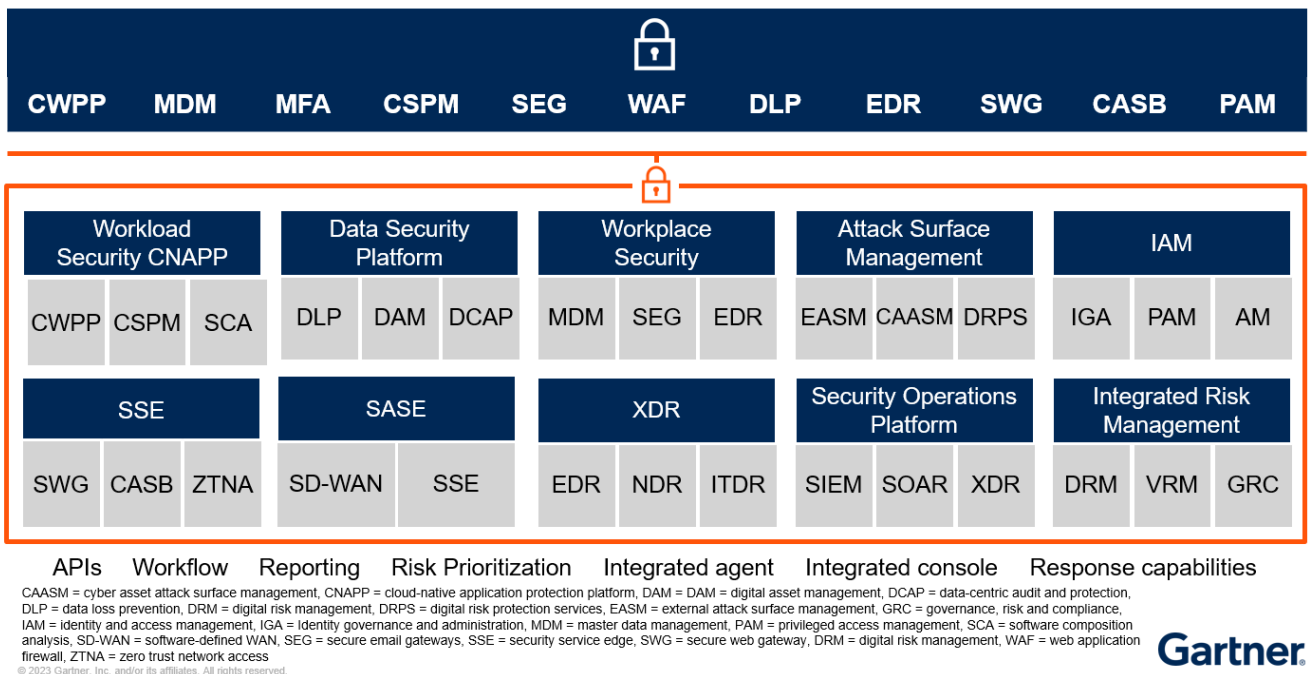
We expect the next evolutionary step to gradually consolidate the three legs of identity security (AM, IGA, and PAM) into a single platform for identity management and control. Automation and interoperability of the pillars are critical to ensure that all applications, systems, APIs, policies, and processes are synergistic and in sync. The consolidation can bring all stakeholders (IT, security ops, and compliance) closer, eliminating identity silos, reducing management complexity, and ensuring compliance with rules and regulations. The number of vendors planning to offer a fully converged identity platform is steadily rising.

Extended Detection and Response (XDR). Organizations historically overlaid their existing EDR tools with SIEM/SOAR for incident response and security analytics. This approach was expensive, required constant tuning of configurations, and took work to operate and scale. XDR aims to address these issues by leveraging a data lake architecture to automatically and centrally collect, normalize, contextualize, and correlate

data/events from multiple security products (EDR, NDR, ITDR, etc.). Once the telemetry is ingested, XDR applies AI and advanced analytics and correlates threat intelligence and signals across various security solutions to provide detection, alert management, and incident response across multiple security domains.

XDR is promising, yet it is still in the early stages of evolution. Most solutions are immature and lack full integrations across all data-feeding security components, and many large organizations still rely on their SIEM platforms as their primary tool for detection and response. These platforms have seen heavy investment and can be difficult to rip and replace. Nonetheless, we expect the adoption of XDR by smaller and mid-size organizations that need a fully built-out SIEM solution or SOC. From a vendor perspective, we expect EDR and SIEM/Security Analytics providers to consolidate adjacent security domains to maintain control over the underlying telemetry. We believe this consolidation could take time to materialize and expect vendors to rely on partnerships to fill product gaps and expand their telemetry collection reach through APIs and integrations near term.

Exhibit 16: Converged Cybersecurity Platforms



Source: Gartner (Invest Quarterly Sector Outlook: Information Security, 3Q23)

Security Market Opportunity & Vendor Map

Based on Gartner's research, we believe the overall security TAM is substantial, totaling \$185.4 billion in 2023 and growing quickly, with Gartner projecting an 11.6% 2023-27 CAGR to \$287.0 billion in total 2027 spending. The overall security TAM aggregates several large market segments and addresses various capabilities across application, cloud, data, endpoint, identity, risk management, and infrastructure security. Of these markets, the most sizable segments are Endpoint & SOC Security (SIEM, SWG, Threat Intelligence, Secure E-mail, and Endpoint Protection Platform), Identity Security (Access Management, Privileged Access, User Authentication, and Identity Governance), and Infrastructure Security (IDPS, Firewall Equipment, Network Access Control/Detection and Response). Security Services is another large spending base, including consulting, hardware support, implementation, and IT outsourcing.

The fastest-growing security segments are Cloud and Data Privacy Security. Cloud Security, which totaled \$5.6 billion in 2023 spending, is expected to grow at a 23.2%

CAGR through 2027 to \$12.8 billion, while the Data Privacy segment is expected to rise at an 18.9% CAGR from \$1.4 billion in 2023 to \$2.7 billion in 2027. The strong growth in these markets reflects the emerging security posture for all aspects of cloud security and the fast-evolving and complex task of securing applications and data from development through runtime while adapting to changes in the underlying infrastructure architecture (microservices, containers, etc.). A dynamic regulatory environment also drives a need for GRC solutions to address data privacy and sovereignty requirements and maintain them wherever collected and used.

While not in hyper-growth mode, other large and established security segments are still expected to grow at a strong pace. This includes Endpoint & SOC Security (\$28.2 billion with a 14.5% CAGR) and Identity Security (\$16.1 billion with an 11.6% CAGR). The strong growth in these markets reflects continued fast-paced user and device security (smartphones, laptops, IoT devices, etc.) and the need to secure an extended security perimeter (remote work, cloud, SaaS, etc.). Infrastructure security is another significant market at \$20.3 billion in spending, though it's growing at a more measured 11.3% CAGR. Low double-digit growth may not be impressive compared to other parts of the security market. However, when considering the shift to the cloud, this pace of spending suggests that enterprises are still investing substantially in their data center security solutions.

Exhibit 17: Total Security Market Opportunity by Segment (estimates in \$Millions)

	(\$Millions)							
(\$Millions)	2022A	2023E	2024E	2025E	2026E	2027E	CY23-CY27 CAGR	
Application Security Testing Software	\$1,755	\$1,979	\$2,237	\$2,553	\$2,887	\$3,222	13.0%	
Vulnerability Assessment Software	1,893	2,156	2,512	2,958	3,432	3,911	16.1%	
Web Application Firewalls Software	1,399	1,612	1,858	2,127	2,418	2,698	13.7%	
Application Security	5,048	5,747	6,607	7,638	8,736	9,830	14.4%	
Cloud Access Security Brokers Software (CASB)	1,269	1,712	2,245	2,955	3,820	4,755	29.1%	
Cloud Workload Security (CWPP, CSPM, CNAPP)	3,221	3,861	4,610	5,608	6,771	8,075	20.3%	
Cloud Security	4,490	5,573	6,855	8,563	10,592	12,830	23.2%	
Consumer Security Software	7,447	7,860	8,236	8,734	9,230	9,702	5.4%	
Consumer Security	7,447	7,860	8,236	8,734	9,230	9,702	5.4%	
Subject Rights Request Automation	727	842	1,015	1,195	1,383	1,583	17.1%	
Consent and Preference Management	420	508	638	782	941	1,116	21.7%	
Data Privacy	1,148	1,350	1,653	1,977	2,324	2,698	18.9%	
Encryption Software	889	1,034	1,193	1,372	1,534	1,693	13.1%	
Enterprise Data Loss Prevention Software	1,402	1,600	1,799	2,030	2,214	2,383	10.5%	
Tokenization Software	806	976	1,160	1,374	1,592	1,786	16.3%	
Data Security	3,097	3,610	4,153	4,776	5,339	5,862	12.9%	
Access Management Software	4,963	6,112	7,366	8,677	9,896	11,154	16.2%	
Identity Governance and Administration Software	3,156	3,601	4,073	4,627	5,184	5,774	12.5%	
Privileged Access Management Software	1,887	2,149	2,373	2,589	2,771	2,928	8.0%	
User Authentication Software	3,976	4,282	4,543	4,815	5,000	5,167	4.8%	
Identity Security	13,982	16,144	18,355	20,708	22,851	25,022	11.6%	
Endpoint Protection Platform (Enterprise) Software	12,166	14,455	17,256	20,501	23,733	26,951	16.9%	
Secure E-mail Gateway Software	2,692	3,069	3,451	3,850	4,234	4,595	10.6%	
Secure Web Gateway Software	2,965	3,423	3,942	4,511	5,105	5,726	13.7%	
SIEM Software	4,927	5,675	6,361	7,020	7,666	8,319	10.0%	
Threat Intelligence Software	1,354	1,572	1,834	2,145	2,461	2,791	15.4%	
Endpoint & SOC Security	24,105	28,194	32,844	38,027	43,197	48,382	14.5%	
Integrated Risk Management	4,972	5,461	5,970	6,417	6,793	7,134	6.9%	
Integrated Risk Management	4,972	5,461	5,970	6,417	6,793	7,134	6.9%	
Firewall Equipment	14,586	15,299	16,974	19,009	21,034	22,994	10.7%	
IDPS	990	917	882	858	822	775	-4.1%	
Network Detection and Response	1,350	1,563	1,801	2,080	2,372	2,647	14.1%	
Network Access Control	943	948	923	855	764	647	-9.1%	
Zero Trust Network Access	1,010	1,500	2,038	2,655	3,302	3,993	27.7%	
Infrastructure Security	18,878	20,227	22,618	25,458	28,295	31,056	11.3%	
Consulting	30,027	34,695	39,307	44,989	50,146	54,568	12.0%	
Hardware Support	1,665	1,707	1,774	1,903	2,038	2,168	6.1%	
Implementation	19,046	19,554	20,517	22,208	23,978	25,709	7.1%	
IT Outsourcing	22,656	24,001	25,626	28,014	30,495	32,974	8.3%	
Security Services	73,395	79,959	87,225	97,114	106,657	115,418	9.6%	
Other Information Security Software	8,003	11,251	14,185	16,629	17,885	19,117	14.2%	
Total Enterprise Security	\$164,563	\$185,374	\$208,701	\$236,042	\$261,899	\$287,053	11.6%	

Source: Gartner, Oppenheimer & Co. Inc.

A deeper examination of the security TAM reveals many sub-segments growing at robust levels. The fastest-growing sub-segments are Cloud Access Security Brokers (29.1% CAGR) and Zero Trust Network Access (27.7% CAGR). This fast-paced growth is coming off a comparatively small sales base, highlighting their adoption's early nature and the growing investment in SSE & SASE platforms. Other sub-segments estimated to be

quickly growing include Consent and Preference Management (\$0.5 billion with a 21.7% CAGR), Cloud Workload Security (\$3.9 billion with a 20.3% CAGR), and Endpoint Security (EPP/EDR) (\$14.5 billion, 16.9% CAGR). Finally, we highlight the importance of security-oriented services for consulting, hardware support, implementation, and IT outsourcing. In aggregate, services accounted for \$80 billion of 2023 spending, with a 2023-27E CAGR of 9.6% to \$115.4 billion in 2027.

We view the strong security market growth and variety of sub-segments growing at robust levels as a testament to the long-term health of the market and the central nature of security to enterprise success, even though overall IT spending faces lingering spending uncertainty from macroeconomic conditions. This growth and its diversified sources also reflect the diversity of the demand catalysts across the industry, including structural changes such as remote work and cloud adoption, growing vulnerability to business disruption from ever-increasing cyberattacks, escalating technical challenges as the security perimeter expands, and complexity grows; and operational challenges related to talent shortages, application development and deployment, and management complexity (too many tools, too many alerts, etc.).

Exhibit 18: Vendor Map – Identity Security, Endpoint Security, Security Analytics

- Fully Developed/Strong Presence
- ◐ Expansion/Moderate Presence
- New Expansion/Nascent

Vendor	Identity Security				Endpoint Security					Security Analytics				
	AM	PAM	IGA	Secrets Management	Email Security	EDR	XDR	ITDR	MDR	SIEM/SOAR	Vulnerability Management	Threat Intelligence	Digital Risk Protection	Attack Surface Management
Abnormal					●									
aqua											○			
ARCTIC WOLF									●					
ARMIS											◐	◐		●
AXDNUS														●
BigID														
BlueVoyant									●			●	●	
CATO						○	○							
CheckmaxX														
CHECK POINT					●	◐	◐		◐					
CISCO	●					●		○		●				
CROWDSTRIKE						●	●	●	●	●	●	●		◐
CYBERARK	◐	●	○	◐										
cybereason						◐	◐							
elastic						○				●				
eSENTIRE							●		●		○			○
exabeam										●				
FORTINET						○	○		○			●		
illumio														
JFrog														
LACEWORK														
Lookout						○						○		
MENLO SECURITY														

Source: Company Documents, Oppenheimer & Co.

Exhibit 19: Vendor Map – Identity Security, Endpoint Security, Security Analytics (Continued)

Vendor	Identity Security				Endpoint Security					Security Analytics				
	AM	PAM	IGA	Secrets Management	Email Security	EDR	XDR	ITDR	MDR	SIEM/SOAR	Vulnerability Management	Threat Intelligence	Digital Risk Protection	Attack Surface Management
Microsoft	●	◐	◐		●	●	●			●				
mimecast					●									
netskope														
okta	●	◐	◐					○						
orca security											○			
paloalto				○		●	●	○	○	◐				○
PingIdentity	●		●											
proofpoint					●									
Qualys						◐	◐				●	●		◐
RAPID7							◐			◐	●	●		
Recorded Future												◐	●	◐
SALT														
SentinelOne						●	●	◐	●	○				
SecurityScorecard											●	●		○
Skyhigh Security														
splunk>										●				
snyk														
sysdig														
tenable											●	●		●
TESSIAN					●									
VERACODE														
VERSA														
vmware						◐								
WIZ											●			◐
zscaler								○						

Source: Company Documents, Oppenheimer & Co.

Exhibit 20: Vendor Map – Network Security and Cloud & Application Security

Vendor	Network Security							Cloud, Data & Application Security								
	Firewall/FWaaS	CASB	SWG	ZTNA	SD-WAN	Remote-Browser Isolation	Microsegmentation	CWPP	CSPM	CIEM	DSPM	SCA/SSCS	IaC	Application Security Testing	API Security	Container Security
Abnormal																
aqua								●	●			●	●			
ARCTIC WOLF									●							
ARMIS																
AXONIUS																
BigID											●					
BlueVoyant																
CATO	●	●	●	●	●	●	●									
Checkmarx												●	○	●	●	○
CHECK POINT	●	●	●	●	●	●	●	●	●							
CISCO	●			●	●		●									
CROWDSTRIKE								●	●	●				○		●
CYBERARK										○						
cybereason																
elastic								○	○							
eSENTIRE																
exabeam																
FORTINET	●	●	●	●	●			○	○							
illumio							●									
Jfrog												●	○	●		●
LACEWORK								●	●	○	○	●	○	○		○
Lookout		●	●	●												
MENLO SECURITY		●	●	●		●										

Source: Company Documents, Oppenheimer & Co.

TECHNOLOGY ANALYSIS OF DATA SECURITY AND INFRASTRUCTURE APPLIANCE
 Exhibit 21: Vendor Map - Network Security and Cloud & Application Security (Continued)

Vendor	Network Security							Cloud, Data & Application Security								
	Firewall/FWaaS	CASB	SWG	ZTNA	SD-WAN	Remote-Browser Isolation	Microsegmentation	CWPP	CSPM	CIEM	DSPM	SCA/SSCS	IaC	Application Security Testing	API Security	Container Security
Microsoft		●	○	○				●	●				●			
mimecast																
netkope	●	●	●	●	●	●	●									
okta																
orca security								●	●	●	○		●		●	●
paloalto	●	●	●	●	●	●	●	●	●	●	○	●	●	○	○	●
PingIdentity																
proofpoint																
Qualys								●	●				○			○
RAPID7								○	○					○		
Recorded Future																
SALT															●	
SentinelOne								●	●							
SecurityScorecard																
Skyhigh security		●	●	●				○	○							
splunk>																
snyk									○			●	●	○		●
sysdig								●	●	●			●			●
tenable									○			●		○		
TESSIAN																
VERACODE												●		●		
VERSA network	●	●	●	●	●											
vmware				○	●		●									
WIZ								●	●	●	○	●	●			●
zscaler	●	●	●	●	●	●	●		●							

Source: Company Documents, Oppenheimer & Co.

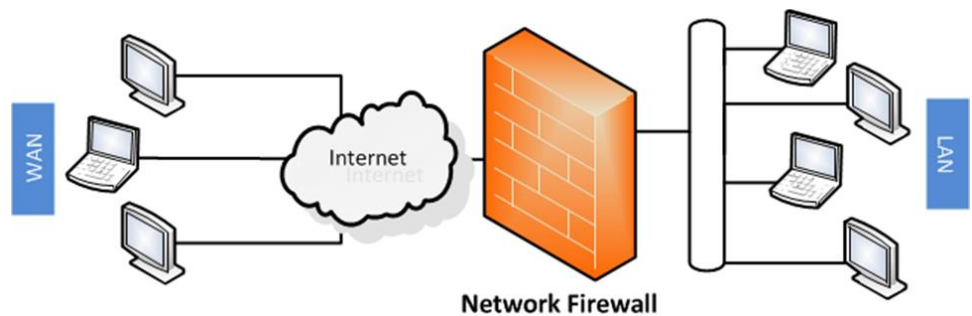
Network Security

Network Firewalls

Network firewalls are one of the oldest cybersecurity solutions, dating back to the early days of the Internet. At its core, a firewall acts as a barrier between two networks, offering bidirectional (incoming and outgoing) monitoring and control of network traffic based on predetermined security rules. As such, firewalls establish a barrier between a trusted network and an untrusted network (the Internet, for example), a barrier that can be on-premise, hybrid (on-premises and cloud), or the public or private cloud. Today, firewalls are a critical component within the network security architecture, and they have evolved from traditional stateful inspection to more advanced Next-Generation Firewalls (NGFWs).

Digital Equipment Corp. developed Firewalls in the late 1980s to restrict outside access to particular network and data center resources. These “first-gen” firewalls were built on a simple packet-filtering system, which discarded network data packets after analyzing the packets' destination address, protocol, and port number. Packet-filtering firewalls offer many advantages, including high processing speeds and flexibility in implementing network security policies. These first-gen firewalls analyzed packets without context and made binary pass/fail decisions based on pre-set corporate access policies. They were typically deployed as the “first line” of defense to secure the outermost network perimeter.

Exhibit 22: Firewall Location within a Network



Source: WeSolveIT

While packet-filtering firewalls were a groundbreaking development in network security, they could not recognize the state of a connection and had limited logging capabilities. The next generation of firewalls, known as “stateful” firewalls, proved to be a significant leap forward. They could retain data packets until enough information was available to make a broader judgment about their state. Developed during the late 1980s/early 1990s, these new circuit-level gateways added a “connection state” rule that made filtering more accurate in determining if a packet was part of a new or existing connection. Stateful firewalls were more manageable than first-gen firewalls, making them increasingly popular during the 1990s when network technology rapidly developed, and firewall manageability became a key challenge. Check Point released its first stateful firewall, the FireWall-1, in 1993 and established its leadership in the market at that time.

While stateful firewalls addressed many of the shortcomings of packet-filtering firewalls, they were imperfect. They were vulnerable to Denial of Service (DoS) attacks, whereby attackers would overwhelm the firewall with fake connection packets, overloading its connection-state memory and rendering it ineffective. The introduction of the application firewall (also referred to as a proxy firewall) and the Firewall Toolkit (FWTK) in the mid-1990s helped address these vulnerabilities. This third generation of firewalls could identify whether a communication protocol was abused or attempted to bypass the firewall on an allowed port. Filtering at the application layer allowed the firewall to “perceive” how File Transfer Protocols (FTP) or Hypertext Transfer Protocols (HTTP) work and adapt on the fly to the ways applications made use of these protocols. This process separates legitimate connection requests from malicious ones.

We believe it's helpful to consider the first three generations of firewalls in the context of the Open Systems Interconnection (OSI) model. The OSI model is a conceptual

framework that divides computing functions within a network into seven layers (Exhibit 23). Each firewall generation added functionality at a higher layer. The OSI model's first-generation packet-filtering firewalls examine data at the Network and Transport layer. Stateful Firewalls, which can recognize the state of a connection, add functionality at the Session Layer, and proxy firewalls, which conduct most of the firewall control and filtering in software, add functionality at the Application layer.

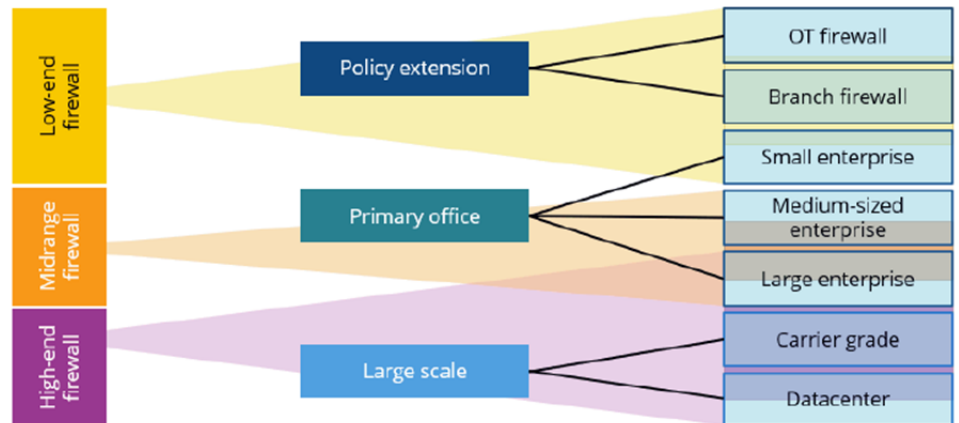
Exhibit 23: The Open Systems Interconnection (OSI) Model

Layer 7	Application	The application layer focuses on the software utilized by the end user, and provides protocols that allow the software to send and receive information and data to users
Layer 6	Presentation	The presentation layer converts data into a usable format in preparation for use in the applications layer
Layer 5	Session	The Session layer maintains connections and controls ports and sessions
Layer 4	Transport	The transport layer transmits data using transmission protocols including TCP and UDP
Layer 3	Network	The network layer routes and constructs data from network devices into packets. Network layer protocols include IP, ICMP, IPsec, IGMP protocols
Layer 2	Data Link	The data link layer creates and eliminates connections between two connected nodes on a network using MAC and LLC identifiers.
Layer 1	Physical	The physical layer defines the physical components of a network infrastructure that provides the physical interface between network nodes

Source: International Organization for Standardization (ISO) and industry contributors, Oppenheimer & Co. Inc.

In the mid-2000s, increased Internet bandwidth and data volumes gave rise to a new firewall implementation mode with NetScreen's ASIC-built firewall appliance. This became a popular choice as it offered faster inspection rates, lower latency, and higher throughput at a lower cost. While NetScreen didn't have a central management platform, a focal selling point for firewalls, it gained significant traction with its ease of use and higher performance (hardware accelerated). Juniper Networks ultimately acquired NetScreen and one of its founders, Ken Xie, left NetScreen, applied its ASIC-driven approach, and launched Fortinet. The explosion in Internet speeds pushed firewall vendors to continuously upgrade their firewall hardware to keep up with the network inspection demands. It also opened up a lengthy philosophical debate on the merits of developing hardware/ASICs (Cisco and Fortinet) versus leveraging third parties for hardware/ASICs and focusing on software (Check Point and Palo Alto Networks).

The stateful inspection firewall was the industry standard for over a decade. However, more innovation was incorporated into the firewalls as time passed. In 2010, Palo Alto introduced a new offering that combined traditional firewall capabilities with newer technologies such as Deep Packet Inspection (DPI), Intrusion Prevention System (IPS), Sandboxing, URL filtering, and VPN. This latest offering, Next-Generation Firewall (NGFW), relied on the same analysis as proxy firewalls but with a greater focus on deep-packet inspection. NGFWs can define policies and control traffic based on layer-7 application identity regardless of port and protocol. Using a single-pass analysis, they also provide user-based access controls, irrespective of IP address, location, or device, at performance levels similar to traditional stateful firewalls. The introduction of NGFWs marked the convergence of independent network security functions (IDS/IPS, VPN, SSL, IPsec) into a single platform offering that can be delivered on-premise and in the cloud.

Exhibit 24: IDC Worldwide Firewall Classification**Worldwide Firewall Classification**

Source: IDC

The firewall market continues to evolve, and we see several drivers ahead shaping the market's future. These include the (1) need to support greater traffic throughput, (2) rise in cloud usage (multi- and hybrid-cloud architectures), (3) emergence and adoption of Firewall-as-a-Service (FWaaS) and the move toward zero trust with SSE and SASE enabling technology consolidation, and (4) the introduction of AI/ML capabilities in NGFWs.

Looking first at the need to support greater traffic throughput, firewalls were too slow in the past to keep up with the rapidly growing network throughput and traffic volumes. They were often deployed in high numbers next to high-performance routers. In recent years, firewall performance has quickly increased, closing the performance gap versus networks (Fortinet's introduction of a 1Tbps firewall is a good example). We expect the vendors to continue to push for higher traffic throughput support as firewalls look to keep up with network throughput needs, become multi-purpose, and add capabilities and functionality.

As for the cloud, the rise in cloud infrastructure adoption, growth in cloud-native applications, and adoption of multi- and hybrid-cloud architectures have led to new firewall deployment models. While legacy firewalls were designed to sit within a customer's data center, they are not well-suited to secure traffic within cloud environments. This led to the introduction of virtual firewalls, such as Palo Alto's VM-series, which function similarly to traditional firewalls but are deployed as software running as virtual instances at the gateway of any public/private cloud environment.

Virtual firewalls can (1) be scaled up or down based on workload requirements, (2) maintain a policy that is consistent with on-premise footprints, and (3) be deployed as virtualized instances of NGFWs, enabling inspection of perimeter traffic in cloud environments, and of traffic flowing between clouds and data centers in multi- and hybrid-cloud architectures. Enterprises are also increasingly leveraging containers, pushing for firewalls designed for Kubernetes container environments (for example, Palo Alto's CN-Series). Container firewalls offer many of the same capabilities as NGFWs, specifically securing all container traffic, including east-west, north-south, and container-to-non-container traffic. Similar to virtual firewalls, container firewalls are deployed in each container that needs to be secured.

It is important to note that while the traditional firewall vendors have introduced virtual and container-based firewalls, the major public cloud providers have also entered the market and offer cloud-native firewalls (for example, AWS Firewall). While these cloud solutions are capable and have seen some adoption, many enterprises prefer vendor-based virtual and container firewalls to maintain a consistent policy in hybrid-cloud environments, which cloud providers can't deliver.

Another outcome of the transition of applications to the cloud and the explosion in the number of remote workers was the introduction of Firewall-as-a-Service (FWaaS). Instead

of backhauling traffic to a centralized corporate data center, the historical standard, firewall vendors have introduced cloud-based FWaaS services that offer on-demand NGFW capabilities with unlimited scale and without the need to purchase, manage, and update firewall appliances. FWaaS enables customers to minimize costs by offloading service maintenance to the firewall provider, leaving customers only responsible for policy configuration and with the flexibility to decide when and how to deploy protections. For example, by leveraging FWaaS, customers can pinpoint which part of a cloud-based data chain they want to protect (e.g., deploying FWaaS only to protect CI/CD processes within a DevOps framework).

FWaaS offers multiple advantages over on-premise and virtual NGFWs. These advantages include the ability to (1) use a proxy-based architecture to inspect SSL/TLS traffic and detect malware hidden in encrypted traffic; (2) deliver cloud-based IPS, regardless of connection type, to inspect all on- and off-network user traffic; and (3) deliver DNS resolution with detailed controls preventing DNS tunneling. In addition, FWaaS delivers centralized control, policy management, and real-time visibility, analyzing logs to provide insights into threats and vulnerabilities across all users and applications. With the growth in work-from-home, enterprises also adopt FWaaS for identity segmentation for application-specific access. This gives enterprises greater access control than traditional VPNs and users with greater mobility within a network once access is granted.

We expect a more normalized firewall growth outlook as supply/demand imbalances after the COVID-19 pandemic have been largely resolved. Nonetheless, we expect demand for FWaaS and distributed/branch firewalls to remain robust as enterprises look to implement zero trust principles to better address a distributed workforce (WFH/hybrid) and application environments (on-premise, private/hybrid/public cloud). This is achieved by Secure Access Service Edge (SASE), which combines network (SD-WAN) and security capabilities (FWaaS, Zero Trust Network Access (ZTNA), SWG, CASB, and other technologies) into a single, cloud-delivered deployment model. It allows customers to implement secure access regardless of where users, applications, or devices are located and combines multiple network infrastructure capabilities into a single platform, reducing cost and complexity. According to market research firm Gartner, 80% of enterprises will unify web, cloud services, and private application access using SASE models by 2025. We discuss SASE in more detail later in the note.

From a vendor perspective, outside of continued SASE investments, we expect a greater focus on integrations with the major public cloud platforms (AWS, Azure, GCP) to enable effective enforcement of cloud-native security policies from a single management console. We also expect the major firewall vendors to continue to expand into adjacent markets beyond network security to enable customers to consolidate their architectures. Vendors such as Palo Alto, Fortinet, and Check Point have expanded their platforms into areas such as cloud security (CNAPP), security analytics (SIEM/SOAR), secure networking, and email security, allowing customers to gain greater visibility into their security posture and reduce tool sprawl. Lastly, with the rise of generative AI, we expect firewall vendors to introduce AI/ML capabilities that enable a proactive posture and provide faster threat detection and greater visibility. These include in-line ML-assisted blocking, zero-day signature detection, automated IoT classification, and intelligent policy recommendations.

Network Access Control (NAC)

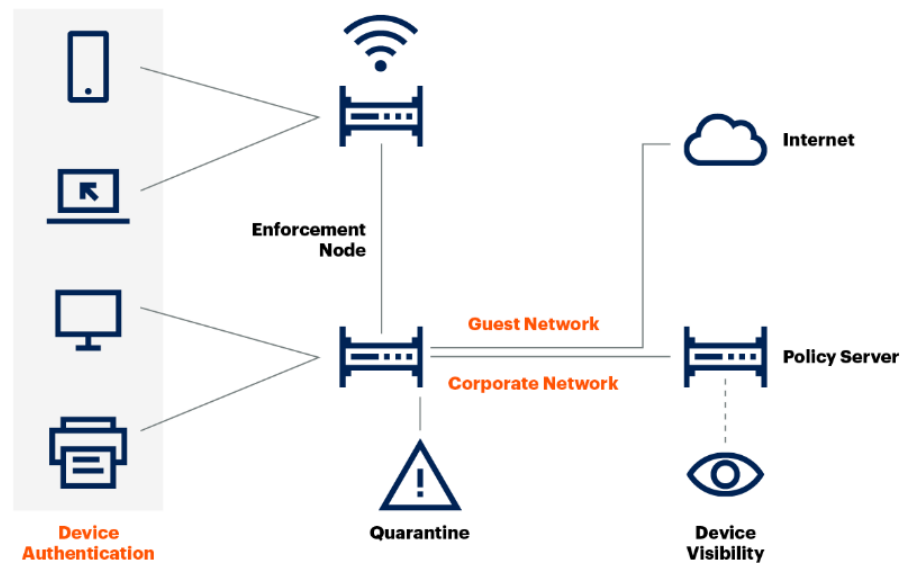
NAC uses a set of protocols to define and implement secure access policies to enterprise networks. NAC was first introduced to provide granular controls to govern network access for mobile devices (guest users with laptops, for example) within an organization's IT infrastructure. Modern NAC capabilities include policy management, device profiling and visibility, guest network access, and security posture checking. Organizations leverage NAC systems for various use cases, including securing access for non-employee/contractor traffic, BYOD endpoints, and IoT/OT devices.

NAC systems authenticate endpoints at enforcement nodes on network hardware (switches, routers, firewalls, etc.) based on predefined policies set on a central policy server. These policies define conditions endpoints must meet to access the organization's network. This highly scalable policy-oriented model allows IT administrators the flexibility to update policies across an entire fleet of devices automatically. NAC systems ultimately help organizations mitigate zero-day attacks, authorize and authenticate network

connections, encrypt traffic for wireless and wired networks, and apply role-based controls based on user, device, application, or security posture.

Early NAC solutions predominantly focused on policy management and enforcement. In contrast, modern NAC solutions offer additional features such as (1) identifying and profiling endpoints before malicious code can infect the network, (2) evaluating security-policy compliance for users, devices, and operating systems, (3) enabling incident response by enforcing policies to block, isolate, and remove noncompliant endpoints automatically, and (4) API-based integration with other security and network solutions like SIEM/SOAR. The agent-less, network-based architecture of NAC systems also enables security for IoT/OT devices (which can't run agents), leading to outsized adoption by customers with large IoT fleets (hospitals, manufacturing, energy, etc.).

Exhibit 25: NAC Architecture



Source: Gartner

The NAC market is mature and highly concentrated, with two vendors, Cisco (~35%) and Fortinet (~30%), the dominant players. Given the high concentration, we do not expect new vendors to enter the market but expect increasing competition from ZTNA solutions. While initially targeting remote access use cases, ZTNA vendors have matured their offerings, adding device authentication and segmentation capabilities that offer improved visibility and unified policy management for campus-based and remote workers. According to estimates from Gartner, more than 15% of enterprises are expected to replace their NAC with ZTNA by 2027.

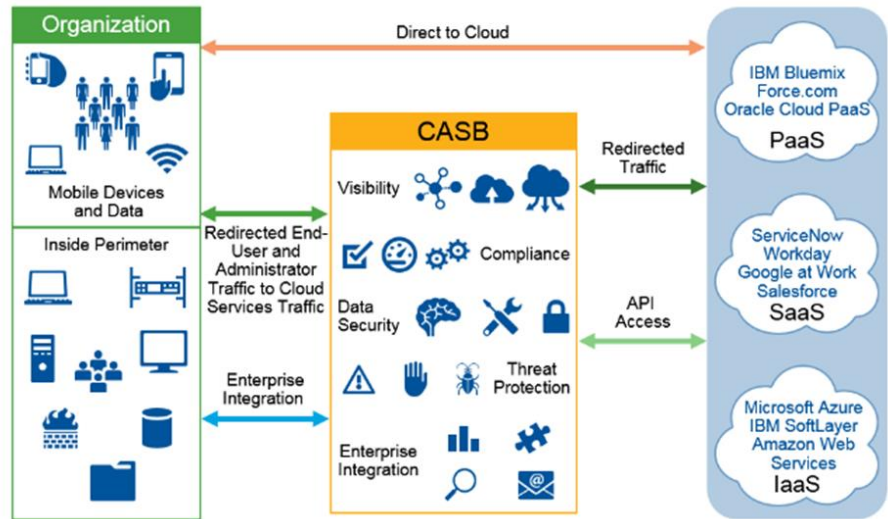
Cloud Access Security Broker (CASB)

CASBs ensure that security and IT professionals have visibility into and control of all cloud apps, files, data, and user activity. In recent years and since the COVID-19 pandemic, organizations have accelerated their transition to the cloud and use of SaaS applications. At the same time, workers have shifted to working from anywhere using personal devices for work purposes. In the past, web proxies and firewalls were used to govern applications and protect sensitive data from outside threats. Yet, with the rapid transition to cloud/SaaS and the rise in shadow IT, IT professionals have found it difficult to know where critical data is located, who has access to what applications and datasets, and what confidential information is shared against corporate policy and regulation (intentionally or unintentionally).

CASBs address these challenges by acting as a control point to secure cloud services and unifying several security measures used across the cloud to make detection, management, and enforcement much easier to deploy. CASBs intermediate between users and cloud-based applications and deliver a granular data protection and policy

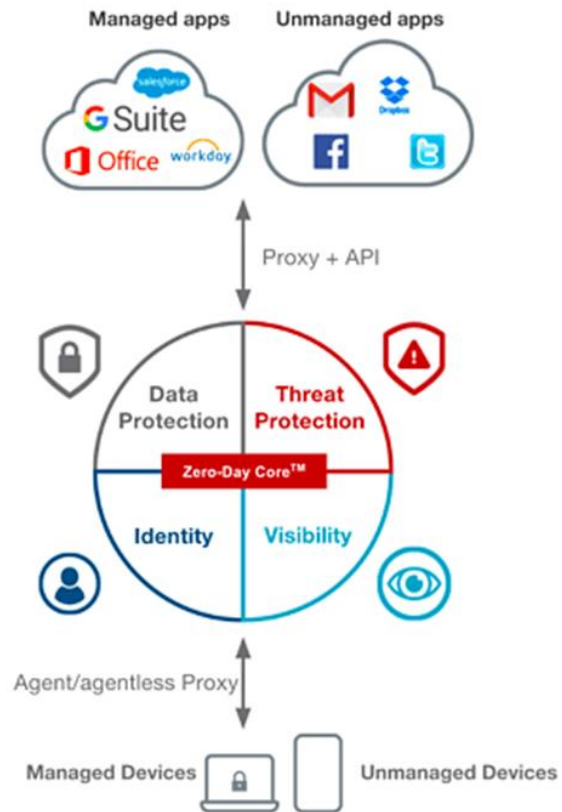
enforcement approach. They monitor user authentication to SaaS applications, analyze contextual data such as user behavior and device posture, and provide data encryption services for third-party applications such as Salesforce, ServiceNow, and Workday.

Exhibit 26: CASB Workflow



Source: ManagedMethods, Inc.

Exhibit 27: CASB Architecture



Source: Bitglass

Although gaining visibility into cloud posture and monitoring shadow IT were the initial use cases that drove CASB adoption, modern CASBs deliver a wide range of capabilities, including data loss prevention (DLP), UEBA controls, malware detection, data encryption,

and integrations with third-party IAM tools. Four fundamental pillars can characterize the functionality of modern CASB solutions:

- **Visibility.** CASB solutions offer comprehensive visibility into SaaS application usage, related contextual data, and risk assessment for each cloud service used. They can provide detailed logs on all cloud transactions (logins, uploads, downloads), file-sharing activity, and monitor and catalog shadow IT usage.
- **Compliance.** CASBs enable organizations to safeguard sensitive data within their cloud environments and enforce compliance with regulations. They can pinpoint the highest compliance risk areas within an organization's SaaS application stack and maintain and protect against costly breaches.
- **Data Security.** CASBs can enforce data-centric security policies with applied controls, including audits, alerts, quarantines, and data encryption. Organizations can specify which applications their workforce can access when on or off the network (for example, allowing access to Salesforce when in the office but not when working remotely).
- **Threat Protection.** CASBs provide threat protection by applying user and entity behavior analytics to detect abnormal behavior. For example, they can track which datasets users typically access within an application. If an employee attempts to download or access data out of character with their historical activity, CASBs can block access in real-time.

In addition to these pillars, CASBs provide threat intelligence and incidence response workflows, assign classification labels to content, encrypt structured and unstructured data, tokenize structured data, and integrate with DLP solutions. They can also perform CSPM for IaaS and PaaS workloads and SaaS security posture management (SSPM) for SaaS applications. SSPM continuously assesses the security posture of SaaS applications and can improve native SaaS security settings, manage identity permissions, and identify interconnected applications.

We expect organizations to deploy CASB solutions as their usage of SaaS solutions rises and as they look to monitor and control shadow IT. Consequently, API integrations are a competitive focal point for CASB solution providers. Given the significant R&D investment needed to build these integrations, we view large vendors such as Zscaler, Netskope, and Palo Alto as best-positioned. From a vendor perspective, we expect continued consolidation between CASB, ZTNA, and SWG as vendors look to deliver integrated SSE architectures (discussed in more detail later in the note). Most CASB vendors have expanded their offerings to include ZTNA and SWG, with the most notable stand-alone vendors, Netskope and Microsoft, now offering complete SSE suites. Looking ahead, we expect the longer-term shift to SASE architectures to act as a multi-year demand tailwind. We discuss these trends in greater detail in the SASE section of this report.

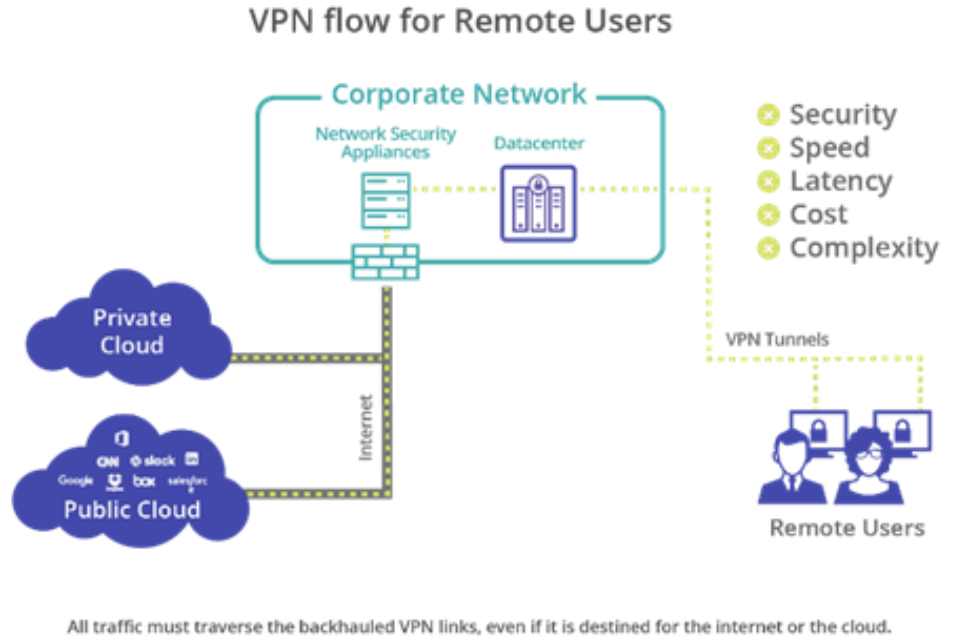
Zero Trust Network Access (ZTNA)

ZTNA is a cloud-based network security technology that leverages identity- and context-based access policies to provide secure remote access to applications and data. ZTNA solutions start with a default "deny" posture based on the principles of zero-trust architectures and are most commonly deployed in the cloud. However, they can also be implemented using on-premise appliances. The solution enables user authentication through a cloud controller that communicates with Identity Access Management (IAM) infrastructure to confirm identity. Once a user is authenticated, a tunnel is created between the application and the user's device through the ZTNA cloud service, and all traffic flows through the cloud service encrypted.

Historically, remote workers connected to the network using IP-based VPNs, which granted users a valid login key access to an organization's network and applications. While VPNs performed this vital role for years, their limitations became clear as COVID-19 triggered a massive jump in remote worker access. Specifically, VPNs proved to be slow, complex, and expensive to scale and granted access to the entire underlying network, giving would-be attackers unlimited lateral movement and access to internal resources.

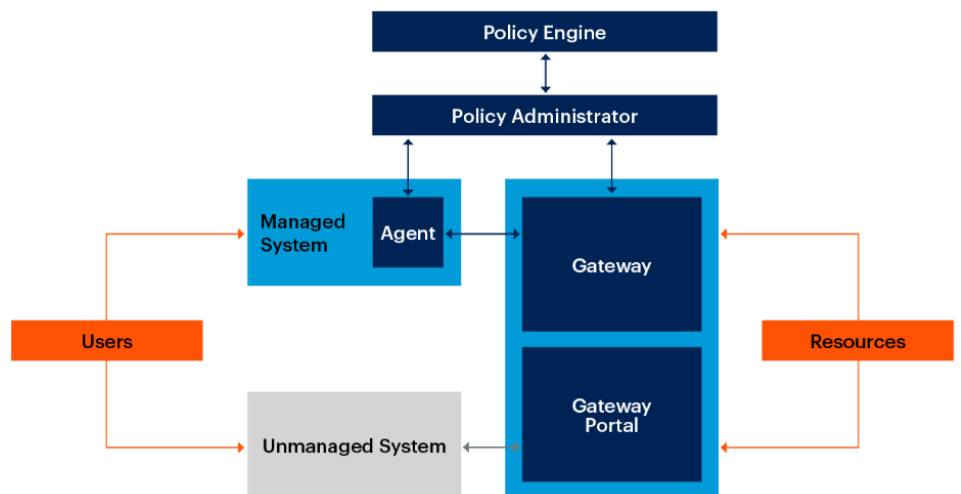
ZTNA addresses many of these VPN shortcomings by (1) creating a software-defined perimeter dividing the corporate network into micro-segments and preventing the lateral movement of threats; (2) creating virtual darknets and preventing application discovery on the public Internet and securing organizations from data exposure, malware, and DDoS attacks; (3) enabling secure, fast, uninterrupted, direct-to-cloud access to private applications, providing a consistent experience to remote users accessing SaaS and private applications; and (4) continuously analyzing contextual data such as user location and device posture to detect abnormal behavior and providing the ability to terminate remote sessions. Ultimately, ZTNA offers more granular access to a specific set of applications and data sources authorized for each user, restricting user access to applications on a “need to know” basis and reducing the attack surface.

Exhibit 28: VPN Workflow



Source: McAfee

Exhibit 29: ZTNA Workflow



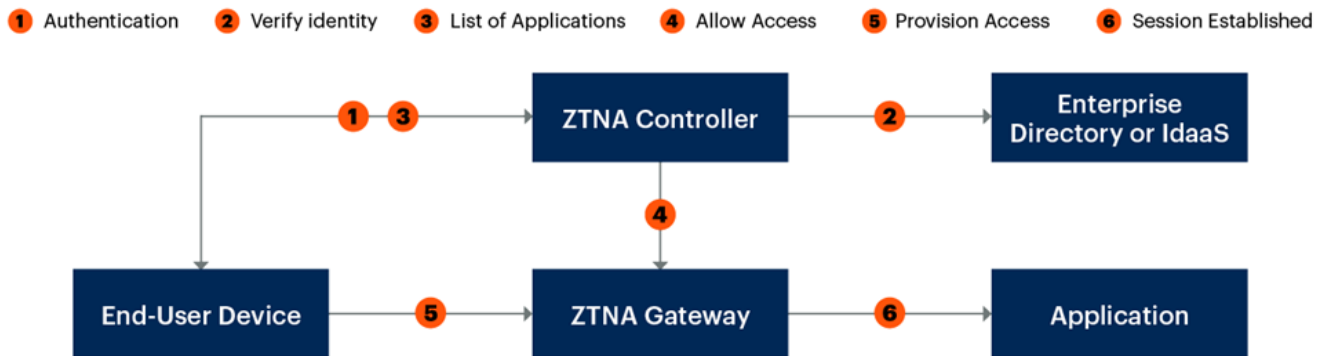
Source: Gartner

Technology-wise, ZTNA solutions utilize a trusted broker between the user and an application and evaluate the user’s credentials. Unlike VPNs, ZTNA does not use IP addresses or a fixed location to establish trust and instead relies on adaptive identity and

context-based characteristics to authenticate a user. Once authenticated, the trust broker communicates with a gateway function that creates a tunnel between the user and the desired specific application (not the entire corporate network as VPNs do). Trust brokers can be deployed via a cloud service managed by a third-party vendor, as a physical appliance within an organization's data center, or as a virtual appliance within an organization's public cloud environment.

There are two predominant methods for implementing ZTNA: (1) endpoint-initiated ZTNA; and (2) service-initiated ZTNA. With endpoint-initiated ZTNA, an agent installed on the user's endpoint device communicates with a ZTNA controller, authenticates the user's identity using the enterprise directory or a third-party IDaaS provider, and then grants access to a list of approved applications. Exhibit 30 outlines endpoint-initiated ZTNA.

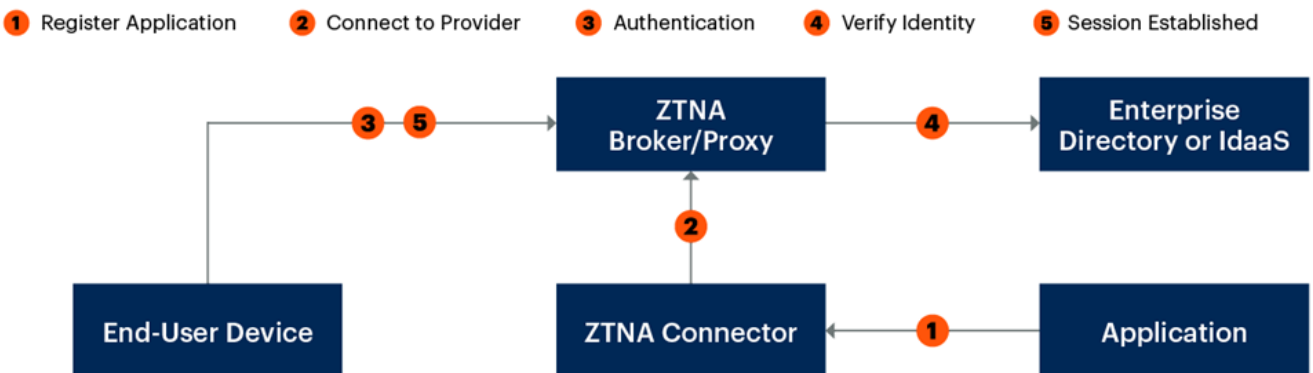
Exhibit 30: Endpoint-initiated ZTNA



Source: Gartner

With service-initiated ZTNA, the user authenticates with the ZTNA provider's cloud (Zscaler, for example), validating the user's identity with an enterprise identity management solution. The provider then connects with a connector within the organization's network. Traffic from the user then passes through the provider's cloud, isolating the required applications using a proxy. Service-initiated ZTNA eliminates the need to create openings in the organization's network firewall and creates an additional layer of network security instead. Exhibit 31 outlines service-initiated ZTNA.

Exhibit 31: Service-initiated ZTNA



Source: Gartner

Vendors currently offer agent-based and agent-less architectures. The majority of ZTNA deployments are agent-based as organizations look to deploy all three major components of SSE (ZTNA, CASB, SWG) with a single agent, although demand for agent-less ZTNA that secures unmanaged devices and third-party access is rising. While VPN replacement

remains the primary driver of ZTNA adoption, organizations are also increasingly replacing their existing campus security solutions (like NAC) with ZTNA.

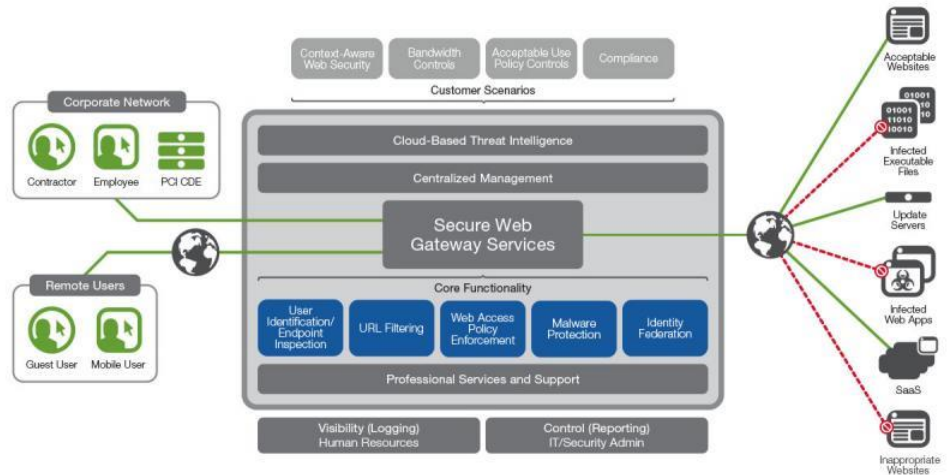
Looking ahead, we expect healthy ZTNA adoption from clients looking to replace legacy VPN tools, adopt zero-trust security postures, and shift to SSE and SASE architectures. As noted, SSE consolidates three adjacent cloud security capabilities (ZTNA, CASB, and SWG) into a single cloud architecture, reducing operational complexity and overhead costs. Given the immediate value of replacing legacy VPN, we view ZTNA as the “gateway product” to broader SSE adoption. We believe organizations will emphasize vendors with strong ZTNA capabilities as part of their SSE offerings and vendors who can deliver unified ZTNA, CASB, and SWG capabilities from a single-agent platform. Considering this, we expect stand-alone ZTNA vendors to expand their capabilities to address the broader SSE opportunity or be acquired.

Secure Web Gateway (SWG)

SWGs provide an additional layer of protection against attacks, enable safer and more efficient adoption of cloud-based services, monitor and filter incoming web traffic, and protect employees from web-based threats in compliance with corporate Internet access policies. SWGs deliver these capabilities by implementing various security technologies such as URL filtering, advanced threat defense (ATD), malware detection, web application control, remote browser isolation (RBI), and threat protection.

Historically, organizations used firewalls and VPNs as a web proxy or a web filter and implemented controls over employee Internet access and browsing, blocking what they deemed inappropriate or high-risk web content (pornography, gambling, etc.). In recent years, enterprises have seen a dramatic increase in the use of the Internet, cloud services such as Salesforce and Microsoft Office 365 (more than half of web traffic today is related to apps and cloud services), and the number of employees working remotely. These shifts have raised security risks as users often bypass traditional in-line firewalls, limiting enterprises’ ability to detect data transfers between the company and personal cloud applications.

Exhibit 32: Secure Web Gateway



Source: AT&T

SWGs are typically deployed as an agent on an endpoint or as a gateway (proxy) within a data center (between users and the Internet). They inspect Internet traffic in real-time against preset corporate policies, monitor all inbound/outbound web traffic, block access to restricted URLs, analyze web traffic for malicious code, provide application-level controls that analyze outbound traffic, and prevent unauthorized data downloads from SaaS applications, such as Salesforce or Microsoft Office 365.

In recent years, firewall vendors have broadened their capabilities, adding URL filtering and deep-packet inspection features to their NGFW offerings. However, the data encryption/decryption associated with URL filtering greatly strains firewall CPUs and

negatively impacts performance. In addition, firewalls lack the native DLP capabilities that SWG solutions offer, particularly for applications, cloud services, web browsers, and mobile applications. Thus, enterprises increasingly run proxy-based SWG solutions alongside traditional firewalls to take advantage of additional cloud security capabilities without undermining firewall performance.

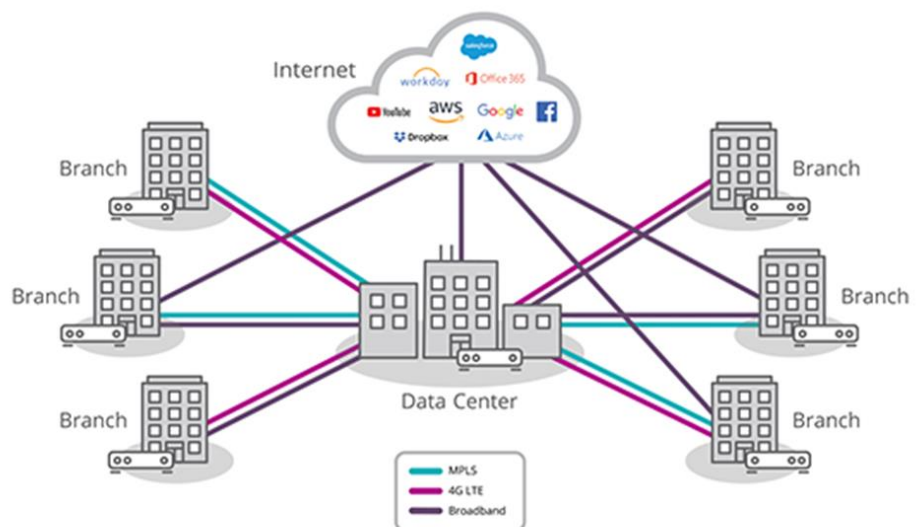
While we expect SWGs to consolidate longer-term with CASB and ZTNA solutions into SSE/SASE platforms, the SWG market continues to evolve from a technology standpoint. Recently, we have seen the emergence of start-up vendors such as Talon and Island.io, which deliver SWG functionality via a browser-based approach called Secure Browser isolation. This new approach layers security features on top of the open-source Chromium code base, widely used in standard web browsers like Google Chrome and Microsoft Edge. Secure Browsers deliver a native user experience while providing SSE security capabilities such as SWG, in-line CASB, and lightweight ZTNA. However, they lack API integrations, leaving gaps in securing SaaS applications. We believe this technology is better suited for small and mid-sized businesses, and we expect more prominent SSE vendors to introduce their own Secure Browser capability.

The SWG market has seen a rapid increase in adoption, coinciding with the adoption of cloud-based network security architectures like SSE and SASE. Modern SWG solutions have matured significantly and now offer capabilities historically found in enterprise firewalls and CASBs. These include anti-malware engines, decrypting and scanning websites, DLP, and lightweight SaaS application access. We expect most SWG adoption to come via converged SSE offerings.

Software-Defined Wide Area Networking (SD-WAN)

SD-WAN is a virtual WAN architecture that enables organizations to manage several transport technologies, such as MPLS, LTE, 5G, and broadband Internet, in a centralized way to securely and efficiently connect users directly to the Internet and applications. SD-WAN achieves this by separating applications from the underlying network services with a policy-based virtual overlay that monitors the real-time performance characteristics of the underlying networks and selects the optimal network path for each application based on configuration policies. This added software layer runs on top of the traditional WAN network, enables application-aware routing, intelligently directs traffic, and provides administrators with a centralized management overlay to implement changes to configuration policies.

Exhibit 33: SD-WAN Architecture

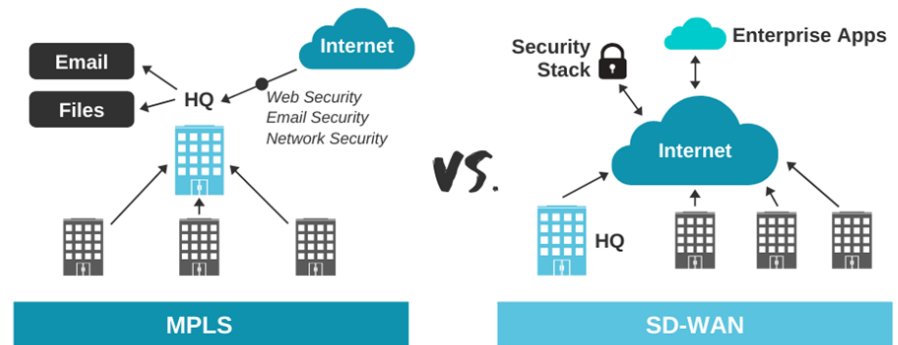


Source: Silver Peak

Traditionally, organizations backhauled all network traffic from branch offices over wide-area Multiprotocol Label Switching (MPLS) networks to a central data center. From there, traffic was routed to the Internet. This approach was practical when applications commonly resided in traditional data centers and Internet usage was light. However, this backhaul approach has become less effective as Internet traffic skyrocketed, organizations shifted applications to the cloud, and workers increasingly used SaaS applications, overloading the MPLS networks. This created management complexity, added costs, and yielded poor application performance.

SD-WAN addresses these challenges by applying a software-defined networking (SDN) approach to traditional WAN architectures. Its software sits across the WAN and enables enterprises to use any transport service intelligently to direct traffic across the network. While traditional WANs route all traffic to a central data center before distribution to the Internet, SD-WANs can forward any branch office cloud-bound traffic directly to the Internet (not through the data center) using any broadband connection (5G, LTE, broadband, etc.) and over encrypted tunnels, while routing sensitive enterprise data over MPLS back to the data center.

Exhibit 34: MPLS-Based WAN vs. SD-WAN



Source: Portknox

SD-WAN provides customers with several benefits beyond improved application performance. First, by intelligently routing traffic over various transport services, SD-WAN reduces the reliance on and usage of expensive MPLS connections, allowing the transport of less sensitive data over cheaper connections directly to the Internet. Second, enterprises gain complete network visibility by delivering a centralized management overlay that seamlessly implements configuration changes. Last, enterprises benefit from enhanced security controls such as integrated threat protection, secure traffic across broadband Internet connections, and integrations with the NGFWs.

Looking ahead, we see multiple drivers for the adoption of SD-WAN solutions. First, we expect enterprises to continue to look for ways to manage their cloud traffic and reduce the costs associated with MPLS connections. Second, we expect the shift to SASE architectures to serve as a multi-year demand tailwind for SD-WAN adoption. In the near term, we expect most organizations to leverage a dual-vendor SASE architecture and purchase SD-WAN and SSE separately. Longer-term, we believe many organizations will consolidate their internal security and networking teams and leverage single-vendor SASE platforms. According to Gartner, 60% of SD-WAN purchases will be part of a single-vendor SASE solution by 2026.

To take on the large SASE opportunity, many vendors have begun offering SD-WAN and SSE in a converged offering. Vendors like Cato Networks and Versa Networks have expanded their security capabilities, while security vendors like Netskope (via its

acquisition of Infot) have added SD-WAN. One notable exception here is Zscaler, which currently does not offer a native SD-WAN solution and partners with SD-WAN vendors instead. Lastly, we expect vendors to incorporate AI/ML into their offerings to help streamline the initial network configuration and offer simplified management.

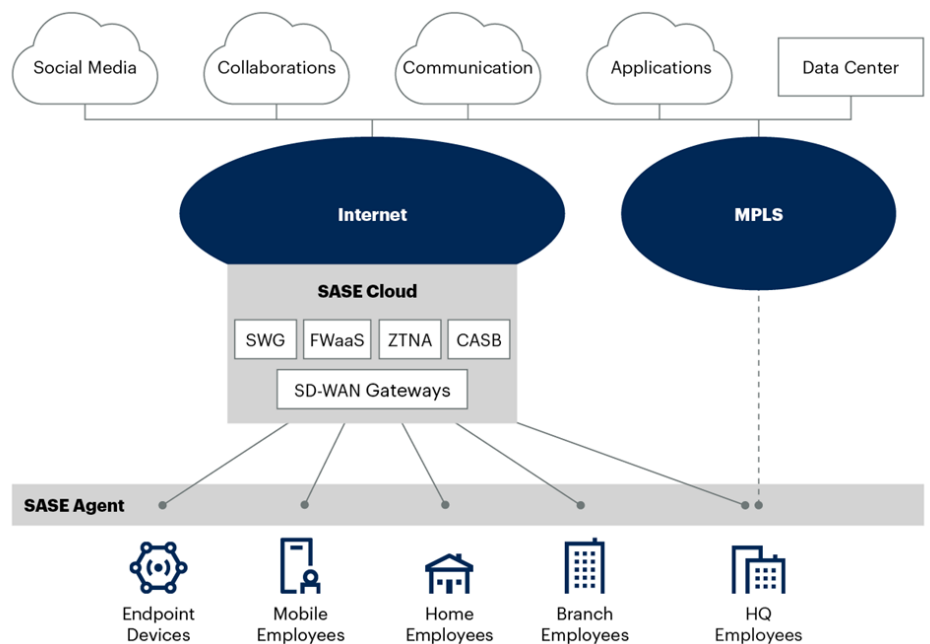
Security Service Edge (SSE)/Secure Access Service Edge (SASE)

Current network security architectures were designed with the enterprise data center as the focal point for access and control. Yet, digital transformation, cloud and edge computing adoption, and the shift to remote work have increasingly inverted access requirements with users, devices, applications, and data outside the traditional enterprise perimeter. This shift has rendered traditional network security models (based on data center perimeter security) ill-suited to address the dynamic needs of modern digital businesses and their distributed workforce. This has accelerated the adoption of policy-based cloud-based security solutions (SWG, CASB, etc.) that apply zero-trust principles.

To address the shift to outbound connections, enterprises have increasingly adopted cloud-delivered security solutions (from proxy-based web content inspection through SaaS application discovery and access control to cloud-delivered remote access for on-premise and cloud resources). Such solutions negate the need for on-premise hardware while offering secure direct routes to cloud resources. Nonetheless, with a growing number of stand-alone solutions addressing different aspects of cloud security, the benefits of cloud-delivered security (simplicity, management, control, etc.) have been diluted. Consequently, vendors have increasingly looked to consolidate disparate cloud security solutions into a single cloud-based platform addressing multiple use cases. This marked the emergence of new security architectures, specifically SSE and SASE.

SSE and SASE are emerging security architectures that consolidate disparate networking and network security solutions into a single cloud architecture. SSE incorporates solutions such as FWaaS, ZTNA, SWG, and CASB (the security side), whereas SASE (the total package) builds on the cloud security capabilities of SSE and adds an SD-WAN networking twist. Both architectures enable organizations to apply a consistent, cloud-centric approach to network security policy using a modular architecture designed to scale based on their cloud usage.

Exhibit 35: SASE Architecture

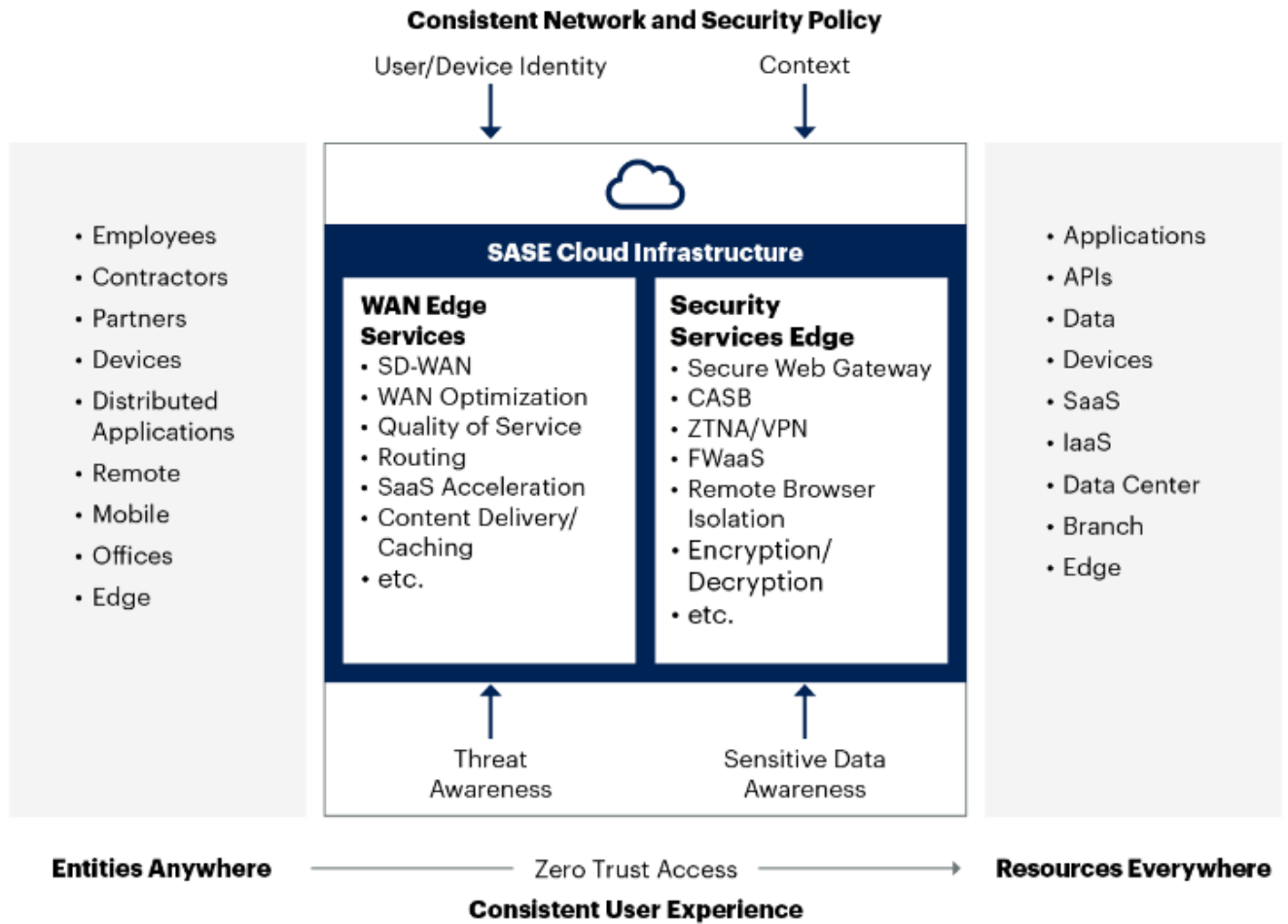


Source: Gartner

SASE and SSE use local agents installed on devices to connect to the closest PoP. User traffic is then decrypted once, inspected by multiple engines based on corporate policy,

then encrypted again, and sent to the final destination. This architecture eliminates the need to backhaul traffic to the data center. It uses a flexible, micro-services framework that can quickly scale to meet an organization’s cloud usage. This zero-trust architecture embeds all access forms (remote, on-campus, branch) while securing branch offices (via an SD-WAN appliance) and edge devices (via an agent). SASE offers many benefits, including (1) lower WAN and VPN congestion and cost, (2) reduced latency (direct to cloud, one-step decryption/encryption), (3) single-pass scanning for sensitive data and malware, (4) fewer agents under management, and (5) unified management responsibility for network/security teams simplifying policy management and enforcement.

Exhibit 36: SASE – Convergence of Network and Security Architectures



Source: Gartner

The ability of SSE to consolidate multiple different security tools into a converged cloud offering, reducing complexity and costs, has led to an acceleration in adoption. Customers increasingly buy SWG, CASB, and ZTNA from a single vendor offering a converged solution. According to Gartner, 85% of organizations will obtain CASB, SWG, or ZTNA from a converged offering by 2026. However, while we expect single-vendor SSE to become the norm, we expect more gradual adoption for single-vendor SASE offerings. SASE adoption requires a convergence of security and networking teams to unify policy creation, a complicated and challenging process for large organizations. Many organizations still have legacy on-premises hardware investments with long refresh cycles, making adopting new and all-encompassing cloud-delivered solutions challenging. As a result, we expect small- and mid-size organizations, who often have a single security and networking team, to be the primary buyers of single-vendor SASE offerings. We expect most large enterprises to leverage a dual-vendor strategy, with one vendor addressing networking needs and another addressing security needs.

From a vendor perspective, as noted, parts of the SSE market have already seen considerable convergence, most notably between CASB, ZTNA, and SWG vendors (Netskope and Zscaler, for example). In fact, even new emerging vendors often come to market with multiple SSE components, while pure-play vendors are expanding their offerings. The market has also seen an increase in vendors offering a complete SASE offering that includes SSE and SD-WAN (aka single-vendor SASE). These include vendors like Palo Alto Networks, Cato Networks, Versa Networks, Cisco, Fortinet, and, more recently, Zscaler. While we expect vendors with leading security platforms (Zscaler, Netskope, Palo Alto Networks, Versa Networks) to gain share, the market is highly crowded and competitive.

Micro-segmentation

The explosion in the number of applications deployed and changes in their underlying architecture (virtualization, microservices, containers, cloud, etc.) have led to a dramatic increase in east-west data center traffic (i.e., traffic between servers and within the data center domain). However, most perimeter-based security solutions focus on monitoring north-south data center data traffic (i.e., traffic between the data center and the public network) and are not granular enough to bind policies to individual applications. This has enabled attacks to propagate and spread laterally within the enterprise domain with little to no interruption once the perimeter-based solutions were breached. Micro-segmentation aims to solve this problem.

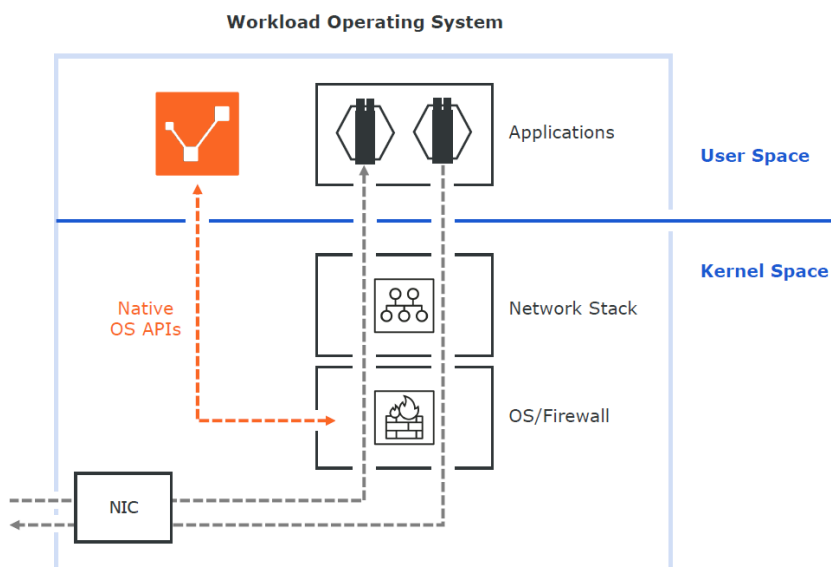
Segmentation aims to parse the IT environment into smaller logical sections that can be quarantined or isolated if a cyberattack successfully penetrates outside defenses. Traditionally, security teams used ACL (access control list), VLAN, and firewall-based cloud security policies for segmentation. Yet these technologies lack intra-application communication visibility and require significant manual monitoring of application-to-application communication. Micro-segmentation (also identity-based segmentation) is a form of zero-trust networking that uses policy and application workload identity to isolate workloads, applications, and processes in data centers, the public cloud, and containers. Micro-segmentation can enforce security policies, limit the lateral spread of attacks, reduce the attack surface, and offer visibility and control into East-West communications in the network.

Micro-segmentation divides the data center into segments by tapping into the native stateful firewall within each workload's operating system. Security teams can then define policy controls at the application level, prevent unrestricted lateral movement, and limit the spread of attacks, significantly reducing the attack surface. While segmentation can also be achieved by deploying many firewalls throughout the network, the associated costs and operational complexity are high and difficult to scale. It's important to note that while micro-segmentation offers greater granularity and scale, its deployment is not without challenges and requires lengthy planning and step-by-step implementation. Micro-segmentation can be delivered in three ways: (1) agent-based; (2) network-based; or (3) hypervisor-based.

- **Agent-based micro-segmentation** deploys an agent on endpoints, monitoring and analyzing traffic to identify and group related traffic flows. Agent-based segmentation is most useful for customers with mature workload deployment processes who need the flexibility to move protections and accompanying workloads across hybrid environments. Agent-based micro-segmentation is the most commonly deployed method, as it provides greater flexibility for customers with heterogeneous environments and multiple networking vendors.
- **Network-based micro-segmentation** relies on the centralized controllers of software-defined networking (SDN) solutions to define security policies. These controllers can analyze all application traffic passing through the network, allowing them to implement micro-segmentation for workloads.
- **Hypervisor-based micro-segmentation** refers to segmentation capabilities in the hypervisor layer. These products abstract the network and security services from the hardware and apply them across each virtual machine. This form of micro-segmentation delivers comprehensive coverage and can be used for virtual workloads in data centers, public cloud environments, and IoT systems.

Micro-segmentation can be applied across a variety of DevSecOps (segmenting workloads through the CI/CD process), cloud security (segmenting containers and Kubernetes workloads), and Zero Trust (implement least-privilege access) use cases. Major micro-segmentation vendors include Illumio, Akamai (Guardicore), Cisco, VMware, and Palo Alto Networks. Illumio, the only pure-play micro-segmentation vendor, uses a very lightweight agent with a modern OS (Virtual Enforcement Node (VEN)) that is controlled and centrally managed by a server (Policy Compute Engine (PCE)). The telemetry it collects includes the OS type, running processes, and IP addresses the workload communicates with. With this telemetry, Illumio creates a live visibility map of communications channels to establish a segmentation policy. The company uses an allow-list model, which means all traffic is blocked by default unless it is on the allow-list. Ultimately, Illumio delivers improved visibility and policy enforcement without performance degradation scaling parallel to the workload.

Exhibit 37: Illumio's Agent-based Architecture



Source: Illumio

While demand for micro-segmentation has increased as customers look to adopt zero-trust architectures, our conversations with industry partners suggest a slow rate of adoption due to the complex challenges of implementing micro-segmentation technology as (1) organizations need to gain a complete view of the traffic within their data center and then establish a thorough risk governance framework, which can be time-consuming, (2) security teams often do not know which applications should be communicating with others, leaving them hesitant to rely on automatically generated protections rules, and (3) traditional data center firewalls also offer broader east-west traffic segmentation, which can create operational challenges for micro-segmentation implementation due to conflicting policies. Over time, as existing micro-segmentation solutions mature and become easier to deploy, we expect adoption to improve.

Enterprise Browsers

Web browsers were introduced in the early 1990s to access the Internet. While browsers had limited business use early on, today, they are the de-facto user interface for accessing internet-based resources and applications. With the growing use of SaaS applications, remote work, work from home, and BYOD devices, threat actors have increasingly targeted web browsers to gain access to sensitive business data. Traditional browsers have weak security controls and are ineffective at preventing malware attacks, safeguarding sensitive data, and blocking malicious redirect attacks. Threat actors commonly target browsers, hijacking browser sessions, installing malware, and stealing user credentials and confidential data. To protect against these attacks, customers have relied on security tools such as ZTNA, CASB, and anti-virus. However, managing and integrating multiple security solutions can be cumbersome. This has led to the emergence

of Enterprise Browsers that deliver integrated security capabilities directly in the browser or extensions. Today, Enterprise Browsers' most common use cases are securing employee internet access against malicious attacks and protecting sensitive data in critical cloud applications.

An Enterprise browser is effectively a hardened sandbox that offers secure access to critical business web applications & resources. These browsers incorporate security capabilities like malware detection, malicious code scanning, cookieless browsing, and session monitoring. In a breach, enterprise browsers can terminate a session and prevent malware from spreading across the network. These browsers also offer granular role-based access, and DLP controls that allow security teams to prevent the theft of sensitive data by threat actors and rogue employees. Security teams can set access policies based on users, device posture, location, time, and network. Notably, many Enterprise Browsers do not install an agent on personal devices, allowing customers to protect sensitive business data without violating employee or third-party contractor privacy.

Exhibit 38: Key Capabilities of Enterprise Browsers

Prevention and Detection	Centralized Management	Visibility and Response	Productivity and Collaboration
Web Content Security	User Device Onboarding	Endpoint Posture Assessment	Custom Browser Automation
Data Loss Prevention	Security Policy Settings	Logging and Forensics	Built-In Productivity Tools
Phishing Protection	Identity Provider Integration	Security Tools Integration	Messaging and Calling
Malware Protection	Reporting and Analytics	Browser Extension Audit	Secure Remote Access
Identity Protection	Policy-Driven Configurations	Block Malicious Extension	Biometric Authentication
Compromise Isolation	Access Control Policy	Role-Based Access Control	Cloud Access Security

Browser Extension*

Enterprise Browser

Source: Gartner

The market for Enterprise Browsers is nascent but is gaining traction among mid-sized vendors looking to adopt a zero-trust security posture. Major vendors in the space include the leading browser vendors (Google and Microsoft) and stand-alone security vendors like Island.io, Talon (now part of Palo Alto Networks), and LayerX. We note that the browser extension space is much broader, with vendors like Check Point, Microsoft, Perception Point, and LayerX all offering browser extensions. Browser extensions are plug-ins that can be installed onto standard browsers (like Chrome, Safari, or Edge) to deliver enhanced security controls to protect against malware attacks and data theft while allowing employees to use their browser of choice. While they add security capabilities, they lack the advanced policy controls of Enterprise Browsers.

Looking ahead, we expect customers to evaluate Enterprise Browsers as part of their web security posture. While we see the potential for displacements of SWG and CASB solutions in small and mid-sized customers who lack the resources to manage a complete SSE platform, we believe the adoption of Enterprise Browsers will most likely complement SSE platforms in large-sized enterprises. We note that Gartner expects 25% of enterprises to use managed browsers or extensions by 2026 (vs. 10% today).

Network Security Market Vendor Overview

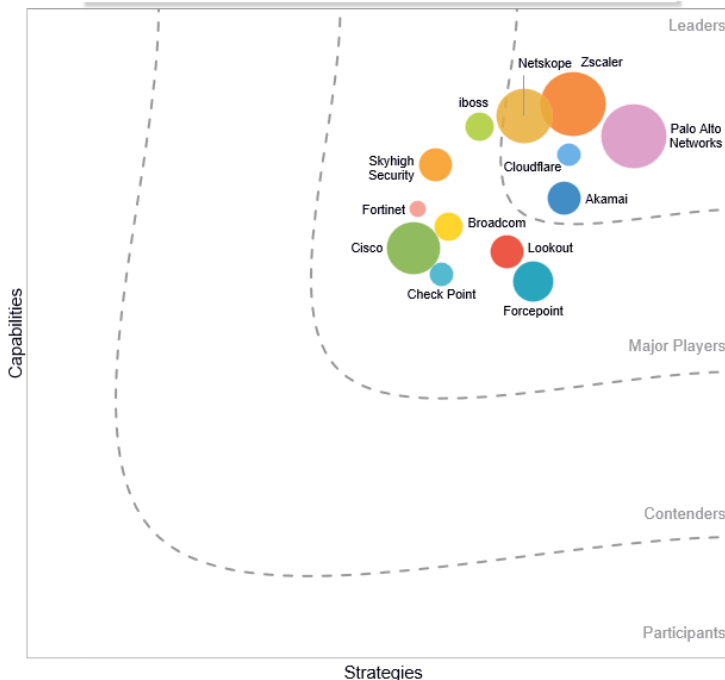
From a vendor perspective, the network security market includes some of the most mature and long-standing security vendors, such as Cisco, Check Point, Fortinet, and Palo Alto. This group has a broad presence in many market sub-segments and has recently addressed the emerging cloud opportunity. Emerging vendors such as Zscaler, Netskope, Menlo Security, Lookout, and iboss have disrupted the market with cloud-optimized platforms and have moved quickly to address the SSE opportunity. They represent the greatest threat to the network security incumbents. Illumio stands out as a micro-segmentation specialist in the market, while Versa Networks and Cato Networks stand out as SD-WAN vendors pushing into the SASE market.

Exhibit 39: Gartner Magic Quadrant for Single-Vendor SASE



Source: Gartner

Exhibit 40: IDC Network Edge Security-as-a-Service MarketScape 2023



Source: IDC

Exhibit 41: Forrester Enterprise Firewall Wave



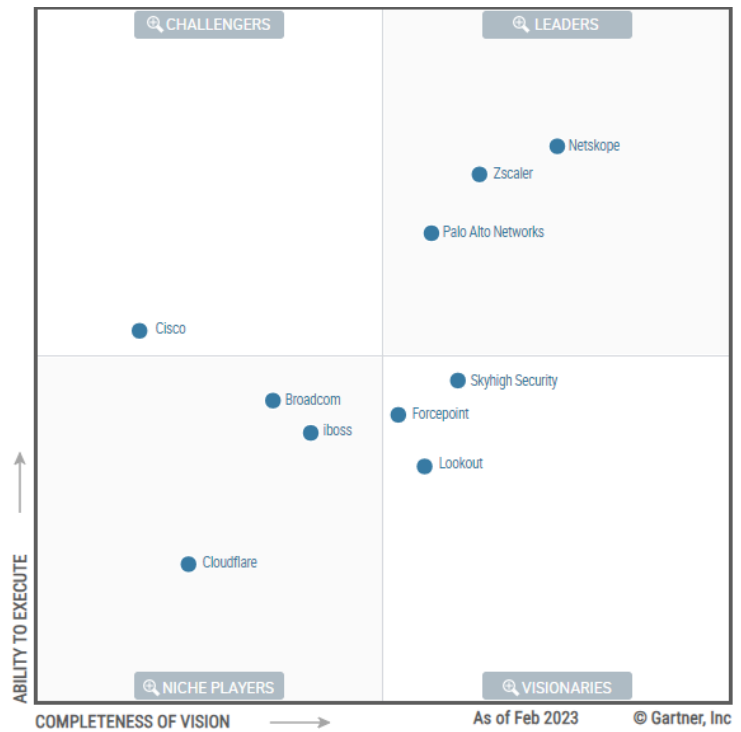
Source: Forrester (4Q22)

Exhibit 42: Gartner Magic Quadrant for SD-WAN



Source: Gartner

Exhibit 43: Gartner Magic Quadrant for Security Service Edge



Source: Gartner

Exhibit 44: Forrester Microsegmentation Wave

Source: Forrester

Below, we review key vendors in the Network Security market that were not already discussed in detail in this section.

- Palo Alto Networks** is one of the major vendors in the network security market. The company offers a complete portfolio of firewall solutions supporting various deployment models (on-premises, VM, FWaaS) and all major cloud container environments, including Google (Google Kubernetes Engine), Microsoft Azure (Azure Kubernetes Service), Amazon's AWS (AWS Elastic Kubernetes Service), and Red Hat's OpenShift. Prisma Access, addressing SSE (FWaaS, CASB, ZTNA, SWG), and Prisma SD-WAN (through the CloudGenix acquisition) are the company's next-generation SASE components with SD-WAN incorporating ML and automation capabilities. Together, the solutions form Prisma SASE, which converges security, SD-WAN, and Autonomous Digital Experience Management into a single cloud-delivered service. Palo Alto also offers micro-segmentation that relies on workload identities rather than traditional network IP addresses and an Enterprise Browser via its acquisition of Talon Security.
- Fortinet** offers a broad network security portfolio, including a next-generation firewall, Security-as-a-Service for Networks, WAN edge (SD-WAN, LTE, 5G), and cloud-delivered security (SASE), which can be centrally managed through FortiManager. The company's FortiGate firewalls support all deployment models (on-premises, virtual, cloud-based, and containerized). FortiGate NGFWs come with built-in micro-segmentation capabilities for securing ICS/OT networks. Fortinet Secure SD-WAN (via OPAQ Networks (2020) acquisition) is an ASIC-accelerated SD-WAN powered by FortiOS. The solution allows customers to centrally manage firewalls, switches, access points, and LTE/5G extenders from a centralized management center. Lastly, the company's cloud-based FortiSASE solution combines Fortinet's SD-WAN capabilities with FWaaS, ZTNA, SWG, and CASB. Fortinet is one of a few security vendors to offer a portfolio of security-driven networking gear (switching and WLAN).

- Cisco** is a major player in the firewall market and offers a complete SASE portfolio. Cisco Umbrella is the company's cloud-based Secure Internet Gateway (SIG) platform, incorporating a firewall, FWaaS, SWG, CASB, RBI, DLP, malware protection, DNS layer security, and various other capabilities. Cisco also offers ZTNA through its Duo Beyond product and two SD-WAN platforms, Meraki and Viptela. Meraki is known for its intuitive, visual-based management capabilities and centralized, cloud-based controller, which can configure, manage, monitor, and secure routers, switches, security devices, etc. Viptela also employs a cloud-first approach but uses a different architecture leveraging individual appliances for scale and deployment customization. Cisco's portfolio depth, deployment flexibility, and extensive channel reach have helped it build a strong position in the SD-WAN market. Cisco Umbrella is fully integrated with Meraki and Viptela, while Duo Beyond (ZTNA) is a separate overlay.
- Check Point** is one of the early vendors in the firewall market. It offers a broad network security portfolio, including appliance-based and cloud firewalls, SD-WAN, SWG, CASB, and ZTNA for an end-to-end SASE portfolio. Check Point is known for its strong firewall capabilities, offering the fastest firewall on the market (Quantum Lightspeed). In addition to its network security capabilities, the company offers EDR, MDR, and email security via its Harmony portfolio and CSPM, CWPP, and threat hunting via its CloudGuard portfolio. The company's broad offering makes it an ideal vendor for customers seeking to consolidate security solutions. Check Point's mature platform is widely adopted among customers with hybrid architectures, who often need strong management capabilities to handle complex workflows. The company has a global presence and derives almost half of its revenue from Europe.
- Zscaler's** core offering, Zscaler Internet Access (ZIA), is a cloud-based SWG solution that evolved into an SSE platform with capabilities such as CASB, ZTNA, DEM, browser isolation, and FWaaS. The company's Zscaler Private Access (ZPA) solution is a ZTNA offering (VPN replacement) for access to a customer's internally managed applications, and it provides additional security functionality similar to ZIA, such as CASB, DEM, browser isolation, FWaaS, etc. The company's Zscaler Digital Experience (ZDX) is a user experience management platform that can be deployed across its network of users. Zscaler has expanded its offerings to include workload segmentation, CWPP, CSPM, and CNAPP capabilities (excluding security related to application development) as part of its Posture Control offering (Zscaler Cloud Protection). Lastly, the company released an SD-WAN solution via its Branch Connector VM, rounding out its SASE capabilities. Zscaler sells its products on an annual, per-user, or per-workload (for cloud protection) subscription basis and notes broad adoption by large enterprises drawn to the platform's ease of use, straightforward deployment, and comprehensive capabilities.
- Netskope** is a cloud-native security vendor offering comprehensive SASE with CASB, SWG, ZTNA, and FWaaS capabilities. The platform is based on a microservices architecture and known for its advanced data security capabilities, low latency (15ms), strong support for Kubernetes environments, simple deployment process, and ease of use. Netskope's growing SSE traction builds on its strong position in the CASB market, where its broad SaaS application coverage and governance capabilities have been vital adoption drivers. Netskope's cloud firewall includes RBI capabilities, gained in its 2021 acquisition of Randed. The company added SD-WAN to its platform via its acquisition of Infio, enabling it to deliver a single-vendor SASE offering.
- Menlo Security** offers a comprehensive, cloud-native security platform built on its Elastic Isolation Core (EIC). It provides a layer of abstraction from the web and uses zero trust isolation to protect against known and unknown threats. The platform includes a full suite of SSE solutions, including SWG, CASB, ZTNA (Menlo Private Access), and DLP. Menlo's products can be managed from a single console and leverage its core RBI capabilities. The native integration of RBI is a point of competitive differentiation, as most vendors only offer RBI as a standalone solution. In contrast, Menlo uses its RBI isolation core to abstract all traffic to the end user, separating the web from the user. The company has leveraged its core technology to offer a secure cloud-based browser, which helps prevent phishing and malware

attacks. Menlo's platform offers low latency (<100ms) and 99.995% uptime and is designed to scale to customers' needs. It also provides purpose-built solutions for securing Office 365 and G-Suite. Menlo has established a strong presence in the financial services sector.

- **Cato Networks** offers a comprehensive SASE offering through its Cato SASE Cloud. The platform includes the Cato Socket SD-WAN, which connects a customer's physical location to the nearest Cato point of presence (PoP) over various connections (cable, xDSL, 4G/LTE). The company's SSE platform includes an application-aware FWaaS, SWG, CASB, IPS-as-a-Service, and anti-malware protection. Cato rounds out its SASE offering with Secure Remote Access (ZTNA) for on-premise and cloud applications. Cato's offering provides complete visibility into the network as all WAN and internet traffic passes through its SASE Cloud.
- **Versa Networks** is a SASE vendor that offers SSE capabilities centered on a leading SD-WAN solution. Versa's SD-WAN solution has one of the market's most mature sets of abilities and is adopted by over 19,000 customers. The company offers a fully-featured SD-WAN that can be deployed in the cloud and on third-party hardware and a simplified, cloud-delivered offering for lean IT teams. Versa offers a comprehensive, tightly integrated SSE portfolio that includes CASB, ZTNA, SWG, FWaaS, and RBI, which, combined with its SD-WAN offering, makes up its Versa Secure Access Fabric (VSAF). The company also offers Titan, a SASE product dedicated to price-sensitive SMB customers, and leverages a broad network of carriers for global distribution and managed services offerings.
- **Lookout** offers an integrated SSE offering that includes CASB, SWG, ZTNA, and endpoint security products. The company's solution is known for its strong technological capabilities, particularly for data security. The company offers advanced features like watermarking, encryption, tokenization, and automated data classification. Lookout has developed an efficient sales strategy centered on strong relationships with ISPs, MSSPs, and telcos to gain an impressive presence among mid- and large-sized enterprises in the US and EMEA.
- **Skyhigh Security** is the SSE arm of McAfee Enterprises. The company offers a full SSE suite, including CASB, SWG, and ZTNA. Skyhigh's offering is highly regarded for its data security and malware detection capabilities embedded within its ZTNA solution and native integrations with McAfee's enterprise DLP offering. The company offers advanced features such as SSPM and integrated RBI. Skyhigh was late to the market and is still early in gaining broad adoption, although it benefits from selling to its large installed customer base. Skyhigh offers a simple pricing structure with three tiers.
- **Illumio** is a micro-segmentation vendor for workloads, cloud environments, and endpoints. The company uses an agent-based approach that operates at the user level rather than in the kernel space. These agents (virtual enforcement nodes (VEN)) are installed on various workloads, including VMs, bare-metal servers, public cloud instances, and containers, to collect information such as which IP addresses the workloads communicate with. VENs then send the telemetry to the Policy Compute Engine (PCE), creating application dependency maps and enforcing policies for host-based firewalls within each workload's operating system. According to management, Illumio's agents are lightweight and scale without affecting performance. The company's platform can be deployed on-premises and in all major cloud environments and is priced per agent. Illumio also offers an agentless solution, Illumio CloudSecure, that provides segmentation and zero-trust connectivity for public cloud workloads.
- **Forescout** is a pure-play NAC vendor that offers a platform that can be deployed on hardware, virtual appliances, and public clouds. It delivers an agent-based and agent-less solution, although its agent-less solution provides greater device visibility and coverage for IoT/OT devices, per Forescout. Notably, its platform is vendor-neutral and can be deployed in heterogeneous environments. Forescout's platform can connect with third-party security solutions such as an EDR or SIEM and automatically remove an endpoint from a network if a vulnerability or breach is detected.

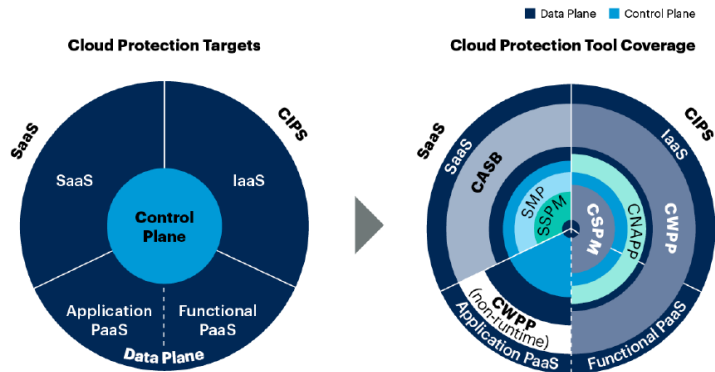
- Island.io** is a pure-play Enterprise Browser vendor. The company's Browser is a stand-alone application with integrated security and centralized policy management, built on open-source Chromium. Island addresses a broad range of use cases, such as securing (1) SaaS applications, (2) access for third-party contractors, (3) BYOD access, (4) zero trust security, and (5) VDI and VPN replacement. The company prices its solution on a per-user basis, with an annual fee for the central management console.

Cloud Workload Security

As organizations adopt multi-cloud environments and incorporate cloud applications, they also need to adopt security solutions to monitor, configure, and protect IaaS and PaaS environments. Multiple security solutions have emerged to address the cloud shift: Cloud Access Security Broker (CASB; part of network security and detailed in the prior section), Cloud Workload Protection Platforms (CWPP), Cloud Security Posture Management (CSPM), and SaaS Security Posture Management (SSPM). While these tools are adopted independently today, we see an evolution toward broader and more converged Cloud-Native Application Protection Platforms (CNAPP) in the longer term. In addition to CWPP and CSPM, CNAPP incorporates security capabilities such as KSPM, CIEM, and API security and spans the development and deployment sides of applications. We discuss this shift in detail in the Application Security market overview (next section). Separately, SSPM capabilities are already getting subsumed within CASB and CSPM.

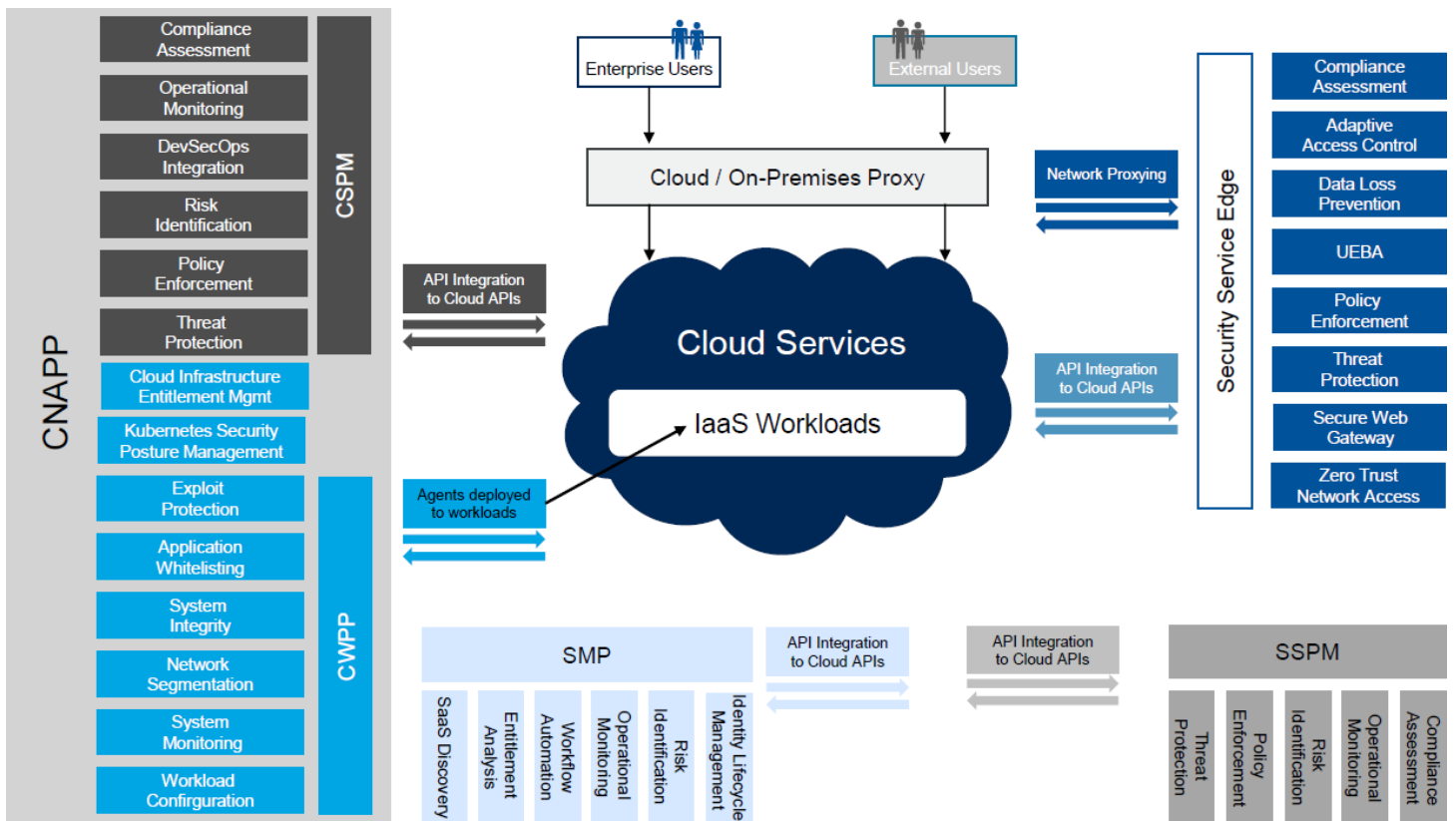
Exhibit 45: Cloud Protection Tool Coverage

Cloud Protection Tool Coverage



Source: Gartner

Exhibit 46: Structure for Cloud Security Tooling



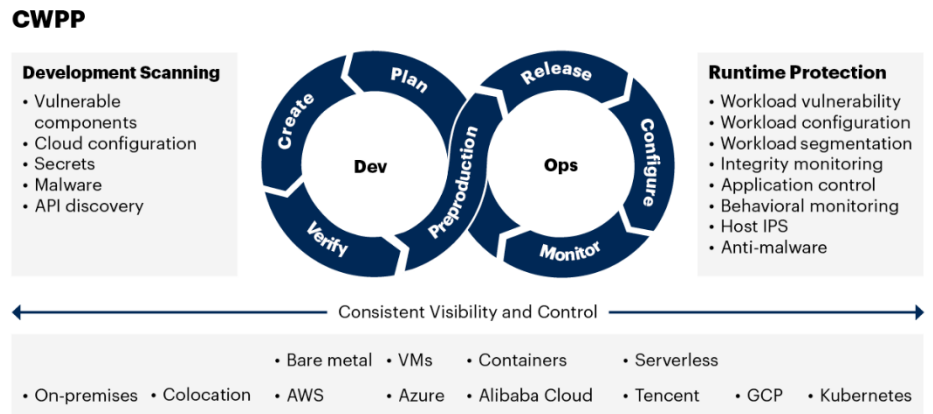
Source: Gartner

Cloud Workload Protection Platforms (CWPP)

Historically, servers in on-premise data centers were secured like desktops—using endpoint protection solutions. These solutions addressed compliance needs and delivered a single security management view of compute resources. While endpoints and servers require hardening, configuration, and vulnerability management, they diverge in their security needs. For example, endpoint devices are exposed to email, website, and application threats, which servers are not. Conversely, servers (on-premise and in the cloud) have a more predictable and generally predefined set of processes and activities, making default-deny models to prevent untrusted processes from executing more appropriate. Also, nearly all successful attacks on cloud services result from misconfiguration, mismanagement, and operational mistakes. Hence, server workloads in hybrid and multi-cloud environments require different, dedicated, and reliable cloud workload protection and configuration.

CWPPs are similar to endpoint security tools but focus on securing and providing consistent visibility into and control over physical machines, virtual machines, containers, and serverless deployments within cloud environments. Effective CWPPs address workload protection holistically from application development to runtime. They scan workloads for vulnerabilities in the development stage and protect the applications in runtime by applying system integrity protection, application control, behavioral monitoring, intrusion prevention, and runtime malware protection. Overall, we see several drivers for CWPP adoption, including (1) the rapid growth in cloud workloads, (2) the shift to cloud-native application development and container-based application architectures, and (3) improving ease of deployment as vendors mature their offerings.

Exhibit 47: CWPP Capabilities



Source: Gartner

There are different types of CWPP offerings in the market, which Gartner segregates into eight variants (Broad Spectrum, Container, Serverless-focused, EDR-focused, etc.). While most variants provide standard capabilities such as hardening and configuration, application control, user behavior monitoring, etc., each variant adds a unique capability. The primary driver for the variety of CWPP variants highlights the technological background of the providers before their evolution into CWPP vendors. Below, we list the differences in approach and sample vendor set for the different variants.

- **Broad Spectrum** is offered by larger legacy vendors that combine multiple tools to provide a multi-faceted approach across OSs. Vendors include Broadcom (Symantec), McAfee, Microsoft, and Sophos.
- **Container-focused** – vendors in this category have a broad set of capabilities with a particular focus on container deployments. Vendors include Aqua Security, NeuVector, Palo Alto Networks, and Sysdig.
- **Serverless-focused** – vendors that address serverless cloud computing with a focus on application and access control and insight into user behavior analytics. Representative vendors significantly overlap with container-focused CWPP and include Aqua Security, Palo Alto, and Sysdig.
- **Memory and process integrity protection** – vendors concerned with memory and process integrity to protect compute resources. Incremental services such as application control, hardening, and configuration have also been added. Vendors include Morphisec, Palo Alto, Polyverse, and Virsec.
- **Identity-based segmentation and visibility** – utilizes strict entitlement control and process isolation by logically segregating compute platforms. While some representative vendors are solely focused on network micro-segmentation, all provide network and application-level control and threat intelligence capabilities. Vendors include Cisco, Akamai (Guardicore), Illumio, Palo Alto, and Zscaler.
- **EDR-focused** – EDR vendors working to grow their solutions to encompass cloud workloads. EDR capabilities have been supplemented with cloud configuration, application hardening, workload behavior monitoring, and cloud-specific threat detection. Vendors include CrowdStrike, Lacework, SentinelOne, and VMware (Carbon Black).
- **Vulnerability, hardening, and configuration compliance** – historically included compliance vendors primarily focused on continuous compliance, inventory, and vulnerability reporting. Vendors include AWS, CloudAware, and Tripwire.
- **Application control and desired state enforcement** – primarily focused on delivering specific security parameters to all application software on the platform. Abnormal behavior is countered with regression back to a pre-determined “secure

state” with optional auto-remediation capabilities. The predominant vendor here is VMware (Carbon Black).

Exhibit 48: CWPP Variants and Capabilities

CWPP's "DNA Markers"/ Capabilities		CWPP Variants							App. Control / Desired State Enforcement
		Broad Spectrum	Container-Focused	Serverless-Focused	Memory, Process Integrity Protection	Identity Based Segmentation & Visibility	EDR-Focused	Vulnerability, Hardening & Config. Compliance	
Attack Surface Reduction	Hardening and Configuration	Dark	Dark	White	Dark	Dark	Dark	Dark	Dark
	Host-Based Network Firewalling	Dark	Dark	White	White	Dark	White	White	White
	Microsegmentation	Dark	Dark	White	White	Dark	White	White	White
	Exploit Prevention and Memory Protection	Dark	White	White	Dark	White	White	White	Dark
	Vulnerability Management	Dark	Dark	White	White	White	White	Dark	Dark
	Application Control	Dark	Dark	Dark	Dark	Dark	White	Dark	Dark
	Privileged Account Management	Dark	Dark	Dark	White	White	White	White	White
Pre-execution Protection	Antivirus	Light Blue	White	White	White	White	Light Blue	White	White
	Vulnerability Shielding	Light Blue	White	White	Light Blue	White	White	Light Blue	White
Post-execution Protection	Integrity Control	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey
	User Behavior Monitoring	Grey	White	White	White	Grey	Grey	Grey	Grey
	Intrusion Detection/Prevention	Grey	White	White	White	Grey	Grey	White	White
	Workload EDR	White	White	White	White	White	Grey	White	White
	Autoremediation	Grey	Grey	White	White	Grey	Grey	Grey	Grey

Source: Gartner

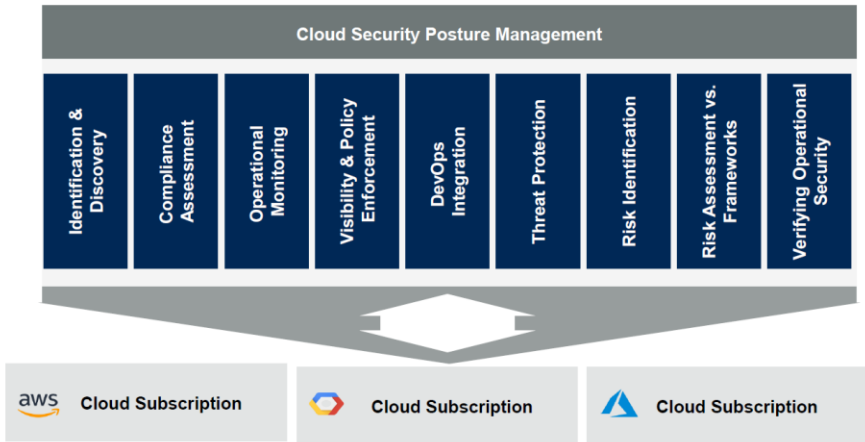
The rise in IaaS usage has created gaps in the security posture that can be cumbersome to manage. In fact, according to Gartner, 95% of cloud security issues result from misconfigurations. Consequently, several CWPP vendors have expanded their offerings to include CSPM and KSPM solutions, focusing on the control plane within a multi-cloud environment and providing configuration management for IaaS and PaaS environments. Examples of this evolution include Aqua Security’s acquisition of CloudSploit, Palo Alto’s acquisition of RedLock, and CrowdStrike’s release of its CSPM solution, Horizon.

Cloud Security Posture Management (CSPM)

Security is ultimately a shared responsibility between the enterprise and the cloud service provider in cloud environments. The cloud service provider is responsible for the “security of the cloud” (physical and external facing), whereas enterprises are responsible for “security in the cloud” (applications level, internal-facing). For enterprises, this means proper configuration and continuous monitoring of all cloud IaaS, PaaS, IAM, and firewall assets. CSPM tools are designed to identify misconfiguration issues, gaps in security policy enforcement, and compliance risks in the cloud by comparing cloud environments against a predefined set of best practices, stated policies, and known security risks.

The key features of CSPM tools include the ability to detect and auto-remediate cloud misconfigurations, maintain an inventory of best practices for cloud configurations and services, map existing configurations to compliance and regulatory frameworks and standards, and monitor storage buckets and encryption and account permissions for misconfigurations and compliance risks. More sophisticated CSPM tools have evolved from control plane monitoring to scalable platforms that can contextualize alerts, prioritize risks, and even initiate workflows by automatically assigning alerts to the right security team for remediation.

Exhibit 49: CSPM Capabilities

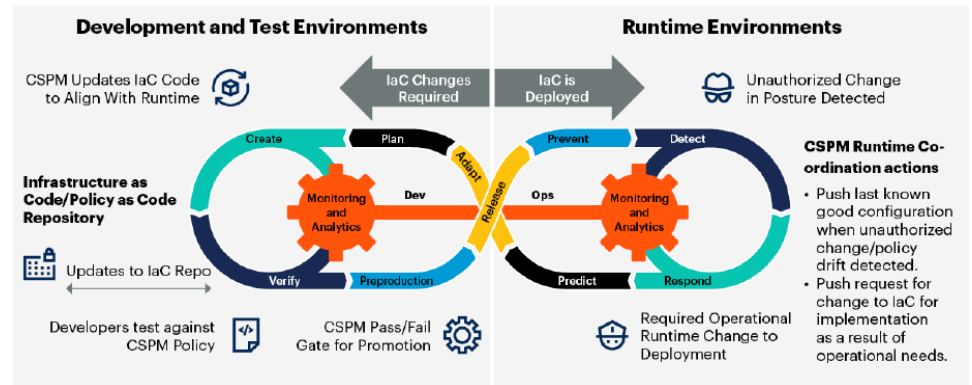


Source: Gartner

With the shift toward auto-remediation, CSPM vendors have integrated with application development cycle features such as infrastructure-as-code (IaC) and policy-as-code (PaC). Operational misconfigurations discovered at runtime can then be pushed back to the application code, removing potential vulnerabilities and attack paths in the IaC or PaC.

Exhibit 50: CSPM Integration with DevSecOps

CSPM Integration With DevSecOps



Source: Gartner

While CSPM solutions can be purchased stand-alone, their capabilities are gradually becoming part of a broader CNAPP solution. In fact, several CWPP vendors, such as CrowdStrike and Palo Alto Networks, have expanded into CSPM through acquisitions and technology evolution. At the same time, CSPM vendors such as Orca Security, Lacework, and Wiz have worked to round out their capabilities and have added CWPP capabilities.

We believe CASB vendors could also add CSPM functionality to address SaaS services such as OneDrive and DropBox and provide SaaS Security Posture Management (SSPM) capabilities such as managing and reporting the configuration of SaaS security settings, integrating with identity permission security vendors, and offering remediation for SaaS misconfigurations or risky postures based on standard industry frameworks.

In the long term, we expect the CSPM and CWPP markets to become essential components in converging into a new Cloud-Native Application Protection Platform (CNAPP) market focused on securing the entire cloud-native application development and deployment lifecycle. In fact, Gartner estimates that by 2025, 60% of vendors will have a consolidated CSPM and CWPP platform, up from 25% in 2022. We discuss this shift in more detail in the Application Security market overview.

Cloud Workload Security Market Vendor Overview

Exhibit 51: Forrester Wave Cloud Workload Security



Source: Forrester (1Q24)

Below, we describe several broader Cloud Workload Security market vendors not reviewed in detail in the note.

- Aqua Security** offers a CNAPP platform to secure applications in development and runtime. The platform provides developers with vulnerability scanning and dynamic threat analysis to scan artifacts for various risks (vulnerabilities, malware, secrets, etc.) during the build phase for comprehensive software supply chain security (SSCS). The platform also offers security teams VM, container, and serverless security for workloads with granular controls and real-time detection and response (CWPP) and comprehensive CSPM and KSPM capabilities to monitor cloud and Kubernetes configurations against best practices and for IaC scanning to eliminate risks during deployment. Integrations address the cloud-native application lifecycle, including standard CI/CD (Gitlab and Jenkins) and SIEM (Splunk and Datadog) tools.
- CrowdStrike** commonly leverages its EDR modules to secure cloud servers. This has led the company to develop purpose-built CWPP, CSPM, and CIEM modules as part of its Falcon platform, which includes (1) Falcon Horizon, which provides posture management coverage for public cloud, Kubernetes, and serverless environments, and where CrowdStrike has added CIEM functionality; and (2) Falcon CWP, which applies CrowdStrike's EDR agent technology to secure cloud servers and containers at runtime. Falcon CWP can be deployed in several Kubernetes environments,

including EKS, AKS, and GKE. Most recently, CrowdStrike acquired ASPM vendor Bionic, expanding its security capabilities into the application code.

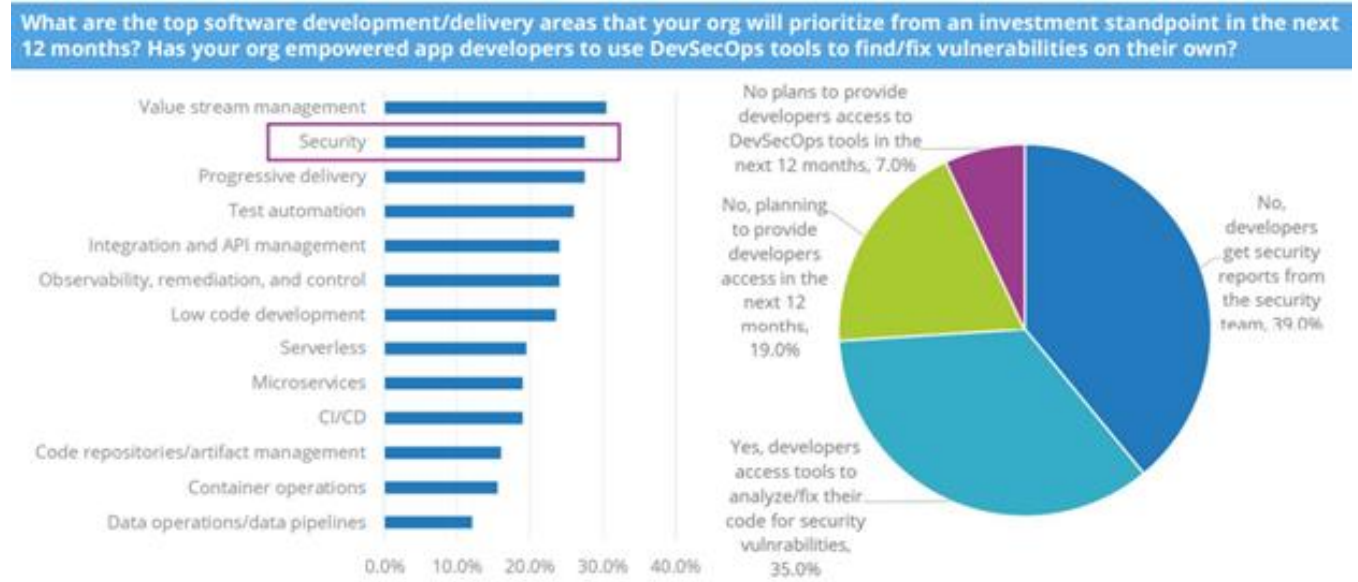
- **Lacework** is a cloud security vendor addressing application development and runtime. The company utilizes ML-based models to identify application behaviors and groups them across containers or VMs based on common behaviors. Its architecture protects dynamic cloud workloads without manually defining policies, rules, or tags, allowing full automation, a critical requirement for securing scalable cloud-native applications. Lacework's solutions can be integrated with public (AWS, Azure, GCP, etc.), private cloud, Kubernetes, and Docker container environments. While Lacework's platform initially addressed CSPM use cases, it now addresses CWPP, IaC security, KSPM, CIEM, container security, cloud-based vulnerability management, and code-level security with SCA and SAST. It also has a CNAPP offering for customers, combining all the technologies mentioned above.
- **Orca** offers an agentless first cloud security platform. The platform's agentless approach, known as SideScanning, reconstructs workloads from static VM images and uses out-of-band image analysis to provide visibility into IaaS and PaaS environments. This allows Orca to reduce dependency on DevOps collaboration and provide malware detection, sensitive data discovery, and vulnerability analysis without performance degradation. The platform reduces alert fatigue by mapping cloud assets and analyzing their contextual behavior to prioritize alerts. Orca has extended its CSPM core, adding CWPP capabilities such as runtime container image scanning and serverless protection while also addressing KSPM use cases and functionality around CIEM, API security, application development security (container image directory and IaC scanning), DSPM and CDR (with attack path analysis). According to the company, it is on track to launch an agent-based cloud security offering in C1Q 2024.
- **Palo Alto Networks** offers broad capabilities through its Prisma Cloud CNAPP platform. The platform was put together through a string of acquisitions. It acquired CSPM technology in 2018 (RedLock); container security and serverless application security in 2019 (Twistlock and PureSec, respectively); IaC scanning in 2021 (Bridgecrew); and ASPM and DSPM in 2023 (Cider Security and Dig Security). Palo Alto now offers full CSPM and CWPP functionality, "shift-left" container and IaC code scanning, KSPM, web application and API security (using its web application firewalls), basic CIEM, and ASPM.
- **Wiz** offers a comprehensive CNAPP security platform to identify and remove risks within cloud environments. Its solution uses an agentless, graph-based architecture, leveraging APIs and log data, to contextualize relationships within cloud workloads (network exposure, VM/container images, vulnerabilities, secrets, user identities, etc.) and track multi-cloud assets. The solution shortens the time to investigate and remediate incidents and enables predictive security assessments of proposed changes to cloud deployments. Wiz's workload scanning capabilities can run in development and runtime environments, an essential prerequisite for a capable CNAPP solution. The platform leverages integrations across cloud, CI/CD, ITSM, and other cyber security vendors to unlock its full value. Product offerings include CSPM, full-lifecycle container security, IaC scanning, KSPM, cloud vulnerability management, cloud detection and response (CDR), CIEM, DSPM, software supply chain security (SSCS), artificial intelligence security posture management (AI-SPM), and a comprehensive CNAPP solution. The company recently added a runtime sensor for KSPM and CDR for continuous monitoring, adding to its agentless function for those capabilities.

Application Security

Software is crucial to almost everything we do. Moreover, it has become central to enterprise digitization activities, aiming to accelerate and improve business decision processes, customer service experiences, and market competitiveness. As software has risen to mission-critical status, shifted to cloud-native micro-services architectures, containers, and functions, and incorporated more APIs, so have the challenges of making software work, secured, continuously and smoothly updated, and delivering a compelling

experience. This rising complexity has expanded the attack surface and raised the importance of application security tools and practices ensuring that data and operations are secure from attacks and compliant with regulatory and corporate governance requirements. An IDC survey listed security as the No. 2 most important area of focus for software development and delivery.

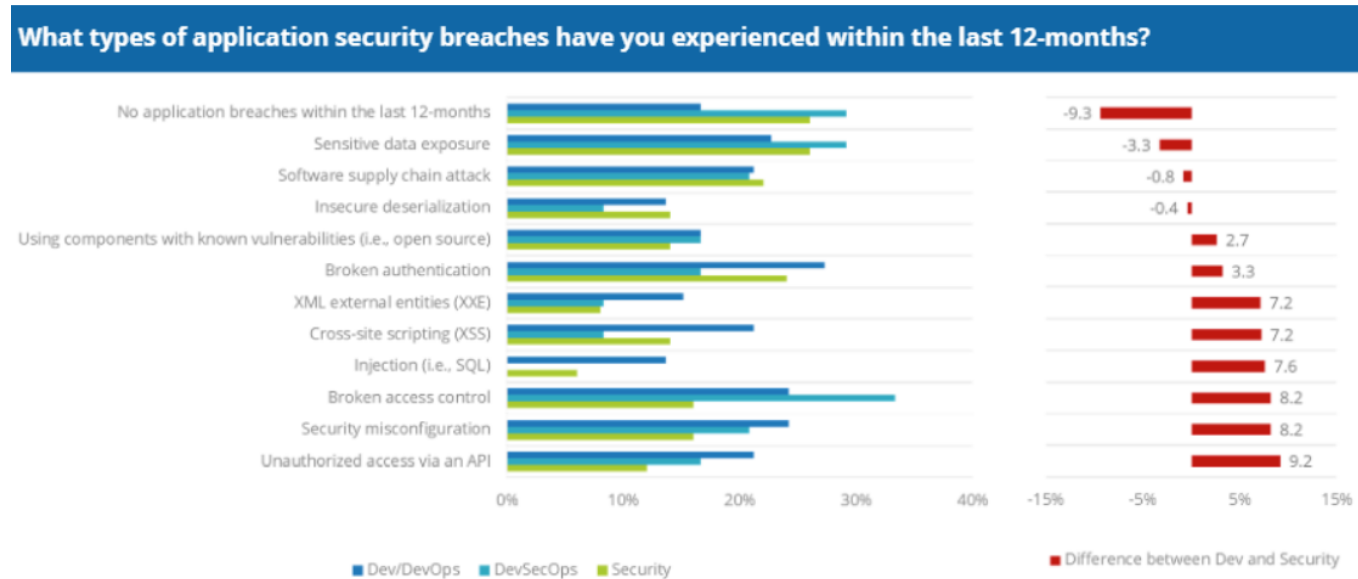
Exhibit 52: Software Development and Delivery, 2022 Survey Results



Source: IDC

Another survey by IDC from January 2023 noted that ~70% of organizations had experienced an application security-related breach in the last 12 months. In terms of the type of security breaches, according to DevSecOps, broken access control was the most prevalent, followed by sensitive data exposure, software supply chain attacks, and security misconfigurations.

Exhibit 53: Application Security Breaches, 2023 Survey Results

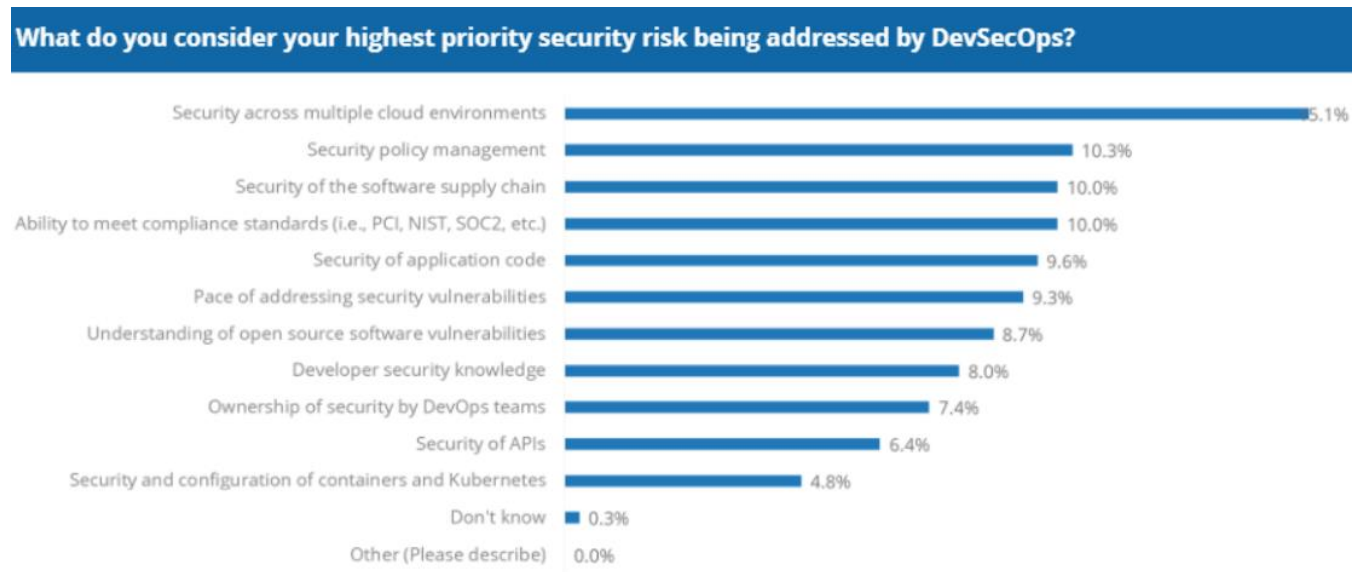


Source: IDC

Respondents to the IDC survey also highlighted propagating security challenges with rising infrastructure and architecture complexity that are now addressed by DevSecOps. The most common challenges noted were security across multiple clouds (15.1%),

security policy management (10.3%), software supply chain security (10.0%), and the ability to meet compliance standards (10.0%). As a comparison, respondents to a Gartner survey noted a need for more security knowledge in cloud-native DevSecOps as their No. 1 challenge.

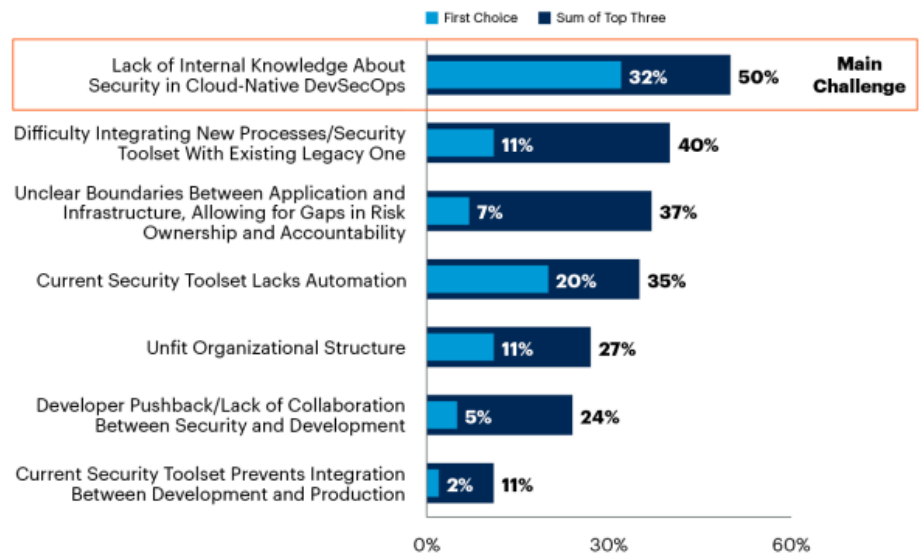
Exhibit 54: Largest Application Security Risks Addressed by DevSecOps, 2023 Survey Results



Source: IDC

Exhibit 55: Top Security Challenges in the DevSecOps Pipeline

Top 7 Security Challenges in DevSecOps Pipeline
Percentage of Respondents



Source: Gartner

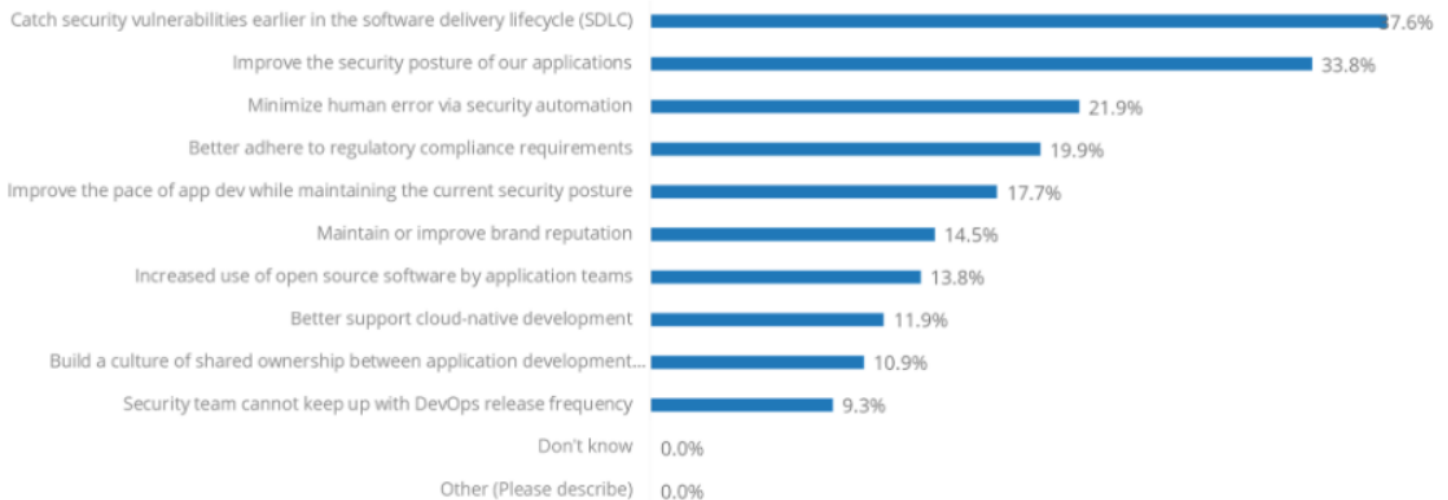
The complexity of providing a comprehensive and efficient application security framework has been compounded as application development evolved from a waterfall development model to agile, CI/CD (continuous integration/continuous delivery), and DevOps frameworks that cut application development time and improve software quality. The traditional implementation of security in development is often a bottleneck to rapid software delivery as it takes a “look back approach,” which results in extensive code rewrites. In recent years, there’s been a concerted effort to incorporate continuous security testing earlier in the development and design cycle (“shift left” or “DevSecOps”) to prevent security bottlenecks from arising before applications are released. In addition,

organizations are pushing developer teams to train on secure coding and assigning security champions to work with dedicated security teams continuously. The goal is to address security issues as early as possible in the application build process, ahead of application release, when addressing security issues is costly in terms of time, user experience, reputation, and cost.

As we look to future drivers of DevSecOps adoption, respondents to an IDC survey noted several factors influencing their decision. Namely, the ability to catch security vulnerabilities earlier in the SDLC (37.6%), improvement in application security posture (33.8%), minimization of human error via security automation (21.9%), better adherence to regulatory compliance requirements (19.9%), and improvement in the pace of application development while maintaining security (17.7%).

Exhibit 56: Drivers for Adopting DevSecOps, 2023 Survey Results

What are the top two drivers for adopting DevSecOps at your organization?

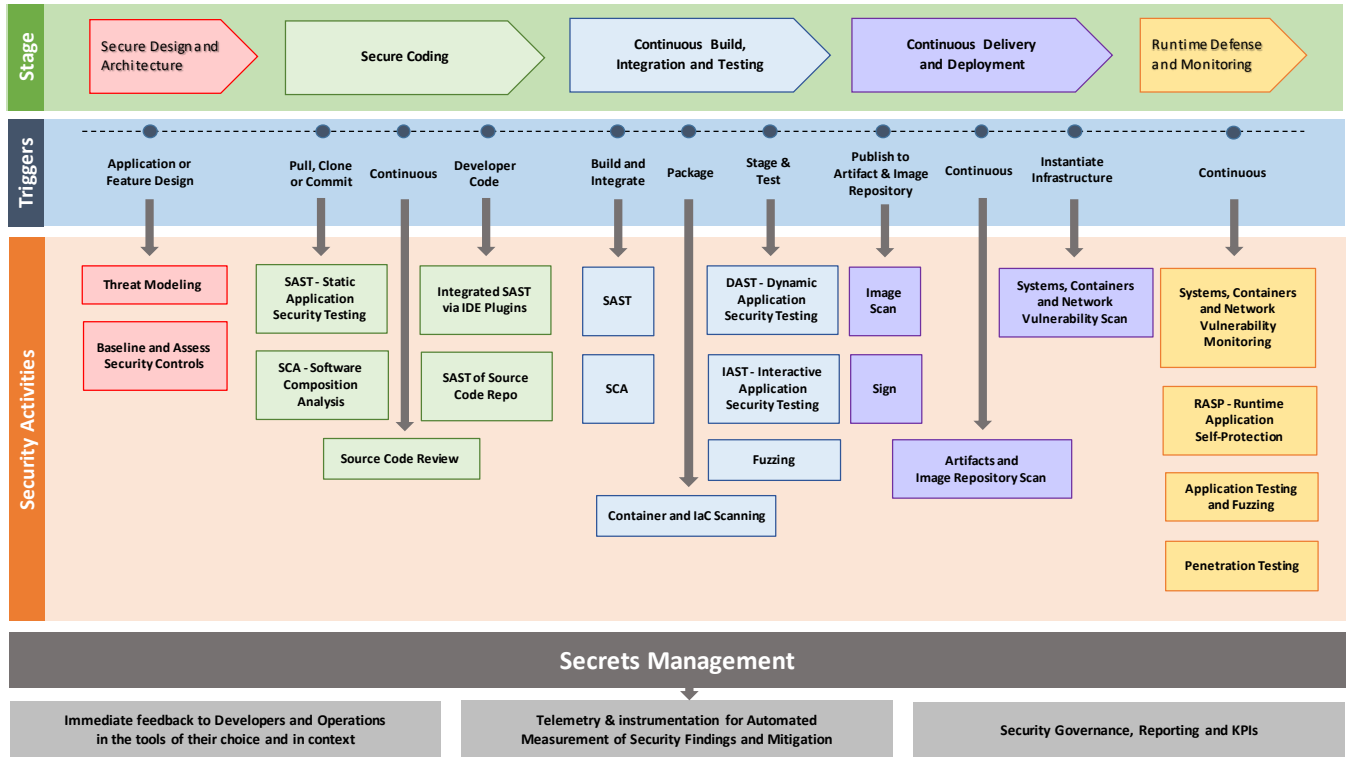


Source: IDC

The market for application security refers explicitly to tools, capabilities, disciplines, and processes used to prevent, detect, and respond to security vulnerabilities and breaches at the application layer. Various scanning and testing tools and software agents are commonly used in the application development and design life cycle. However, they can also address security vulnerabilities in deployed applications (runtime) and the underlying supporting infrastructure. Hence, the market is split into two distinct segments:

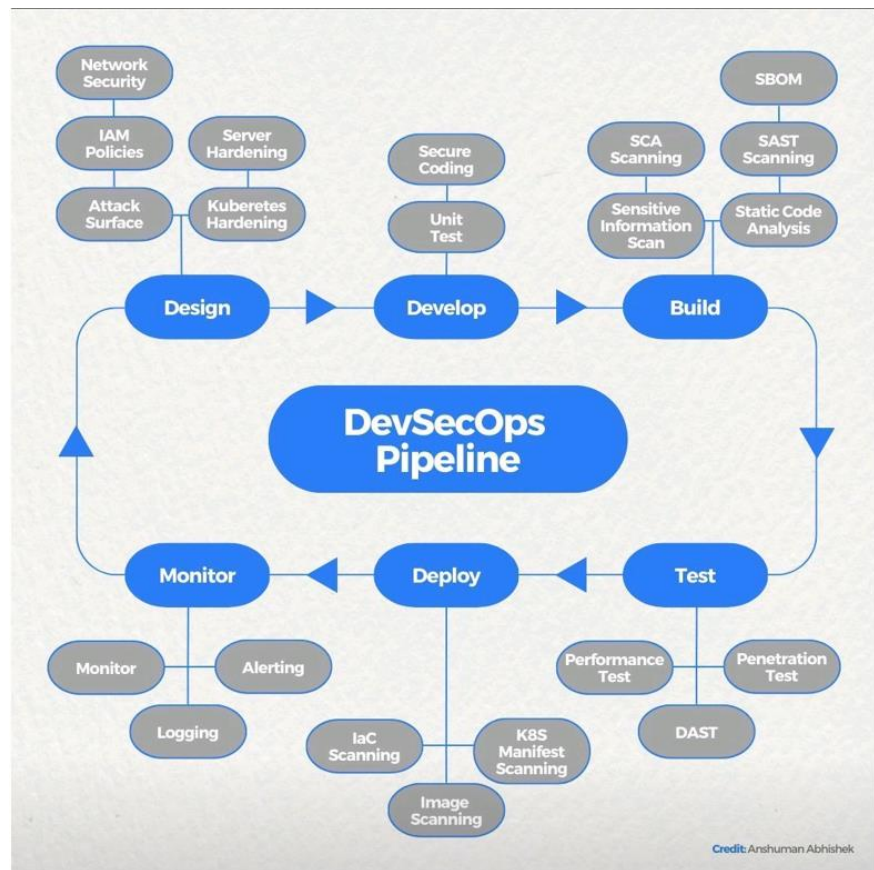
1. **Application Security Testing (AST)**—Security tools used in the software development lifecycle (SDLC) to discover and remediate vulnerabilities before deployment.
2. **Application Runtime Security (ARS)**—Security tools used to detect and respond to threats and breaches within the application and supporting infrastructure post-deployment at runtime.

Exhibit 57: Application Security Tools During Software Development Lifecycle



Source: Cloud Security Alliance, Oppenheimer & Co.

Exhibit 58: DevSecOps Pipeline



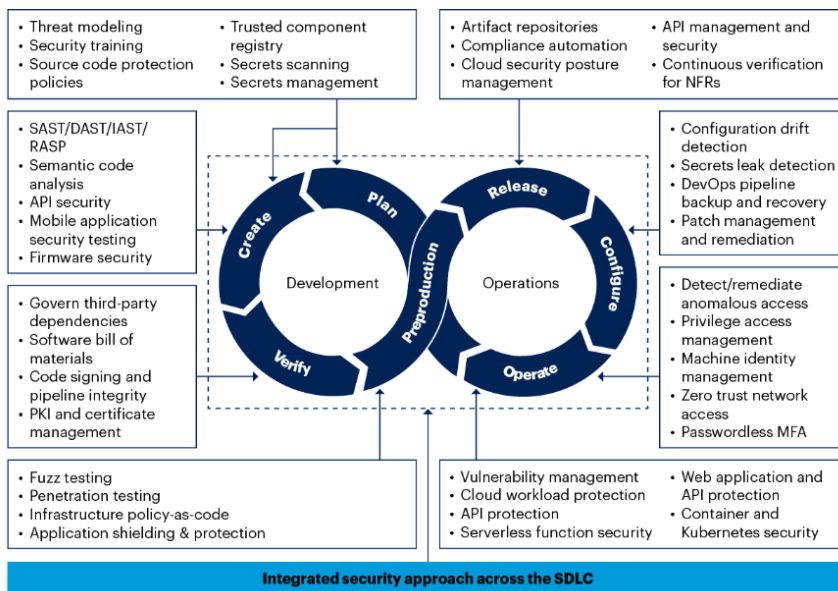
Source: Anshuman Abhishek

Application Security Testing (AST)

AST is a crucial component of secure application development. It incorporates various tools and processes to detect and remediate known and unknown weaknesses and vulnerabilities in the source code during the software development lifecycle (SDLC). The use of AST tools can minimize potential security threats and significantly reduce the remediation cost of applications in deployment.

Exhibit 59: Application Security in DevOps Environment

Map Security Needs to DevSecOps Tools in the SDLC



Source: Gartner

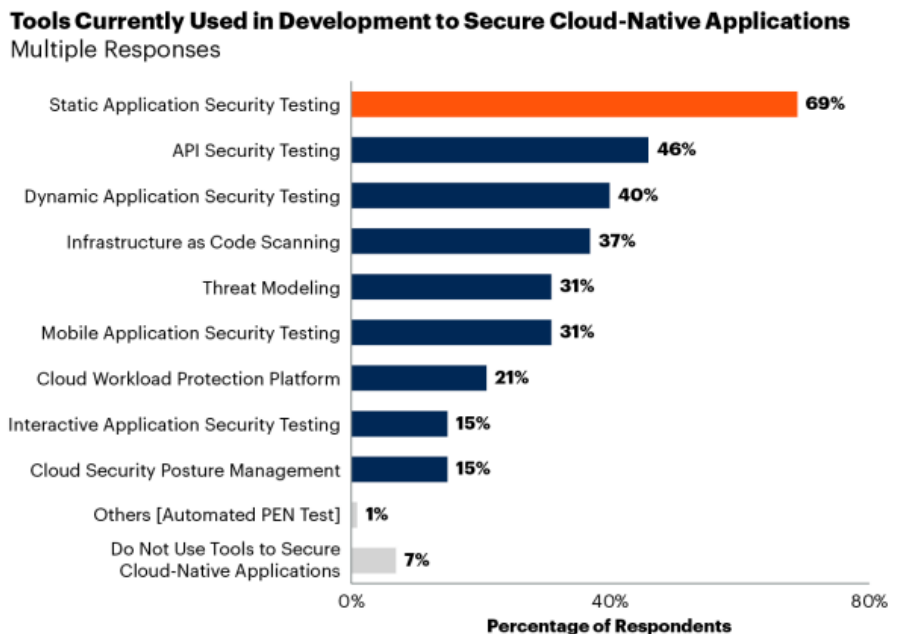
Several types of AST tools are commonly used during the software development lifecycle, including (1) Static Application Security Testing (SAST), (2) Dynamic Application Security Testing (DAST), (3) Interactive Application Security Testing (IAST), and (4) Software Composition Analysis (SCA). We also highlight Software Supply Chain Security (SSCS), a framework that utilizes a combination of tools to ensure application development hygiene, and Application Security Posture Management (ASPM), a relatively new tool that has quickly gained prominence among the cloud-focused application security vendors. Other AST tools and capabilities include threat modeling, fuzz testing, penetration testing, API scanning/vulnerability assessment (API monitoring is a part of runtime security), Chaos Monkey, Mobile Application Security Testing (MAST), etc.

- **SAST** – Inspects the source code to find errors and validation issues and reports on security weaknesses to the development team. It is known as a “white box” testing approach, as it has access to the source code.
- **DAST** – Runs many test cases against the application code, impersonating a hacker to detect security vulnerabilities. It can identify how the software will respond to expected/unexpected user actions and its response time, usability, and reliability. It doesn’t access the underlying source code, making it a “black box” testing approach.
- **IAST** – Takes an inside (code-level) and outside (runtime) view of application security. It uses an agent to run dynamically and analyzes code for security vulnerabilities while an automated test runs the application. It reports valuable root cause vulnerability information in real time and the affected lines of code. It can broadly analyze source code, configurations, third-party code, and APIs.
- **SCA** – Identifies all third-party libraries and open-source software components used in the code and benchmarks them against known and unknown vulnerabilities. SCA tools can identify licensing issues and security vulnerabilities affecting the code components and highlight how to remediate them.

- **SSCS** – Is a set of processes and tools to mitigate security vulnerabilities during the application development phase. These include security concepts, development frameworks, a detailed SBOM, and SCA.
- **ASPM** – Ingests, correlates, and assesses security vulnerability data across many application security tools during the testing and runtime phase. It also orchestrates various security tools, sets security policy, provides a comprehensive risk assessment and prioritization, conducts root cause analysis, and offers remediation suggestions.
- **MAST** – Specifically analyzes and identifies vulnerabilities in applications used with mobile platforms (iOS, Android, etc.). It may include mobile-focused security checks using SAST, DAST, IAST, and API testing.
- **Fuzz testing** – Automated software testing performed by randomly feeding the application with invalid and uncommon inputs and data to uncover coding errors or security vulnerabilities.
- **Penetration testing** – Simulates attacks to find and exploit vulnerabilities in the application software.
- **Infrastructure as Code (IaC) security** – IaC is code embedded in applications to provision and configure infrastructure resources (compute, storage, and networking). Security tools for IaC scan it for discrepancies from set policies and configuration standards. They also evaluate IaC code for embedded secrets and security issues related to company-specific environments and compliance requirements.
- **Container Security Scanning** – Scan container images for vulnerabilities such as secrets, hardcoded credentials, and authentication keys, among others. They also look for misconfigurations and may offer hardening for remediation. These tools can be part of the application deployment process or integrated within a container repository.

Gartner identifies SAST (69% of survey respondents) as the most commonly used application security tool during the development phase of a cloud-native application, followed by API security testing (46% of respondents), DAST (40% of respondents), and IaC scanning (37% of respondents). We note that API security, container scanning, and IaC scanning are performed during the application development and runtime lifecycle.

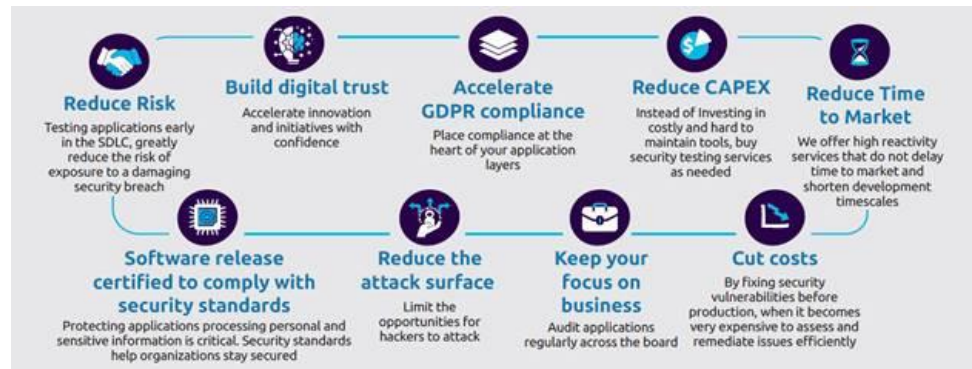
Exhibit 60: Tools Used in Development Phase of Cloud-Native Application Security



Source: Gartner

AST platforms offer many benefits, including: (1) reduced security risk—by incorporating AST tools earlier in the SDLC, organizations can significantly limit potential known and unknown vulnerabilities in the application code and reduce the “attack surface”; (2) reduced cost—earlier identification and remediation of vulnerabilities can eliminate software deployment bottlenecks at security teams, limit expensive and lengthy remediation, and improve time to market; (3) enhanced digital trust—AST tools can build customer confidence around application usage and brand image by reducing data leaks; and (4) ensured compliance—AST tools can maintain security standards and compliance with regulations such as GDPR, HIPAA, etc. by addressing security vulnerabilities at the application layer.

Exhibit 61: Benefits of AST



Source: Capgemini

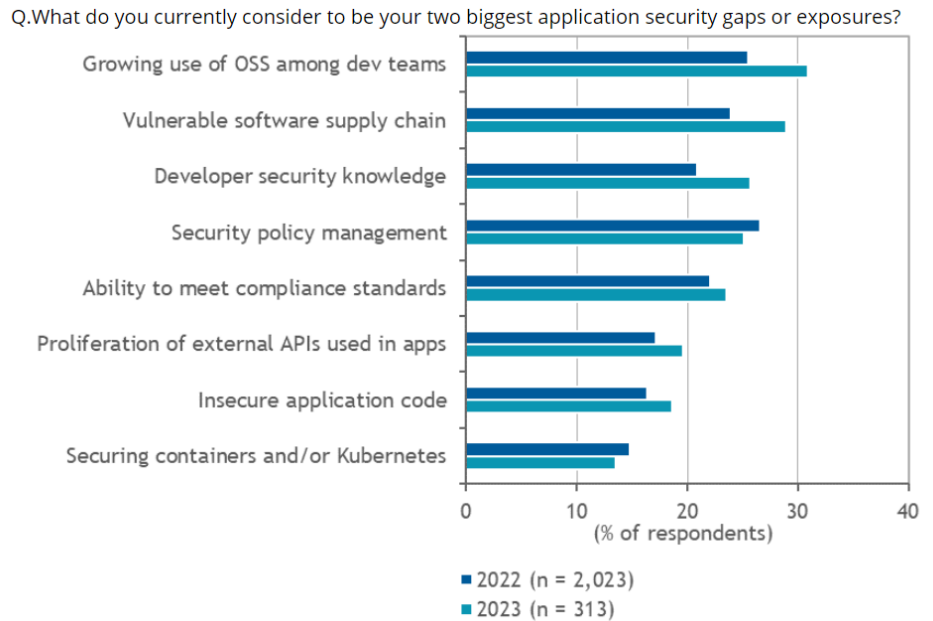
Software Composition Analysis (SCA)

SCA is an automated process for auditing software. SCA tools identify and scan all underlying open-source software and third-party components in the codebase to find security vulnerabilities and ensure compliance with licensing requirements. SCA tools inspect various elements, including package managers, manifest files, source code, binary files, container images, and other code components. They inventory all open-source code components used in the code build and evaluate them against vulnerability databases such as the National Vulnerability Database (NVD) and Open Source Vulnerability Database (OSVDB) to identify security gaps.

Developers have substantially increased their reliance on open-source software (OSS) to help cut development time and costs. In fact, according to research from Mend.io, 60-80% of the proprietary code today comes from open-source software. While there are advantages to leveraging OSS, there are also risks and challenges: (1) OSS is commonly maintained by volunteering contributors who are not always well-governed or proficient in secure coding; (2) discovered vulnerabilities in OSS are posted on community boards, visible to all participants, and thus can be quickly exploited by malicious actors before the code is edited with security patches; (3) manually monitoring and tracking OSS is complicated given the volume and frequency of updates; (4) the shift to cloud-native applications has opened new vulnerabilities in OSS; and (5) each OSS project has its licensing model, making it difficult for enterprises to track and ensure compliance with license requirements. Threat actors have taken note of the rising use of OSS and increasingly target OSS repositories to penetrate the software supply chain and introduce backdoors that can be later exploited.

Even though SCA tools evaluate the entire code base, they have gained popularity because of their ability to parse through OSS, which is frequently used and has been identified as essential by DevOps managers. The effectiveness of SCA tools is generally tied to the vulnerability databases used to analyze the codebase and the number of programming languages they support. Therefore, they are best used with SAST tools to ensure a higher level of security.

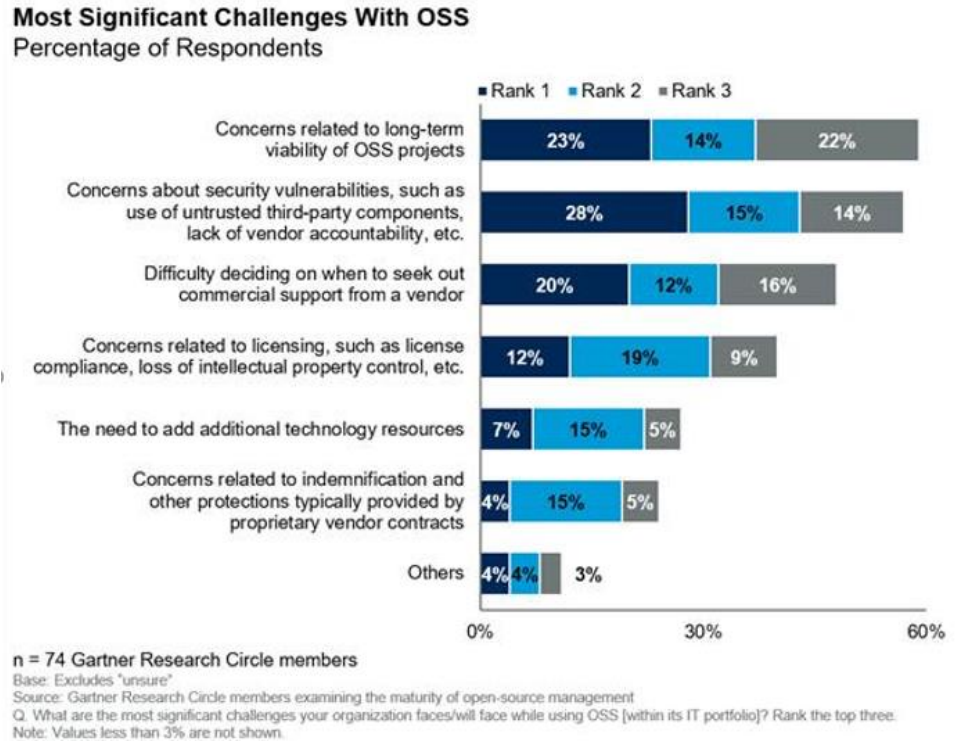
Exhibit 62: Open Source Software & Security Concerns 2022 vs. 2023 Survey Results



Source: IDC

Snyk is one of the primary vendors in the SCA tool market. Its Snyk Open Source leverages a dependency scanner to seamlessly and proactively find, prioritize, and fix vulnerabilities and license violations. Snyk’s paid SCA tool offers: (1) accuracy in dependency detection, including transitive dependency; (2) a high-quality vulnerability database, providing a broader assessment and better information surrounding the vulnerability; and (3) remediation solutions to developers. The company also allows customers to evaluate or export SBOMs (via APIs or CLI) and integrate them with its SCA tool for a comprehensive SSCS offering. Snyk has broadened its reach by adding container/Kubernetes (Snyk Container), IaC configuration scanning (Snyk Infrastructure as Code), SAST (Snyk Code), CSPM (Snyk Cloud), and ASPM (Snyk AppRisk) solutions that integrate with its cloud-native application security platform leveraging semantic analysis (ML technology from DeepCode) to reduce false positives. The ASPM solution was recently added to the product portfolio (December 2023) through the recent acquisition of Enso Security. In January 2024, the company announced the acquisition of Helios, a provider of application runtime insights for security and observability, expanding the AppRisk platform’s functionality and rounding out Snyk’s application security platform from “code to cloud.” It is important to note that Snyk maintains a developer-first approach targeting the build and deployment cycles while partnering with Sysdig to provide runtime threat analysis for containers. We expect the company to continue this approach and add partnerships and integrations with other runtime security vendors.

Exhibit 63: Challenges with Open-Source Software



Source: Gartner Inc.

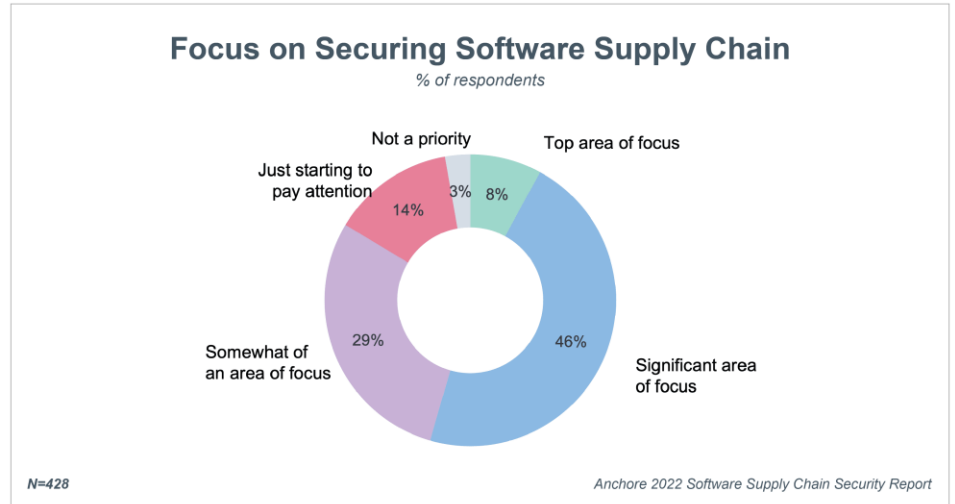
In recent years, SCA tools have evolved from a passive posture, used just for vulnerability scanning and inventory/license record keeping, to a more sophisticated and active stance involving vulnerability prioritization and auto-remediation utilizing various methods. This includes removing vulnerable open-source code, uploading software patches to tackle vulnerabilities, and rolling back code to older, more secure versions of OSS.

From a vendor perspective, there are only a few standalone SCA vendors. Most have broadened their portfolios to include other AST tools (e.g., Snyk) or were acquired (e.g., BlackDuck's acquisition by Synopsys). Other notable vendors include CAST, Checkmarx, Contrast Security, Flexera, Microsoft (GitHub), GitLab, Datadog (Hdiv Security), Ion Channel, JFrog, Mend.io (formerly WhiteSource), NTT Security (WhiteHat Security), Sonatype, Synopsys, and Veracode. We expect the vendors to continue to expand their offering suite into adjacent AST tools and, in some cases, the broader application security market (including runtime).

Software Supply Chain Security (SSCS)

As noted earlier, developers increasingly rely on OSS and third-party code and use a distributed model to write modern-day cloud-native software applications, making them highly susceptible to vulnerabilities that threat actors can exploit. Recently, a novel discipline has emerged, Software Supply Chain Security (SSCS), which looks to combine various security concepts, development frameworks, detailed Software Bill of Materials (SBOM), and tools such as Software Composition Analysis (SCA) to deliver better security measures during the software development phase.

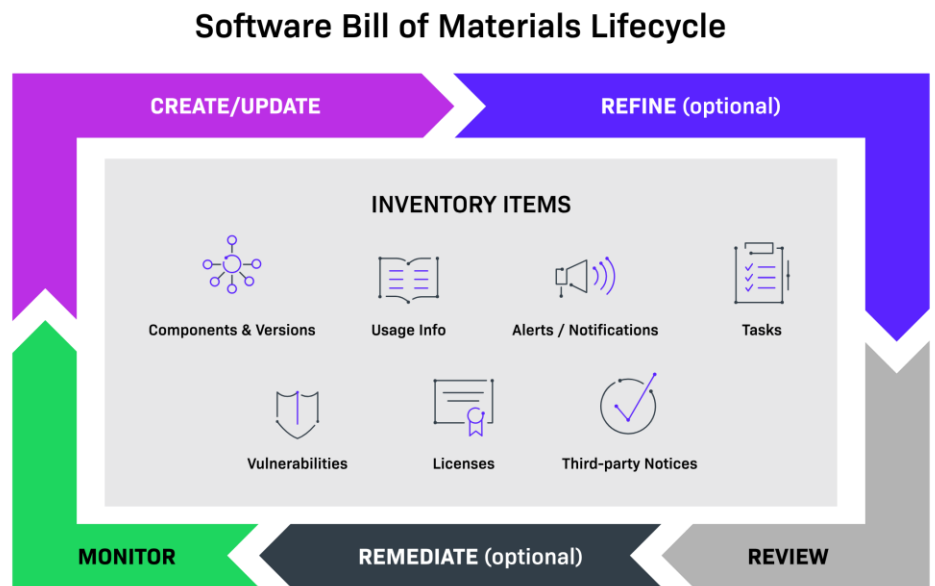
Exhibit 64: Securing the Software Supply Chain a Key Focus



Source: Anchore

Two tools make up the core of SSCS—SCA and SBOM. SBOM is a relatively new tool that provides structured, machine-readable metadata to uniquely identify a software package and its various third-party and open source components. SBOMs track and share auditable and traceable details, providing greater code transparency and compliance for the software application. This is crucial as 40–80% of code in new software applications comes from open source and third-party sources and is often presumed to be secure. We do note that a few challenges remain with managing SBOMs. According to an IDC survey, the top four challenges are keeping SBOM accurate given constant changes (27.9%), consolidating data across silos (27.4%), tracking application SBOM in production (25.5%), and a process of sharing SBOM with users (24.5%).

Exhibit 65: SBOM Lifecycle



Source: Revenera

As noted, SSCS combines the capabilities of SBOM with SCA, which scans the open source code for vulnerabilities, creating a robust solution for securing the software supply chain. Over time, we expect to see a unified SSCS product emerge, which combines the

SCA and SBOM tools into one platform while adding additional security frameworks, creating a comprehensive solution for securing code development.

Notable SBOM vendors include Apiiro, Cybeats, Invicti Security, OX Security, Revenera (Flexera), and Rezilion. Notable SSCS vendors include Arnica, BluBracket (HashiCorp), Chainguard, Cybeats, Cypcode, Flexera, GitGuardian, Legit Security, Mend.io, OX Security, Palo Alto Networks (Cider Security), Snyk, Sonatype, and Synopsys.

Static Application Security Testing (SAST)

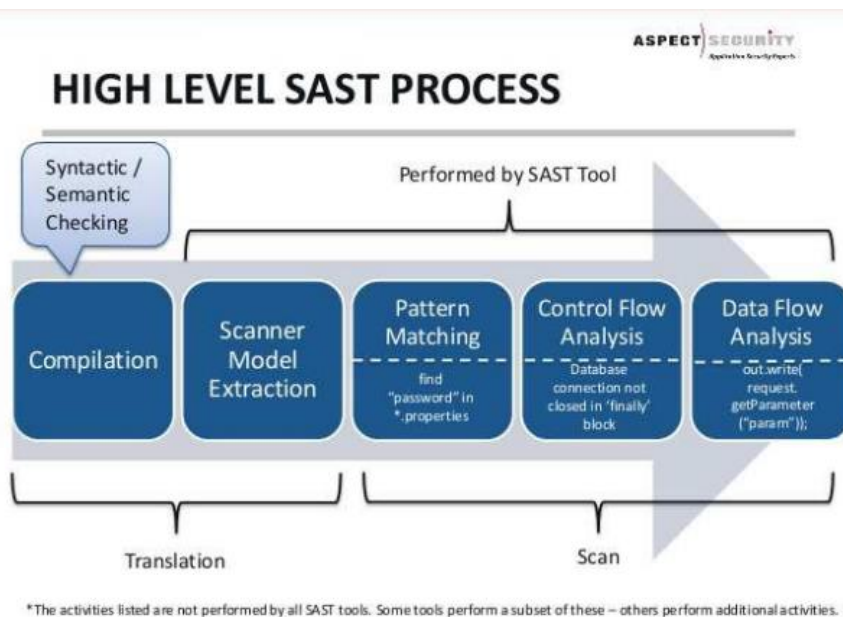
Code reviews and vulnerability analysis are automated and applied early in the software development lifecycle to accelerate application development without compromising security. SAST is one of the most used application security tools early in the software development lifecycle. It scans and analyzes the entire codebase, rapidly evaluates millions of lines of code, and identifies design and coding errors and vulnerabilities that bad actors can exploit. Typical vulnerability assessments include cross-site scripting, denial of service/DOS, buffer overflows, SQL injection, and private data leakage.

By addressing errors and vulnerabilities in the initial stages of the application design cycle and providing developers with real-time feedback, SAST tools closely align with build cycles and eliminate issues/vulnerabilities before the production stage. Developers use SAST to create custom dashboards and reports, which can be shared and used to track and remediate issues. SAST tools support common coding languages like C#, C++, Go, Java, JavaScript, and Python. Given that they have access to the underlying source code and internal structures of an application, they are known as “white box” testing tools.

SAST offers several benefits in its testing approach in that it: (1) does not require functional application code and can scan compiled or un-compiled software; (2) analyzes the source code and has access to the underlying framework and implementation design, making it developer-friendly; (3) is highly automated and scalable, capable of analyzing millions of lines of code within minutes; and (4) addresses code issues early in the SDLC, facilitating faster remediation, often well before reaching quality assurance (QA).

Developers often run SAST on the source code as it's updated with every release. The tools can vary in sophistication, with some highlighting exact vulnerabilities or weaknesses in the code and others offering more in-depth guidance to developers on how and where to fix the code, even if the developers don't have in-depth security knowledge. SAST vendors are increasingly adding remediation features to drive broader developer adoption and accelerate development time, which all Application Security tools are implementing. Last, since SAST tools are used in pre-production, they are often complemented with runtime-focused AST tools such as DAST and IAST.

Notable SAST vendors include Checkmarx, Contrast Security, ShiftLeft, Microsoft (GitHub), GitLab, HCL Technologies, IBM, Mend.io (formerly WhiteSource), Micro Focus, NetSPI, NowSecure, NTT, Perforce, SonarSource, Synopsys, Snyk, and Veracode. All offer other application security tools (i.e., none are a standalone SAST vendor).

Exhibit 66: Static Application Security Testing (SAST)

Source: Aspect Security

Dynamic Application Security Testing (DAST)

Today's applications run in increasingly complex environments (public cloud, hybrid/multi-cloud, containers, etc.) and are more architecturally complex and integrated (APIs, external dependencies, micro-services, etc.). This complexity can introduce unforeseen challenges when applications are deployed and as secure components interact. AST tools such as SCA and SAST evaluate the underlying code pre-production for potential vulnerabilities. Still, they cannot predict or assess vulnerabilities that surface when the various components of the deployment are put together. SAST and SCA tools are also limited by the quality of the vulnerability databases used for baseline comparison.

DAST is a "black box" testing approach executed at runtime, sometimes called a web application vulnerability scanner. It attempts to detect vulnerabilities by simulating automated "real world" external attacks and test cases on compiled code ready for release. Typical tested vulnerabilities include cross-site scripting, SQL injection, and path traversal (evaluated across query strings, headers, fragments, verbs (GET/POST/PUT), and DOM injection). DAST tools also assess vulnerabilities in server or infrastructure configuration and authentication. It is essential to highlight that, unlike SCA and SAST tools, DAST tools don't have access to the underlying source code. Thus, the code needs to be re-evaluated after DAST identifies vulnerabilities.

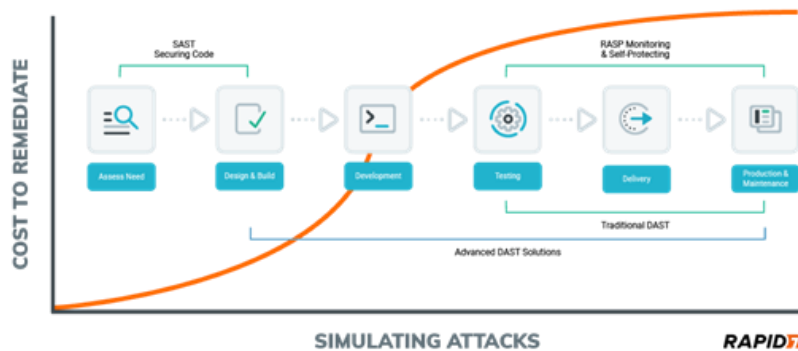
DAST tools offer key advantages in that they: (1) simulate real-world attacks, which can uncover unknown or unrealized vulnerabilities in the code; (2) can be applied at scale and run scans continuously; (3) are not language-dependent (a limitation for SCA and SAST); (4) can be customized for a set of specific or complex tasks; and (5) have a low rate of false positives. Conversely, DAST tools (1) lack access to the source code, limiting their effectiveness in eliminating untested vulnerabilities; (2) are unable to provide developers with an exact location and a remediation path in the source code, making it time-consuming to address discovered issues; (3) are typically applied at the end of the build cycle, slowing the agile CI/CD process; and (4) require upgrades and manual inputs to write and manage test conditions.

Considering the various test approaches (development/runtime, open-source/proprietary code, etc.), DAST tools are generally best combined with SCA and SAST. DAST is also complementary to RASP as a runtime tool, as it is best for evaluating vulnerabilities pre-production, while RASP provides continuous vulnerability monitoring and remediation post-deployment. Vendors offering DAST tools have historically been standalone or offered other non-static tools such as vulnerability assessment (Qualys, Rapid7, or

Tenable). However, multiple SAST vendors have added DAST capabilities in recent years. Over time, we expect the application security vendors to expand their AST offerings further and add RASP for a more comprehensive toolset.

Notable DAST vendors include Checkmarx, Contrast Security, Detectify, GitLab, Microsoft (GitHub), HCL Technologies, IBM, K2 Security, Micro Focus, NowSecure, NTT, Qualys, Rapid7, Synopsys, StackHawk, Tenable, WhiteHat, and Veracode.

Exhibit 67: Dynamic Application Security Testing



Source: Rapid7

Interactive Application Security Testing (IAST)

IAST tools take on the best of SAST and DAST capabilities by identifying and managing security risks associated with discovered vulnerabilities in running web applications using dynamic testing techniques. DAST has shortcomings due to its lack of access to the underlying source code, slowing remediation, and the application development cycle. However, it is valuable in simulating “real world” attacks against applications in runtime and uncovering unknown configuration errors and vulnerabilities in the application code and associated infrastructure. Like DAST, IAST runs sophisticated tests simulating real-world attack scenarios in production and QA, and similar to SAST, it has access to the underlying codebase. Consequently, IAST can test more pointed and directed attacks and identify code vulnerabilities to which DAST may not have visibility.

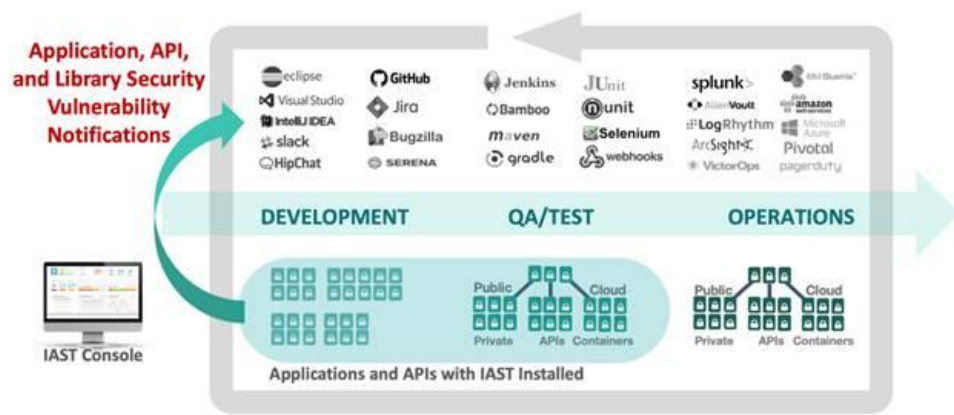
IAST tool design, however, is very different from SAST and DAST, as it works from inside the application. IAST first implements agents and sensors in the application post-build and then maps the external states and application changes to the source code while simulating attacks and test cases. Observing the application’s instrumentation can accurately identify areas of the code affected by vulnerabilities such as hardcoded API keys, unsanitized user inputs, or connections without SSL encryption. It is important to note that, unlike SAST, IAST does not scan the entire code base.

IAST offers several benefits, including: (1) access to the underlying code base, framework, and implementation, making it developer-friendly, facilitating quick remediation; (2) running “real world” attacks and scenarios; (3) applicability in scale, running tests continuously and rapidly; (4) high customizability addressing complex scenarios; and (5) a very low rate of false positives. However, it also inherited some of the limitations of other AST tools in that it: (1) does not scan/test the entire code base, making it much less comprehensive than SAST; (2) is programming language dependent and can only provide functionality for a set number of popular languages, which vary by vendor; (3) requires upgrades and inputs to write and manage complex test conditions; (4) is costly to implement as instrumentation needs to be inserted into the application code; and (5) adds overhead to the code (agent) and can slow down functionality. This is an issue for performance-sensitive applications.

IAST is often deployed as a replacement for DAST. We believe DevOps teams will shift to IAST as it matures, adds additional features, and supports more programming languages. However, we do not expect IAST to replace SAST as an application security tool, as SAST is far more comprehensive in evaluating the entirety of the application codebase. DAST vendors have already been adding IAST tools to their product offerings.

Notable vendors include Checkmarx, Contrast Security, Hdiv Security, HCL Technologies, K2 Security, Micro Focus, NowSecure, Synopsys, and Veracode.

Exhibit 68: Interactive Application Security Testing

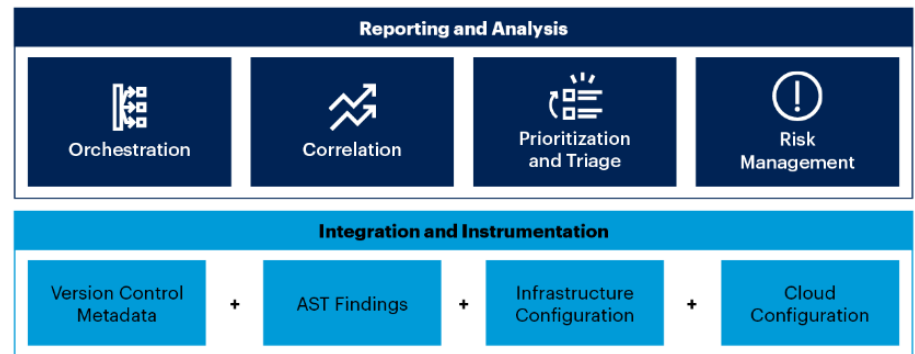


Source: DZone

Application Security Posture Management (ASPM)

Modern software applications, particularly cloud-native applications, are complex, utilize several new technologies or development techniques, and leverage open-source and third-party software, containers, and IaC using a CI/CD framework. Several legacy and new tools are available to address the various security issues during the development cycle. However, these tools rarely communicate and share vulnerability data and instead create silos of security data sources, and visibility and control issues, which can lead to security gaps in the application. Application security orchestration and correlation (ASOC) tools that deliver an orchestration and monitoring layer were developed to address these issues. They integrate data from the various AST tools, automate security tests and release controls, holistically assess critical risks, and prioritize and address subsequent security issues. In recent years ASOC functionality has expanded to include a broader scope and functionality beyond the correlation of test results from various AST tools to include ARS and greater coverage, particularly across cloud-native functionality, root cause analysis, prioritization, and remediation, and has been rebranded as ASPM.

ASPM tools incorporate the following core functionality—(1) expanded coverage from AST tools during the SDLC to data from runtime environments across cloud, containers, and physical infrastructure; (2) ability to orchestrate testing, integrate, and control security tools across the SDLC; (3) integration into workflow tools and ticketing systems, providing a possible set of remediation solutions; (4) correlation of security vulnerabilities presented across the various AST and ARS tools providing a comprehensive view of the security issues within the application; (5) provide risk assessment and prioritization of the various security vulnerabilities; (6) provide root cause analysis of the vulnerability by analyzing and correlating security risk data across various tools; and (7) provide risk assessment and indicators for the various software application components.

Exhibit 69: Application Security Posture Management**Application Security Posture Management**

Source: Gartner

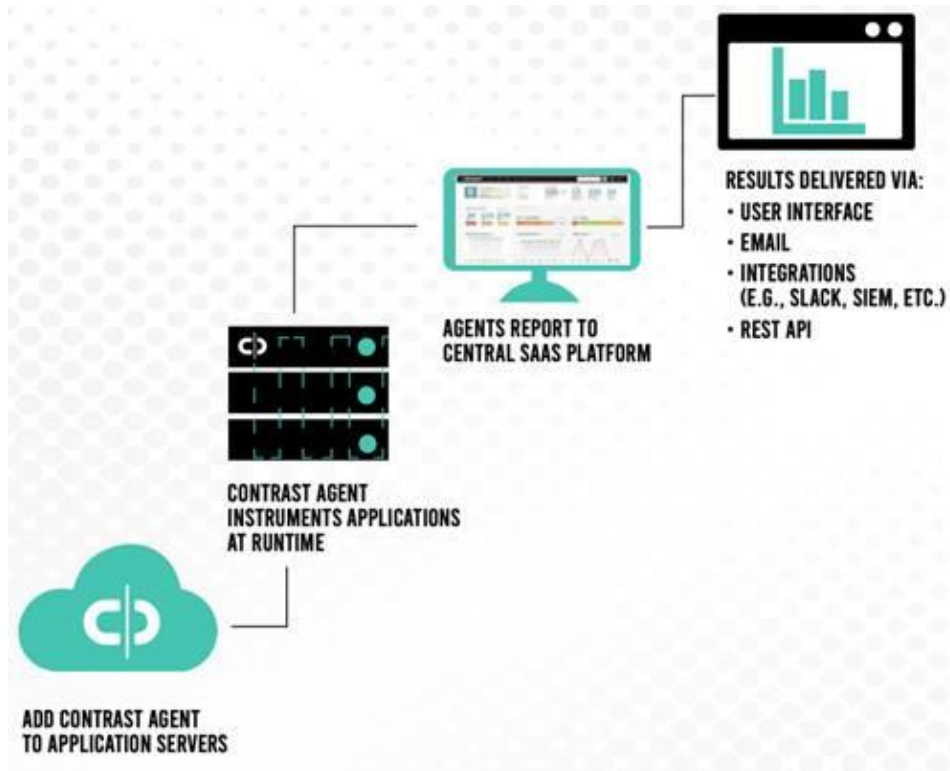
ASPM remains a relatively nascent tool, with only about 5% of organizations currently using it to administer their application security. However, it is expected to become a crucial component of application risk management, with at least 40% of organizations expected to use a third-party or proprietary ASPM tool by 2026, according to Gartner. We believe that, over time, ASPM will become crucial to every SDLC and provide a comprehensive set of coverage, orchestration, and remediation functionality for the application.

That said, a few concerns or drawbacks to ASPM have limited widespread adoption. First, comprehensive ASPM tools need to ingest, process, correlate, and respond to vast amounts of data across the AST/ARS tools, which has yet to be proven in complex environments. Second, most ASPM tools assume organizations are mature enough to understand the potential system risk and their policies, which may not be accurate. Third, broad integration capabilities are required across the entire application security toolset, without which the quality of ASPM assessment can quickly deteriorate. Lastly, incorrectly constructed policies can lead to false positives and de-prioritization of critical vulnerabilities.

Multiple ASPM vendors have been acquired over the past year by vendors such as CrowdStrike (acquired Bionic), Palo Alto (acquired Cider Security), and Snyk (acquired Enso Security and Helios). We expect further M&A as AST providers also look to create a comprehensive application security portfolio. Only a few AST providers have an ASPM offering today (Synopsys is an exception), as historically, they have operated without integrating with ARS vendors, and as integration with runtime security tools and functionality beyond orchestration and monitoring became critical requirements for ASPM. In the long term, we believe standalone ASPM providers will find it difficult to compete with broader platforms and expect ASPM capabilities to be integrated into broader platforms.

Application Runtime Security (ARS)

The other side of delivering application security comes post-deployment and focuses on monitoring the applications' health, emerging vulnerabilities, and the hosting infrastructure. These tools run in real time and provide security teams with alerts and associated threat notifications. The security command center can then address the threats and take the steps necessary to eliminate any security breach. The challenge with real-time alerts is their sheer volume, the prevalence of false positives, and the time and management constraints of the security team managing them. ARS tools are increasingly applying analytics, ML, and automated actions and remediation to address these challenges.

Exhibit 70: Application Runtime Security

Source: Contrast Security

While ARS tools can alleviate some of the noted challenges, they are most effective when complemented with other security tools (outside the application). For example, EDR/MDR and CWPP tools can add end-point security telemetry, IAM tools can address user identification, and infrastructure security threat detection and response tools can offer insight into the underlying infrastructure state. In addition, SIEM/SOAR security solutions can consolidate telemetry and alerts from a broad range of runtime security tools across the application, endpoint, and infrastructure layer and provide an overarching unified view of the security landscape.

We see four major types of ARS tools used in deployment: (1) runtime application self-protection (RASP), (2) Web Application Firewall (WAF), (3) Container security, and (4) application programming interface (API) security. Other runtime tools include infrastructure-as-code (IaC) scanning, bot management, user and entity behavior analysis (UEBA), application performance monitoring (APM), and correlated vulnerability assessment (CVA).

- **RASP** – Enables fully automated monitoring of applications' internal state and change in behavior in runtime. RASP can address threats by observing anomalous activity, including novel or "zero-day" attacks.
- **WAF** – A firewall between an application and its underlying infrastructure and monitors threats from HTTP traffic.
- **API security** – A framework rather than a specific technology. Combines API scanning and vulnerability testing during the DevOps cycle, API threat monitoring and management, WAFs, IAM, and in-app protection during runtime.
- **Container security** – Also a framework rather than a specific technology. Includes container image scanning for vulnerabilities and configuration issues during the DevOps cycle and container and Kubernetes monitoring for threat detection, misconfigurations, policy management, and other vulnerabilities in runtime.

- **laC scanning** – Scans IaC templates such as Terraform, CloudFormation, Azure Resource Manager (ARM), etc., for vulnerabilities and misconfiguration issues.
- **Bot management** – Uses various techniques and technologies to assess and block incoming HTTP traffic from malicious and unwanted bots.

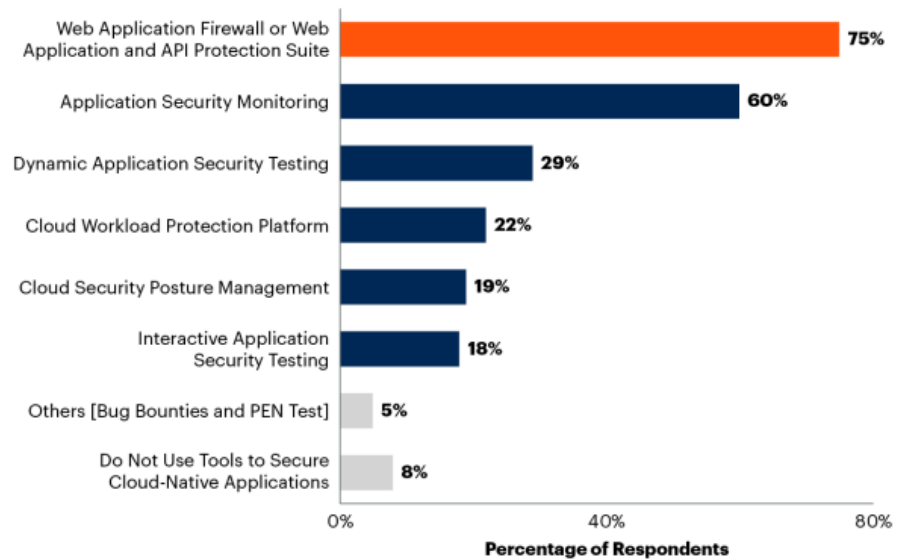
Gartner identifies WAF or Web Application and API Protection Suite (75% of survey respondents) as the most used application security tool in the production phase of a cloud-native application (runtime), followed by application security monitoring (60% of respondents) and DAST (29% of respondents).

Given the sophistication of cyber threat actors and application deployment and the level of management complexity, AST tools can't address all unknown application vulnerabilities or capture every known vulnerability. Therefore, it is imperative to apply several security tools to monitor the applications and associated infrastructure at runtime. While remediation costs at runtime are much higher than at the application development phase and can require security patches or code rewrite/rollback, ARS tools offer another layer of protection to organizations. They can mitigate financial, operational, regulatory, and reputational damage.

Exhibit 71: Tools Used in the Production Phase of Cloud-Native Application Security

Tools Currently Used in Production to Secure Cloud-Native Applications

Multiple Responses



Source: Gartner

Runtime Application Self-Protection (RASP)

Not all known security vulnerabilities can be discovered with SCA or SAST/DAST/IAST tools, and applications can still be exposed to unknown threats and vulnerabilities. Therefore, developing and maintaining a secure application would not be complete with only AST tools. It's also essential to monitor the health of the application and its immediate hosting infrastructure while checking for vulnerabilities in runtime.

RASP tools complement AST tools by controlling application execution, detecting vulnerabilities, and preventing attacks in real-time at runtime. Unlike other runtime application security tools focused on perimeter-based networks, cloud, container, or endpoint protection (such as IPS, WAF, bot management, and UEBA), RASP protects applications from the inside. It deploys an embedded call in the application's source code or a wrapper around an application that can intercept calls from the application to a server. This call/wrapper validates data requests, ensures calls are secure, and analyzes application behavior (internal state) and changes in behavior and context to identify and mitigate threats. When abnormal behavior is determined, RASP checks for malicious

attacks (such as SQL injection and cross-site scripting) and issues alerts or blocks the attack by preventing user access or terminating the session. RASP tools are fully automated and don't require human intervention.

RASP offers several advantages in that it: (1) keeps the underlying application design and features unchanged and operates on the server running the application; (2) runs in real-time and does not require human intervention to prevent and mitigate threats and vulnerabilities; (3) provides feedback to developers, who can add secure coding or implement patches to the application; (4) is not limited by vulnerability databases and can address a wide range of threats including novel or "zero-day" attacks; and (5) has a high degree of accuracy because of its insight into application logic, data flow, and configuration.

The one major drawback of RASP is that it cannot access the application source code, pinpoint the location of the vulnerability in the code, or offer remediation. Another drawback is that RASP consumes application server resources to run and can impact application performance. Hence, RASP complements AST tools such as SCA and SAST/DAST and is often deployed with other network and endpoint-related runtime security tools. We also view RASP as a complementary solution to WAF rather than a replacement technology, given that it is an in-app solution while WAF offers perimeter app defense.

AST vendors have added RASP as one of the few runtime security tools as part of their platform offering, and we expect this trend to continue. We've also seen APM (Application Performance Monitoring) and CDN (Content Delivery Network) vendors acquire RASP vendors. For example, APM provider Datadog gained RASP capabilities through its acquisition of Hdiv Security (2022), while Imperva (a CDN) attained RASP functionality with the acquisition of Prevoty (2018).

Notable vendors include Avocado Systems, Contrast Security, Digital.ai, Datadog (Hdiv Security), Imperva, K2 Security, Micro Focus, Veracode, and Waratek.

Exhibit 72: Runtime Application Self-Protection (RASP)



Source: AppSealing

Web Application Firewall (WAF)

The traditional approach to protecting network traffic involves a physical firewall, which offers a perimeter-based defense. However, a more special-purpose Web Application Firewall (WAF) is commonly used when protecting web-based applications at runtime. WAF protects the application layer (layer 7 of the OSI model), which traditional firewalls are less able to do (more effective in layers 3 and 4 of the OSI model). WAFs entered the market in the late 1990s when web-server attacks became more prevalent, and they can filter, monitor, and block any malicious Hypertext Transfer Protocol (HTTP)

communication between external users and the web application server where web content is hosted.

A WAF is typically programmed to adhere to a range of policies from OWASP (Open Web Application Security Project), an international non-profit organization dedicated to web application security that regularly outlines security concerns and critical risks. WAF policies can be easily modified and implemented to quickly and effectively respond to attacks, and they can address attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, cookie poisoning, SQL injection, and threats that could degrade or compromise traffic, such as DoS/DDoS (denial of service/Distributed-DoS) attacks.

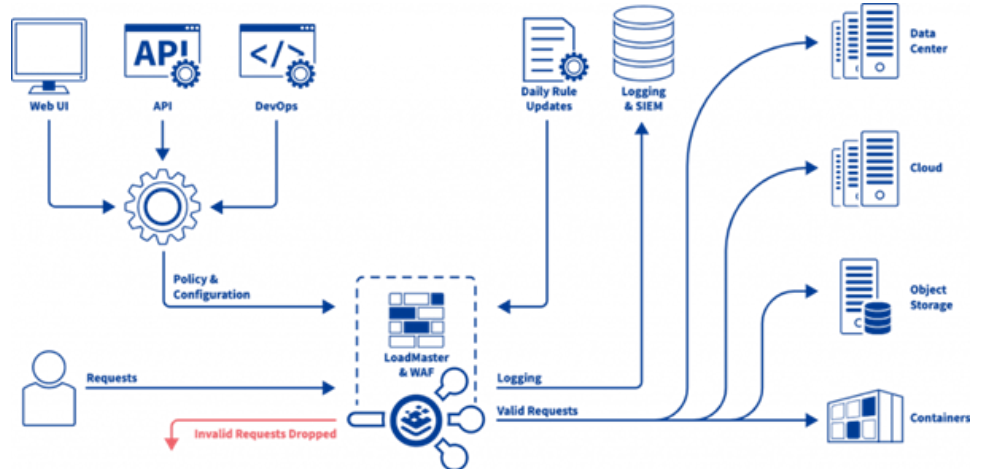
A WAF can be deployed as a hardware appliance or as software (virtual WAF) and set up in one of three ways: (1) Reverse Proxy—WAF acts as a proxy to the application server, and all traffic is directed to the WAF before passing through; (2) Transparent Reverse Proxy—similar to a reverse proxy, but with transparent mode, which allows for IP masking of the application server; and (3) Transparent Bridge—HTTP traffic is directly sent to the application server, making the WAF “transparent.”

WAFs offer several advantages, including: (1) protection from a diverse range of attacks and threats (SQL, injection, XSS, DDoS, etc.); (2) great flexibility in policy implementation; (3) a high degree of customization in layer 7 protection; (4) integration with other network-based security tools, making it an effective in mitigating DDoS attacks; (5) real-time and granular monitoring, reporting, and insights; and (6) data leakage prevention. However, there are also a few drawbacks to WAFs. WAFs sit between users and applications, add latency, and can negatively impact the user experience. Their effectiveness can be tied to the quality of configuration and governing policies, which may need to be updated and fine-tuned. Lastly, they deliver many false positives (blocking legitimate user traffic) and must be implemented with other network-based security features.

The WAF landscape is broad and includes traditional networking, firewall, and load balancing vendors (Cisco, Palo Alto Networks, Fortinet, Imperva, F5, etc.), CDN vendors (Akamai, Fastly, Cloudflare, etc.), and CSPs (AWS, Azure, GCP, etc.). Security has been top of mind with the proliferation of applications and the shift to cloud-native architectures. Thus, adding a mature perimeter technology, such as WAF, was an easy add-on for cloud and CDN vendors. Nonetheless, traditional networking vendors remain the providers of choice for on-premise data center WAF deployments.

We expect WAF to overlap with RASP solutions for runtime application security. In fact, networking/firewall vendors have already expanded their portfolio to include RASP. For example, Imperva acquired Prevoty (2018), Palo Alto acquired Twistlock (2019; has RASP in addition to container security), and Cisco has leveraged AppDynamics (2017) to add a RASP solution to its portfolio. Nonetheless, we believe the WAF market will remain robust for two reasons. First, WAF solutions differ from RASP solutions and approach runtime application security from a networking perspective, offering a perimeter defense. In contrast, RASP solutions offer real-time in-app protection from attacks and vulnerabilities, making the two technologies complementary rather than overlapping. Second, WAF policies are highly customizable and far easier to modify and implement, whereas changing a RASP agent is more complicated and may require agent redesign.

Notable vendors include Amazon AWS, Akamai, Barracuda, Check Point, Cisco, Cloudflare, F5, Fastly, Fortinet, Google, Imperva, Microsoft Azure, Palo Alto, Radware, and VMware.

Exhibit 73: Web Application Firewall (WAF)

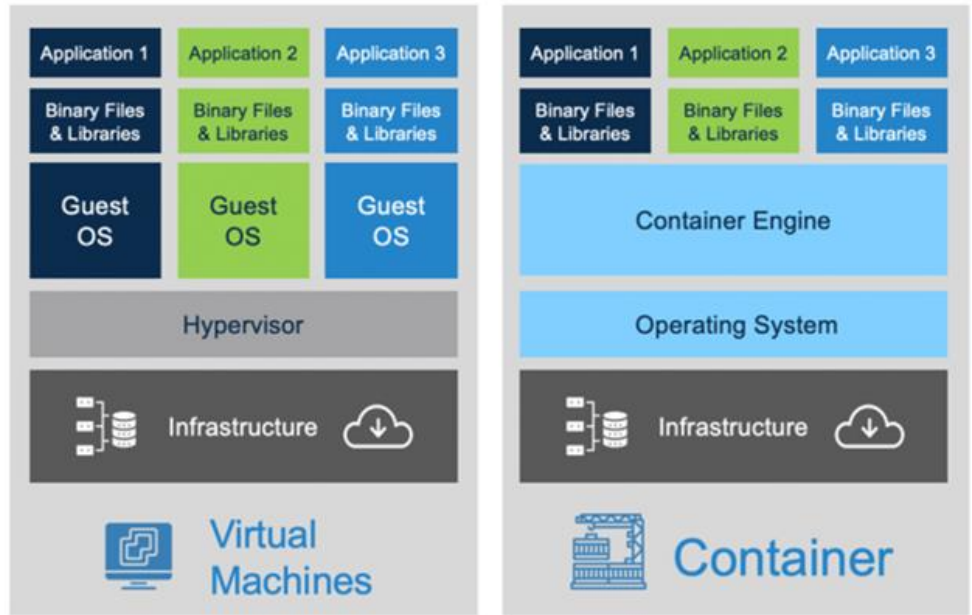
Source: Kemp Technologies

Container Security

A container is a software package containing all the necessary elements and dependencies to run an application or micro-service independently. A container includes all the executables, binary codes, libraries, and configuration files, making it completely portable, without errors or issues, between different deployment environments (a public cloud, private cloud, or an individual computer). Although containers are similar to virtual machines (VMs), they do not run a separate operating system on the physical hardware like VMs. Instead, multiple containers can run on the same operating system kernel, whereas VMs run a complete virtual operating system. As a result, containers are more lightweight than VMs, require fewer physical resources, and are faster to spin up/down. Today, containers are crucial in running modern applications built on micro-service architectures, enabling developers to accelerate application development and deployment cycles.

A container image is an immutable (i.e., cannot be changed) static file with executable code that can create a container consistently in any deployment environment. These images include the container engine (such as Docker or CoreOS), system libraries, and configuration settings. They also specify the type of workload to be deployed. And to deploy containers rapidly, the container images are maintained and stored in repositories. Owing to their complexity, containerized applications, and related micro-services are typically managed through their lifecycle and across a distributed cluster of compute nodes with orchestration tools such as the open-source container orchestration Kubernetes (K8s created by Google) and other platforms, such as Docker Swarm.

Exhibit 74: Containers vs. Virtual Machines



Source: AKF Partners

In terms of container and Kubernetes adoption, a 2022 survey by IDC lists several drivers and challenges for IT organizations, the most significant drivers of which were improved security (35.3% of respondents), followed by significant data/ML/AI initiatives (30.3%), improvement in operational efficiency/reduction in management costs (28.7%), and increased developer productivity (28.6%). At the same time, the most significant challenges to adoption were security concerns (28.7% of respondents), data management (28.3%), multi-cloud/multi-datacenter deployment and management (25.1%), and the reliability and scalability of containers (24.6%).

Exhibit 75: Drivers and Challenges for Kubernetes & Container Deployment

Are Kubernetes & Containers drivers for or impediments of security?
 Yes. They make us more secure and create new complexity

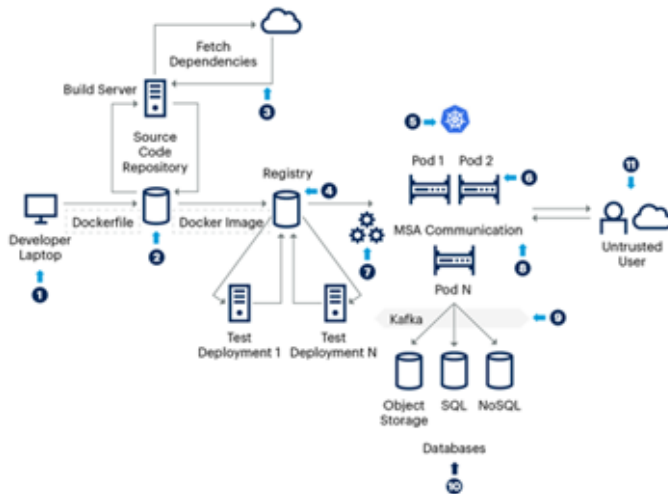


Source: IDC

As the IDC survey shows, security is a positive driver and a challenge with container adoption. Security for containers and Kubernetes is more complex and dynamic than for virtualized servers and applications. First, containers can be linked to hundreds of loosely coupled micro-services, significantly increasing the number of intrusion points. Second, the highly distributed and ephemeral nature of containers makes them highly complex to monitor, making cyber threats to containers challenging to identify and remediate. Third, containers and Kubernetes are richer metadata sources, making anomalous behavior challenging to locate. Overall, IT organizations often need more visibility into what is happening inside their container infrastructure and what vulnerabilities they may be exposed to. According to a survey published by VMware, 97% of technology leaders have concerns about Kubernetes security, with 1 in 5 citing securing containerized workloads at runtime as their most significant concern.

Exhibit 76: Threat Vectors in Container Deployment

Threat Vectors in an Automated Deployment Process



- Threat Vector 1: Development System
- Threat Vector 2: Git-Based Repository
- Threat Vector 3: Retrieval of Dependencies
- Threat Vector 4: Image Registry
- Threat Vector 5: Unsecured Orchestrator Platform
- Threat Vector 6: Host-Container Relationship
- Threat Vector 7: Rapid Rate of Change (Ephemeral)
- Threat Vector 8: Microservices Architecture (MSA) Communication and Network Segregation (East West Traffic)
- Threat Vector 9: Interprocess Communication (IPC) (message brokers - Apache Kafka, RabbitMQ, etc)
- Threat Vector 10: Increased Number of Databases
- Threat Vector 11: Application Layer Attacks

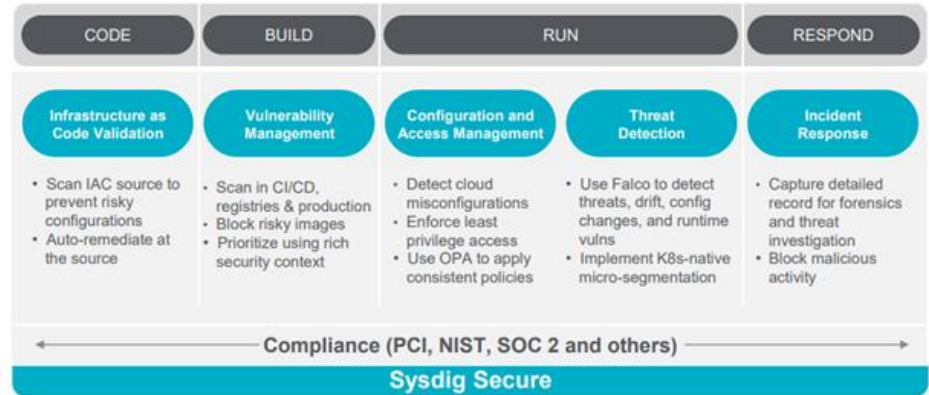
Source: Gartner

Considering the complexity of securing containers, we view container security as an end-to-end effort involving several security monitoring and assessment points. This spans the entire container lifecycle from testing at development (container image scanning, vulnerability assessment, and validation) to threat monitoring, configuration, and posture management at runtime. Most vendors in this space offer AST or runtime security, separately addressing the development and runtime stages of the container lifecycle. Only a few vendors provide DevSecOps and runtime security within the container lifecycle.

They include Aqua Security, Lacework, NeuVector (SUSE), Palo Alto, Sysdig, and VMware (Carbon Black and Tanzu).

Exhibit 77: Container Security

Secure Containers, Kubernetes and Cloud Services



Source: Sysdig

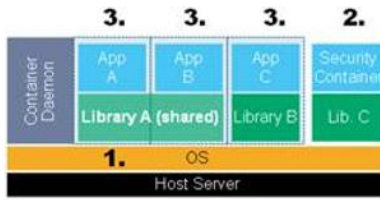
Container security can be implemented across the entire application development and deployment lifecycle. In the application development stage, container security is primarily associated with scanning for vulnerabilities and misconfigurations. We see four points of implementation:

- **Coding** – container image and infrastructure-as-code (IaC) scanning to prevent risky or vulnerable configurations.
- **Build** – container image scanning in CI/CD pipelines, registries, and production, blocking container images that can be open to threats. Assessments include discovering vulnerabilities, malware, issues with secrets and keys, and compliance violations (30–40% of containers today are believed to have unpatched malware).
- **Deployment** – policy-based deployment controls enabling container images to run only when pre-set security criteria and permissions are met.
- **Production** – continuous compliance with intermittent container scanning for known vulnerabilities (N-Day).

In runtime, container security is aimed at detecting container misconfigurations, enforcing least privilege access and policies (usually aligned to standards such as MITRE ATT&CK), and detecting threats (including workload anomalies), drifts, and other runtime vulnerabilities. A container exposed to malicious activity can be terminated or isolated, with detailed records captured for subsequent forensics investigation. Vendors in this area typically offer dedicated container runtime monitoring tools and integrate with privileged access systems, although CSPM can also be used for containers within CNAPP. In addition, container runtime security vendors often send alerts to the SOC rather than auto-remediate.

Exhibit 78: Container Runtime Security

**What About Container Runtime Security?
Four Strategies for Container Security at Runtime**



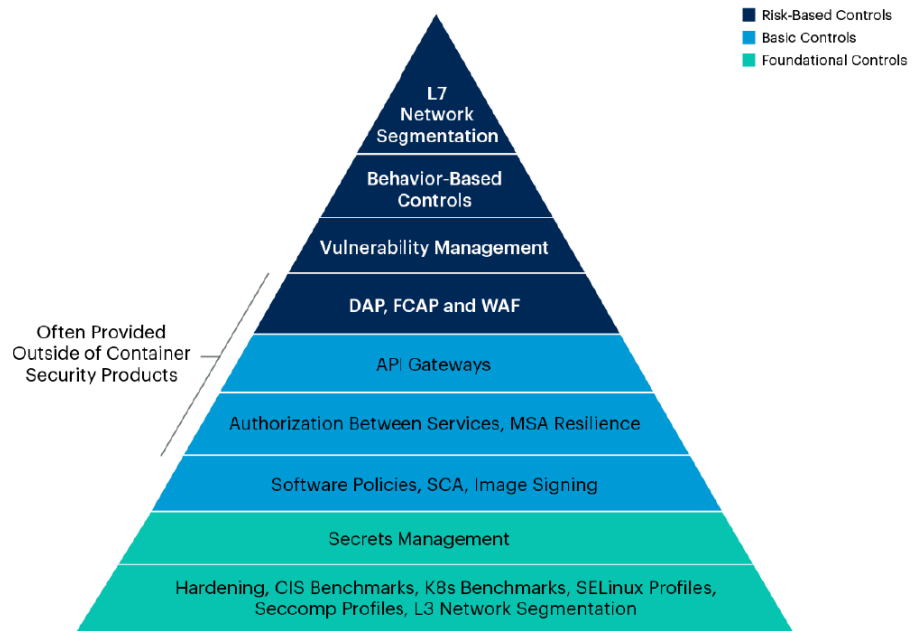
1. Host agent in host OS
2. Privileged security container/daemon
3. Layered into each container
4. No runtime controls, just strong configuration and drift management combined with vulnerability scanning in the development pipeline

Source: Gartner

Another approach to segregating container security is separating threat mitigation into three control system categories, including: (1) Foundational controls—functionality such as Kubernetes hardening, benchmarking, L3 network segmentation, and secrets management. These functions are widely used and generally available. (2) Basic controls—These describe the current approach to protecting containers, including software policies, SCA scanning, container image scanning, inter-service authorization, API gateways, etc. And (3) Risk-based controls—These are specialized capabilities for specific use cases and include database audit and protection (DAP), file-centric audit and protection (FCAP), WAF, vulnerability management, behavior-based controls, L7 network segmentation, etc.

Exhibit 79: Containers Security Control Hierarchy

Container Security Control Hierarchy



Source: Gartner

Sysdig is a cloud security vendor addressing DevOps and runtime protection. The company began as an open-source project dedicated to monitoring containers in production, with deep visibility into files, network, and user activity, without deploying an agent or sidecar and operating at the kernel level (a key competitive advantage). It has expanded its security implementation to include intrusion and threat detection, container

vulnerability assessment, and policy violation (Falco) across all orchestration tools (K8s, Docker, Linux, etc.), cloud vendors (AWS, Azure, GCP), and vendors such as Okta and GitHub (Microsoft). On the runtime side, the company expanded functionality to include monitoring for virtual machine (VM) and serverless workloads, while on the dev side, it has added image scanning in repositories (“shift left”), IaC scanning in development and runtime, and KSPM (acquisition of Apolicy in 2021), delivering container security for the entire application lifecycle. As such, Sysdig offers a comprehensive runtime and DevOps security, capturing the wide breadth of metadata and real-time monitoring audit logs.

Most recently, it announced additional runtime insights with its Cloud Attack Graph (multi-domain co-relation across cloud assets and credentials), Risk Prioritization (ranked vulnerabilities tied to real-time usage), Attack Path Analysis (visualization of exploitable vulnerabilities and dependencies), Inventory (searchable list of cloud resources across users, workloads, hosts, etc.), and Complete Agentless Scanning (expanded agentless capabilities with host scanning of prior misconfiguration and threat detection functions).

Significant acquisition activity and consolidation in the container space has occurred, and few independent container security vendors remain. Palo Alto acquired container security vendors Twistlock (2019) and Bridgecrew (2021), while Cisco acquired Portshift (2020). Infrastructure software vendors have also expanded into containers, with SUSE acquiring NeuVector (2021). Last, existing container security vendors have bolstered their offering through M&A (Sysdig acquired Apolicy (2021)) and partnerships (Sysdig and Snyk (2022)). We expect the consolidation and partnership trends to continue and for container security vendors to work to provide an end-to-end solution (i.e., vendors with container image scanning in DevOps to expand into runtime and vice versa). We also see expansion into security offerings around other cloud-native technologies such as IaC (Snyk acquired Fugue (2022)) and CSPM to deliver a complete CNAPP solution. Still, we expect the evolution to a comprehensive CNAPP offering to take time. We will discuss CNAPP in more detail later in the note.

Notable vendors include Anchore, Aqua Security, Cisco (Portshift), IBM RedHat (StackRox), Lacework, NeuVector (Acquired by SUSE), Palo Alto (Twistlock and Bridgecrew), Snyk, Sysdig, Tigera, VMware (Carbon Black), and Mend.io (formerly WhiteSource).

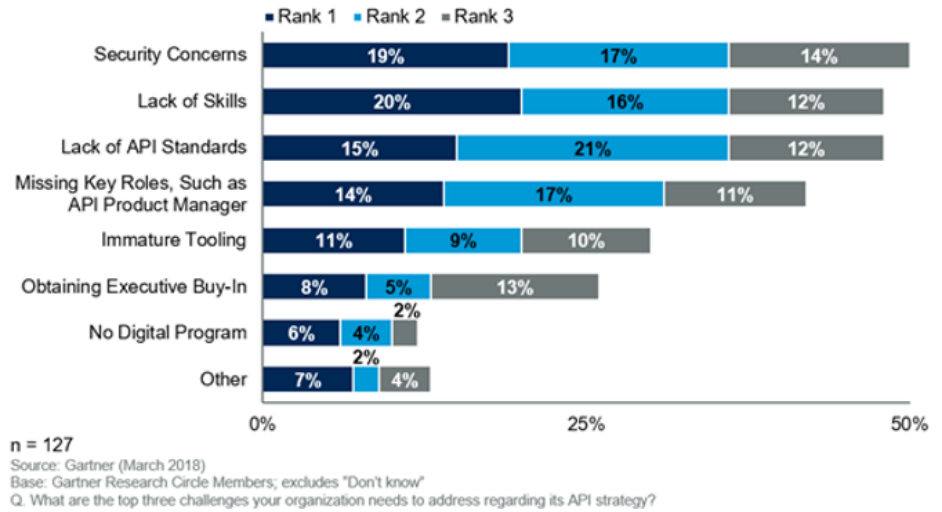
API Security

APIs, or application programming interfaces, enable a controlled interaction and communication between applications (using HTTP, JSON, and XML). APIs have become a crucial component of enterprise digital transformation efforts as they: (1) facilitate the integration of enterprise systems (CRM, accounting, etc.), enabling more efficient operations and faster innovation; (2) shorten software development cycles and save development costs by giving developers access to established available code blocks and data instead of building code from scratch; (3) improve connectivity and collaboration, internally and externally; (4) facilitate faster and more accessible data sharing and collection for intelligence analytics; and (5) drive business value by enabling enterprises to engage with customers (personalized user experience) and vendors (tighter supply chain, order, and payment automation, etc.). APIs have grown so much that CDN vendor Akamai estimates that today, 83% of internet traffic is driven by API calls.

Using APIs also comes with a new set of security threats and concerns, the most important of which is unauthorized access to the underlying data via APIs. Attacks and data breaches involving poorly monitored and secured APIs occur frequently. According to Gartner, client interest in API security recently increased 30% YoY, with API security now ranked as the top challenge to API strategy.

Exhibit 80: Challenges in API Strategy

Top Three Challenges of an Organization’s API Strategy
Percentage of Respondents



Source: Gartner

Several factors contribute to API security vulnerabilities. First, modern-day applications have multiple architectures (mobile, micro-services, hybrid cloud, etc.), making for a large number of “gateways” or “access points” where API security has to be enforced. Second, developers have historically cataloged APIs manually and relied on gateways (which only monitor configured APIs) to create active API directories. This process has broken down with the growth in application development, leaving many APIs undocumented. In fact, API discovery solutions routinely show that organizations typically have 3x the number of APIs versus what internal API directories record. Third, the frequency of API changes has shortened to minutes from months, making it difficult for security teams to keep pace with API documentation and evolution. Fourth, even when APIs are documented, security granularity is limited. Documentation analysis below the token layer is required to protect an API completely but is generally unavailable. Lastly, threat actors have shifted from traditional “one and done” API call attacks (SQLi, XSS, etc.) to “low and slow” API attacks utilizing a sequence of API calls over time to breach applications and data sources. This shift has made static API security unreliable, requiring a change to continuous monitoring of API history and behavior.

Exhibit 81: Evolving API Security Challenges

These API security incidents keep happening because the world has changed

Attacks

- Known attacks (SQLi, XSS, etc.)
- “One-and done” - single API call



- Business logic attacks
- “Low and slow” - sequence of API calls



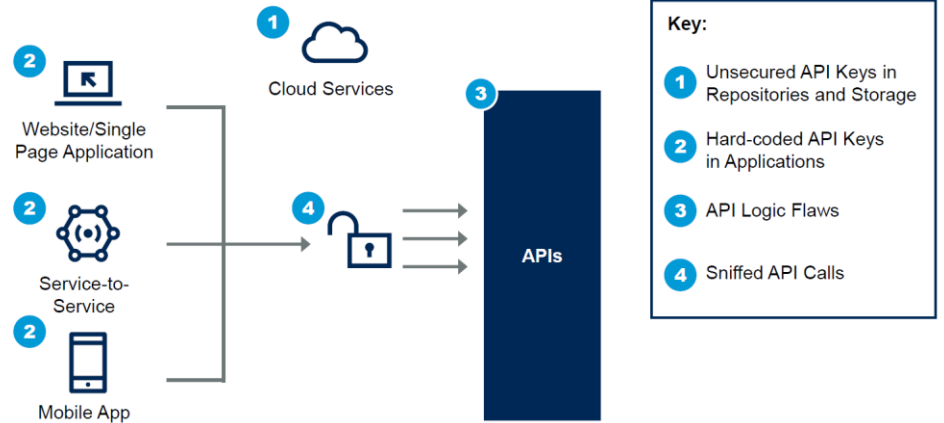
Source: Salt Security

There are multiple vulnerability paths in terms of attack vectors that expose APIs. The following are the most common: (1) unsecured APIs, which are APIs or other private keys that may have been accidentally left with access control in public repositories such as GitHub or GitLab or may have been discovered in cloud-based storage services such as

AWS and Azure; (2) hard-coded APIs, which are API keys or credentials that may have been hardcoded in applications, leaving them subject to attacks; (3) API logic flaws or bugs that can be exploited; and (4) sniffed API calls, which reflect situations where API traffic is “sniffed” using techniques such as “man-in-the-middle,” following which uncovered or unsecured APIs are opened to unauthorized access.

Exhibit 82: API Attack Vectors

API Attack Vectors



Source: Gartner

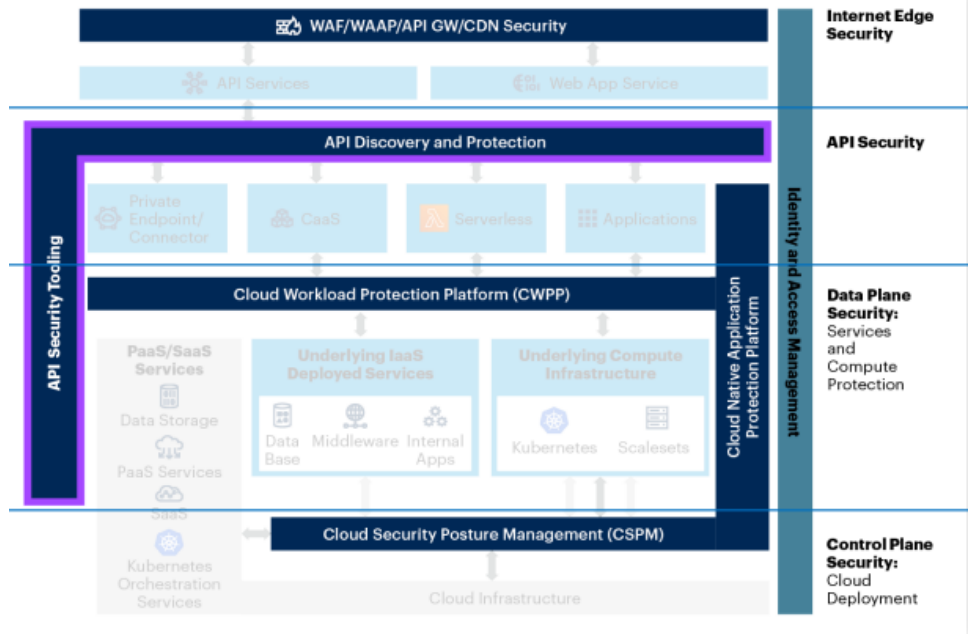
We view API security as a framework rather than a specific technology, encompassing a range of technologies, including API management, WAF/WAAP, IAM, in-app protection (API discovery and vulnerability testing during development and runtime monitoring), and CWPP tools. To fine-tune this point, we note that runtime API security includes API threat protection and API access control. API threat protection validates content, detects incoming threats, and can throttle/block traffic during attacks. WAF, API management, and application delivery controllers (ADCs) enable threat protection using attack signatures, reputation-based controls, and anomaly detection and validation technologies. APIs are authenticated with proper identity and authorization management with API access control, aligning more with IAM and general API management. Both threat protection and access control are required for robust API runtime security. The exhibit below shows the breadth of tools necessary for effective API security.

Exhibit 83: Three Components of API Security



Source: Gartner

Exhibit 84: API Security Framework

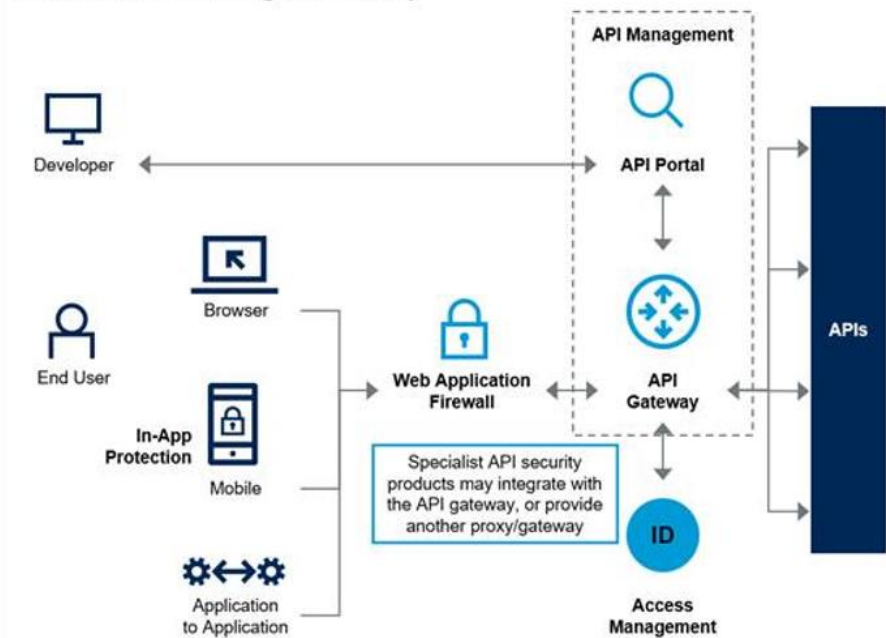


Source: Gartner

We note that traditional and broad-based application security methods are ineffective for API security as they mainly cover runtime security as a perimeter defense, lacking the breadth of API coverage and the depth of API documentation to provide a comprehensive runtime solution. Accordingly, specialist API security vendors that address API scraping and discovery during application development and API configuration and threat mitigation at runtime (by acting as a proxy or gateway) are critical to delivering API security. Nonetheless, we expect a growing overlap with traditional vendors as more sophisticated API runtime functionality is added to existing WAFs and API management tools.

Exhibit 85: API Security Workflow

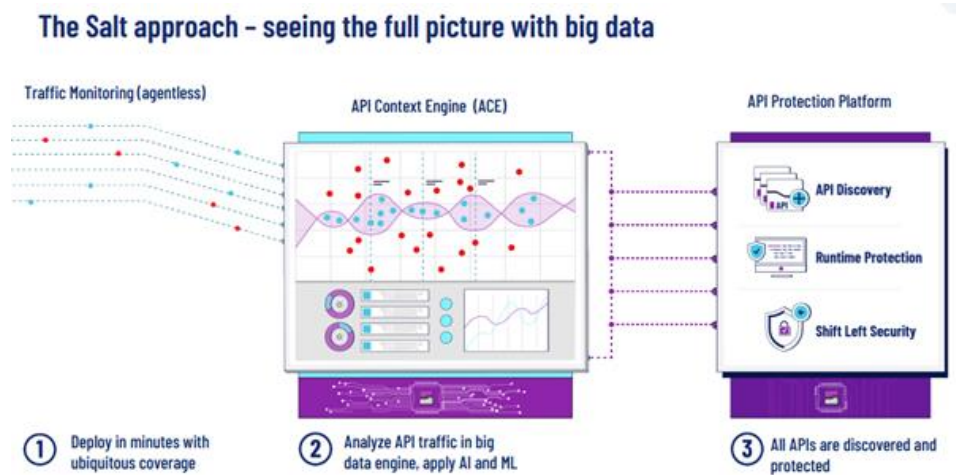
Infrastructure Providing API Security



Source: Gartner

Salt Security is an emerging API security vendor. The company offers API security across the API lifecycle, including identifying security gaps in the OAS analysis (Open API Specification) and the ability to “discover” APIs, including shadow or zombie APIs, to create a dynamic API catalog with associated metadata. It provides a comprehensive roadmap into the particular APIs’ features versus the common practice of manual cataloging. Salt’s platform analyzes data traffic in runtime with its API Context Engine (ACE). It leverages big data and AI/ML techniques to perform contextual analysis across the different metadata dimensions gathered during the discovery phase, and then it creates baselines of API behavior. The platform then observes behavioral anomalies across APIs, detecting malicious attacks across various known (SQLi, XSS, DDoS, OWASP API Security Top 10, MITRE, etc.) and unknown vulnerabilities. It can also detect “low and slow” attacks, particularly for OWASP API Security Top 10, by analyzing data traffic history across various APIs and customer data. This is a critical feature of its product offering. The company integrates with DAST and IAST security vendors (such as StackHawk, Invicti Security, and Contrast Security) to enhance the API intelligence of its platform.

Exhibit 86: Salt Security Approach to API Security



Source: Salt Security

Noname Security is another emerging API security vendor offering a comprehensive end-to-end API security platform addressing misconfiguration, vulnerability, and threat management. The platform sits out-of-band without the need for agents or network modifications and offers deep visibility into APIs compared to API Gateways or WAFs, and provides comprehensive API security around industry frameworks such as OWASP API Security Top 10. Its platform consists of three components: (1) API Security Posture Management, which inventories every single API and identifies misconfigurations and vulnerabilities in its policy and specs; (2) runtime API threat detection in real-time using AI/ML models, and with automated and semi-automated blocking and threat remediation availability; and (3) continuous, automated, and dynamic API security scanning and testing during the CI/CD pipeline (DevSecOps). In early 2023, the company introduced a Public Sector Hardened Virtual Appliance for dedicated usage across US Federal and highly regulated industry customers.

Other notable vendors include 42Crunch, Cequence Security, CloudVector (Imperva), Contrast Security, Data Theorem, Neosec (Akamai), NTT Application Security, StackHawk, and Traceable.

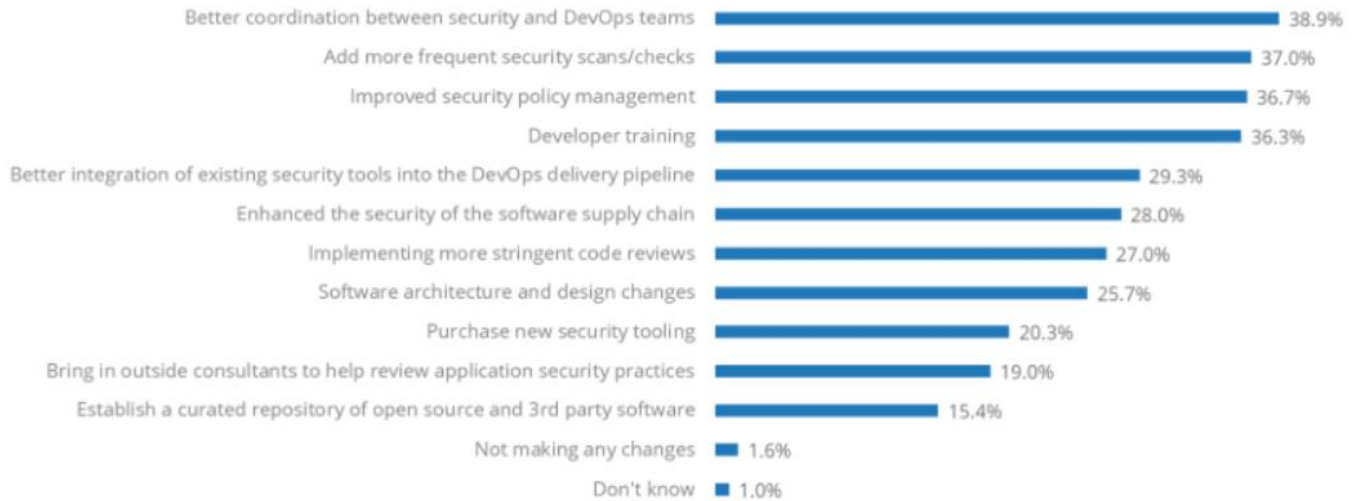
Application Security Market Evolution

Returning to discuss the broader application security sector, the market has evolved substantially over the past few years, particularly with agile CI/CD development (move toward DevSecOps) and the growing use of cloud-based infrastructure and cloud-native applications. Modern security vendors are taking a more holistic approach to security, addressing as many lifecycle domains as possible to protect the application at every development and deployment life cycle step. This process gradually drives AST and ARS

tools closer to delivering more comprehensive security coverage. However, we are still early in this process and expect toolset consolidation to take time.

Exhibit 87: Organizational Plan to Address Security Breaches, 2023 Survey Results

What types of changes are you making to address the security breach(s) in the future? [SELECT ALL THAT APPLY]

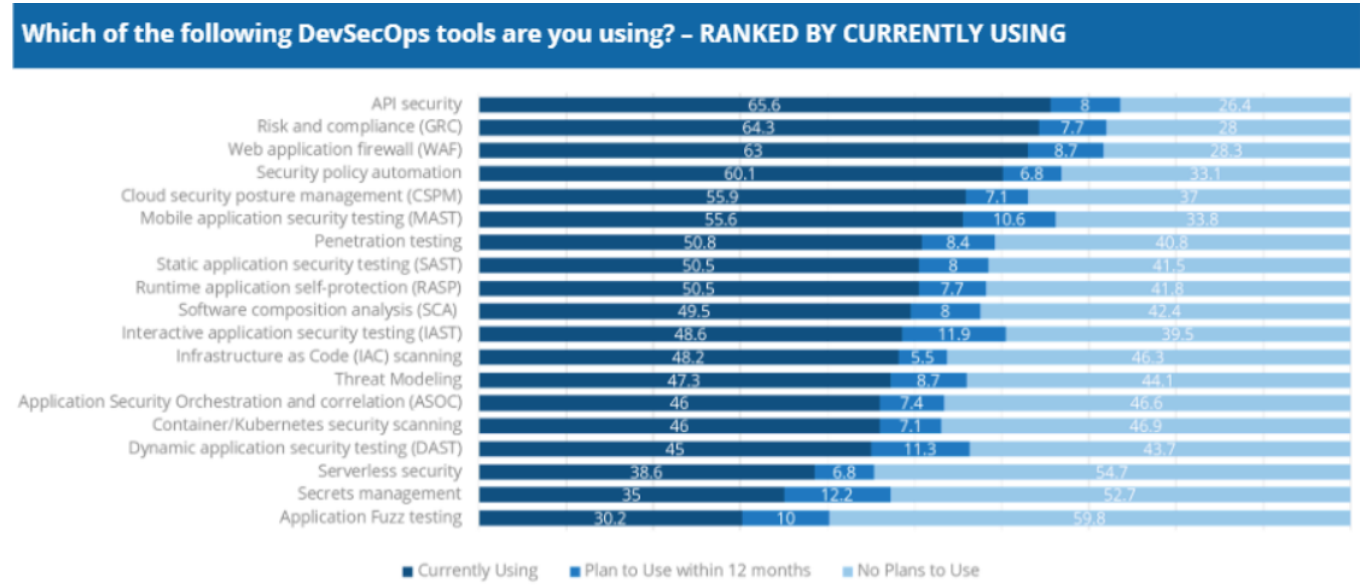


Source: IDC

We expect several technology trends to play out within application security. First, given the rapidly growing use of open-source software, we see SCA (and now SSCS) as an increasingly important application security tool for organizations. Second, we expect Container and IaC scanning usage to grow due to a shift toward cloud-native apps and the lack of mature security solutions for these new technologies. Third, ASPM is relatively new, and we expect rapid adoption along with AST tools. Fourth, we expect AST vendors with point solutions to broaden (organically or through M&A) their AST reach (SCA, SAST, DAST, IAST, ASPM, MAST, API vulnerability assessment, fuzzing, etc.) and add complementary application runtime tools such as RASP and Container/IaC scanning to deliver on the broader CNAPP vision (discussed later in this section). Similarly, we expect ARS vendors to shift left and add AST tools, particularly in Container/IaC runtime security.

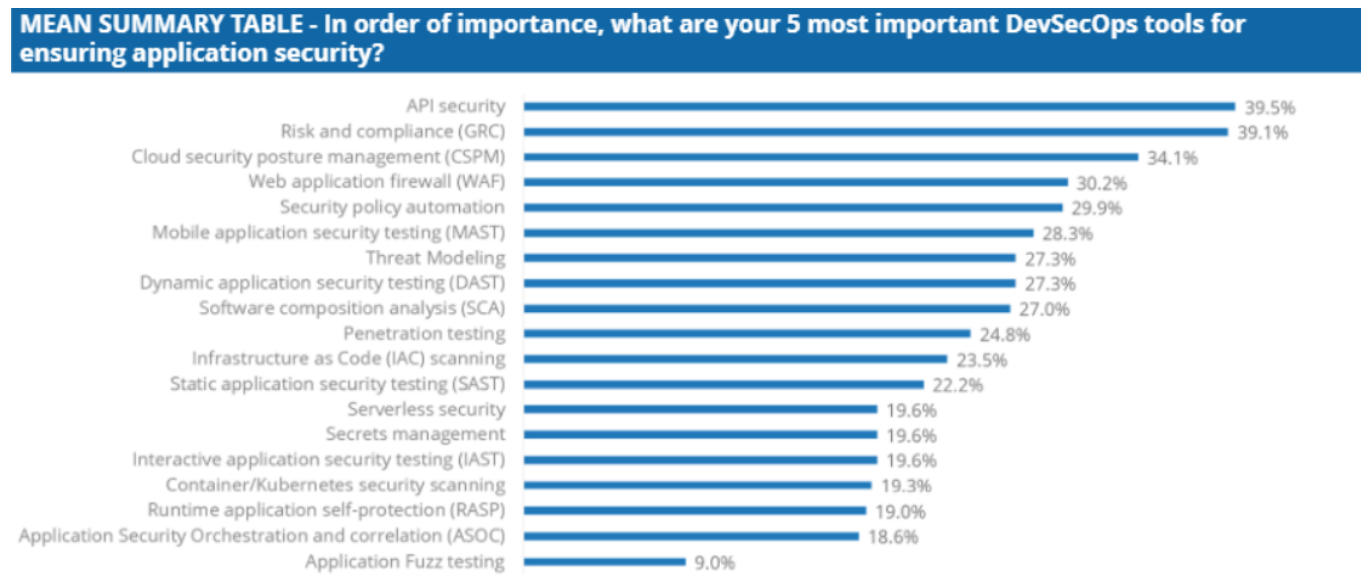
We note that vendors from other security domains are also moving into application security. Traditional network security vendors are expanding into application runtime tools such as WAF and Container/IaC scanning (e.g., Palo Alto and Cisco with recent acquisitions). In contrast, Application Performance Monitoring (APM) vendors have broadened their reach to provide threat intelligence for application runtime security (Datadog, Elastic, etc.). Last, we expect security tools across the board to increasingly use analytics and ML and automate remediation, moving beyond traditional detection capabilities.

Exhibit 88: Tools Used in DevSecOps, 2023 Survey Results



Source: IDC

Exhibit 89: Most Important DevSecOps Tools, 2023 Survey Results



Source: IDC

Reinforcing our views, we have seen accelerated M&A activity in the application security market. Application security vendor Snyk most recently acquired ASPM vendor Enso Security (2023) and previously purchased CSPM vendor Fugue (2022) and SCA vendor FossID (2021). Aqua Security acquired software supply chain security vendor Argon and Terraform (IaC) security scanner tfsec (2021). DevOps vendors have also added application security capabilities to offer a complete software development toolchain. For example, GitLab acquired Peach Tech and Fuzzit (2020) to expand its DAST and fuzz testing capabilities, while GitHub acquired Semmie and Dependabot to add SAST and SCA functionality (2019). Network and cloud security vendor Palo Alto Networks acquired Cider Security for ASPM and previously acquired IaC scanning provider Bridgcrew (2021), container security vendor Twistlock (2019), and serverless application security vendor PureSec (2019).

Adjacent cybersecurity companies such as CrowdStrike, HashiCorp, and Cisco have also moved into the application security market through M&A. CrowdStrike acquired ASPM

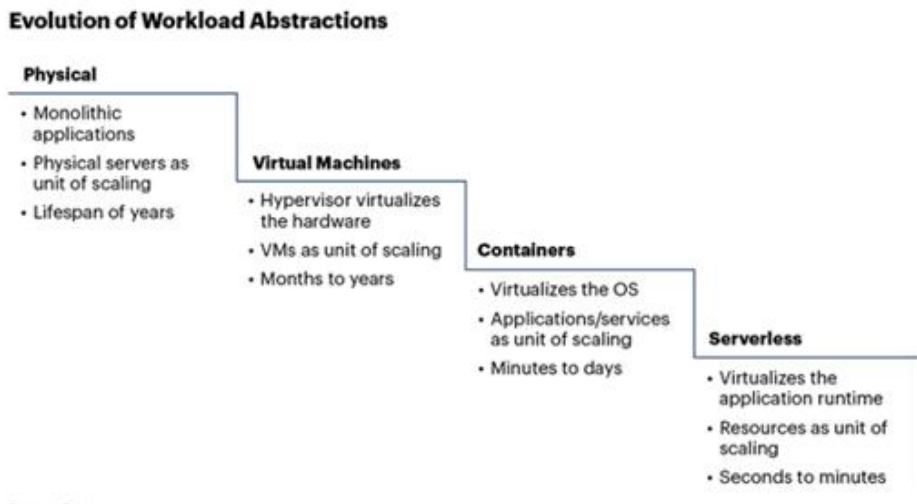
vendor Bionic (2023), HashiCorp acquired SSCS vendor BluBracket (2023), and Cisco acquired Kubernetes security specialist Portshift (2020). We expect the M&A activity to continue as application security vendors expand their toolsets and non-traditional vendors strive to provide more comprehensive and integrated security solutions.

Last, it is essential to note that not all portfolio gaps will be addressed through acquisitions. Partnerships between application security vendors are on the rise. For example, Sysdig and Snyk have a deep partnership, where Sysdig's container/Kubernetes security scanning and runtime monitoring tools integrate with Snyk's developer security platform to address cloud-native applications (even though Snyk has a container security scanning tool).

Cloud-Native Application Protection Platforms (CNAPP)

In recent years, workload abstraction has evolved from traditional monolithic physical servers and VM-based deployments to containers and serverless architectures. Cloud-native applications today are deployed in cloud-hosted environments and leverage the broad feature set of cloud computing platforms. They are built with software containers, utilize cloud-based micro-services and serverless infrastructure, communicate with VM-based on-premise data centers, and facilitate end-to-end DevOps-style agile development.

Exhibit 90: Evolution of Workload Abstraction toward Cloud-Native Environments



Source: Gartner

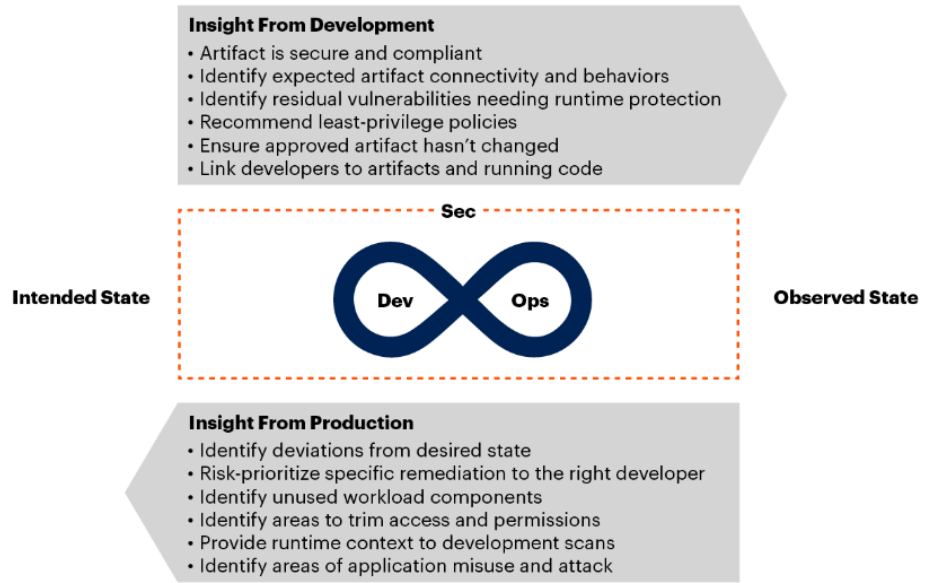
This evolution presents many new challenges requiring a security paradigm shift, as traditional workload protection tools need to secure these new infrastructure elements effectively. For example, containers are highly ephemeral, often running for only seconds or minutes. Thus, any data written to the container file system will be deleted along with the container, ruling out interactive troubleshooting on a running container (deleted before the security team can investigate). Software agents commonly run on endpoints are also unsuitable for containers as they are too heavy in code, take time to set up, and degrade container performance. Serverless architectures further complicate the security picture as the underlying infrastructure is invisible to the user.

To overcome these issues, developers and security teams need cloud-native application protection platforms that utilize modern-era application security tools such as IaC scanning and container scanning/runtime monitoring (such as sidecars, monitoring DaemonSets, eBPF instrumentation, etc.). It is imperative for such cloud-native protection platforms to support real-time bidirectional feedback, with developers receiving insights from observed states at runtime and security teams receiving artifact security confirmations and residual vulnerability assessment from the application development tools.

This approach marked the introduction of a unified Cloud-Native Application Protection Platform (CNAPP) that focuses on securing the entire cloud-native application development and deployment lifecycle. CNAPP combines both sides of the application life cycle under one end-to-end platform, offering an optimal way to ensure that modern cloud-native architecture applications are secure. It significantly overlaps with AST and ARS application security tools, which are more optimized for traditional application development and deployment and are not cloud-native.

Exhibit 91: CNAPP Bidirectional Feedback

Bidirectional Integration Between Development and Runtime

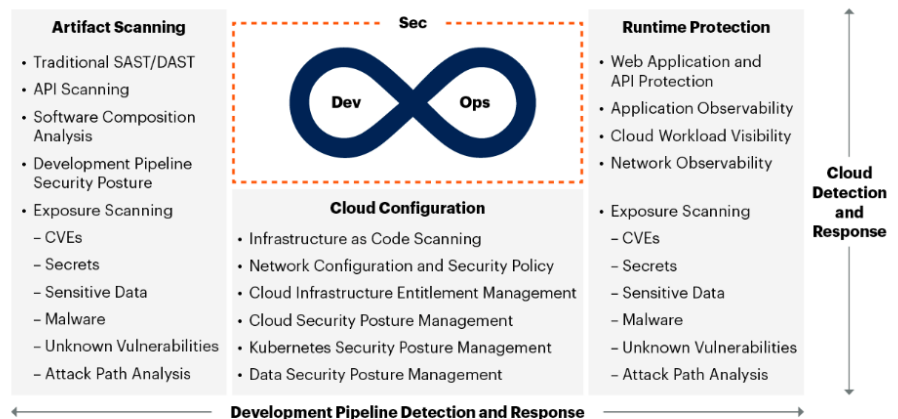


Source: Gartner

CNAPP thus represents the effort to solve the challenges discussed by consolidating the entire application security, cloud workload protection, and posture management into a single framework. CNAPP effectively includes three segments: (1) AST scanning tools (SCA, SAST, DAST, etc.), (2) cloud configuration tools (IaC, CSPM, CIEM, KSPM, etc.), and (3) runtime protection tools (RASP, CWPP, WAF, etc.). This architecture offers immediate and real-time insights across the application lifecycle domain and better addresses modern-day cloud-native infrastructure and application characteristics.

Exhibit 92: CNAPP Detailed View

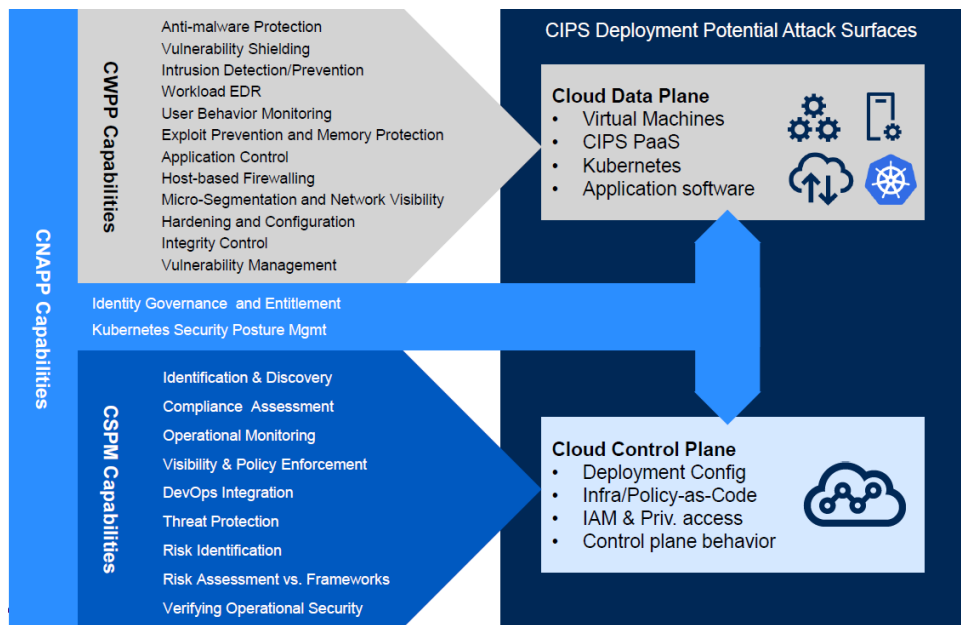
CNAPP Detailed View



CVEs = common vulnerabilities and exposures

Source: Gartner

Exhibit 93: CNAPP Attack Surface



Source: Gartner

It's important to highlight that CNAPP development and adoption are still in their early stages. Not one vendor can provide an end-to-end CNAPP solution today. In our view, the evolution of this market will take time to materialize and take hold in two steps. First, we expect CSPM, KSPM, CIEM, CWPP, and ARS tools (including API security) to come together as one platform. Later, we expect AST tools (beyond container image scanning and IaC scanning) to gradually be incorporated by vendors. This process will take time to materialize as many toolsets are still immature. In support, Gartner estimates that by 2026, 80% of organizations will consolidate the number of vendors securing the life cycle of cloud-native applications but will still use up to three vendors, illustrating the long consolidation cycle ahead to delivering on CNAPP.

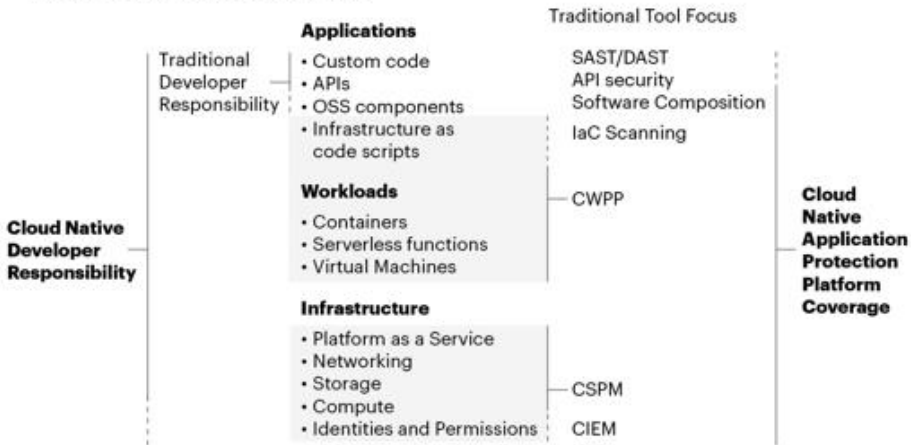
We note that CNAPP vendors have approached the market from different starting points. Some were runtime security vendors within specific verticals (such as EDR, Serverless, Container) that have added additional capabilities for CSPM and CIEM and shifted left technologies in the DevSecOps chain. Examples include Palo Alto, Zscaler, CrowdStrike, SentinelOne, VMware, Sysdig, and Aqua. Another common starting point in the shift to CNAPP was that of CSPM vendors, which first integrated with the DevSecOps toolchain and then expanded to include CWPP capabilities (with agentless and agent-based offerings). Examples of such vendors include Orca, Wiz, and Lacework.

That said, several challenges today prevent the widespread adoption of CNAPP solutions. These include: (1) security organization responsibility for CNAPP is spread across multiple silos, including DC security, application security, and cloud security teams, making it difficult to have a unified solution; (2) an adversarial relationship exists between developers and security, where priorities during application development may differ between the two; (3) existing investments across CWPP and CSPM may be spread across multiple vendors; (4) adjustment to change in infrastructure architecture is difficult as CNAPP solutions are developed with a SaaS-based cloud delivery model mindset; (5) there is a lack of technical maturity across an end-to-end CNAPP solution currently available in the market (each vendor has a different area of expertise); and (6) a majority of applications used today are still legacy and not fully cloud-native, and thus require high reliance on legacy security tools.

Exhibit 94: CNAPP Encompasses AppSec, CWPP, CSPM, and CIEM

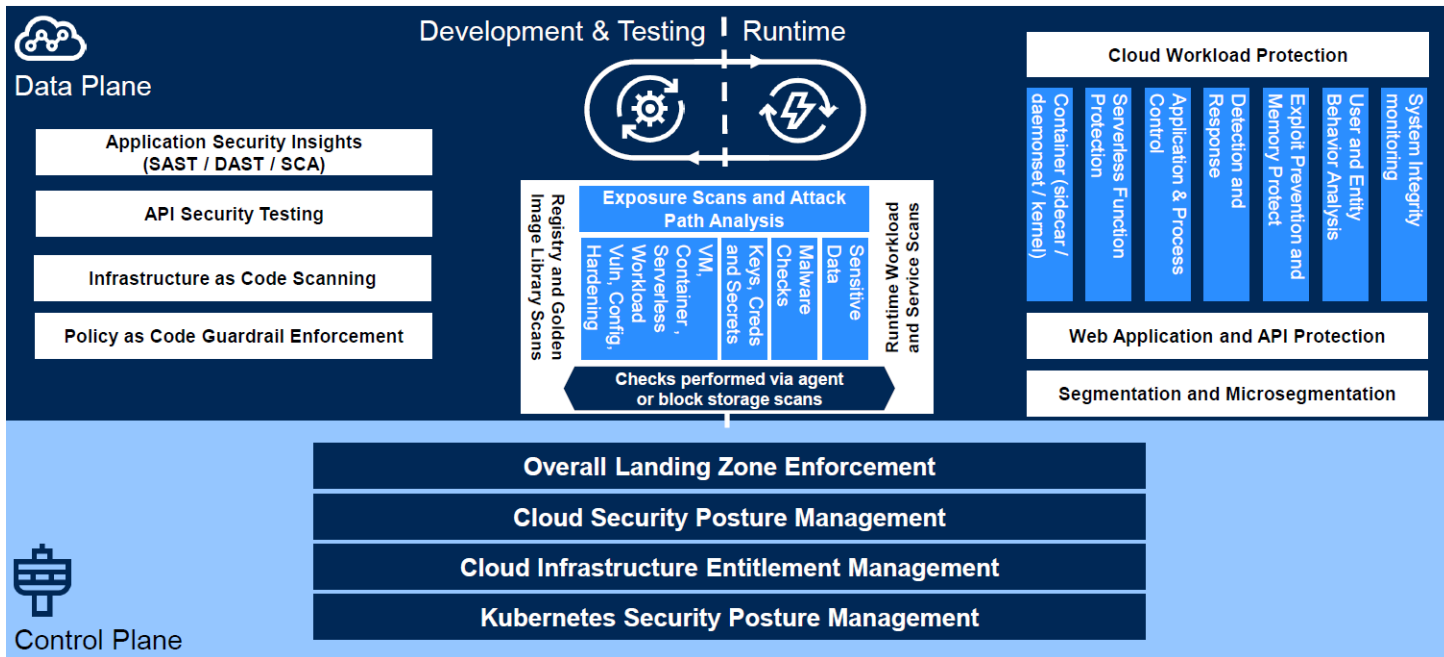
Blurring Boundaries of Responsibilities

-- Indicates Areas Where Responsibility/Coverage Varies



Source: Gartner

Exhibit 95: CNAPP Capabilities



Source: Gartner

Application Security Market Vendor Overview

Within AST, mature vendors such as Checkmarx, HCL Software, Micro Focus, Synopsys, and Veracode have a broad presence in many AST sub-segments and have made efforts to address emerging cloud and agile CI/CD opportunities. Emerging vendors in AST with an increased focus on SCA/SSCS, container scanning, IaC scanning, and ASPM technologies include Contrast Security, Snyk, Mend.io, and, to a lesser extent, Sysdig.

Within ARS, the market is more fragmented by type of technology. We note that mature technologies such as WAF are dominated by established players such as Akamai, Cloudflare, F5, Fastly, Fortinet, and Imperva, which usually have a broader network offering. Emerging technologies are where startups play, including Salt Security, Noname

Security, and StackHawk for API security, and Aqua Security, Lacework, Sysdig, and Twistlock (acquired by Palo Alto) for container runtime security.

Exhibit 96: Gartner Magic Quadrant for Application Security Testing



Source: Gartner

Exhibit 97: Forrester Wave for Software Composition Analysis 2Q23



Source: Forrester Research

Below we review several of the broader Application Security (AST and ARS) market vendors that were not reviewed in detail in the note.

- **Aqua Security** offers a CNAPP platform to secure applications in development and runtime. The platform provides developers with vulnerability scanning and dynamic threat analysis to scan artifacts for various risks (vulnerabilities, malware, secrets, etc.) during the build phase for comprehensive software supply chain security (SSCS). The platform also offers security teams VM, container, and serverless security for workloads with granular controls and real-time detection and response (CWPP) and comprehensive CSPM and KSPM capabilities to monitor cloud and Kubernetes configurations against best practices and for IaC scanning to eliminate risks during deployment. Integrations address the cloud-native application lifecycle, including standard CI/CD (Gitlab and Jenkins) and SIEM (Splunk and Datadog) tools.
- **Checkmarx** offers a range of tools for DevSecOps environments. Its primary focus has been on SAST, SCA/SSCA, and IAST tools (provides DAST through a partnership with Invicti) on the application security testing side. Additionally, the company leverages its SAST technology for API discovery in code to provide API security during the development cycle. The company has also added an open-source IaC scanning tool supporting multiple environments such as Terraform, Kubernetes, Docker, AWS CloudFormation, and Ansible. Lastly, Checkmarx provides secure code training to developers (Checkmarx Codebashing).
- **Contrast Security** is a provider of runtime application security. It began as an IAST vendor (Contrast Assess) and has expanded to provide RASP (Contrast Protect) capabilities through its application sensor. Its IAST solution supports various languages, including Java, .NET, Node.js, Ruby, Python, and Golang. The company also provides scanning capabilities with SCA (Contrast SCA) and SAST (Contrast Scan) to address functionality around legacy programming languages not monitored by its runtime services. With the acquisition of CloudEssence in 2021, Contrast added to its cloud-native capabilities and now offers vulnerability testing for serverless applications and APIs (Contrast Serverless). It partners with NowSecure for a MAST solution. The IAST and RASP modules require an agent within the application, while the SCA and SAST scanning are agentless.
- **JFrog** addresses application security through its SCA tool (called Xray). It scans repositories by breaking down software packages at a binary level, utilizing the metadata to uncover potential vulnerabilities, policy violations, and compliance issues across the SBOM for a complete SSCS offering. The company has enhanced its functionality, adding CVE analysis & remediation, secrets detection, greater malicious code detection, container contextual analysis, and IaC vulnerability assessment as part of its Advanced Security package (available as a consumption-based add-on product to Xray). JFrog also provides SAST-type scanning for zero-day vulnerability detection based on its Vdoo technology (acquired mid-2021).
- **Lacework** is a cloud security vendor addressing application development and runtime. The company utilizes ML-based models to identify application behaviors and groups them across containers or VMs based on common behaviors. Its architecture protects dynamic cloud workloads without manually defining policies, rules, or tags, allowing full automation, a critical requirement for securing scalable cloud-native applications. Lacework's solutions can be integrated with public (AWS, Azure, GCP, etc.), private cloud, Kubernetes, and Docker container environments. While Lacework's platform initially addressed CSPM use cases, it now addresses CWPP, IaC security, KSPM, CIEM, container security, cloud-based vulnerability management, and code-level security with SCA and SAST. It also has a CNAPP offering for customers, combining all the technologies mentioned above.
- **Mend.io** (formerly WhiteSource) offers SCA and SAST tools supporting 27 programming languages. It recently expanded its product offering to include SBOM for a complete SSCS solution. Its SCA solution is developer-friendly, continuously scans dozens of open-source repositories, and cross-references the data with open-source components in the build, including package dependencies and APIs. It also automates the creation and enforcement of licensing policies. In terms of container scanning, Mend provides vulnerability and license management for containers during

the build, in the registry, and production, and includes scanning for a range of registries, including Amazon ECR, JFrog Artifactory, Azure Container Registry, Docker, Google Container Registry, and GitHub Packages. It acquired SAST vendors Xanitizer and DefenseCode (2022), open-source malware and threat detection vendor Diffend (2021), and GitHub and GitLab repository-focused dependency scanner Renovate (2019). Most recently (December 2023), the company acquired Atom Security, which specializes in container image vulnerability prioritization, bolstering its container security capabilities.

- **Palo Alto Networks** has expanded into application security through M&A, acquiring container security vendor Twistlock in 2019, serverless security vendor PureSec in 2019, IaC security vendor Bridgecrew in 2021, ASPM vendor Cider Security in 2023, and DSPM vendor Dig Security in 2023. Within application security, it now provides complete container image scanning during the build, in the registry, and deployment phase of the CI/CD cycle, as well as continuous vulnerability management for runtime container security. Its IaC scanner (Checkov) is part of the shift-left strategy and continues to build upon Bridgecrew's traction with developers. The company leverages the above technologies to analyze software bill-of-materials (SBOM), Git repository vulnerabilities, secrets management, and OSS license compliance as part of a comprehensive SCS solution. All products are available as part of Cloud Code Security within Palo Alto's Prisma Cloud offering.
- **Veracode** offers a range of AST tools with products across SAST, SCA, DAST, IAST, container security (pre-production), and penetration testing. The company started as a SAST vendor and has grown its product line primarily organically, adding DAST, IAST, and SCA capabilities over time and API scanning capabilities within its DAST solution more recently. Over the past year, Veracode has expanded its container security scanning functionality and now addresses IaC scanning as well. Utilization of the SCA tool has also expanded to provide an SBOM and address software supply chain security, although no dedicated SBOM tool has been available so far. Finally, it provides developers with security testing training (Veracode Security Labs).

Data Security

Data Security Posture Management (DSPM)

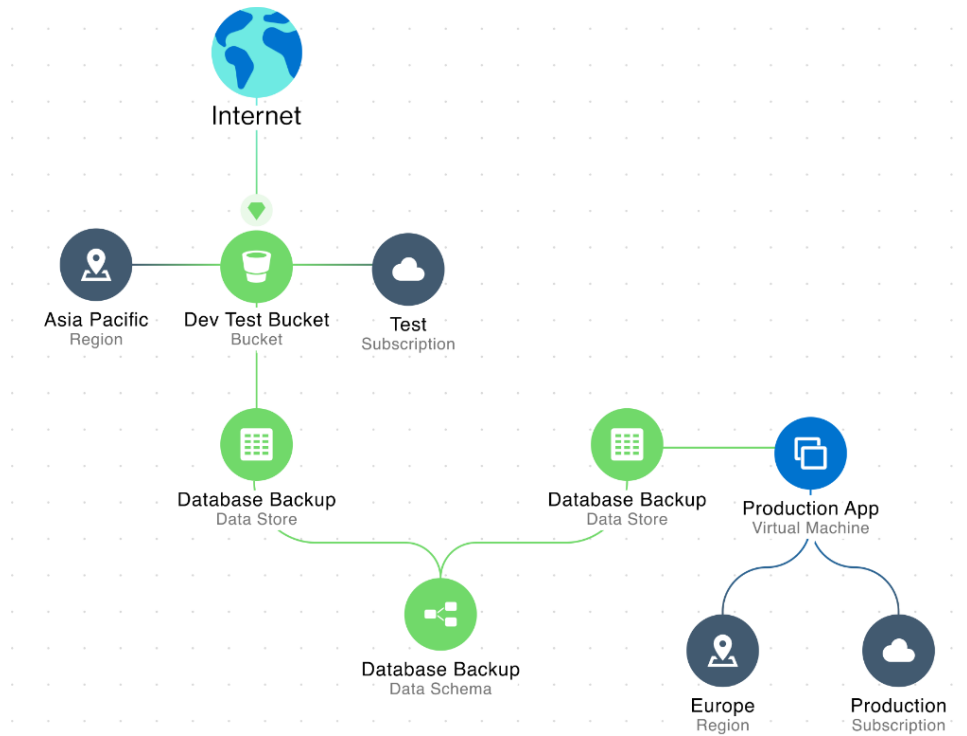
As organizations continue to expand and evolve their IT architectures, data proliferates across multiple cloud environments, on-premises systems, and geographies. This proliferation, along with the growth in cloud backup, application security testing environments, and unmonitored SaaS applications, often leads to the creation of unidentified data stores (shadow data). Shadow data stores are typically disconnected from core business projects/processes and represent an unmonitored attack surface that threat actors can leverage to access sensitive information (such as PPI, PCI, and PHI data). DSPM, an emerging data security technology, addresses this issue by identifying, contextualizing, and securing sensitive data (structured and unstructured). DSPM is a foundational layer of the data security posture of cloud-oriented organizations dealing with siloed, shadow data stores.

Traditionally, enterprises relied on native data security capabilities of various security tools (IAM, Network Security, etc.) to protect the respective data repositories these tools managed. However, these tools lacked policy integration capabilities with other security tools, were insufficient in data discovery, and couldn't handle sensitive data, making for an inconsistent data security posture. This created siloed data environments with multiple management consoles, leaving large portions of data undiscovered. Although the traditional approach created complexity and was cumbersome to manage, IT & security teams could minimize blind spots as long as the repositories were located in traditional on-premises environments. The shift to the cloud drastically changed this balance, spread data across IaaS environments and SaaS applications outside the corporate perimeter, and worsened the shadow data problem.

DSPM tools address these challenges by offering a bottom-up approach to map all the data repositories across IaaS and PaaS environments and analyze the connected data pipeline to identify unmanaged stores, combined with a top-down analysis of data

privileges among employees. The bottom-up mapping is accomplished with an agent or by leveraging the cloud privileges for each major public cloud and by tracking metadata to identify combined, fragmented, or changed data sets. The complementary top-down approach pinpoints employees with access to sensitive data sets via integrations with common IAM and SaaS applications. This hybrid approach enables organizations to identify attack paths within their posture, prioritize data stores with the highest concentration of sensitive data, and remove excessive privileges from unauthorized users.

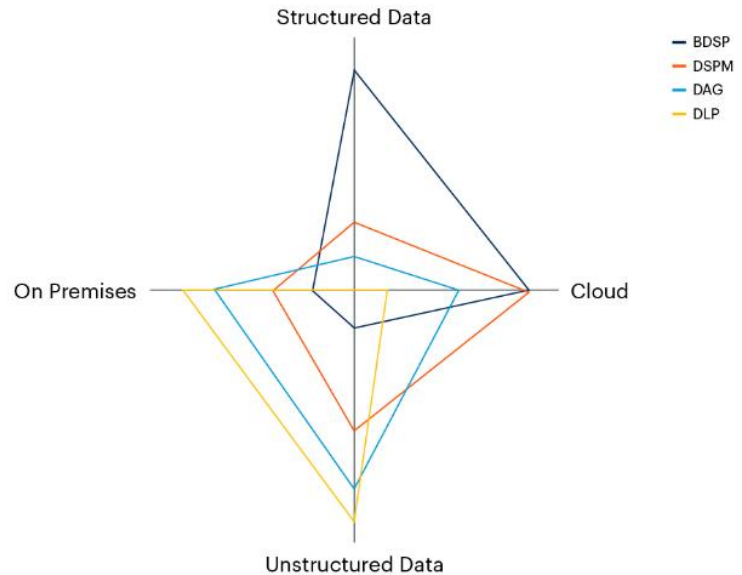
Exhibit 98: Data Mapping Example



Source: Wiz

While the DSPM market is early in its development and adoption cycle, the competitive landscape is already crowded and includes startups like BigID, Wiz, Dig Security (now part of Palo Alto Networks), Securi as well as established vendors like IBM (via its acquisition of Polar Security) and Varonis. Many vendors have added DSPM to address the shortcomings of their existing data security offerings (Palo Alto acquired Dig Security, and Rubrik acquired Laminar). In contrast, cloud security vendors like Wiz have added DSPM to provide organizations with a holistic view of their cloud security posture.

Looking ahead, we expect the adoption of DSPM to accelerate as organizations deploy cloud infrastructure and increase the amount of structured and unstructured data within their environments. Over time, we expect the DSPM market to roll up into a broader Data Security Platform (DSP) market that consolidates DSPM with DLP, broad-spectrum DSP (bDSPs), and Data Access Governance (DAG). bDSPs offer data discovery and monitoring for structured data in cloud databases, and DAG implements access policies for unstructured data. DSP provides structured and unstructured data coverage across Cloud and on-premise environments as a combined solution. In the near term, we expect the DSPM, DLP, and DAG markets to converge, given the overlapping focus on securing unstructured data.

Exhibit 99: DSP Capability Coverage

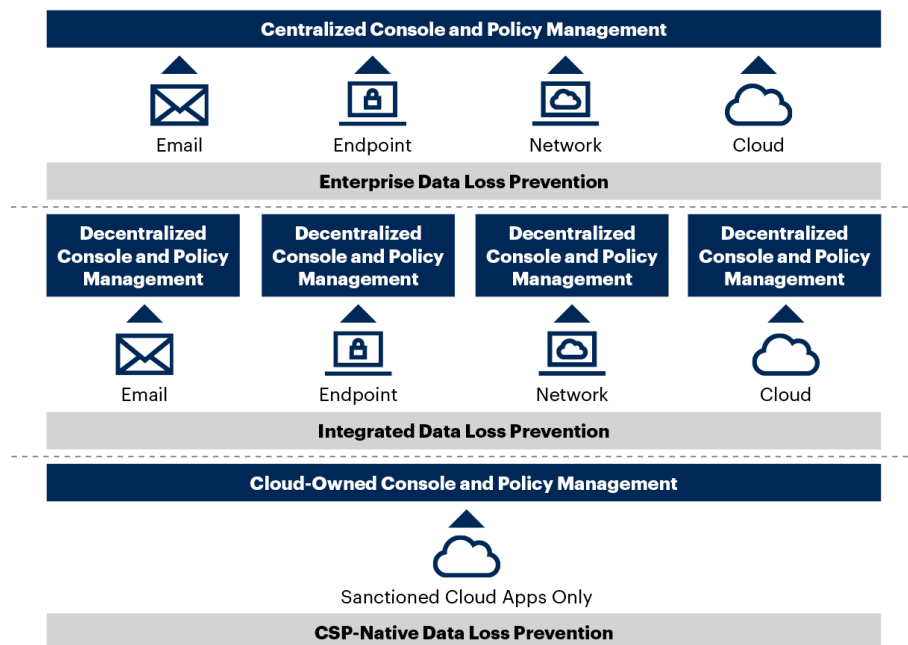
Source: Gartner

Data Loss Prevention (DLP)

DLP solutions prevent the leakage of sensitive data and the accidental transfer or loss of data. DLP is implemented according to dynamic content- and context-based policies and offers visibility into and contextual analysis of data-at-rest and in-transit across on-premise and cloud environments. The underlying technology uses data classification labels and tags and content inspection techniques to identify sensitive content and analyze actions related to its use. Standard DLP capabilities include content inspection, monitoring, alerting, warning, active blocking, and other remediation features executed based on pre-defined security policies.

Three types of vendors address the DLP market: (1) enterprise DLP (EDLP), (2) integrated DLP (IDL), and (3) cloud-native DLP (CSP-native DLP) vendors.

- **EDLP** vendors provide standalone DLP solutions addressing email, endpoints, network, and cloud environments. They include a central management console from which security policies can be defined and advanced content inspection and remediation capabilities incorporated. EDLP solutions are typically feature-rich and apply to a broad range of use cases, such as regulatory compliance, internal policy management, and intellectual property protection.
- **IDL** vendors offer DLP capabilities as a broader security technology such as a CASB, SWG, SEG, or an EPP/EDR solution. These solutions often have limited policy implementation and reporting capabilities and require manual integrations with other IDLP solutions within an environment (for example, integrating a CASB DLP with an EDR DLP). With that said, IDLP vendors have significantly improved their content inspection capabilities and now recognize classification tags from more sophisticated DLP tools.
- **CSP-native DLP** refers to the native built-in DLP capabilities within common IaaS and SaaS cloud providers such as Microsoft Azure, Amazon AWS, Salesforce, and Box. These capabilities offer better data visibility for their respective cloud ecosystems and are often a leading choice for organizations further on the cloud migration process.

Exhibit 100: EDLP vs. IDLP vs. CSP-native DLP

Source: Gartner

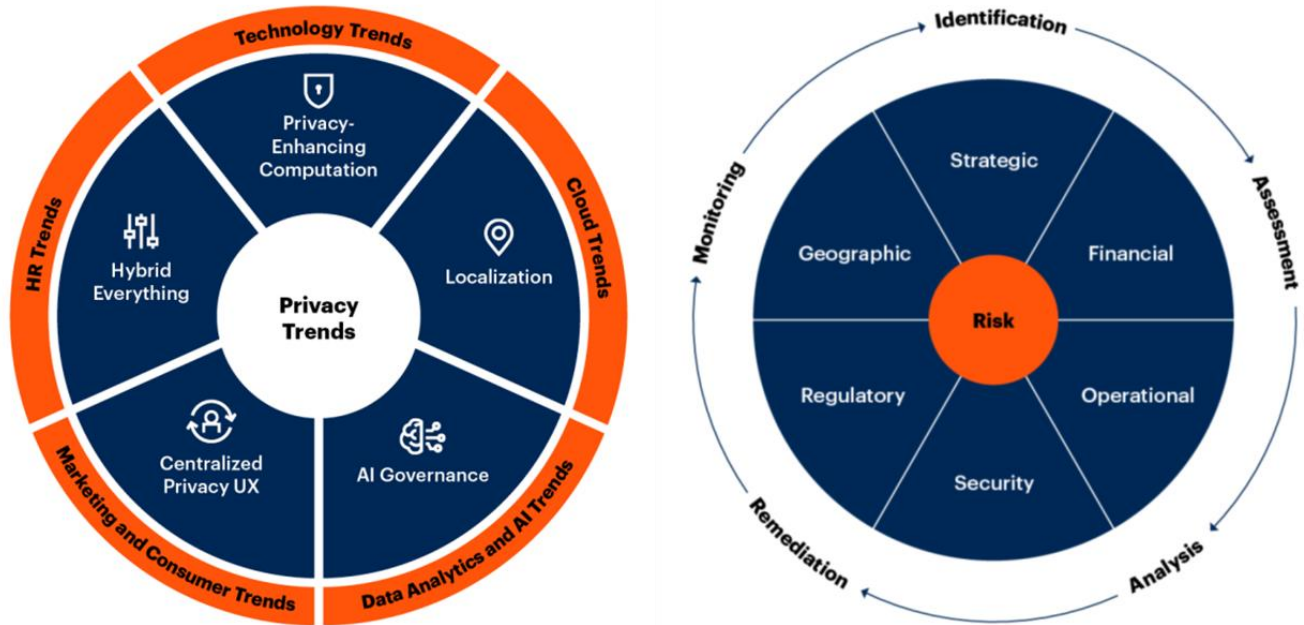
The overall DLP market is mature and is addressed by various vendors, including EDLP vendors such as Forcepoint and McAfee and several IDLP vendors such as CrowdStrike and Netskope. On the CSP side, all three major IaaS providers offer native DLP capabilities, including encryption, access permissions, and activity monitoring, as do SaaS providers such as Salesforce, Box, and others. Among the three large CSPs, Microsoft has a broad set of capabilities embedded in Exchange, Office 365, SharePoint, OneDrive, and Teams.

We expect the standalone DLP market to decline gradually and for its capabilities to blend into other security offerings. We expect: (1) cloud and email security to be the most common DLP use cases; (2) cloud-first organizations to heavily rely on CSP-native DLP and DSPM for their data security architectures; and (3) SSE and EDR vendors to continue to enhance their DLP capabilities organically and through M&A, with a focus improving integrations with other IDLP solutions. In response, we expect legacy EDLP vendors to: (1) shift toward managed DLP offerings, addressing first-time buyers within the small- and mid-sized enterprises that have limited resources and cannot maintain policy consistency, and (2) continue to add UEBA capabilities to provide improved data visibility to monitor user behavior and how data is shared, to better detect malicious behavior.

Data Privacy and Risk Management

Enterprise digitization and exhaustive user, workflow, and event data collection and analysis are significant catalysts driving improved workflow efficiency and enterprise productivity. However, they have amplified the challenges associated with data privacy, compliance, governance, and risk management, especially considering the realities of an always-connected world where a user's activity, location, and personal information can be tracked, stored, and monitored across multiple devices and applications. The growing use of generative AI and the COVID-19 pandemic have also raised questions about what constitutes responsible and ethical use of proprietary corporate data and personally identifiable user data. All of this is happening with the proliferation of distributed and hybrid work models (remote work, work from home, hybrid work, etc.), which have raised the data risk profile for all enterprises. These themes highlight the growing importance and central role data privacy and risk management fill in enterprises, as represented in Exhibit 101.

Exhibit 101: Data Privacy and Risk Management Framework



Source: Gartner (May 2022 and June 2021)

In addition to the inherent complexity of addressing new data-intensive workloads like generative AI, and managing an ever-changing workforce and the dynamic patchwork of databases and endpoints that are the foundation of organizational workflow, enterprise privacy workflows must adapt to a constantly evolving, increasingly restrictive, and geographically fragmented regulatory landscape related to personal information, data sovereignty, and international data transfers. This is coming as consumer and employee awareness and demand for privacy are rising globally and the privacy regulatory environment has fundamentally changed.

Data privacy regulations such as the European Union’s General Data Protection Regulation (GDPR), California’s California Consumer Protection Act (CCPA) / California Privacy Rights Act (CPRA), and China’s Personal Information Protection Law (PIPL) have been enacted requiring protection of individual data, data sovereignty, and restrictions on cross-border data transfers. And while GDPR is the most well-known data regulation, other regulations exist across regions and enterprise verticals (healthcare, banking, federal, etc.). Examples include Brazil’s Lei Geral de Proteção de Dados Pessoais (LGPD), India’s Personal Data Protection Bill (PDPB), Singapore’s Personal Data Protection Act (PDPA), the US Health Insurance Portability and Accountability Act (HIPAA), the US Fair Credit Reporting Act (FCRA), and the US Children’s Online Privacy Protection Act (COPPA), which can be more restrictive than the baseline requirements of GDPR. The pace of regulatory expansion has been substantial and expansive. GDPR came into effect relatively recently (May 2018). Since then, we’ve seen steady progression, with Gartner projecting that in 2024, approximately 75% of the world’s population will have its data covered under some privacy regulation.

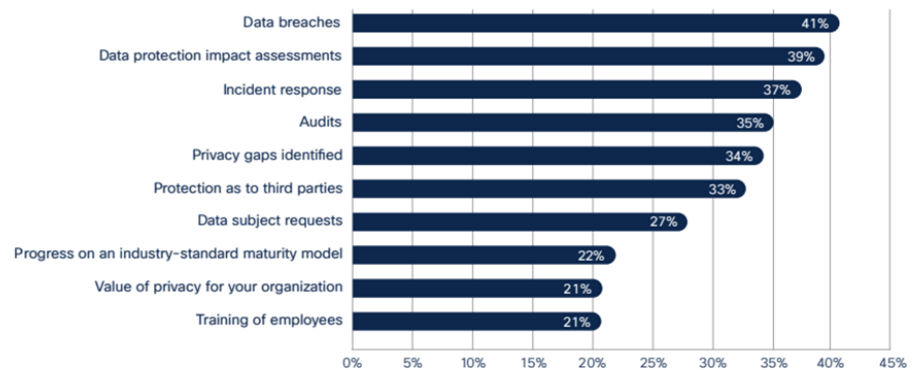
While the global regulatory frameworks are diverse, for many organizations across the globe, meeting GDPR requirements is a crucial data privacy and compliance test. As noted, GDPR is a data protection and privacy regulation for the European Union (EU) and the European Economic Area (EEA). It was adopted in 2016 and enforced in May 2018 (replacing the outdated Data Protection Directive). GDPR gives individuals control and rights over their data, including provisions and requirements for processing personal data. It addresses PII such as names, addresses, dates of birth, social security numbers, health and genetic data, racial and ethnic data, sexual orientation, and other data. It also covers data related to user location, IP address, cookies, and RFID tags. GDPR requirements are considerable and detailed in 99 articles and 173 recitals covering various requirements such as the security of personal data, records of processing activities, information access, and penalties for non-compliance. Importantly, GDPR applies to any enterprise processing

personal information of individuals inside the EEA (regardless of the data subjects' citizenship or residence). While GDPR is an EU regulation, its reach is much more significant as it has become a blueprint for similar regulation in other regions. As the UN Conference on Trade and Development research highlights, 71% of countries have privacy legislation, and another 9% have draft legislation.

Regulations will also address AI model frameworks, data use, and AI governance. The European Union Artificial Intelligence Act (EU AI Act) is poised to be the first regulation enacted to address this space. It aims to classify and regulate AI applications based on their risk of causing harm and is not intended to confer rights to individuals. This classification effort falls into three categories: banned practices, high-risk systems, and other AI systems. Similar to GDPR, we believe the EU AI Act could become a global regulatory framework leading to similar regulation in other regions, including the US, China, and India. The EU AI Act and other potential AI-related regulations would define new compliance requirements organizations must meet on top of existing data privacy and vertical-specific regulations (healthcare, banking, federal, etc.).

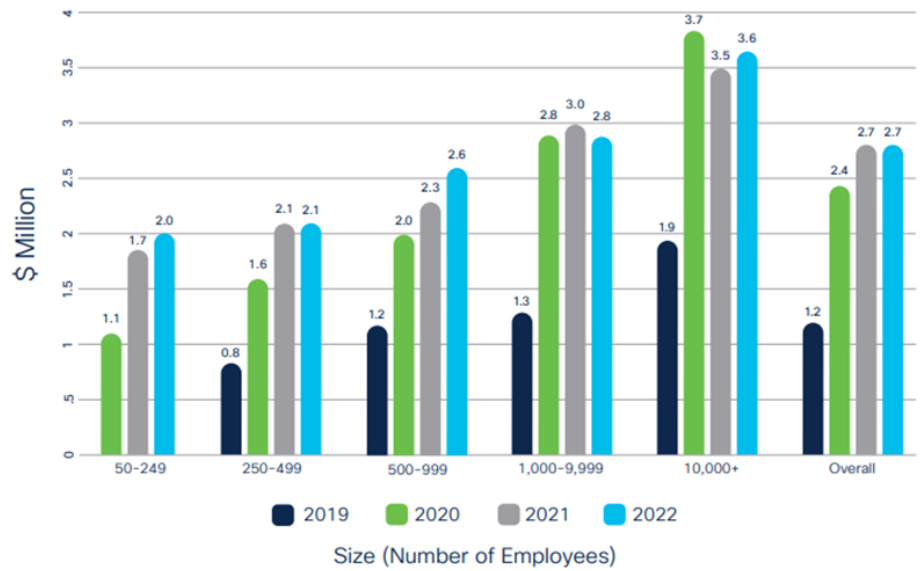
To meet data privacy regulatory requirements and to avoid punitive fines (Gartner estimates fines due to mismanagement of subject rights could top \$1 billion by 2026), organizations need to manage and monitor sensitive data for workflow, organizational location, and geographic location everywhere data is used, and work is done. The punitive and reputational exposure has raised awareness of data privacy and risk management to the highest level of company leadership (Exhibit 102). This awareness has driven substantial corporate investment in privacy-related IT infrastructure to ensure compliance. In particular, software that can automatically monitor and map an enterprise's entire data environment while constantly adapting to changing regulatory requirements has become a critical need. To put context around the size of spending already in place to ensure data privacy, we highlight Cisco's 2023 Data Privacy Benchmark Study. This study found that the average corporate privacy budget was \$2.7 million in 2022, flat YoY but up significantly from \$1.2 million in 2019 (Exhibit 103).

Exhibit 102: Privacy Metrics Reported to the Board



Source: Cisco 2023 Data Privacy Benchmark Study

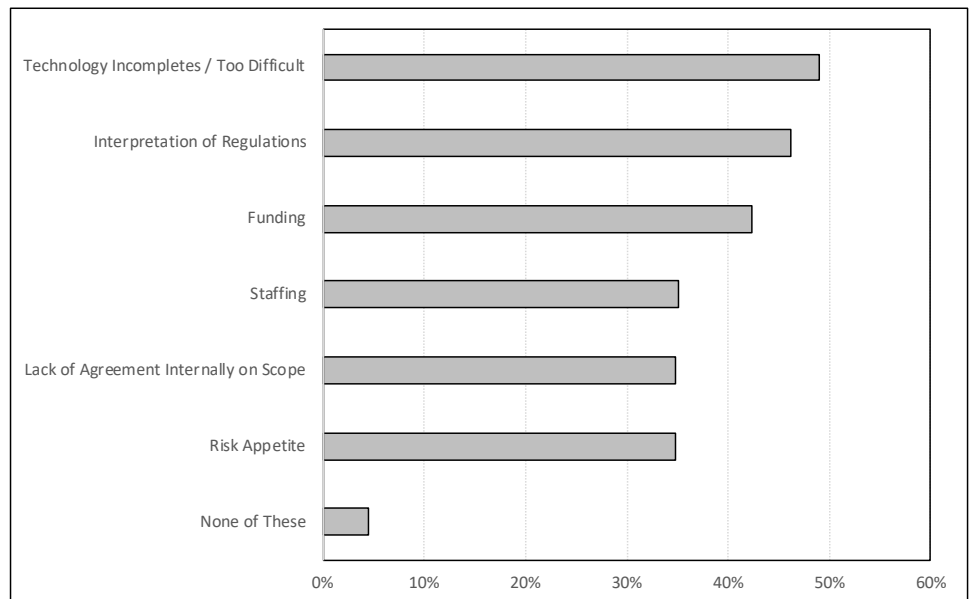
Exhibit 103: 2019-2022 Privacy Spending by Organization Size



Source: Cisco 2023 Data Privacy Benchmark Study, Note: 50-249 category initiated in 2020

Ensuring data privacy requirements are met is a cross-functional exercise that requires a coordinated response from various stakeholders in IT, cyber security, legal, compliance, and other organizations where the data resides and is managed. For enterprises with the resources, employing a dedicated team, such as a Privacy Compliance Department (note that GDPR requires a Data Protection Officer (DPO)), is the best way to manage this effort. Yet even then, the task is challenging given the technical and financial resources needed, the scope of data collected, and the infrastructure complexities noted. IDC research found (as presented in Exhibit 104) the most common challenge with respect to implementing privacy technology was the overall complexity of the endeavor and its lack of maturity (incompleteness). In addition, difficulties with interpreting the regulatory environment, staffing and funding requirements, and still developing internal plans concerning the appropriate scope and risk appetite related to data privacy have also been yet to be fully addressed.

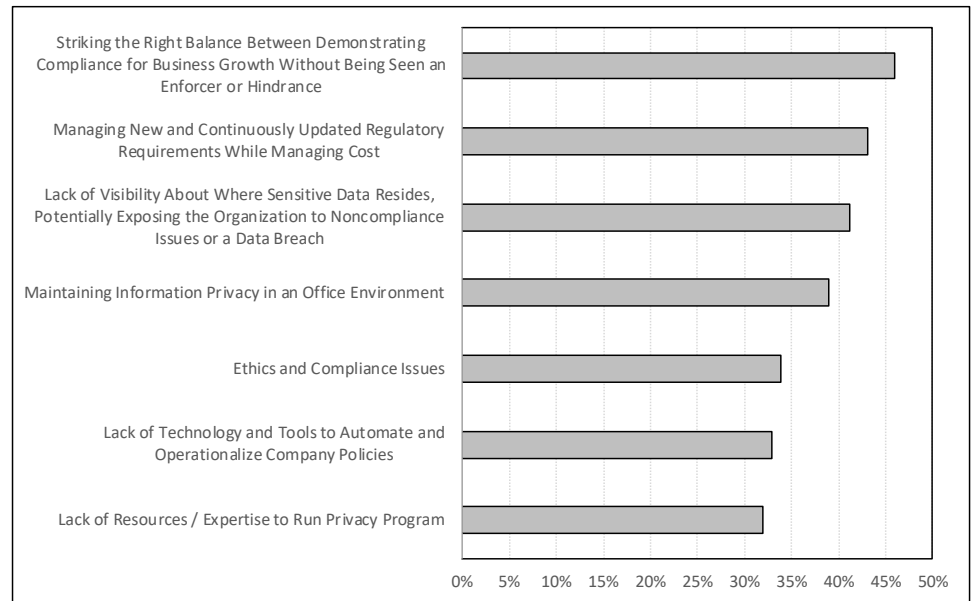
Exhibit 104: Key Challenges with Implementing Privacy Technology



Source: IDC Data Privacy Survey, December 2022 (n=316)

IDC also found that many of the implementation challenges persist after data privacy programs are launched and managed (as shown in Exhibit 105). Resources, regulations, data, and technical requirements were again highlighted as challenges. In addition, balancing the need to meet compliance without hindering business objectives and the basic ethics and compliance issues that arise from implementing a data privacy program were also noted as management challenges.

Exhibit 105: Key Challenges Related to Managing Data Privacy



Source: IDC Data Privacy Survey, December 2022 (n=316)

It's also important to consider that data privacy best practices are still developing, and those tasked with implementing these practices are often inexperienced and unaware of the nuances of the regulations involved. As a result, a mix of software tools is increasingly used to simplify and automate the data privacy process, ensuring regulations are correctly implemented and reducing the scale and data complexities involved to a human management level. Software tools can also address operational challenges related to the lack of skilled workers conversant with data privacy requirements while reducing the time and capital investment needed (labor is costly) to implement and manage a successful data privacy program.

Exhibit 106: Vendor Risk Management Solutions, Services, and Data Used to Manage Vendor Risk Efficiently



Source: Gartner (June 2021)

The first step in addressing privacy is establishing a data privacy and risk management practice that can provide visibility into the enterprise's data, where it resides, what it could be used for, and the risk exposure. This information must be correctly aligned with organizational data priorities and regulatory requirements. Currently, many enterprises don't have mature privacy workflows established, nor do they have comprehensive visibility and control of their various data silos. Many enterprises also lack proper consent and preference management and respond poorly to subject rights requests (SRR). This leaves enterprises vulnerable to user complaints, compliance risk, regulatory violations, individual and class action litigation, and reputational risk. Complicating the matter is the fact that modern enterprises need to constantly adapt to the realities of endless proliferation and growth in data volume and variety (digitization, workflows, automation, etc.), changes to the underlying technology (on-premises, cloud, SaaS, etc.), new data-intensive workloads (large language models, generative AI, etc.), and fast-evolving and complex privacy regulations (by region and vertical).

Exhibit 107: Third-Party Risk Management Solutions

Third-Party Risk Management Solutions

Governance Risk Compliance (GRC)/Vendor Risk Management (VRM) Tools			
Risk-Domain-Specific Data and Insight			
Capacity	Competition	Corporate Compliance	Data Privacy
ESG/ Sustainability	Events	Financial	Fraud and Corruption
Geographic	Import/Export and Sanctions	Operational/ Continuity	Performance
Regulatory Compliance	Security/ Cyber	Vendor Strategy	Workplace Health and Safety

Risk Exchange/ Marketplace

Source: Gartner, September 2022)

Deploying software tools that simplify, automate, and manage the data discovery process is fundamental to building a robust data privacy program. This includes the mapping, classification, and inventory of data to provide comprehensive visibility into enterprise applications, workflows, and data collected. These tools need to address core capabilities such as: (1) the collection, tracking, demonstration, and management of data subjects’ consent; (2) tracking and automatic discovery and storage of data subjects’ data; (3) the servicing of data subjects exercising their rights; (4) assessing, monitoring, and managing the progress of the privacy program activities; and (5) dash-boarding and reporting capabilities. They must also seamlessly scale across cloud and on-premises environments while constantly scanning for sensitive data on all endpoint devices. When implemented correctly, data privacy tools provide enterprises with a comprehensive data map/inventory, representing a foundation for a single source of data truth.

The adoption of dedicated software tools to address privacy and risk management use cases is still early. Historically, most privacy-aware enterprises relied on internally developed, custom-built solutions to manage their data privacy requirements. And many SMBs and smaller to mid-sized enterprises used brute force solutions, such as databases and spreadsheets, or outsourced the effort to third-party managed services companies. These legacy approaches gradually give way to modern approaches to managing data privacy, including data governance, risk, and compliance software solutions provided by vendors like RSA Archer, Galvanize, Metricstream, and IBM Open Pages. In some cases, enterprise ticketing systems by vendors like ServiceNow and Atlassian have also been repurposed for data privacy use cases. However, the fastest growing part of the market is for specifically-focused data privacy compliance and management software vendors like BigID, DataGrail, OneTrust, Securiti, TrustArc, and WireWheel, which offer a modern software-lead approach to addressing the various elements of data discovery, privacy management, and data-centric controls.

As enterprise demand for data privacy capabilities has grown, an extended market of software tools has emerged, addressing various key privacy-related capabilities and use cases. In particular, we highlight fast-paced development around (1) Data Discovery and Management, (2) Subject Rights Requests (SRRs) and Data Subject Access Requests (DSARs) Management, (3) Privacy Management, (4) Consent and Preference Management; (5) Privacy Impact Assessments and Data Protection Impact Assessments Automation, (6) Differential Privacy, and (7) Data Security Posture Management. We note that data privacy use cases often overlap with other areas, such as Data Loss Prevention

(DLP), ESG Risk Management, and the more expansive goal of ensuring Data Security. A brief description of these use cases follows.

Data Discovery

Data Discovery tools are the foundation for all data privacy initiatives and life cycle management. They scan multiple structured and unstructured data stores (in on-premises, hybrid, and cloud infrastructures) to identify, search, index, track, and analyze sensitive and regulated data. Ultimately, the data discovery process gives enterprises visibility into their data, where it is stored, and what context it is used for. This information enables enterprises to assess their data privacy posture and compliance and regulatory risk profile while feeding many more focused data privacy and security use cases. Several capabilities are closely aligned with the Data Discovery process, including Data Classification, Data Inventory, Data Flow, Data Mapping, and Data Discovery Management, as highlighted below:

- **Data Classification** tools identify and tag sensitive and regulated data across data stores and applications. This information can be used to assign and organize data into relevant categories and contexts.
- **Data Flow** tools track cross-border and organizational data transfers to ensure regulatory compliance.
- **Data Inventory** tools create a searchable index of sensitive and regulated data. They also enable an audit trail to track the date and time of changes to the data inventory.
- **Data Mapping** tools create a visual map of where sensitive and regulated data resides in an organization's data stores. They also map data for interactions across different environments.
- **Data Discovery Management** tools oversee the data discovery and classification process using the discovery results (metadata, location, volume, context, etc.) to support data management initiatives, regulatory compliance, risk management, and other use cases exposed to sensitive data.

Key vendors driving the extended Data Discovery space include ActiveNav, BigID, Concentric AI, Congruity360, Ground Labs, Netwrix, OneTrust, Securiti.ai, Spirion, and Varonis.

As noted, Data Discovery is a foundational capability powering several other data privacy use cases. Some of the more established use cases leveraging data discovery include Privacy Management, Data Security Posture Management, Privacy Impact Assessments, and Data Protection Impact Assessments.

- **Privacy Management** tools facilitate compliance insights and check processing activities against regulatory requirements. They bring structure and consistency to privacy processes and workflows while providing visibility into data flows and governance maturity. Key vendors include DataGrail, Ketch, OneTrust, Securiti, TrustArc, and WireWheel.
- **Data Security Posture Management (DSPM)** tools provide visibility into sensitive data within data stores while managing the security posture of those data stores and applications. DSPM tools can provide visibility into users' access to the data and how it has been used. Data discovery and data flow analysis are core enablers of DSPM tools. Key vendors include Concentric AI, DIG Security, Flow Security, Laminar, Polar Security, Securiti, Sentra, and Symmetry Systems. We discuss DSPM in more detail in its section within this note.
- **Privacy Impact Assessments** and **Data Protection Impact Assessments Automation** tools automate data privacy assessments while identifying and treating privacy risks. These tools ensure a controlled personal data processing environment and help organizations demonstrate control and adequate deployment of privacy and security controls. Key vendors include 2B Advice, AvePoint, Ohalo, OneTrust, and Responsum.

Rights, Consent, and Preference

In addition to data privacy technology focused on discovering, classifying, and managing sensitive data, there are several associated use cases focused on managing activity with consumers, regulators, and other interested parties with respect to sensitive data. Some

of the important use cases in this category include Subject Rights Requests (SRRs), Data Subject Access Requests (DSARs) Management, and Consent and Preference Management (CPM). There are also use cases, such as Differential Privacy, that make sensitive data available for analysis without revealing personal information.

Exhibit 108: Components of the Data Privacy User Experience

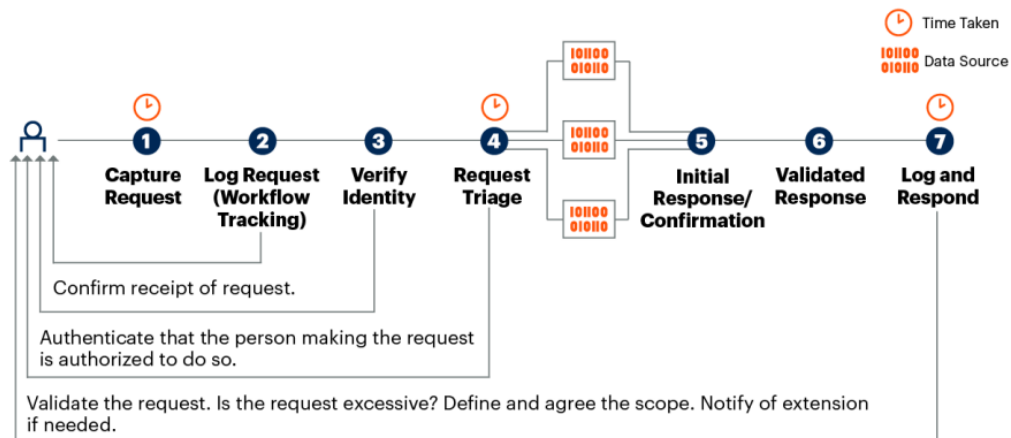


Source: Gartner (G00762813, August 2022)

- Subject Rights Requests (SRRs) and Data Subject Access Requests (DSARs) Management** tools help organizations respond to inquiries from users (consumers, employees, patients, etc.), exercising the rights for visibility into and control over their specific data. For example, a user could request information and access to what personal data is processed, who the recipients of the personal data are, how long the data will be stored, how the data is secured, and other related information. Rights could also extend to deleting and correcting the information stored, limiting the use of the data, and opting out or restricting the sale, sharing, and other uses of the data. To respond to user requests, SSR tools leverage capabilities across the entire data discovery process highlighted and automation to ensure a scalable and repeatable workflow exists to address inquiries promptly. SSR tools also need to be able to track request workflows and maintain detailed records of the requests and responses. In most cases, user requests must be addressed within a defined time frame set by various regulations (e.g., 30 days with GDPR) and are managed in three broad categories: informative, corrective, and restrictive. Informative requests provide subject access request transparency (SAR) into an individual’s personal stored data. Corrective requests allow individuals to request a change to their records (update, deletion, etc.). Restrictive requests enable individuals the ability to control how their data is used. Key vendors include DataGrail, Fair&Smart, OneTrust, Osano, Securiti, TrustArc, and WireWheel.

Exhibit 109: Request Fulfillment Must Follow a Repeatable and Scalable Process

Request Fulfillment Must Follow a Repeatable and Scalable Process



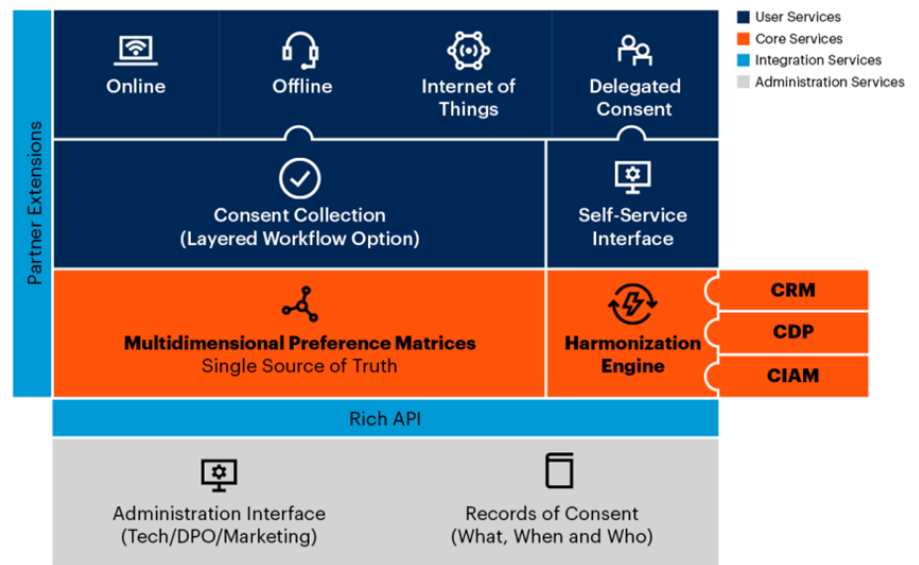
Source: Gartner (April 2023)

- Consent and Preference Management (CPM)** tools support the tracking, collection, consolidation, storage, management, and enforcement of consumer, organizational, and regulatory consent and preferences. These capabilities are an important early

step to enabling end-users visibility and control of how personal information is used and for building a single source of truth for consent across applications, data stores, and third-party affiliates. Other vital capabilities include contextual and learning consent, identity integration, administration, and synchronization of consent across multiple repositories. While the regulatory environment is expanding with respect to consent and preference management, there is still no consistent approach or industry standard in place for collecting and maintaining consent. Changes within the technology ecosystem (adtech, third-party cookies, etc.) are also driving shifts in consent and preference management. Consent and Preference Management is essential to building a robust data privacy posture and a core component for enterprises looking to provide self-service data privacy capabilities to users. This could drive increased automation, lower costs, and more self-determination for users looking to change their preferences at will. Key vendors include BigID, Crownpeak, Didomi, Ketch, OneTrust, PossibleNOW, Salesforce, SAP, Syrenis, Tealium, and TrustArc.

Exhibit 110: Consent and Preference Management Service Ecosystem

Consent and Preference Management
Service Ecosystem



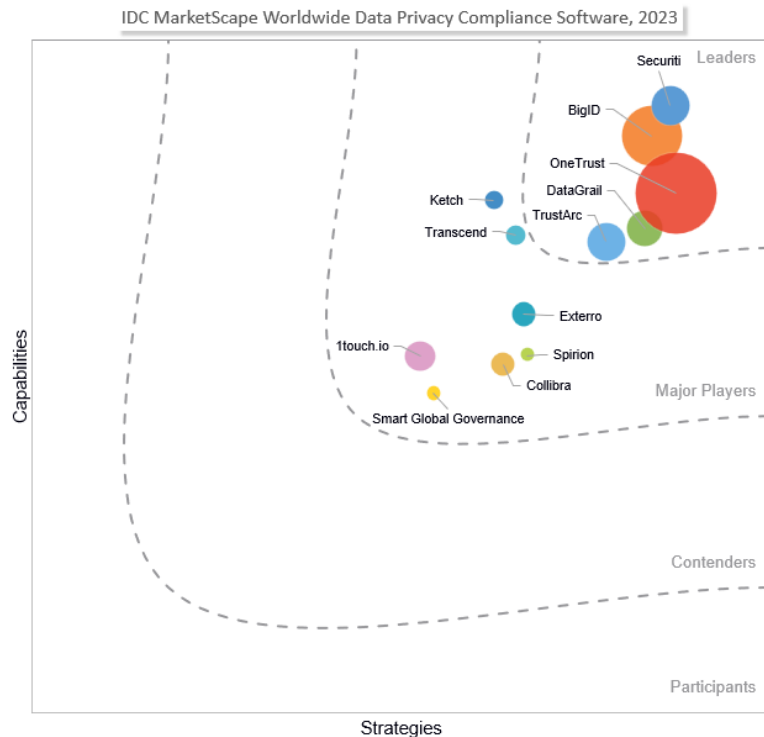
Source: Gartner (October 2022)

- Differential Privacy** tools enable the use and sharing of datasets while withholding or distorting certain information elements (about individual records in the dataset). They prevent unauthorized use or accidental disclosure of PII while ensuring any analysis done on the underlying data source does not significantly change by withholding information. As workflow digitization, ML/AI, and data sharing and analysis become commonplace, protecting data from disclosure and untrusted environments becomes critical. Differential Privacy tools help address these challenges by providing helpful information for analysis and ML/AI model building in a non-identifiable manner. Key vendors include Immuta, LeapYear, LiveRamp, PHEMI, Privitar, and Tumult Labs.
- AI Trust, Risk, and Security Management (AI TRiSM)** tools focus on the emerging AI/ML market, addressing cross-functional needs around AI model governance, trustworthiness, fairness, reliability, efficacy, and data protection. They can (1) help establish AI-related data protection and privacy assurances; (2) provide model interpretability and explainability; (3) identify and eliminate bias from training data and AI algorithms; and (4) provide visibility into data and content anomaly detection, AI data protection, and model operations. Key vendors include AIShield, Arize AI, Arthur, Fiddler, ModelOp, Modzy, MOSTLY AI, Protopia AI, SolasAI, and TrojAI.

Data Privacy, Compliance, and Governance Vendor Overview

The young data privacy management market includes a large base of emerging software vendors, including BigID (founded 2016), Collibra (2008), Drata (2020), OneTrust (2016), Securiti (2018), TrustArc (1997), and others. Across the segment, vendors continue to raise funding (OneTrust, Osano, Securiti) and be active on the acquisition front, as illustrated by Collibra's acquisition of Husprey and Osano's acquisition of WireWheel. This reflects the market's still early stage of development and vendors' effort to address a fast-moving regulatory landscape, fill capability gaps, address the fast emergence of AI, and capitalize on opportunities to move into complementary areas. We also believe it demonstrates the need to evolve toward more broadly capable and fully integrated privacy platforms that provide visibility into data sets and privacy vulnerabilities, enabling privacy controls and remediation of uncovered vulnerabilities end-to-end.

Exhibit 111: Data Privacy Compliance Software Vendor Positioning



Source: IDC

- BigID** offers an end-to-end data intelligence platform leveraging ML and graph-based technology, allowing organizations to discover, manage, protect, and govern their enterprise data. The platform is available as an on-premise and a SaaS solution and includes data privacy management capabilities, data discovery and classification, DSPM, DLP, cookie consent, audit trails, and other features. It also helps customers automate security and privacy controls and includes AI governance capabilities that leverage BigID's data discovery capabilities with ML and automated data mapping tracking. Together, these capabilities give BigID customers a comprehensive solution to control and secure their regulated, sensitive, and personal data across their entire data landscape in an approach that addresses data classification, cataloging, cluster analysis, and correlation. The platform includes bundles tailored for specific customer needs, including Data Lifecycle Management, Data Minimization, Data Rights Automation, Insider Risk Management, and Zero Trust. It also includes a growing base of integrations and is fully integrated with an automated DSAR portal, which enables BigID to manage automated rights fulfillment and ongoing deletion validation.
- Collibra** offers a broadly capable Data Intelligence Cloud platform incorporating data discovery and classification, data lineage, data governance, AI governance, data

quality and observability, data privacy compliance, and analytics. It includes dashboards, reporting capabilities, compliance health checks, and over 100 Collibra-supported out-of-the-box integrations for deeper data analysis and insight. The platform uses machine learning to better classify sensitive data and improve accuracy over time. From a data privacy perspective, the platform automates a customer's privacy operations, including support for data discovery, processing activities, documentation, data mapping, and ready-made native assessments. Collibra has also added an AI Governance product, which enables customers to extend data policies and governance to data in AI models. The platform's persona-based UI simplifies data map presentations, templates, and dashboards to present the data to stakeholders across the data privacy compliance process (data engineers, IT, legal, security, etc.), giving users the appropriate information for their roles. It also supports an open API (to connect to any data source), partner integrations, and a Collibra Marketplace. Collibra works with over 700 customers worldwide.

- **Drata** offers an all-in-one, cloud-based security, risk management, and compliance automation platform that continuously monitors and collects evidence of a customer's security controls. The platform provides a single source of audit documentation (Audit Hub); risk and policy management; security, compliance, and policy reviews (Trust Center); support for 18+ standard framework requirements (GDPR, HIPAA, CCPA, SOC 2, ISO 27001, etc.); and over 120 native integrations providing broad compliance visibility into its customers' technology stack, workflows, and processes. Custom controls and frameworks tailored to specific business needs can also be built, while professional support and an extended partner network further enhance the platform's capabilities. The company notes over 3,000 customers and over 500,000 users.
- **OneTrust** offers a broadly capable data privacy, security, risk, ethics, ESG, and Data & AI governance platform. The company's enterprise-grade Trust Intelligence Platform (including OneTrust AI Governance) provides visibility, action, and automation across privacy and data discovery, GRC, ethics, and ESG. It includes cloud services focused on (1) Privacy & Data Governance, (2) GRC & Security Assurance, (3) Ethics & Compliance, and (4) ESG & Sustainability. Together, customers gain complete data visibility and support for various capabilities such as data discovery and classification, data privacy compliance, data intelligence, data governance, compliance automation, IT and third-party risk management, and more. Pricing is flexible and includes three pricing models for large enterprises (500+ employees), growing business pricing (500 or fewer employees), and special industry pricing (education, public sector, non-profit). Customers can buy OneTrust as SaaS or deploy it as an on-premises solution or on their cloud infrastructure. The company has over 2,000 employees and notes over 14,000 active customers.
- **Securiti's** data privacy platform acts as a comprehensive Data Command Center, enabling the safe use of data and AI. The platform includes a suite of data privacy, security, governance, and compliance solutions, reporting, and dashboard capabilities. Securiti automates and orchestrates much of the privacy compliance process, including DSR automation and end-to-end automation for SRRs; and addresses asset and data discovery, data mapping, assessment automation, vendor assessment, breach management, data consent automation, third party and cookie consent, and more. The platform leverages hundreds of data connectors and data types paired with Securiti's proprietary AI/ML capabilities, enabling it to automate across key data privacy compliance requirements for (GDPR, CCPA/CPRA, PIPL, etc.). Securiti offers its platform as a SaaS, hybrid, or sovereign deployment model and can manage data wherever it resides (on-premises, multi-cloud, and in other SaaS applications).
- **TrustArc** is one of the earliest vendors focused explicitly on the data privacy market. The company initially focused on certifying the privacy practices of other vendors but, over time, transitioned to providing comprehensive privacy solutions enabling continuous compliance, information governance, and data security. TrustArc's data privacy platform includes products addressing Consent & Consumer Rights, Privacy Governance & Data Operations, and Assurance & Certifications. The platform handles data privacy impact assessments, DSARs, cookie consent, consent and

preference management, individual rights management, data inventory and risk profile assessment, and more. TrustArc makes it easy for customers to demonstrate data privacy compliance (GDPR, CCPA/CPRA, PIPL, etc.) and has a deep regulatory library with change management capabilities. TrustArc supports over 1,500 companies.

Identity & Access Management

IAM refers to policies and technologies for managing digital identities and user access to an organization's data, systems, and resources. IAM tools reduce identity-related access risks and ensure that the right individuals access the right resources within the proper context. This is achieved by authenticating and authorizing network users and protecting digital resources. The technologies used in IAM go beyond traditional username and password approaches and include more modern techniques and technologies such as single sign-on (SSO), federated identity, multi-factor authentication (MFA), anomaly detection, and more. It's important to note that these technologies can be applied to different users, such as the workforce, customers, and business partners.

Since humans started communicating, there's been a need to protect and control access to information. The essential components of that control were much the same as they are today: establishing who you are when you try to access systems, applications, and information (i.e., authentication) and determining whether you can access a specific resource or take a particular action once you are authenticated (i.e., authorization). Authentication and authorization remain the core foundational principles of modern-day IAM tools and are incorporated into every access technology. Below, we offer a more detailed definition of both.

- **Authentication** is verifying that users are who they claim to be. Traditionally, this has been accomplished with a username and password, yet in recent years, authentication has expanded to include fingerprint matching, facial recognition, tokens, and multi-factor authentication.
- **Authorization** is determining what resources an authenticated user can access. This is typically accomplished through maintaining detailed lists and directories of all users and the resources they are authorized to access. Single sign-on refers to an authorized user's ability to access accounts after logging in via a central directory.

Looking back, networked computing emerged in the 1960s. At the time, organizations relied on a simple username and password combination as the primary technology for authentication. Knowledge of login credentials was the only requirement for authentication, and with a self-declared password, users gained complete access to internal resources. Each access request was checked against predefined access control lists (ACLs) and directories for authorization. IAM systems at the time commonly consisted of raw spreadsheets, long email chains, and more traditional methods to track and record user accounts, passwords, and access entitlements.

Through the 1990s, companies commonly used username/password combinations for authentication and spreadsheets and ACLs for authorization, as most data was kept behind network firewalls. Yet, as: (1) enterprises expanded globally, (2) the number of employees and devices increased, (3) third-party vendors, partners, and customers increasingly gained external access to corporate resources, and (4) applications gradually moved beyond and outside the traditional network perimeter, IAM systems became more complex and time-consuming to manage, and IT professionals faced the challenge of providing granular access control without inhibiting efficiency and productivity. Adding to the complexity was increased regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and various other regulations introduced in the 1990s and early 2000s. Overall, it became clear that the IAM market needed to evolve beyond the traditional methods available.

In recent years, we've seen: (1) the adoption of more modern authentication and authorization technologies such as biometrics, iris scanning, and facial recognition; (2) the introduction of new access control models such as role-based access control (RBAC—access depending on role of a user within the enterprise) and attribute-based access control (ABAC—access based on a combination of attributes (user, resources, location,

etc.); (3) use of risk-based authentication integrating risk scoring and machine learning into the authentication process; and (4) implementation of task automation throughout the identity lifecycle, centralizing provisioning and enforcing access controls. Lastly, we note the adoption of cloud-based Identify-as-a-Service (IDaaS) or IAMaaS solutions, which provide identity-based security that is persistent, perimeter-less, and context-aware.

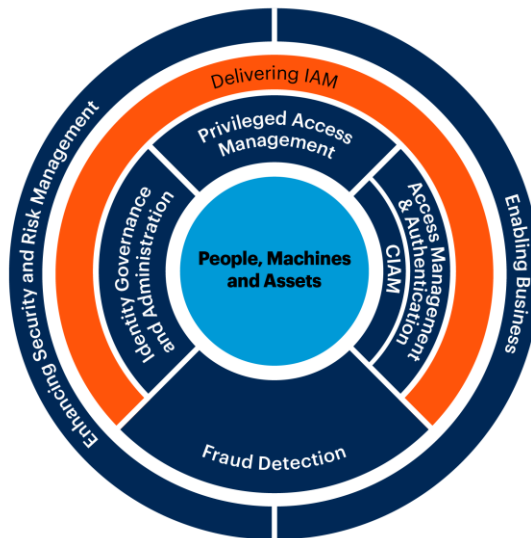
While access management remains a central element in the IAM market, tool categories have surfaced to address distinct, complex, and evolving enterprise needs—specifically, Identity Governance & Administration (IGA) and Privileged Access Management (PAM) tools. Below, we briefly discuss these tool categories. A more detailed discussion on each is included later in the report.

- **IGA.** The IGA market emerged from consolidating traditional user administration and provisioning (UAP) and identity and access governance (IAG) tools. IGA tools work hand in hand with access management tools and commonly: (1) offer a policy-based approach and a centralized orchestration framework to digital identity and access control; (2) help automate workflows for provisioning/de-provisioning users (life cycle management), and (3) offer support in auditing and meeting compliance requirements.
- **PAM.** The PAM market addresses the need to protect against credential theft and privilege misuse (intentional or accidental). PAM tools are based on the least privilege concept and enable organizations to secure highly sensitive accounts with elevated access to corporate resources (IT, data, etc.) above a standard user. Misusing such privileged accounts can have a detrimental effect on a company’s operations. It’s important to note that privileged access can be associated with human users (IT administrator accounts, domain admin accounts, etc.) and non-human users (applications accounts, secrets, etc.).

The following sections review the three main sub-segments of the IAM market. These are (1) Access Management Software, (2) Identity Governance and Administration Software (IGA), and (3) Privileged Access Management Software (PAM). We will also review the emerging Passwordless Authentication, Cloud Infrastructure Entitlement Management (CIEM), and Secrets Management markets.

Exhibit 112: Identity & Access Management Work in Conjunction

Identity and Access Management and Fraud Detection



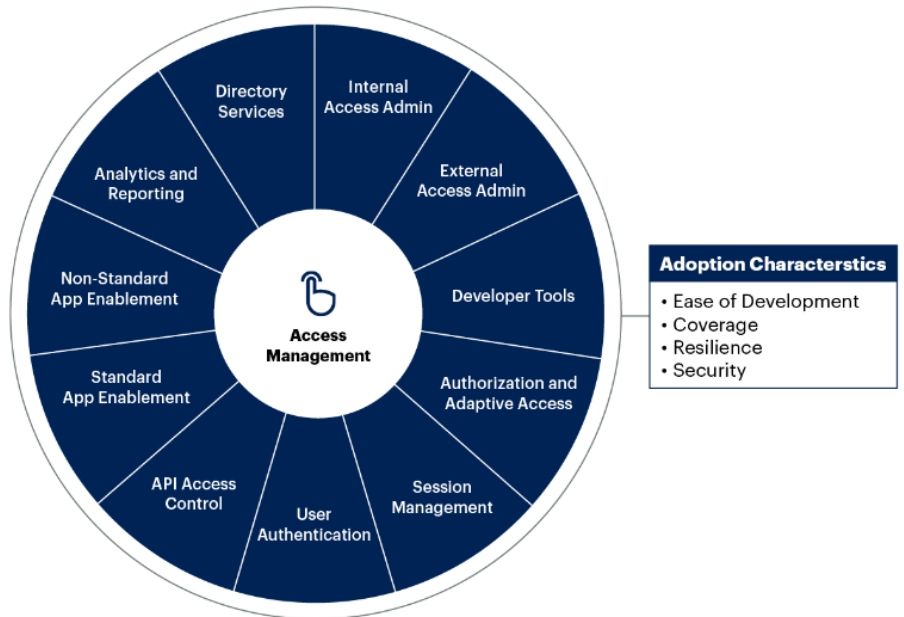
Source: Gartner

Access Management (AM)

Access management tools focus on delivering real-time access control to applications and data through the authentication and authorization of users. Given the complex threat landscape and the number of sophisticated identity-based attacks, organizations are implementing more sophisticated methods of authentication that go beyond traditional username and password combinations. Typical access management solutions today include SSO, MFA, directory, data governance, and API security. AM solutions work with IGA solutions and provide user authentication, trust elevation, risk mitigation, SSO, session management, and authorization decisions.

Exhibit 113: Access Management Core Capabilities

Access Management Offerings

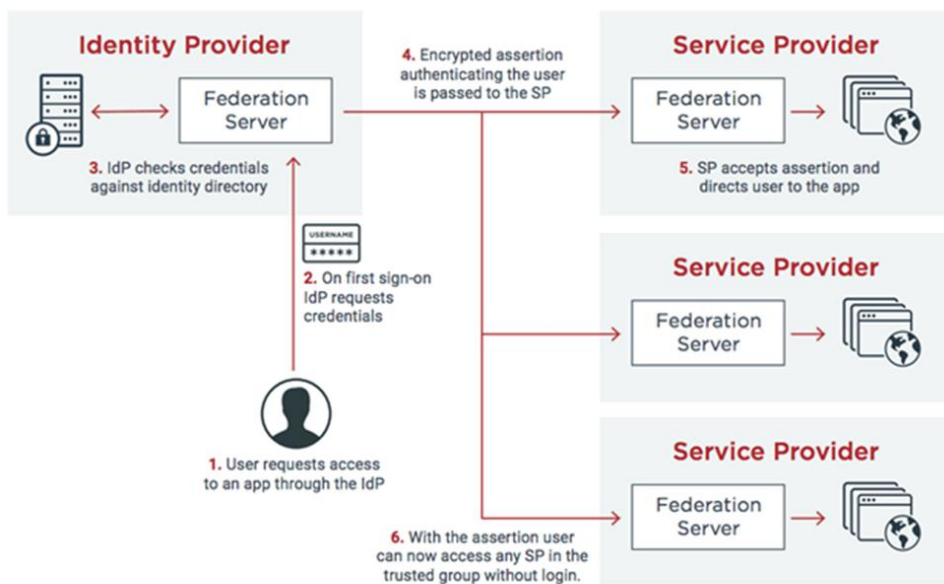


Source: Gartner

SSO allows users access to all entitled applications via a central directory, eliminating the need to sign in again when switching between applications. With SSO, users only need one set of credentials, eliminating the need to remember and track multiple usernames and password combinations. When a user signs in to an application using SSO, an authentication token that contains information about the user (such as email address) is sent to the identity provider delivering the SSO service and is stored in the user’s browser or the identity provider’s servers. When the user attempts to sign into any other related application, their identity is automatically authenticated using the authentication token, eliminating the need to go through the sign-in process again. SSO solutions provide session management, which relies on cookies and security tokens to terminate web sessions after a certain period of inactivity. This limits the time window when potential attackers could access sensitive information.

Traditional SSO was built for use within a single organization, allowing users to access multiple internal applications using a single set of corporate login credentials. Federated Identity Management (FIM) solutions take this further and rely on a trust relationship between different organizations to authorize each other’s users. This enables users to access multiple applications in various organizations with one set of credentials. For example, Gmail login credentials can be used to sign into another application, like Spotify. Exhibit 114 illustrates how federated SSO is achieved.

Exhibit 114: Federated SSO



Source: Ping Identity

FIM makes use of three standard identity protocols: (1) Security Assertion Markup Language (SAML), (2) OAuth 2.0 (Open Authorization), and (3) OpenID Connect (OIDC).

- SAML.** A long-standing XML-based identity protocol dating back to 2001. SAML defines three roles in the authentication and authorization process: (1) the user looking to verify identity (principal); (2) the user's organization or third-party identity vendor (identity provider (IdP)); and (3) the application the principal is seeking to access (service provider). Once the principal authenticates with the IdP, the IdP passes a SAML assertion to the SP to complete authentication.
- OAuth 2.0.** An identity standard protocol that focuses on client developer simplicity. It is essentially an authorization framework for APIs that enables applications to obtain limited access to users' data, known as scopes, to verify their identity. After authenticating identity with an application, the user consents to any subsequent API they seek to access, which then verifies the user's identity using scopes. OAuth 2.1 is in progress and attempts to consolidate and simplify the most commonly used features of OAuth 2.0.
- OIDC.** A protocol that sits on top of OAuth 2.0, adding an authentication protocol that provides additional information in conveying the identity of an end-user. After a user authorizes an application's request for information from the OAuth flow, OIDC sends an access token and an ID token that carries information about the user to the OAuth authorization server, which authorizes the user for access.

MFA is another standard AM solution providing an additional security layer beyond the traditional username and password approach. MFA requires users to provide two (and increasingly more) verification factors to gain access to applications, accounts, or even a VPN. MFA typically demands different types of information to validate a user's identity: knowledge (passwords and PINs), possession (smartphones), and biometrics (fingerprints and voice recognition). MFA methods include one-time passwords, SMS messages, push notifications, automated calls, and biometrics.

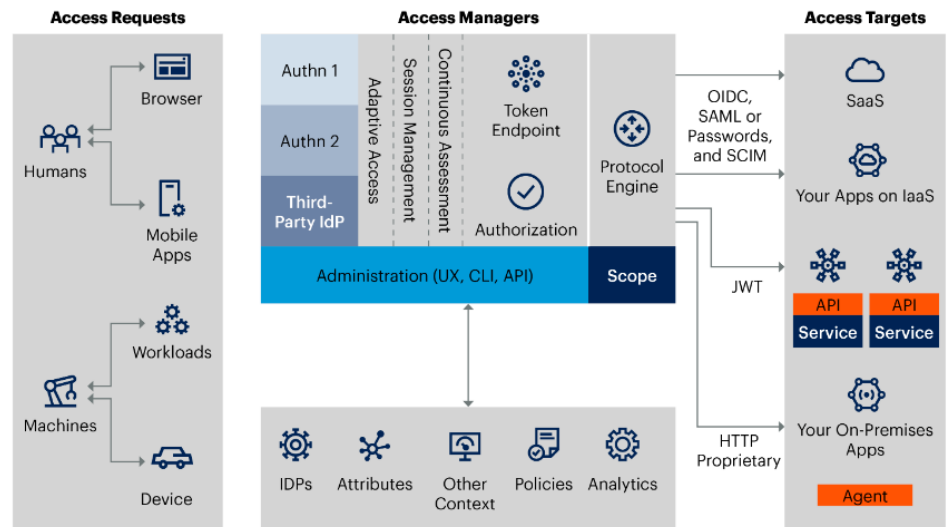
The focus on streamlined and straightforward login experiences has also led to the emergence of passwordless authentication solutions. These solutions rely on the native biometric data stored on a user's mobile device for authentication and improve user experience and security by reducing authentication time and removing the risk of

compromised passwords, the most significant vulnerability risk associated with authentication methods like SSO and MFA. Passwordless authentication also benefits CIAM use cases by eliminating registration fatigue and improving customer experience. While usage of passwordless authentication is currently limited, Gartner estimates that 50% of the workforce and 20% of customer authentication transactions will be passwordless by 2025.

While SSO and MFA are standard AM solutions, the market encompasses other core capabilities such as directory stores, access governance, and API access management.

- Directory stores are a central repository of login credentials, data and privacy consents, and preferences for each user profile, and they enable easy provisioning and management when onboarding new users. Like Okta’s Universal Directory, many directory solutions centralize user management, allowing IT administrators to assemble user profiles with attributes from multiple identity sources, manage lifecycle states, and set consistent user access policies based on different user contexts (location, IP, device, etc.).
- Access governance solutions provide a layer of authentication and authorization to sensitive information, such as customer and user data, facilitating compliance with data privacy regulations such as HIPAA and GDPR. These tools provide IT administrators with a centralized and detailed view of each user’s access entitlements and a comprehensive organization-level view.
- API access management allows companies to extend consistent access policies to APIs, allowing authentication and authorization of API calls. These solutions provide organizations with a centralized platform that combines security and development into a single view, streamlining policy creation and enabling development teams to offload user management and authorization policy decisions to IT admins.

Exhibit 115: Access Management Conceptual Architecture



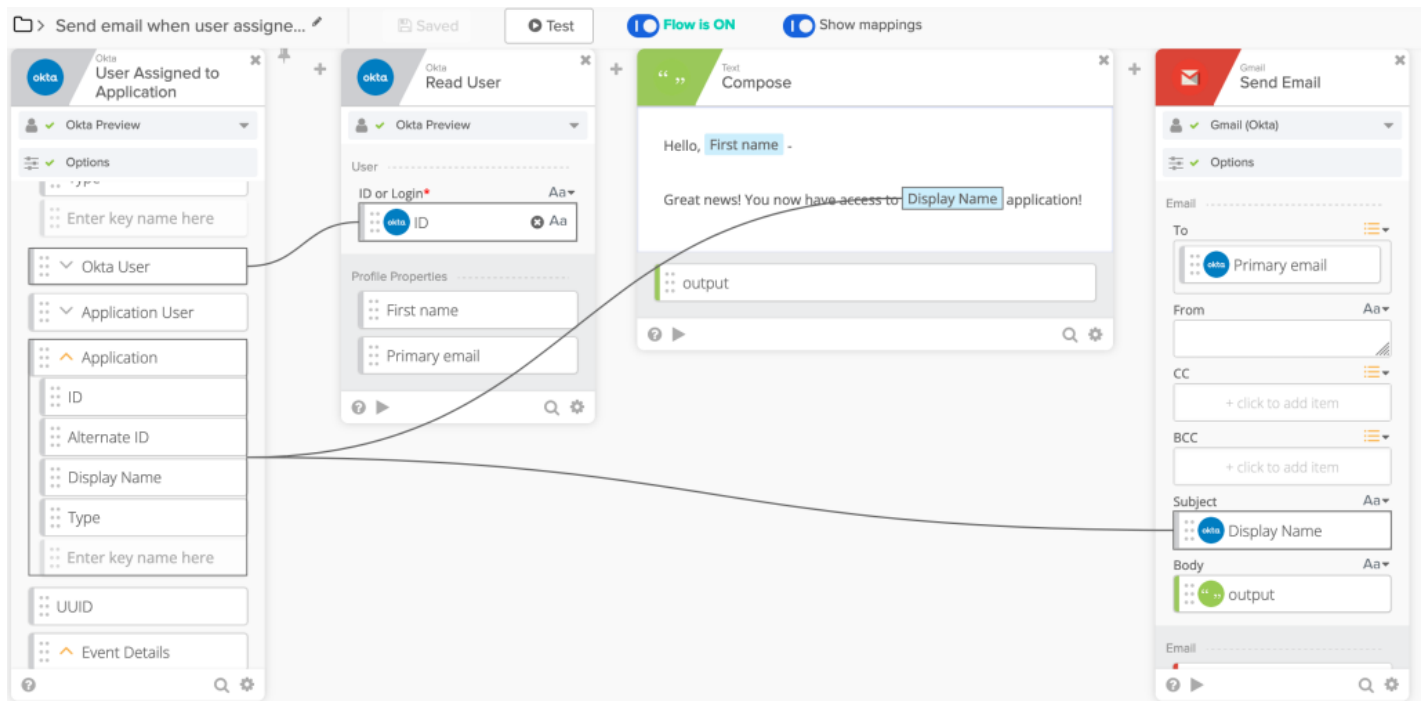
Source: Gartner

Recently, new AM capabilities emerged as points of differentiation between the various AM vendors that may not be available consistently across every IdP. These advanced capabilities include machine identity management, advanced session analytics and user & entity behavior analytics (UEBA), bring your own identity (BYOI), and low-code/no-code identity orchestration.

- Machine identity deals with AM for non-human entities such as bots, workloads (including virtual machines and containers), Internet of Things (IoT) devices, and various endpoint devices.

- Analytics capabilities around sessions include historical data reports, logs, access, and identity analytics. These analytics can also overlap with UEBA capabilities (a separate feature), which analyze individual historical user/entity behavior against baseline behavior that has been previously exhibited.
- BYOI is a type of federated SSO where a user signs on with an independent third party (such as Apple, Microsoft, Google IDs, etc.) to gain access across various applications.
- Identity orchestration, which effectively provides consistent access to users across applications in a hybrid and multi-cloud environment, applying user policies across the board and managing access management tool sprawl by integrating with disparate external IAM tools (such as authentication, identity proofing, fraud detection, etc.). These solutions are typically low-code/no-code in nature and provide a visual interface with the entire user interface and a workflow mapped out graphically. Gartner estimates that low-code/no-code identity orchestration will become a core capability for all AM vendors by 2024.

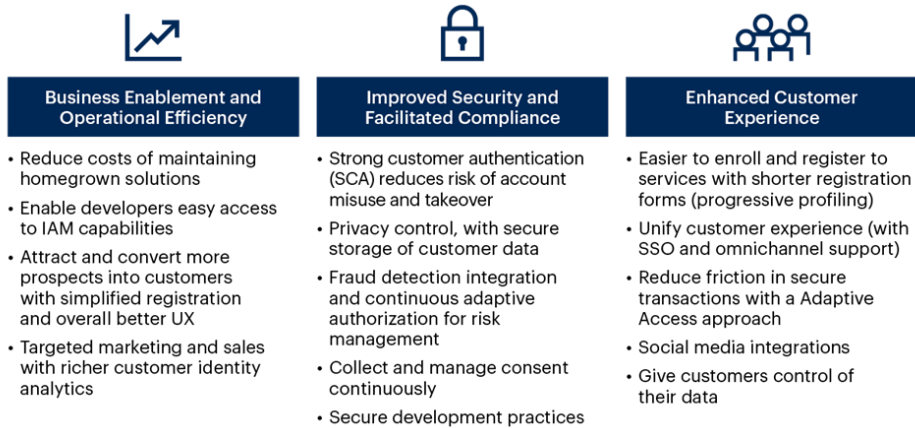
Exhibit 116: Okta Workflows—Identity Automation and Orchestration



Source: Okta

The solutions we've reviewed focus on securing and managing workforce identities. However, in recent years, vendors and organizations have extended these concepts to customer identity. This new use case, Customer Identity and Access Management (CIAM) is vital for organizations looking to create secure, seamless customer experiences within their public customer-facing applications. As more companies invest and expand their customer digital engagement footprint, the complexity of privacy requirements (HIPAA, GDPR, CCPA) increases, and the number of high-value digital transactions rises, adding complexity and risks. CIAM solutions are gradually becoming necessary for organizations looking to improve their user experience (UX) and provide a secure digital experience and engagement with their customer base.

Exhibit 117: Key Business Benefits of CIAM Technologies



Source: Gartner

A common way to address CIAM involves a Bring Your Own Identity (BYOI) approach, which allows customers to use social media identity to create an account. BYOI, a form of federated identity, allows customers to register with multiple websites and applications using a single social media account. The social media host (usually Facebook, LinkedIn, Twitter, or Gmail) acts as the identity provider. By applying BYOI in the registration process, organizations can eliminate friction and enable customers to seamlessly create an account without generating separate credentials. CIAM leverages many of the same capabilities as workforce AM to deliver on this, including MFA, SSO, password management, and API access management.

Exhibit 118: CIAM and IAM Capability Overlap



Source: Gartner

While most AM solutions were historically deployed on-premise, organizations have increasingly adopted cloud-based AM solutions (Identity-as-a-Service (IDaaS)). This shift has occurred as more applications shift to the cloud and employees move to work from anywhere and increasingly engage with cloud-based SaaS applications. Today, IDaaS is the preferred deployment model for AM. With IDaaS, remote employees no longer need to send authentication requests for cloud-based applications back to the corporate data center. Instead, requests are sent directly to the cloud where the applications reside. IDaaS solutions also offer organizations cost savings and reduced complexity. They

remove hardware expenses and simplify IT management, making for an easy implementation process, faster time-to-value, and lower total cost of ownership. Gartner estimates that 80% of new AM purchases were SaaS-delivered in 2022, up from 20% in 2019. And with the ongoing persistence of remote/hybrid work since COVID-19, we expect the cloud-delivered AM to become the default method of delivering identity management.

Fraud Detection

CIAM vendors have recently expanded their offerings to address fraud detection use cases. Fraud detection was historically focused on protecting digital channels (primarily browsers and mobile applications) with a particular emphasis on preventing malicious bot activity. As the threat landscape evolved, organizations needed to protect against human threat actors from gaining unauthorized account access and stealing funds or PII data. CIAM vendors have stepped in with capabilities such as identity proofing & affirmation and account takeover (ATO) protection, which are increasingly becoming the focal point of fraud detection programs.

Identity proofing & affirmation focuses on: (1) confirming the existence of a real-world identity; and (2) confirming that the individual claiming the identity is the true owner. Identity proofing technologies secure account openings, registration processes, and application enrollments. The most common method for identity proofing is a document-centric approach (aka "ID plus selfie"), which tests for genuine human presence by asking an individual to provide an image or video of a form of ID (passport, driver's license, etc.) and themselves. Once collected, the identity affirmation process checks the identity data (name, address, phone number, DOB) against public data sources (electoral records, credit bureau data, census information). Many vendors also analyze device information and location data to prove and affirm identities.

Exhibit 119: Identity Proofing and Affirmation Capabilities



Source: Gartner

CIAM vendors' role in governing the account creation process often makes them a target for ATO attacks. In response, many CIAM vendors have introduced capabilities such as journey-time orchestration (JTO) that analyzes contextual signals from various points of the account creation & access process to map the user journey and detect takeover attacks. These signals include device IDs & telemetry, IP addresses, and behavioral biometrics (user keystrokes, mouse movements, typing speed, etc.). Once mapped, JTO solutions monitor for anomalies in behavior and then trigger actions such as requiring further authentication or declining access altogether.

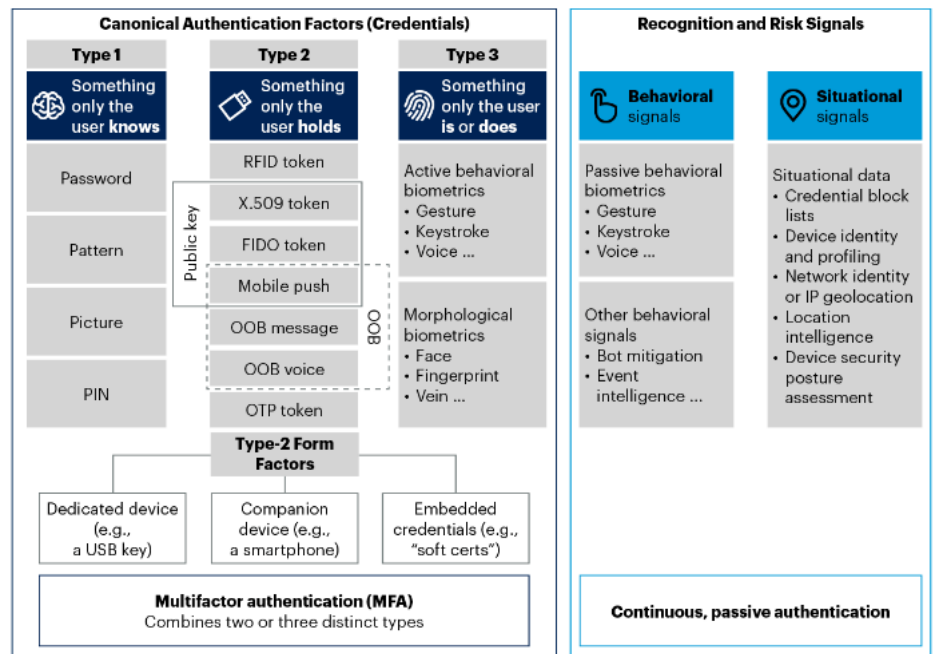
Looking ahead, we expect CIAM vendors to add fraud detection capabilities to further differentiate their offerings. We expect vendors to focus on adding orchestration capabilities to manage risks across the entire customer journey and not just at account creation. Ping Identity, for example, has acquired orchestration vendor Singular Key, and we expect more CIAM/IAM vendors to leverage M&A to expand into fraud detection. Lastly, we expect more CIAM vendors to integrate with bot management/mitigation vendors to prevent automated ATO attacks.

Passwordless Authentication

According to Gartner, compromised passwords make up more than 60% of breaches (due to hacking) and result in account takeover or digital identity risk. While some technologies, such as MFA, attempt to mitigate this risk, its implementation adds friction to the access process and undermines the user experience on the platform. This is a much more significant factor for CIAM than workforce identity access. Organizations are increasingly adopting passwordless authentication capabilities to improve the user experience while still maintaining a high level of secure access management capabilities.

Passwordless authentication is a methodology that uses a combination of credentials or signals to verify a user without using passwords. These can include Type 1 (something the user knows) authentication such as Patterns, Picture, or PIN; Type 2 (something the user holds) authentication such as non-standard token, public-key tokens, out-of-box (OOB) authentication, or one-time-password (OTP) tokens; or Type 3 (something the user is or does) authentication such as biometrics or behavior, and Recognition, Situation, and Risk Signals such as contextual device data, behavior analytics, and knowledge-based verification. Passwordless authentication in an MFA format that uses a combination of these authentications to verify the user and grant access.

Exhibit 120: Taxonomy of User Authentication



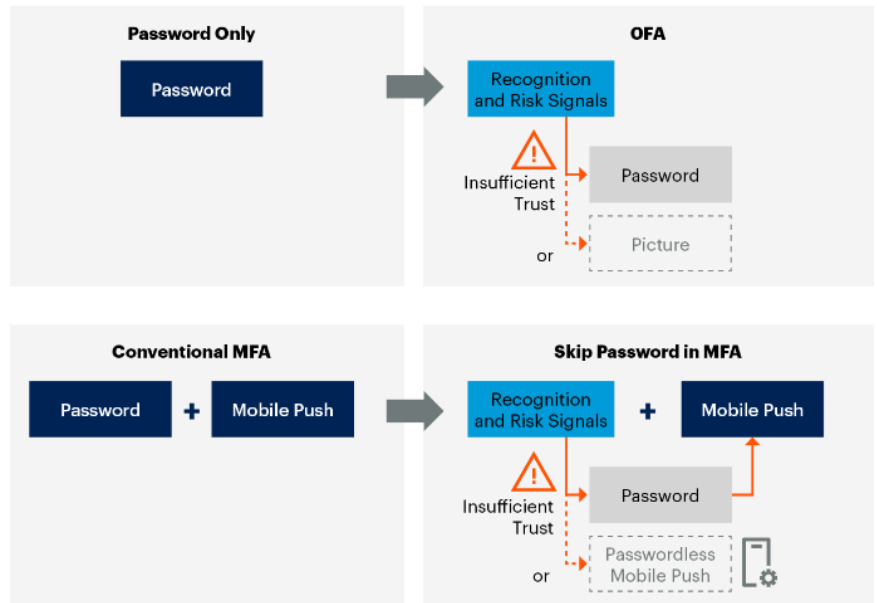
Source: Gartner

There are currently four popular approaches to passwordless authentication:

- (1) Windows Hello for Business – Based on the FIDO2 standard, it uses a combination of local authentication (biometrics and/or PIN) and embedded public-key credentials. This approach is available on all PCs with Windows 10 or later software. When using Azure AD, users must enroll in Azure MFA and can use Azure AD Conditional Access through a synchronized account.
- (2) Phone-as-a-token or Mobile MFA – Is a widely used methodology to verify workforce and customer identities. It utilizes an OTP message through SMS or a mobile push. Additional verification, such as Apple Touch ID or Face ID, can be used for MFA.
- (3) Magic links – Some AM vendors provide out-of-box authentications via emails or SMS links rather than OTPs.

- (4) Signals-first authentication flows – Recognition and risk signals are first used to skip the password stage. If there is insufficient trust via signals, then a password may be required. This is not a complete “passwordless” approach.

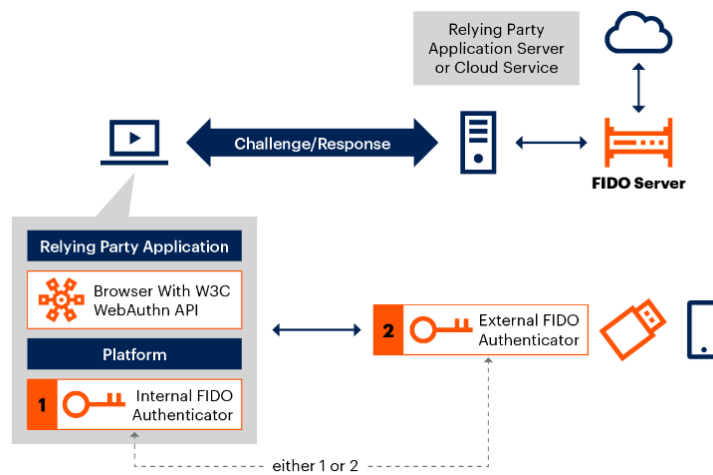
Exhibit 121: Signals-First Authentication Flows



Source: Gartner

FIDO2 authentication – Is a passwordless authentication method, and the latest specification of the FIDO Alliance (Fast Identity Online) which uses 2FA with security keys to authenticate users. It comprises the Client to Authenticator Protocol (CTAP) and W3C standard WebAuthn and utilizes credential authenticators such as biometrics and PINs, or FIDO keys, to connect to a WebAuthn remote peer (website or application). Gartner estimates that FIDO2 will be the dominant authentication token for passwordless workforce identity verification and will see more than 25% adoption in the next three years.

Exhibit 122: FIDO2 Authenticators



Source: Gartner

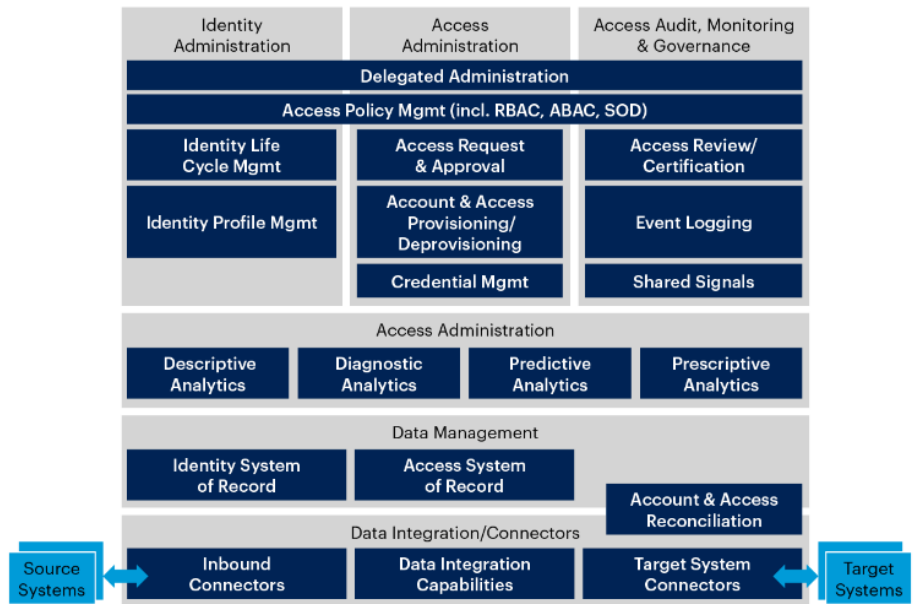
Overall, the use of passwordless authentication continues to increase, and Gartner estimates that over 50% of the workforce and over 20% of customer authentication will be passwordless by 2025, up from less than 10% today.

Identity Governance & Administration (IGA)

IGA is a policy framework and security solutions that enable digital identities and access rights management across disparate enterprise systems. IGA tools achieve this by automating the creation, management, and certification of user accounts, roles, and access rights and aggregating and correlating disparate identity and entitlement data from the entire IT landscape. When implemented, IGA tools give IT administrators a comprehensive view of the various digital identities within their organization and streamline user provisioning, password management, policy management, access governance, and access reviews. As a core building block of the IAM architecture, IGA helps organizations improve identity process maturity, ensure regulatory compliance, and reduce the risk of unauthorized access. Essential IGA functions include identity lifecycle management, entitlement management, access requests and certification, policy and role management, segregation of duty (SOD) controls, workflow orchestration, auditing, and identity analytics and reporting.

Exhibit 123: IGA Capabilities

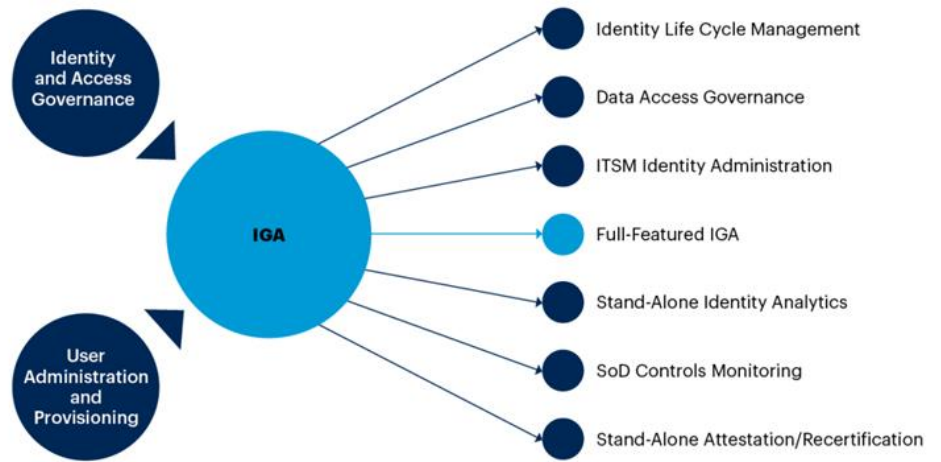
How IGA Capabilities Fit Together



Source: Gartner

The IGA market developed a few years ago when user administration and provisioning (UAP) capabilities were gradually blended with identity and access governance (IAG) tools, a process led by IAG (SailPoint) and UAP (IBM) vendors. While almost every company has some IGA processes in place (vendor-based or home-grown manual process), they are more commonly used by mid-sized to large enterprises as they offer more value in large and complex organizations with multiple departments and disparate systems requiring mature and well-staffed IAM programs. IGA tools have a distinct purpose within the overall IAM suite: defining and enforcing IAM policies and ensuring IAM functions meet audit and compliance requirements. IGA is typically the most complex component within IAM architectures and is time-consuming to implement, given the amount of integration, customization, and executive approvals necessary. Consequently, organizations often rely on third-party professional services for deployment and SaaS IGA solutions.

Exhibit 124: UAP and IAG Convergence

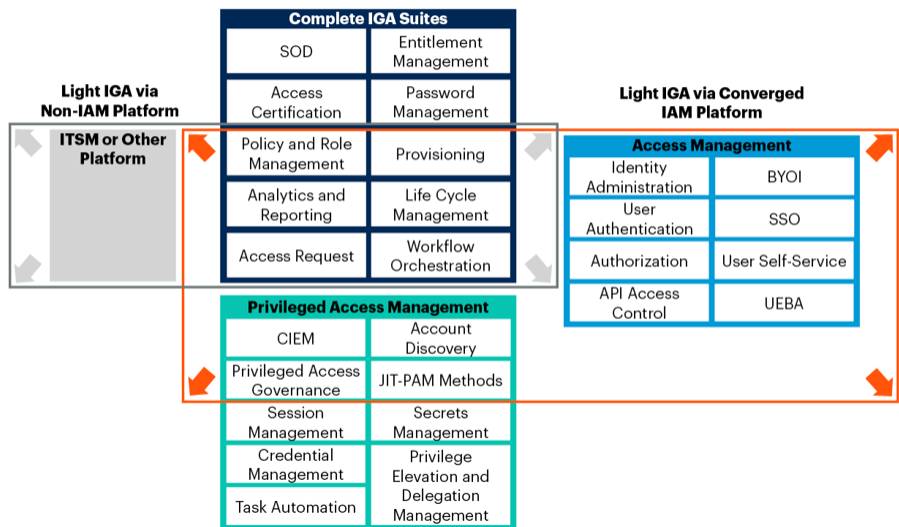


Source: Gartner

The IGA market is considered mature, with little differentiation between the vendors from a feature development standpoint. As a result, most new sales are brownfield deployments with innovative solutions such as predictive governance and identity analytics, driving higher win rates. To differentiate, IGA vendors have shifted to adjacent opportunities. Saviynt has added PAM capabilities, and SailPoint has added cloud security capabilities. A shift to the cloud has also gained momentum, offering easier deployment and a lower total cost of ownership. SaaS-delivered IAM platforms offering a converged access management and IGA solution or a converged PAM and IGA solution are also gaining interest, especially among smaller organizations with less complex IGA needs. To reduce cost, such organizations are increasingly shifting toward “IGA-light” deployments that include basic capabilities, such as segregation of duties (SOD) monitoring, identity life cycle management, and attestation/recertification.

Exhibit 125: Light IGA vs. Platform-Based IGA Solutions

Comparison of Complete IGA Suites With Light, Platform-Based IGA Solutions



Source: Gartner

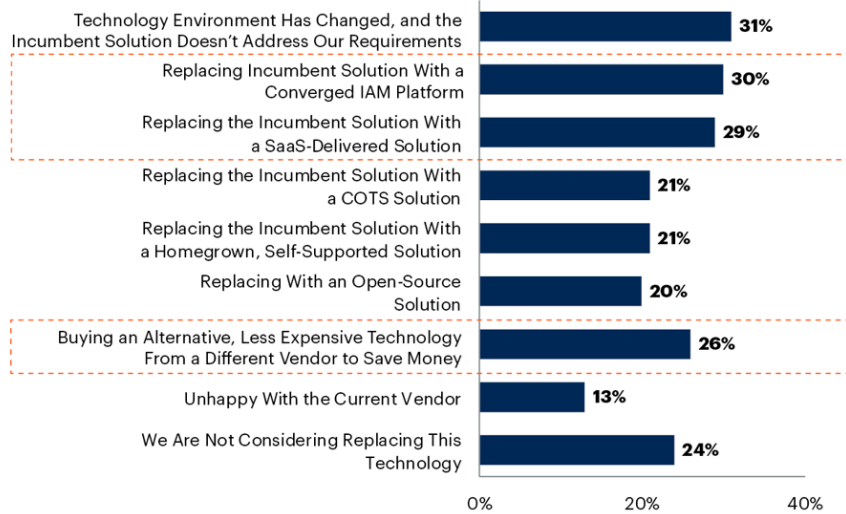
Looking forward, we expect several recent trends to accelerate. Specifically, we expect: (1) organizations that require a fully featured IGA suite to implement solutions with advanced capabilities such as identity analytics and predictive governance leveraging ML/AI; (2) cost-conscious organizations with less intensive IGA needs to shift to SaaS

“IGA-light” IAM solutions that offer a lower TCO and ease of deployment; and (3) organizations to leverage non-IAM tools such as cloud security posture management (CSPM) and non-security solutions such as IT service management (ITSM) software to address discrete IGA needs (like lifecycle management, access certification, SOD monitoring).

Exhibit 126: IGA Tool Displacement

Reason to Replace IGA Technology

Multiple Responses Allowed



Source: Gartner

Exhibit 127: IGA Vendor Landscape

Different Types of IGA Vendors Grouped by Delivery Models and Alternatives

<p>Cloud-Architected SaaS-Delivered IGA:</p> <ul style="list-style-type: none"> • Omada • SailPoint IdentityNow • Saviynt • SecurEnds 	<p>Software-Delivered IGA With Limited Cloud-Architected IGA Components:</p> <ul style="list-style-type: none"> • IBM • One Identity • Oracle • SAP • Forgerock 	<p>Cloud-Hosted SaaS-Delivered IGA:</p> <ul style="list-style-type: none"> • Hitachi ID Systems • Atos Evidian • SailPoint Identity IQ
<p>Software-Delivered IGA:</p> <ul style="list-style-type: none"> • Micro Focus • Broadcom 	<p>Converged IAM Platform (CIP):</p> <ul style="list-style-type: none"> • Okta • Microsoft Azure AD • Ilantus 	<p>ITSM Specific Vendors and Other IAM Tools With IGA Functions:</p> <ul style="list-style-type: none"> • Clear Skye • BrainWave • Authomize

Source: Gartner

Privileged Access Management (PAM)

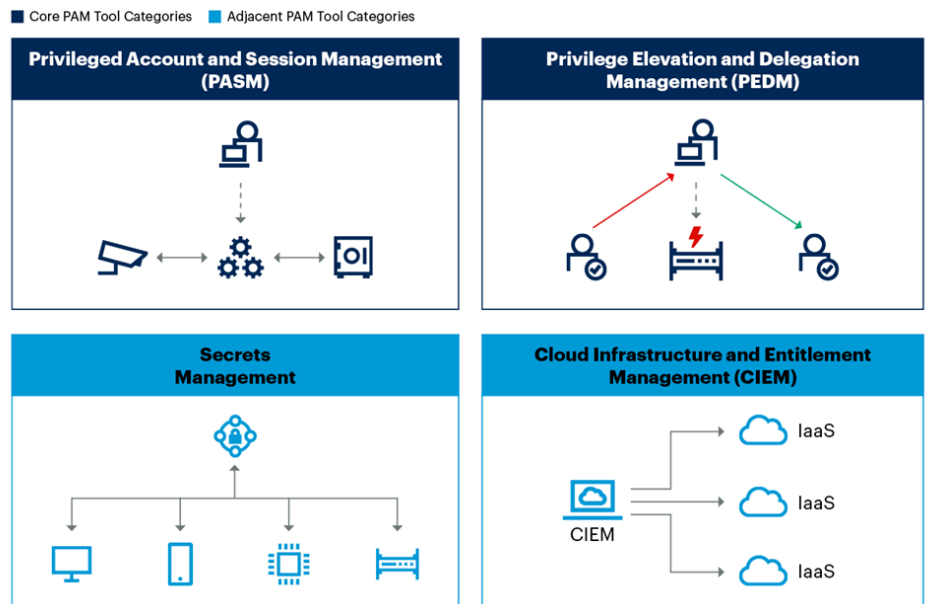
The PAM market consists of solutions focused on securing “privileged” accounts. Administrators typically use privileged accounts and provide access or privileges beyond the scope of standard user accounts. Examples include IT systems administration accounts, domain administration accounts, super-user accounts, and software and machines accounts, such as application and service accounts. These accounts are often called “Keys to the IT kingdom” due to their extensive access and control. Therefore, they require specialized access management solutions to protect from internal and external bad actors.

Historically, organizations addressed PAM use cases by leveraging AM and IGA tools. Yet, this approach had many shortcomings, as neither AM nor IGA solutions were equipped to handle privileged identities comprehensively. Specifically, the workflow approval capabilities of AM and IGA tools often led to long-term access to accounts as opposed to PAM's just-in-time (JIT), per-session access approach, which grants access to accounts only when needed and by applying the principle of least privilege. Also, AM and IGA tools couldn't map out privileged accounts within a network or effectively manage privileged access to software and machine accounts. As a result, PAM solutions have increasingly gained popularity, especially in mid-sized and large organizations.

Today, most large- and mid-sized organizations have a PAM solution, notably in industries facing high-security risk and regulatory hurdles, such as banking, securities, insurance, media, and government. Many large organizations have also extended their PAM tools into more advanced use cases such as secrets management, JIT PAM, task automation, and privilege access management for IaaS environments. In addition, we've seen a growing number of smaller organizations focus on managing privileged identities, given recent identity-related breaches and the proliferation of remote privileged users.

The core capabilities of PAM solutions include the discovery of privileged accounts across multiple systems, credential management for delegation of access to privileged accounts, session establishment, management, monitoring and recording, and controlled elevation of commands. It's also common to see PAM vendors offer secrets management of applications, services, devices and, task automation, and remote privileged access for workers and other external users. Generally, these capabilities are incorporated into four groups of PAM tools: (1) Privileged Account & Session Management (PASM) tools; (2) Privileged Elevation and Delegation Management (PEDM) tools; (3) Secrets Management; and (4) Cloud Infrastructure Entitlement Management (CIEM).

Exhibit 128: PAM Tool Categories

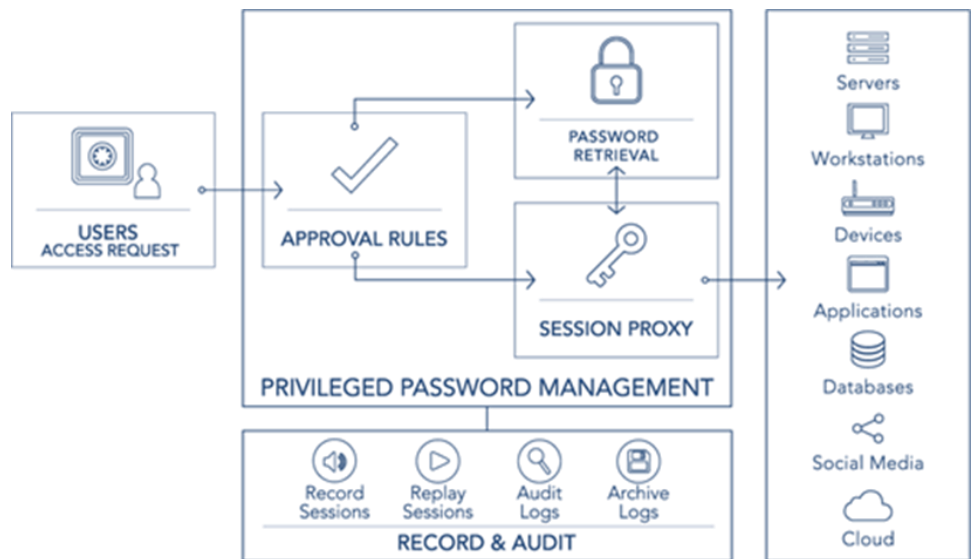


Source: Gartner

PASM tools incorporate privileged password management (PPM) tools, which help verify privileged users and retrieve the appropriate credentials injected to create a session, and privileged session management (PSM) tools, which monitor, record, and maintain oversight of the session. Exhibit 129 depicts a typical PASM session workflow. PASM tools also provide account discovery, helping organizations map their privileged accounts by scanning the corporate network and managing privileged passwords for non-human accounts, such as software and machines. Additional PASM functionality includes application-to-application password management (AAPM) and zero-install remote privileged access.

Non-human accounts can be particularly challenging to manage in terms of privileged access due to the cumbersome process of changing and rotating their respective passwords and keys. Historically, administrators completed this process manually by updating passwords and keys in multiple locations. After an update, the software often had to be rebooted for the new changes to take effect, which led to service disruptions. PASM tools help organizations address these issues by automatically updating these features while keeping track of dependencies and avoiding operational outages.

Exhibit 129: Privilege Password & Session Management Workflow



Source: BeyondTrust

PEDM tools use host-based agents to grant specific elevated privileges to a user on an as-needed basis, removing standing privileged accounts and reducing security risks from always-on access and over-privileged users. For example, with traditional PASM tools, an IT administrator would log on to a server with their administrator account (the privileged account) to make changes. With PEDM, an IT administrator can access the server with their standard user account, and if changes are needed, PEDM tools can enable privileged access to the administrator's standard account. The privileged status expires after a pre-set amount of time or after the administrator delegates access. PEDM tools are built on JIT access and Zero Standing Privileges (ZSP), delivering privileged access to users only when needed and reducing the attack surface and risks associated with unsupervised privileged accounts. Typical PEDM capabilities include application sandboxing, application allow/deny/isolate controls, and file integrity monitoring.

In addition to PASM tools, a separate category of secrets management tools has emerged, focusing on managing machines and software credentials (including passwords, OAuth tokens, SSH keys, etc.). These tools are deployed on a standalone basis or built into PASM solutions. They include generating, vaulting, rotating, and providing credentials to non-human entities using APIs or SDKs. Secrets management capabilities include credential injection techniques, application fingerprinting, and native integrations with CI/CD pipelines for DevOps processes. The secrets management market and its dynamics are covered in depth in a subsequent section of this report.

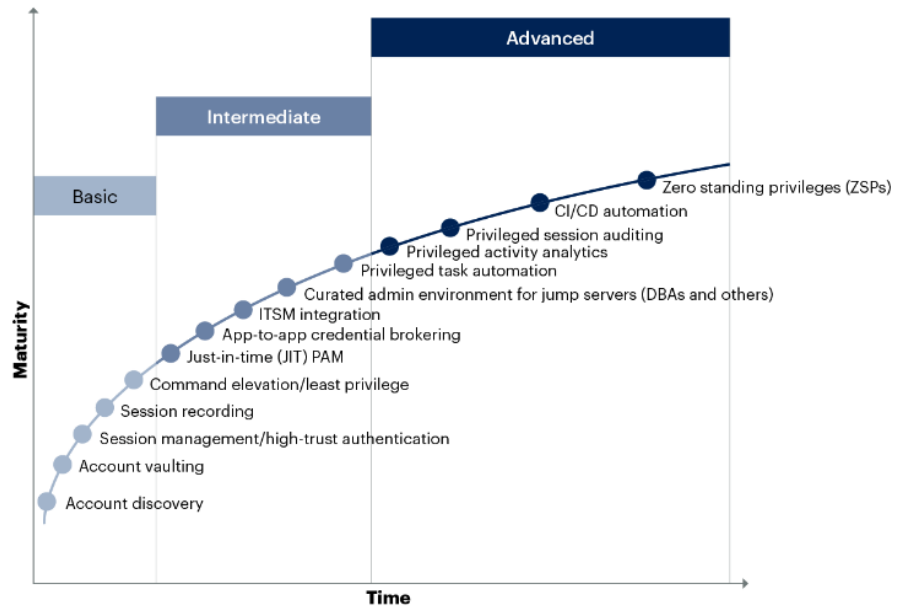
In recent years, a new category of cloud solutions has emerged to provide admin-time controls and governance for hybrid and multi-cloud IaaS environments (i.e., AWS, Azure, GCP), known as Cloud Infrastructure Entitlement Management (CIEM). These solutions apply IGA and PAM principles and AI and ML to manage privileged entitlements in cloud environments. CIEM solutions can detect which accounts within an organization's IaaS are used and which are dormant by analyzing identity events, audit data, and entitlements data. They then provide remediation by removing unnecessary and unused access and applying the concept of ZSP to cloud environments. The CIEM market and its dynamics are covered in depth in a subsequent section of this report.

Looking ahead, we expect convergence trends to impact the PAM market. Several traditional AM and IGA vendors have already added basic PAM capabilities to their platforms, and we expect PAM vendors to do the same, adding AM and IGA capabilities. SaaS-based PAM solution adoption also seems poised to accelerate, especially among smaller and mid-sized enterprises, which may prefer an easier-to-deploy delivery model with lower TCO. However, it's important to note that given the critical nature of the resources

and identities PAM solutions typically secure, organizations with a sizable on-premise footprint are likely to continue deploying PAM solutions components (session management, account rotation) within their data centers. We expect vendors to fully mature their capabilities toward a ZSP solution, delivered mainly via a SaaS-based delivery model (75% of cyber-insurance providers are expected to mandate JIT/ZSP principles by 2025, according to Gartner). And as more organizations adopt a DevOps framework, we anticipate broader adoption of secrets management and CIEM capabilities.

Exhibit 130: PAM Maturity Curve

Sample PAM Maturity Curve

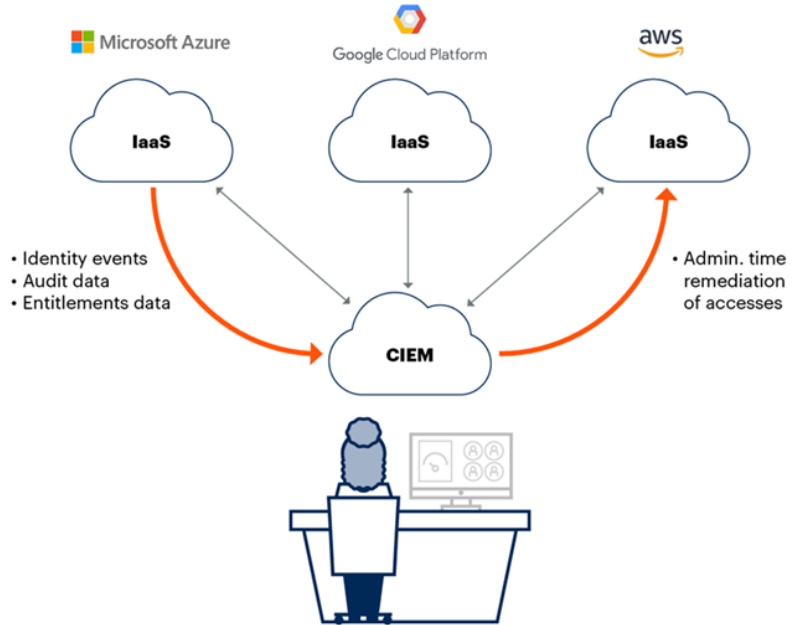


Source: Gartner

Cloud Infrastructure Entitlement Management (CIEM)

While organizations of all sizes are shifting to the cloud, managing access and security risks in cloud environments is still their responsibility. In recent years, this task has been complicated by a jump in the number of new cloud-entitled users (as the cloud providers add more services) with privileged access to critical cloud-delivered applications and data resources. One of the main risks associated with cloud-entitled users is that cloud providers typically offer “always-on” privileges to users that are often either unnecessary or unused. This leaves organizations exposed to identity-based cyber-attacks. While organizations have relied on traditional IAM tools and adjacent security technologies such as cloud security posture management (CSPM) solutions to address such risks, neither has proven effective in handling the dynamic nature of cloud entitlements. To better address this challenge, many organizations have looked into Cloud Infrastructure Entitlement Management (CIEM) solutions, combining traditional PAM and IGA capabilities for IaaS environments with advanced analytics to enable predictive and autonomous governance of IaaS environments.

Exhibit 131: Cloud Infrastructure Entitlement Management (CIEM) Overview






Source: Gartner

It is important to differentiate between typical identity-based access and privileges in a traditional on-premise technology stack versus those in a Cloud environment. To be clear, CIEM solutions are closer to IGA/PAM than AM, which tend to focus on access scalability rather than post-access granularity and user monitoring. Specifically, within CIEM, the standard privileged entitlements for IaaS include (1) resource entitlements—access to file shares, database tables, and workloads, (2) service entitlements—ability to start VMs and containers and set compute and storage, and (3) management entitlements—access to IaaS administrator account, ability to provision entitlements and configure security settings. This is a higher level of privileged access granularity specific to cloud environments than those available with traditional PAM solutions for on-premise access (although PAM solutions offer broader user monitoring capabilities). CIEM solutions also have built-in IGA functionality, which may be an independent solution within the on-premise stack (although the three IAM pillars are consolidating on-premise).

Exhibit 132: Types of Privileged Entitlement in CIEM

Types of Privileged Entitlements and Operations Examples

	 Resource Entitlements	 Service Entitlements	 Management Entitlements
Privileged Entitlements			
Operations	<ul style="list-style-type: none"> • Access file shares • Access database tables • Access workloads 	<ul style="list-style-type: none"> • Start/stop VMs, containers • Set compute/storage/network permissions 	<ul style="list-style-type: none"> • Access IaaS admin. account • Set identities, entitlements and roles (RBAC) • Configure security settings

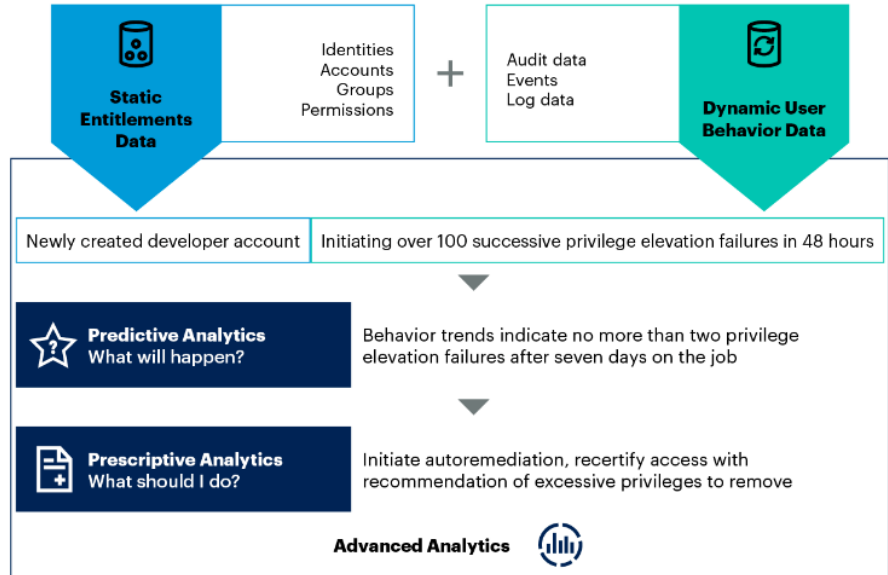
Source: Gartner

CIEM solutions thus provide organizations with visibility into their cloud identity security posture. They leverage identity analytics, take in identity events, audit and entitle data, visualize and discover access paths, trace user entitlements, and outline potential security risks associated with each entitlement. Organizations commonly use CIEM solutions and

visualizations to detect dormant entitlements, enable autonomous governance (detecting anomalies by setting baseline rules and suggesting remediation), and continuously monitor their cloud identity posture to identify gaps between the intended and actual posture at runtime. Advanced functionality in CIEM can also automate remediation.

Exhibit 133: CIEM Vendor Landscape & Adjacencies

How CIEM Leverages Advanced Analytics



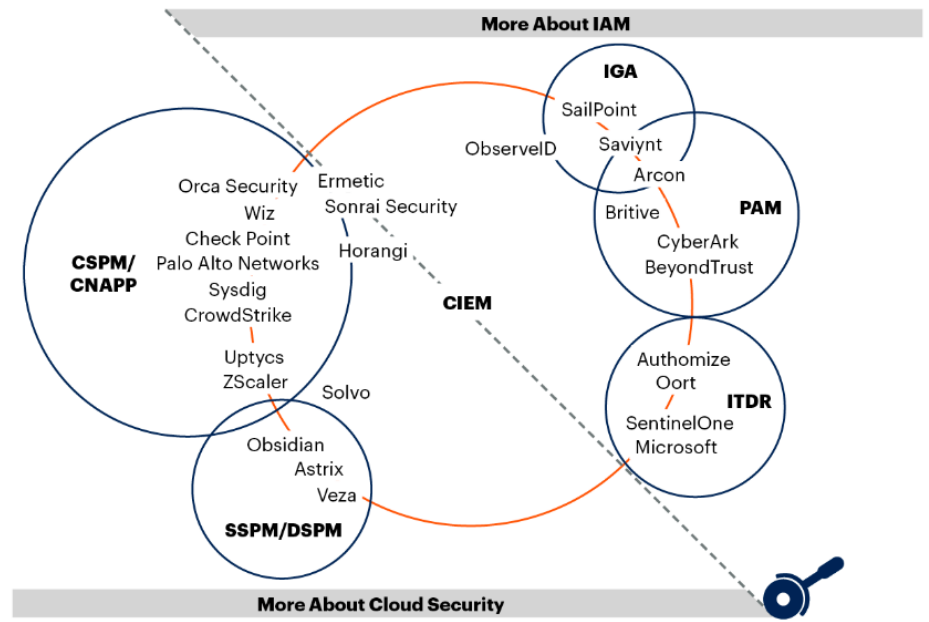
Source: Gartner

Historically, IGA and PAM vendors were slow to address the identity security demands of the Cloud, a driver for the creation of CIEM. However, the convergence of the two solutions is now in play, and we expect the CIEM market to gradually converge with the broader IAM market (most likely subsumed within PAM). Several CIEM vendors, such as Authomize and Britive, have added traditional IAM capabilities, while traditional PAM and emerging CSPM vendors, such as CyberArk, BeyondTrust, CrowdStrike, Wiz, Orca, and SentinelOne, have added CIEM capabilities. CIEM vendors have also broadened their scope to provide analytics-driven discovery and entitlement management, as well as ITDR and security posture dashboards. Given the broad functional overlap, we believe vendors with strong CSPM, IGA, and PAM functionality are best positioned to address the CIEM market long-term. In fact, Gartner estimates that 75% of PAM vendors will have some CIEM technology in the pipeline within the next 1-2 years.

The major cloud providers have also improved their CIEM capabilities, appealing to organizations running in single cloud environments. For example, in early 2021, Microsoft purchased CloudKnox Security, one of the leading CIEM vendors. We also see a growing overlap between CIEM and CSPM technologies. Therefore, we believe that the cloud security vendors will work to move into the CIEM market by developing their solutions, like Palo Alto, or by acquiring pure-play CIEM vendors, similar to Zscaler’s acquisition of Trustdome.

Exhibit 134: CIEM Vendor Landscape & Adjacencies

CIEM Vendor Landscape and Adjacencies



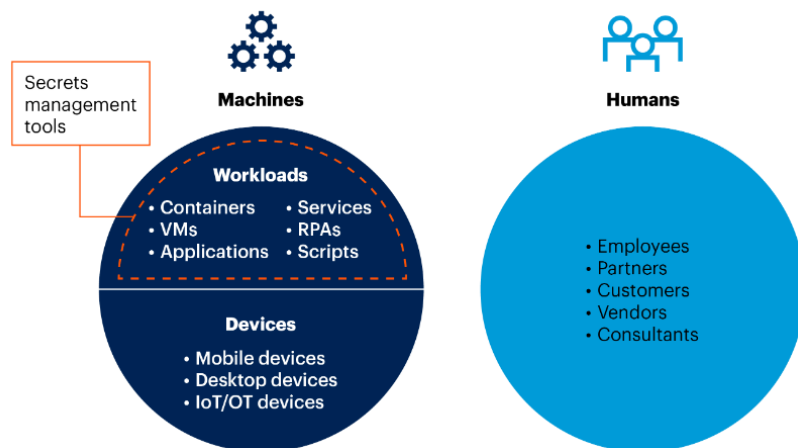
Source: Gartner

Secrets Management

In today’s world, the vast majority of corporate communication is actually between machines rather than humans. This includes two types of machines—physical devices (servers, PCs, and mobile devices) and workloads (applications, virtual machines, containers, etc.). These machines, and in particular workloads, regularly communicate to securely exchange information and connect to databases and services. Their interaction has expanded exponentially in recent years due to the proliferation of cloud-based architectures and micro-services.

Secrets management aims to confirm machines' identities and is crucial to workload-related machine identity management. This includes programmatic management, secure storage, and easy retrieval of credentials (passwords, OAuth tokens, SSH keys, etc.) through APIs, command line interfaces (CLIs), and software development kits (SDKs). Secrets managers often integrate with CI/CD (DevOps), Kubernetes (container orchestration), and RPA tools, and are delivered as SaaS modules.

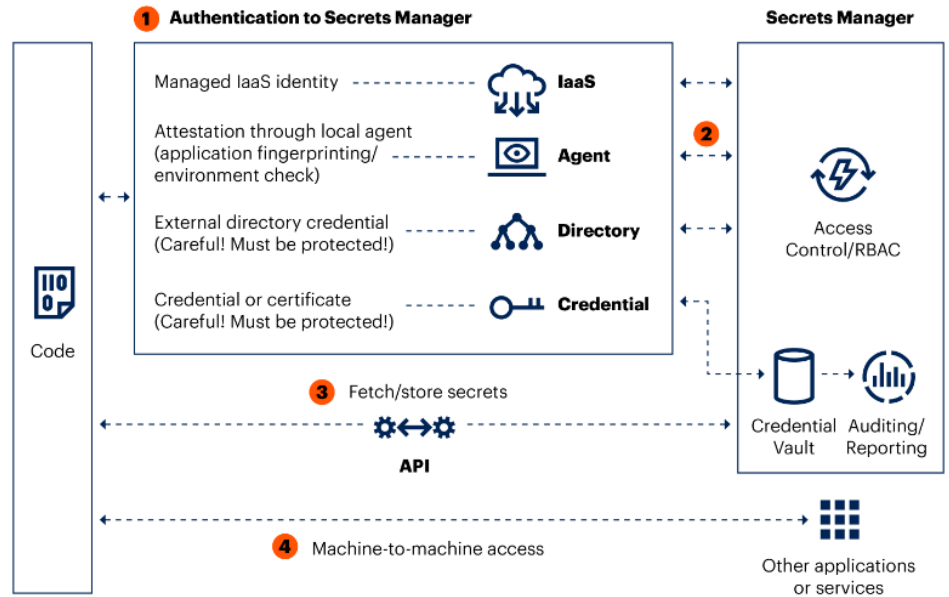
Exhibit 135: Secrets Management as Part of Machine Identity Management



Source: Gartner

The functionality provided by secrets managers includes—(1) securing application and service account credentials; (2) issuing and managing machine identities to workloads; (3) issuing short-lived SSH tokens, X.509 certificates, or JSON Web Tokens (JWTs); (4) storing and rotating secrets used in DevOps pipelines; (5) managing symmetric keys used for encryption; and (6) enabling additional encryption services using protected keys.

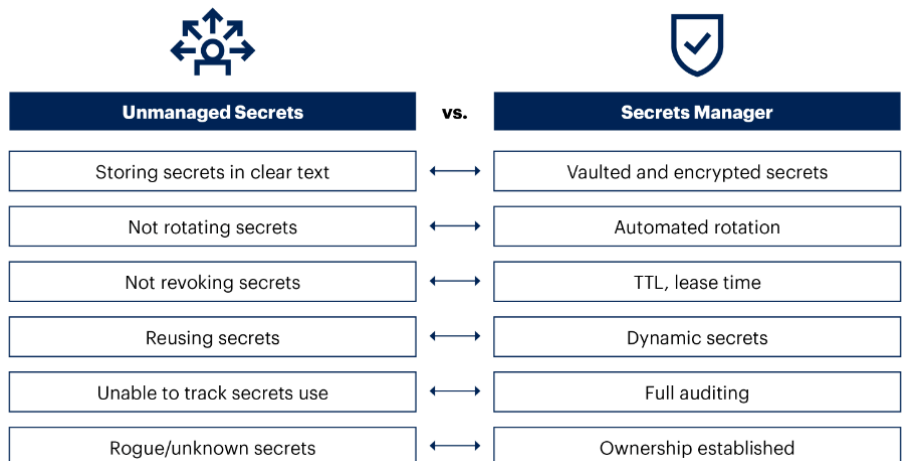
Exhibit 136: Interaction between an Application and Secrets Manager



Source: Gartner

There are multiple benefits to using a secrets manager. These include: (1) better security hygiene and the ability to provide audit trails for said keys and credentials; (2) centralization of credential management vs. independent management by developers and administrators, which create “secrets sprawl” or stale/forgotten credentials; (3) rotation of credentials for risk mitigation practices; (4) hiding credentials from DevSecOps tools and software development artifacts, offering access through API calls; (5) integration with container orchestration platforms (Kubernetes), authorizing or authenticating credentials required to run containers; (6) specialization in lightweight certificates such as SSH tokens and X.509 certificates; and (7) establishing trust between workloads that have never interacted with each other by generating and managing encryption keys. Some secrets managers also have the ability to provide encryption-as-a-service for keys.

Exhibit 137: Managed vs. Unmanaged Secrets



Source: Gartner

Secrets management tools are more dynamic than traditional PAM, as developers can designate secrets storage using only a couple of lines of code. However, they are still in the early stages of adoption. In fact, Gartner estimates that only 30% of organizations are currently using secrets management (albeit at a growing pace). HashiCorp and CyberArk currently dominate the secrets management market. Still, competition is growing from cloud vendors (AWS Secrets Manager, Azure Key Vault, GCP Secret Manager), other PAM vendors (BeyondTrust and Delinea), and startups (Akeyless and Doppler). We expect more vendors to offer secrets management capabilities over time as DevOps and cloud-native processes become more prevalent.

Identity Verification

Identity verification tools focus on confirming the existence of a real-world identity and that the individual claiming the identity is the true owner. Identity verification technologies secure account openings, registration processes, and application enrollments. The most common verification method is the document-centric approach (aka “ID plus selfie”), which tests for genuine human presence by asking an individual to provide an image or video of a form of ID (passport, driver’s license, etc.) and themselves. Once collected, the identity data (name, address, phone number, DOB) is cross-checked against public data sources (electoral records, credit bureau data, and census information).

Exhibit 138: Identity Verification Process



Source: Gartner

The identity verification market is relatively nascent, with several startups competing for market share. These include vendors like AuthenticID, ID.me, and Incode. To differentiate, vendors have introduced capabilities such as low-code implementations that leverage QR codes, device anomaly detection, and enhanced biometrics (face biometrics, voice biometrics). In our view, vendors that can go beyond the core “ID plus selfie” verification process and address fraud detection use cases are best positioned to capture share, particularly due to rising concerns around Generative AI-enabled attacks, which typically involve deepfake image or video used as a selfie during the verification process. To mitigate such attacks, vendors have introduced enhanced fraud detection defenses such as liveness detection, ML-based image inspection, and screen detection that look for the presence of glare or reflections from a secondary device.

While fraud detection was historically focused on preventing malicious bot activity, the increase in human threat actors has created a need for identity verification. Therefore, we expect the adoption of identity verification tools to increase as the number of digital identities created accelerates. We also expect CIAM vendors, who govern the account creation process, to partner with existing identity verification vendors or introduce verification capabilities themselves to secure customer registration and prevent account takeover attacks.

Convergence of Identity Security Capabilities and Offerings

We expect the convergence of the three IAM market sub-segments (AM, IGA, PAM) to accelerate. Organizations are now more frequently looking to address their identity-related security needs with a single vendor to eliminate identity silos and product gaps and to reduce operational costs. The most pronounced convergence thus far has been between AM and IGA tools, with several AM vendors such as Okta, ForgeRock, and Microsoft introducing lightweight IGA functionality. That said, we expect lightweight PAM functionality also increasingly to be consolidated.

AM vendor Okta already offers a fully-featured IGA solution with capabilities such as lifecycle management, access governance, and workflows. It released a PAM solution in

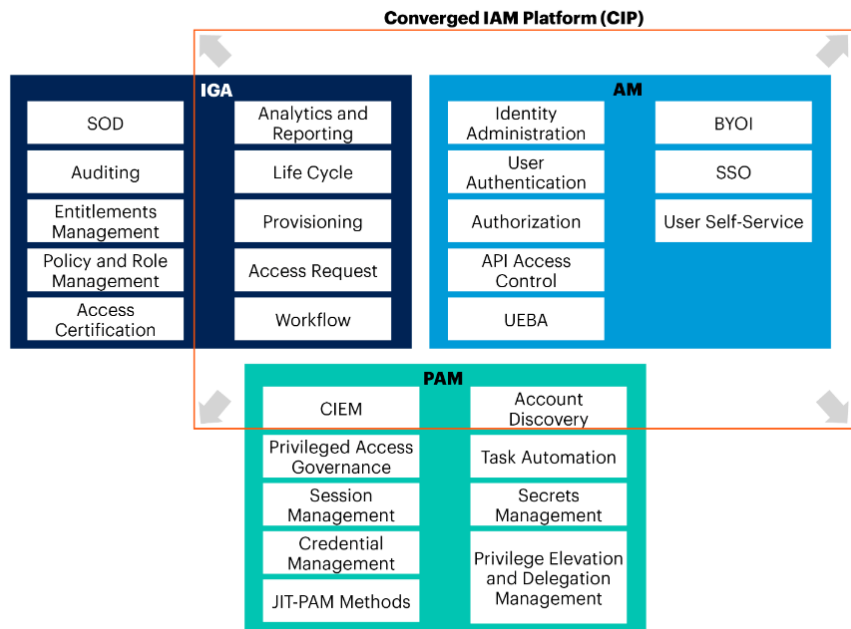
December 2023 with additional capabilities fully integrated with its existing AM platform. Several IGA and PAM vendors are also taking steps to consolidate the market. IGA vendor Saviynt expanded its capabilities and launched a PAM solution in 2019, while PAM vendor CyberArk entered the AM market by acquiring Idaptive in early 2020. Over time, we expect vendors from all three identity “pillars” to expand their capabilities into adjacent IAM sub-segments, eventually offering a converged identity solution.

It’s important to note that the core capabilities for AM and PAM are expanding, with AM vendors adding passwordless authentication and addressing fraud detection use cases (within CIAM) and PAM vendors adding CIEM and Secrets Management capabilities. Hence, we expect the consolidation in the identity security market to incorporate additional adjacent segments over time.

Last, we expect the transition to SaaS-based deployment models to facilitate faster convergence. SaaS-based solutions allow vendors to expand their feature set quickly and customers to seamlessly transition from legacy on-premise solutions. According to Gartner, 45% of new IAM deployments by 2023 were through a converged, SaaS-based offering, with further expansion to 70% of new deployments by 2025. Only a select few vendors, namely Okta and Microsoft, have made plans to offer a fully converged SaaS-based identity solution, although more vendors are likely to follow suit.

Exhibit 139: Converged IAM Platform

Converged IAM Platform



Source: Gartner

Source: Gartner

Identity & Access Management Market Vendor Overview

The AM market landscape is highly concentrated, with the top five vendors accounting for about two-thirds of the market. The competitive landscape consists of legacy vendors offering on-premises solutions and emerging vendors offering modern cloud-based IDaaS platforms. The large vendors have moved to introduce PAM and IGA tools under a single identity platform.

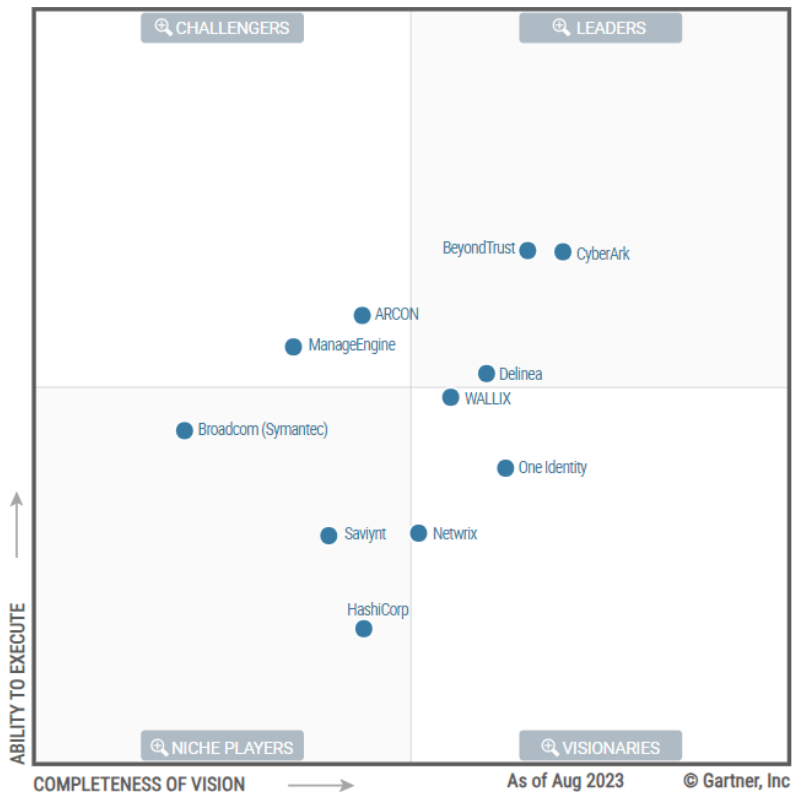
The IGA market is relatively mature, with little differentiation among vendors. Most price their solutions based on the number of identities supported and offer perpetual license and SaaS-based delivery models. Considering the market maturity, most new sales in the segment tend to be competitive displacements prompted by cost or a transition to the cloud. Several IGA vendors have expanded their IAM capabilities in recent years, moving into AM and PAM, a trend we expect to continue.

The PAM market includes established vendors with large market shares and smaller niche players. The strong demand in the market is driven by increased awareness of the crucial importance of PAM solutions in regulating privileged users and accounts, a rise in the number of identity-related breaches, a pandemic-related shift to remote work, and an accelerated migration to the cloud. PAM vendors have reacted to the consolidation efforts of AM and IGA vendors and added AM capabilities.

Exhibit 140: Gartner Access Management Magic Quadrant



Source: Gartner

Exhibit 141: Gartner Privileged Access Management Magic Quadrant

Source: Gartner

Below, we review several Identity & Access Management vendors not reviewed in detail in this report.

- Okta.** Okta is one of the most prominent vendors in the AM market, with the second-largest market share for workforce AM (behind Microsoft) and the largest CIAM market share. It offers a SaaS service with comprehensive capabilities, including universal directory, SSO, MFA, passwordless, lifecycle management, API access management, analytics, and device management. The company is known for its seamless deployment, extensive integrations, and easy-to-configure customizations, and it addresses workforce and customer (CIAM) identity use cases. Okta's CIAM presence was boosted by its acquisition of Auth0, which added a developer-led approach to targeting the CIAM market, positioning Okta as a leader. The company released a fully-featured IGA product in 2022, and in December 2023, a PAM solution (building on its lifecycle management and advanced server access solutions), putting it in a position to lead the market consolidation with a SaaS-based, fully converged IAM platform.
- IBM.** IBM offers on-premise and SaaS-delivered AM solutions. Both deployment models incorporate SSO, MFA, user directory, UEBA, provisioning, passkeys compatibility, and identity analytics/ITDR capabilities. The company is price-competitive with its SaaS solution. Yet, its innovation is lagging with limited B2B and B2C support, and several of its basic OOTB capabilities (i.e., self-service registration) are offered only through its on-premises solution, although developer tool expansion and the addition of CIAM capabilities are on the roadmap. IBM also provides a fully-featured IGA solution with broad integration, SOD monitoring, and data access governance capabilities. The company sells its on-premise IGA suite (Identity Governance and Intelligence (IGI)) as a virtual appliance and as a SaaS-delivered IGA-light solution (IBM Cloud identity). However, its tools still lack comprehensive functionality compared to other vendors. The company remains price-competitive and integrated IGI with its AM solution (IBM Security Verify).

- **Ping Identity & ForgeRock.** Private equity firm Thoma Bravo acquired Ping Identity in late 2022 and ForgeRock in August 2023, combining them into a single identity security company. Ping Identity offers on-premise and SaaS-based AM solutions and is known for its solid application integration, API access controls, and self-service capabilities. It recently added capabilities around decentralized ID service, fraud detection, and protection against MFA bombing. The company has aggressively marketed its CIAM product, which is priced below most competitive products. ForgeRock offers a range of on-premise and SaaS-delivered AM solutions. Its on-premise solution includes SSO, lifecycle management, and a directory. In contrast, its SaaS-based solution, the ForgeRock Identity Cloud, offers lifecycle management, SSO, and MFA, with additional features such as adaptive access, continuous authorization, and CIAM functionality at additional cost. ForgeRock also offers IGA capabilities such as identity administration, governance, and analytics as part of its more significant push toward a converged IAM solution. ForgeRock's capabilities are integrated with Ping Identity but may exist as a separate product line and brand. Ping Identity has broad on-premise capabilities and a strong presence in verticals extensively utilizing legacy, on-premise architectures, such as financial services. ForgeRock has a similarly strong presence with organizations that have legacy on-premise architectures. Both companies have nascent cloud platforms that could be accelerated as a combined entity.
- **Microsoft.** The largest workforce AM provider, Microsoft, offers a tiered AM solution through Azure Active Directory (AD) incorporating SSO, MFA, light IGA, and PAM (privileged identity management (PIM)) capabilities. The company also offers CIAM solutions with Azure AD B2C, although its features are sparse compared to other vendors. Microsoft holds a strong position in the market, as many of its Office 365 customers often choose Azure AD (now rebranded as Entra ID for workforce access management) for their access management needs. However, the company only sells its solution in bundles, and many customers often opt to go with vendors offering more accommodating pricing models. Microsoft currently bundles its AM and IGA features with its Security E3 bundle and only includes PIM in its Security E5 bundle. In mid-2021, the company expanded into the CIEM market by acquiring pure-play CIEM vendor CloudKnox (now part of the Microsoft Entra product family), with the solution supporting Azure, AWS, and GCP cloud platforms. Most recently, Microsoft added capabilities around decentralized identity (Entra Verified ID), machine identity (Entra Workload ID), security posture management (Entra recommendations), and endpoint privilege management (part of the Intune product family).
- **CyberArk.** CyberArk is the largest PAM vendor in the market, and it offers on-premise and SaaS-based PASM and PEDM capabilities, secrets management, and endpoint privilege capabilities. The company is often the first to market with new PAM capabilities and is the only PAM vendor offering full-fledged CIEM functionality (CIEM solution is not integrated into the core PAM offering and is sold as an add-on product). In addition, CyberArk is a leading provider of secrets management and AAPM (application-to-application password management). This positions CyberArk as one of the most expansive solutions in the PAM market. In addition to PAM, the company offers a fully-featured AM solution through its acquisition of Idaptive, although it is predominantly workforce-centric (limited CIAM features and nascent developer tools).
- **BeyondTrust.** BeyondTrust is a leading vendor in the PAM market, and it offers PAM solutions addressing PASM, PEDM, and secrets management use cases. The company's products feature excellent reporting and visualization functionality, and its Linux- and UNIX-based PEDM solutions are considered best-in-class. The company offers three overlapping PASM solutions (Password Safe, Privileged Remote Access, and Privileged Identity) and is merging them into a unified solution. While it doesn't offer any AM or IGA capabilities, the company is currently adding new features to address the CIEM market but is lagging competitors in functionality such as anomaly detection and JIT entitlement.
- **Delinea.** Was formed with the merger of two PAM vendors, Centrify and Thycotic, combining their best features. Delinea's PASM functionality is delivered through its Secret Server product (Thycotic) and PEDM through its Privilege Manager (Thycotic).

In contrast, Server PAM, Authentication Service products, and AD bridging tool functionality (UNIX and Linux) are derived from Centrify. All products are available as SaaS and offer API, DevOps, and ITSM integrations. DevOps Secrets Vault offers secrets management but lags HashiCorp and CyberArk in functionality. Delinea also offers basic CIEM capabilities at this time but has a roadmap to expand functionality. The company is one of the few PAM vendors to obtain FedRAMP certification. (FedRAMP is a Federal Government compliance program.)

- **SailPoint.** SailPoint is a prominent IGA vendor that offers on-premises (IdentityIQ) and SaaS (IdentityNow) suites. The company was the first to introduce a SaaS IGA solution and incorporates a full suite of capabilities, including life cycle, entitlements, access and workflow, policy management, and external API integrations and integrations with other ITSM tools. IdentityIQ is geared to large enterprise use cases, while IdentityNow is more suitable for cost-conscious organizations that require more basic IGA capabilities. SailPoint acquired SecZetta in early 2023, expanding visibility into non-employee identities. Like Ping Identity, SailPoint has not expanded its offering to include traditional other IAM capabilities (AM and PAM in this case) but is expanding into the data access and posture management and the CIEM market, which shares many functional features with IGA.
- **Saviynt.** Saviynt offers a fully-featured, SaaS-based IGA solution that includes basic PAM functionality (PASM-focused). The company's core solution, Security Manager, offers basic IGA capabilities with premium capabilities available through additional modules. Security Manager is primarily delivered as a SaaS solution, although organizations can deploy it on-premise via a virtual appliance. Saviynt excels when deep access insights into unstructured data and business applications such as SAP, Oracle, Salesforce, Workday, and cross-application SOD are required. It has invested early in analytics for predictive and autonomous governance and provides data access governance as a product. It is FedRAMP certified.
- **Transmit Security** is a passwordless identity management security vendor that has pivoted to solely provide cloud-native CIAM solutions. Instead of traditional passwords, the company's solutions rely on biometric data (face or fingerprints) registered with users' mobile devices. This allows organizations to remove passwords from their login process, improve security, and limit data compromise risk. This provides a seamless customer login process that eliminates registration fatigue and forgotten passwords. In terms of functionality, Transmit Security offers passwordless and MFA authentication, embedded identity policy orchestration, user management services, and digital identity fraud protection services, using developer-friendly APIs and SDKs and leveraging industry-standard connectors and integration.
- **1Password** is a secure enterprise-grade password manager that provides end-to-end encryption, security features for individual credential management, and secure password sharing. It has shifted focus solely from consumers towards B2B SaaS in the last five years and now draws most of its revenue from commercial customers. Its top-notch encryption functionality includes 256-bit AES encryption, cryptographically secure pseudorandom encryption key generator, PBKDF2 key strengthening, and secrets management. Additional features such as clipboard management, code signature validation, auto-lock, biometric access, vulnerability alerts, and phishing protection add to password hygiene. Lastly, 1Password leverages multiple open standards, such as OPVault and Agile Keychain, to improve visibility into its technology. The company is expanding to a passwordless platform, and launched additional passkey features in 2023. 1Password is complementary to traditional AM vendors such as Microsoft and Okta and recently added SSO functionality for OIDC-supported identity providers. As for its secrets management product (Secrets Automation), the company focuses on SMB customers rather than competition with enterprise-focused (more feature-rich and higher priced) vendors such as HashiCorp, CyberArk, and Microsoft Azure Secrets Manager. In February 2024, it acquired endpoint security platform Kolide, expanding its enterprise product offerings.
- **Beyond Identity** is a passwordless identity management vendor. The company's Beyond Identity Authenticator, which users download onto their devices, uses biometric data natively stored on the device and a private key associated with an

email or login ID to authenticate user access. For CIAM use cases, organizations can embed the Authenticator within mobile applications to remove customers' need to download it themselves. For DevOps use cases, the author verification API checks into the CI/CD pipeline and verifies that the key making the commit is assigned to an appropriate corporate and device identity. The company's author verification API integrates with leading code repositories and tools such as GitHub (Microsoft), GitLab, Bitbucket, CircleCI, Jenkins, and Azure Pipelines. The platform offers seamless device management and performs automatic security posture checks. Beyond Identity offers several pricing tiers, from free passwordless authentication to advanced risk-based policy orchestration, SIEM integration, and other enterprise-focused capabilities.

- **JumpCloud** is a multi-cloud identity directory and access management solution provider for the SMB market. It combines multiple tools, such as MFA, SSO, device management, PAM for infrastructure, remote desktop, identity management, etc., into one package for easy deployment. Its three products include (1) identity management – cloud directory and identity lifecycle management; (2) access management – SSO, Cloud LDAP, MFA, password manager, conditional access, etc.; and (3) device management – cross-operating system device management and mobile device management. The company's go-to-market approach is product-led and utilizes limited sales and marketing personnel while leveraging marketplaces on AWS and GCP.
- **Keyfactor** is a leading provider of machine-identity security across workloads such as servers, virtual machines, containers, applications, services, and scripts and across devices such as workstations, mobile, and IoT devices. Its use cases span many functions, such as public-key infrastructure (PKI) as a service, certificate lifecycle automation, SSH key management, encryption key management, IoT identity management, etc. For example, as part of certificate key management, Keyfactor assigns a unique identification to each enterprise device at scale and manages them through their lifecycle. The company has expanded into code signing, where every time a developer pushes out a code, it comes out with a signature. Keyfactor can be hosted in a private or public cloud infrastructure at AWS, Microsoft Azure, and GCP.
- **Semperis** provides Active Directory (AD) security and recovery solutions. Its Directory Services Protector (DSP) solution offers comprehensive identity threat detection and response (ITDR) capabilities for Active Directory (Microsoft product) and Azure AD, which include (1) pre-attack scanning for vulnerabilities and indicators-of-compromise (IoCs), a detailed scoring system, and auto-remediation capabilities; and (2) mid-attack visibility into threat actors and changes to AD during the event. DSP can also monitor the sophistication and speed of the attack and preemptively block risky behavior and changes (user behavior analysis or UBA). Its Active Directory Forest Recovery (ADFR) solution focuses on post-attack remediation, provides a low latency full recovery of the Active Directory, and scans the AD environment for malware and other suspicious executables during the recovery phase. The company has expanded its offerings from AD to include Azure AD, and we expect other Cloud AD solutions over time. Customers can purchase different bundles for DSP (Essential, Advanced, and Intelligence) and a single offering for ADFR. The company has so far focused on the largest enterprises across a wide variety of verticals (Technology, Financial Services, Healthcare, etc.) but is expanding with channel partners to target the SMB segment. Semperis also offers a free Active Directory scanning tool called Purple Knight, which provides point-in-time scanning (versus scan history, mid-attack visibility, and more enhanced features for its commercial version). Purple Knight allows Semperis to build a knowledge community around identity attack sophistication while providing an entry point to convert organizations to paying customers.
- **Stytch** is a passwordless identity management vendor. The company offers several passwordless MFA options, such as email magic links, SMS passcodes, WhatsApp passcodes, and OAuth logins, allowing users to leverage existing Google, Facebook, or Microsoft accounts for easy registration without creating new passwords. It also offers session management capabilities that utilize JSON web tokens to enable route-based authentication for sensitive actions. The company's APIs can be embedded

into applications for seamless authentication flows, while its SDKs can be tailored to an organization's fonts, colors, and logos, eliminating UI design time. For its B2B SaaS authentication product, Stytch offers a freemium tier for 1,000 active users and a Pro, Scale, and Enterprise plan for customers looking to secure additional users and expanded features. Pricing-wise, the company offers a freemium version for 5,000 active users and additional Pro and Enterprise tiers for securing additional users and added functionality. Last, the company offers fingerprint authentication (Fraud and Risk protection services) as an add-on product.

- **Venafi** is a machine-identity security vendor. The company offers security for TLS keys and certificates, SSH keys, code signing keys, and open-source machine identities from a single management console. Its platform is open-sourced, enjoys strong adoption, and incorporates native integrations with leading DevOps solutions (such as K8s, Vault, and Terraform) to enable frictionless certificate management for developers. Customers can purchase individual products to manage specific types of certificates (TLS, SSH, OSS) or adopt the entire platform through a SaaS offering, Venafi as a Service (VaaS). In early 2023, the company launched its lightweight machine identity certificate issuer, Firefly, which helps manage identity requirements for cloud-native workloads.
- **HashiCorp** is a broader DevOps vendor that offers two identity security products, Vault and Boundary, as part of its portfolio. Vault focuses on authenticating applications and machine identities and is a secrets and encryption management system that tightly controls access to API encryption keys, passwords and certificates. Vault primarily addresses three use cases: (1) Secrets Management—programmatically creates encrypted secrets, as well as revokes and rotates secrets; (2) Certificate and Key management—leverages APIs to manage certificate and key lifecycles; and (3) Identity-based Access—centralized access controls lists (ACLs) to maintain consistent policy and access controls across public cloud infrastructure. The company acquired BluBracket in June 2023, adding secrets scanning capabilities. HashiCorp Boundary provides PASM capabilities and focuses on privileged session management and remote access capability with zero trust controls. User access is then initiated directly through Boundary (rather than using multiple different systems as is common with other PAM solutions), allowing security teams to simplify management to a single set of controls. Boundary can connect users securely to their infrastructure regardless of cloud platform or identity provider and create a consistent workflow for user authentication and authorization. It has a large ecosystem of integration partners, including the major public clouds (AWS, Azure, GCP) and identity providers (Okta, Ping, Azure AD). However, Boundary is still immature as a complete PAM offering and lacks features such as privileged account life cycle management, discovery, and credential management. Its session management capabilities are also sub-par. Vault and Boundary are available as software or as a service within its HashiCorp Cloud Platform (HCP).
- **Incode** is a provider of identity management for digital access. Its Omni platform provides an end-to-end authentication, onboarding, and ID verification solution leveraging AI/ML capabilities. Its customizable platform consists of multiple unique modules (part of its Integrated Identity Platform/IIP) across biometric authentication, data/identity capture, verification, risk control, etc. This allows customers to create custom and rules-based workflows. The company has gained traction with financial institutions that have KYC (know your customer) and AML (anti-money laundering) requirements and include customers across gaming, public sector, healthcare, hospitality, retail, and telecom verticals.
- **ID.me** is an identity network operator that allows individuals to provide proof of their legal identity online. The company creates a verified digital ID, which can be used to log or access services across the public sector, healthcare, or retail verticals. These include access to federal services such as the IRS, Social Security Administration, U.S. Department of Veteran Affairs, and select state-level labor and employment services across multiple U.S. states. On the retail side, verification of military service provides access to discounts across multiple travel, entertainment, consumer goods, and electronics brands. The company also has partnerships across multiple national

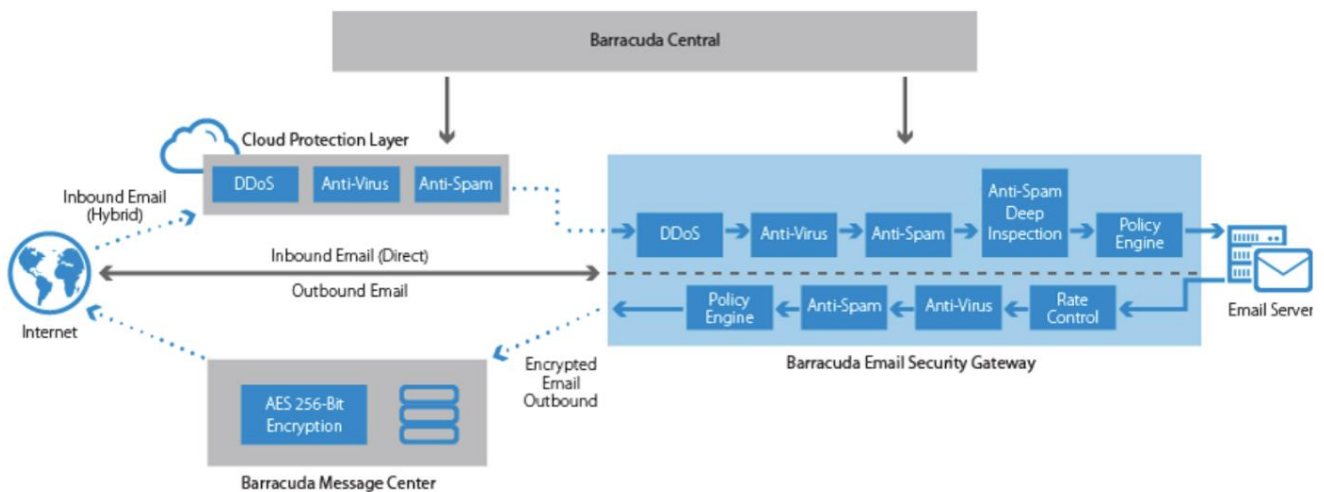
pharmacy chains (CVS Health, Walgreens, Rite Aid, Duane Reade, Walmart, Kroger, Costco, etc.) that provide a discounted price for ID.me Rx users.

Email Security

Email has long been a popular attack vector for bad actors, given its general personal and business use, mission-critical nature to business operations, and the challenges of blocking email-based attacks. According to Gartner, approximately 40% of modern ransomware attacks infiltrate through email. Email attacks have also evolved as email technology has advanced. For example, SPAM attacks on SMTP-based email systems were common in the 1980s. However, in recent years, email attacks have adapted to take advantage of the shift from text-based to HTML-based email, the growing use of email as a business workflow tool, and the inclusion of videos, conferencing capabilities, and other media capabilities directly within email solutions. This has made email highly susceptible to sophisticated malware and phishing attacks and the target of spoofing and business email compromise (BEC) attacks.

Currently, the email security market primarily consists of three types of solutions: (1) Secure Email Gateways (SEGs), (2) native security features from cloud email providers, and (3) Integrated Cloud Email Security (ICES). SEGs are the most commonly adopted email security solution. They offer basic security capabilities such as spam filtering and quarantine capabilities, URL rewriting, antivirus scanning, sandbox integration, post-delivery clawback, and more advanced outbound capabilities such as data leakage prevention and email encryption. SEGs can be deployed as an on-premises appliance, a virtual appliance, or delivered as a cloud-based service.

Exhibit 142: Secure Email Gateway Workflow



Source: Barracuda

Cloud-based email systems such as Microsoft Office 365 and Google Workspace have also gained popularity. These email security solutions incorporate basic native email hygiene security capabilities, including blocking emails from known bad senders, URL filtering, and antivirus scanning. While cloud providers continue to enhance their capabilities and add more advanced security controls, enterprises have more commonly adopted third-party ICES solutions that use APIs to access cloud email providers. This allows enterprises to analyze email content without changing the Mail Exchange (MX) records. ICES solutions offer advanced pre-delivery (intercept emails before they reach a user's inbox) and post-delivery (analyze emails and hide bad ones to prevent the user from opening them before the email is scanned) capabilities. They also incorporate sophisticated anomaly detection capabilities such as natural language understanding (NLU), natural language processing (NLP), and image recognition, and leverage email history and visibility into internal traffic to build ML baselines to improve detection. Some ICES vendors have also introduced context-based warning banners to enhance security awareness and API integrations to filter malicious content or suspicious interactions on

messaging tools such as Microsoft Teams and Slack. Given the maturity of the SEG market, we expect traditional email security vendors to expand their offerings to include API-based ICES. Mimecast and Cisco have already added such capabilities, and we expect other vendors to follow suit.

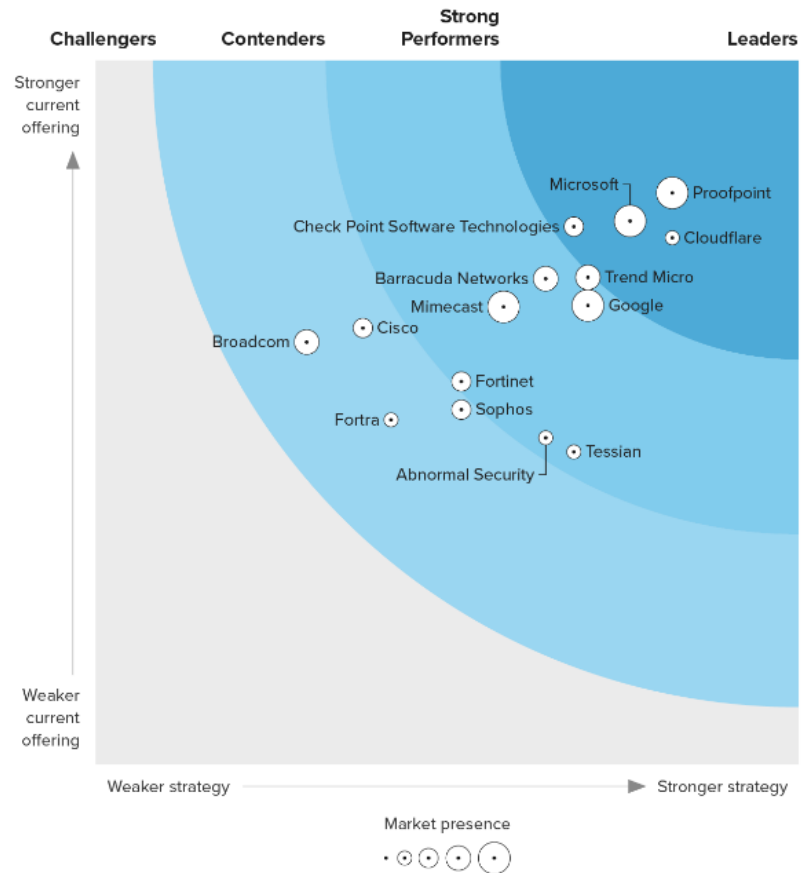
In recent years, BEC attacks that rely heavily on social engineering and take advantage of a user's behavioral characteristics to trick unsuspecting employees and executives into performing unauthorized tasks (for example, impersonating a CFO and approving a wire transfer to an unauthorized account) have become more common. To address these threats, vendors such as Proofpoint and Mimecast have expanded their solutions to include AI/ML-based anti-phishing technology to analyze context-based behavior to detect such fraud. Email security vendors have also implemented Domain-based Message Authentication, Reporting, and Conformance (DMARC) specifications to authenticate emails, detect unauthorized usage of email domains, and automatically block the delivery of unauthorized emails.

We expect small and medium-sized organizations to increasingly utilize the native security capabilities of cloud email providers. This illustrates the significant advances cloud vendors have made in improving the effectiveness of their protection and ease of use benefits from simplified configuration and management. As for large enterprises with more complex email protection needs, we expect them to leverage cloud-based email services with ICES solutions for more advanced protection (AI/ML-based anti-phishing capabilities, conversation history analysis, anomaly detection, BEC protection, etc.).

Looking forward, we expect email security vendors to broaden their APIs and integrations with XDR and SIEM/SOAR solutions from a technology roadmap viewpoint to deliver more contextual awareness of attacks. In this context, we also expect EDR and XDR vendors to add email security capabilities or form partnerships with existing email security vendors to bring in email telemetry and strengthen the efficacy of their broader XDR offerings. In particular, we believe CrowdStrike's XDR alliance, which integrates with leading email security vendors like Proofpoint and Mimecast, is a recent example of this effort.

Email Security Market Vendor Overview

Exhibit 143: Forrester Email Security Wave



Source: Forrester (2Q23)

Below, we review several of the broader Email Security vendors.

- Proofpoint.** Proofpoint offers a range of email security products led by its SEG solution, which secures inbound and outbound email and leverages machine learning to identify and block phishing threats. The company takes a people-centric approach and offers security awareness training to educate users against phishing attacks and malware infections. Proofpoint's SEG is fully integrated with its broader product portfolio, which includes threat response (quarantine malicious messages post-delivery), email fraud defense (authorize legitimate senders and identify lookalike domains), and CASB solutions (identify suspicious logins in cloud applications).
- Mimecast.** Mimecast offers a robust email security platform. Its SEG provides basic capabilities such as phishing and malware protection and advanced capabilities such as real-time URL scanning, attachment scanning, BEC prevention, browser isolation, and post-delivery remediation. Like Proofpoint, Mimecast offers security awareness training, brand protection, and email incident response. It also provides a targeted email security solution for Office 365 that works with Microsoft Exchange Online Protection. The solution integrates email security, cloud archiving, and mailbox continuity, delivering uninterrupted access if Outlook is offline.
- Microsoft.** Microsoft provides email security integrated with Exchange Online Protection (EOP) and Microsoft Defender for Office 365. EOP is Microsoft's basic offering, including anti-spam, anti-malware, and anti-phishing capabilities. Microsoft Defender offers more advanced capabilities, including safe links and attachments and a broad set of integrations with other security tools within the Microsoft ecosystem. While Microsoft's bundled plans can be expensive, its large Office 365 installed base makes it one of the leading competitors in the market.

- **Check Point.** Check Point offers email security by acquiring Avanan, which has been rolled into the company’s Harmony product line. The company’s product leverages an API-based deployment mode that protects Microsoft 365, Google Workspace, Slack, and other collaboration & cloud storage applications (OneDrive, SharePoint, Teams, DropBox). Check Point’s solution addresses many use cases, such as ransomware prevention, account takeover, BEC, phishing, and data loss prevention.
- **Abnormal Security.** Abnormal offers an ICES platform that protects against various attack types, including BEC, credential phishing, payment fraud, account takeover, and supply chain compromise. Abnormal’s offering allows customers to displace their legacy SEG by deploying an ICES alongside Microsoft Office 365 and Google G-Suite. The company’s solution also provides behavioral AI that can integrate with Microsoft’s threat intelligence products to automate alert triage and eliminate the need for manual configurations.
- **Tessian.** Tessian offers an ICES platform that addresses phishing, BEC, and account takeover attacks. The platform also prevents data loss from misdirected emails and data exfiltration from malicious insiders. The company offers a platform solution and four products (Defender, Guardian, Enforcer, and Architect). Tessian provides integration with Microsoft Office 365.

Endpoint Security

Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR)

The Endpoint security market focuses on securing connected endpoints, such as PCs, laptops, tablets, printers, servers, and IoT devices, and remediating threats and breaches. Endpoint security was primarily addressed by Endpoint Protection Platform (EPP) solutions, which use device-installed agents to manage and secure endpoints. They incorporate a range of capabilities, including malware protection, anti-virus protection, signature matching, sandboxing, white- and black-listing, and data encryption, to more advanced intrusion prevention and basic behavioral analysis. The EPP market is dominated by legacy anti-virus vendors such as McAfee and Symantec.

As the threat landscape evolved (advanced persistent threats, fileless attacks, etc.) and remote work became more prevalent, the need to deliver real-time visibility into endpoint activities and more advanced capabilities to address sophisticated attacks became acute. This has contributed to the rise of new cloud-based vendors offering more advanced Endpoint Detection and Response (EDR) solutions.

Exhibit 144: EPP vs. EDR

EPP	EDR
Prevents a wide variety of known threats and some unknown threats	Enables response to unknown threats that EPP could not detect
First line of defense - scan, identify, block	Second line of defense - contain, investigate and respond
Passive threat protection. Does not remediate breaches after they occur - does not provide visibility into endpoint activity	Active - Used to counter evasive threats that get past security defenses. Also provides proactive threat hunting
Does not provide visibility into endpoint activity	Provides visibility into endpoint activity by aggregating event data across all endpoints in the enterprise
Protects endpoints through isolation	Provides context and data for attacks across multiple endpoints

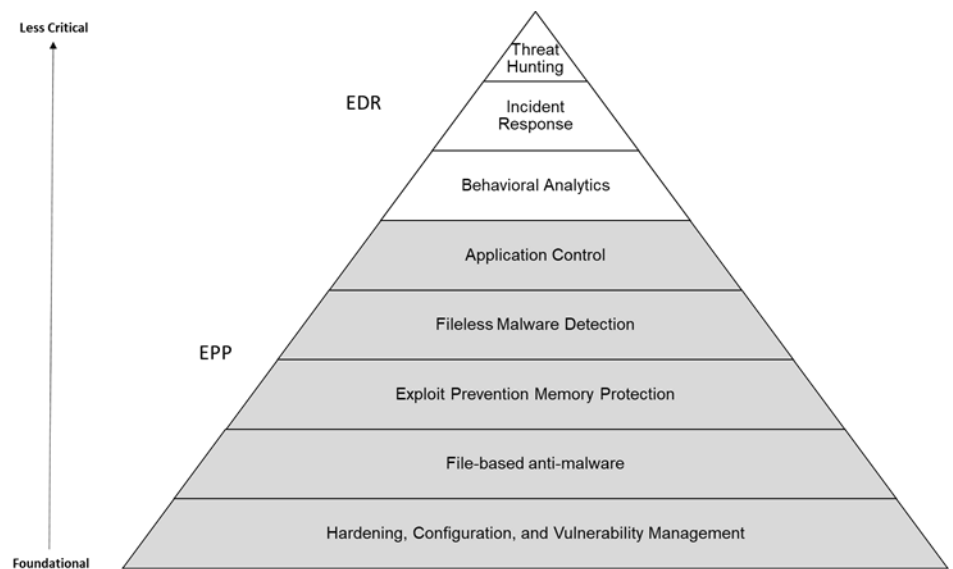
Source: Oppenheimer & Co.

EDR solutions monitor, record, store, and analyze endpoint-specific data and user/file behavior to provide real-time contextual visibility into endpoint activities. Once malicious activity is detected, EDR solutions trigger an incident response and investigation. They can also block malicious activity, quarantine endpoints, and begin remediation. These

capabilities actively address threats and reflect an underlying assumption that a breach has already occurred. In line with this point of view, EDR solutions implement threat-hunting tools and provide visibility and operational tools to locate and contain breaches. The EDR market is broad and consists of legacy EPP vendors such as Symantec, McAfee, and Microsoft and new, next-gen cloud-based endpoint security vendors such as CrowdStrike and SentinelOne.

Modern EDR solutions provide organizations with additional flexibility compared to EPP solutions. EPP solutions only look at file-based malware, do not provide visibility into activity on the endpoint, and rely on previously recognized and known signatures and attributes to detect an intrusion of a known threat. This limits their ability to detect never-before-seen, zero-day attacks. In contrast, EDR solutions take a more active threat detection approach and add an extra layer of defense to EPP solutions by analyzing endpoint behavior. They also use threat-hunting tools to detect and contain zero-day attacks after they occur. Given the rise of fileless attacks, organizations increasingly adopt EDR solutions and leverage behavioral analytics to prevent and mitigate advanced threats.

Exhibit 145: EPP vs. EDR Capability Hierarchy



Source: Gartner, Oppenheimer & Co.

Endpoints are often the landing point for threat actors conducting ransomware attacks. This highlights the importance of preventing endpoint-based attacks and implementing rapid remediation and containment. Consequently, the lines between the EPP and EDR solutions have blurred, and vendors in both markets have expanded their capabilities to provide a holistic endpoint security solution. To put this blurring in perspective, all the leaders in Gartner's last published *EPP Magic Quadrant* (2021) also offer comprehensive EDR solutions. Given the overlap, the EPP and EDR markets are now viewed as a single market.

Exhibit 146: Gartner EPP Magic Quadrant



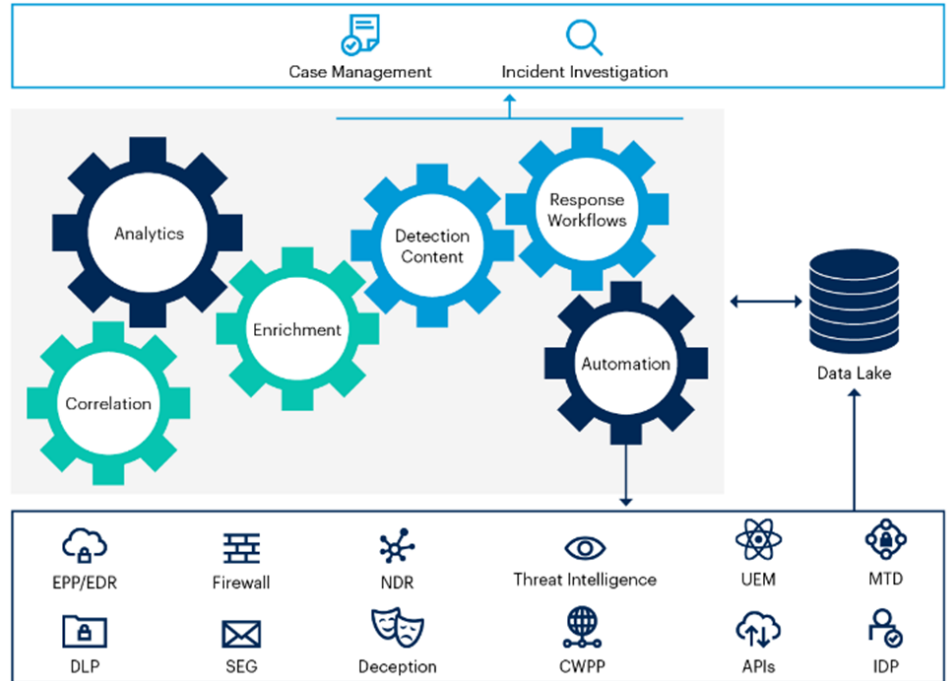
Source: Gartner

In terms of adoption, most enterprises today have implemented an EDR solution, and we expect growth to come from seat expansion. We see a more significant growth opportunity within the mid-market/SMB space, where EDR adoption is still limited, given the significant skills shortage and additional costs required to deploy and actively manage EDR solutions. Compared to EPP solutions, which run with minimal supervision, EDR solutions require active investigation and analysis by security teams to respond to threats appropriately. To mitigate this challenge, many EDR vendors offer Managed Detection and Response (MDR) services that provide fully managed EDR capabilities such as threat monitoring and alert triage. CrowdStrike's Falcon Complete and SentinelOne's Vigilance Respond are good examples of MDR solutions offered by EDR vendors. The rise of generative AI provides an opportunity for EDR vendors to lower the barriers to adoption further by introducing AI assistants. Solutions like Charlotte AI from CrowdStrike leverage generative AI to help security teams improve their ability to stop breaches while reducing operating complexity. We expect other EDR vendors to follow suit and introduce security assistants that leverage generative AI. In the long term, we expect enterprises to adopt Extended Detection & Response (XDR) solutions, which draw telemetry data from different security solutions (firewalls, SWG, email gateways, etc.) into a single security operations system to reduce security product sprawl and improve incident response.

Extended Detection & Response (XDR)

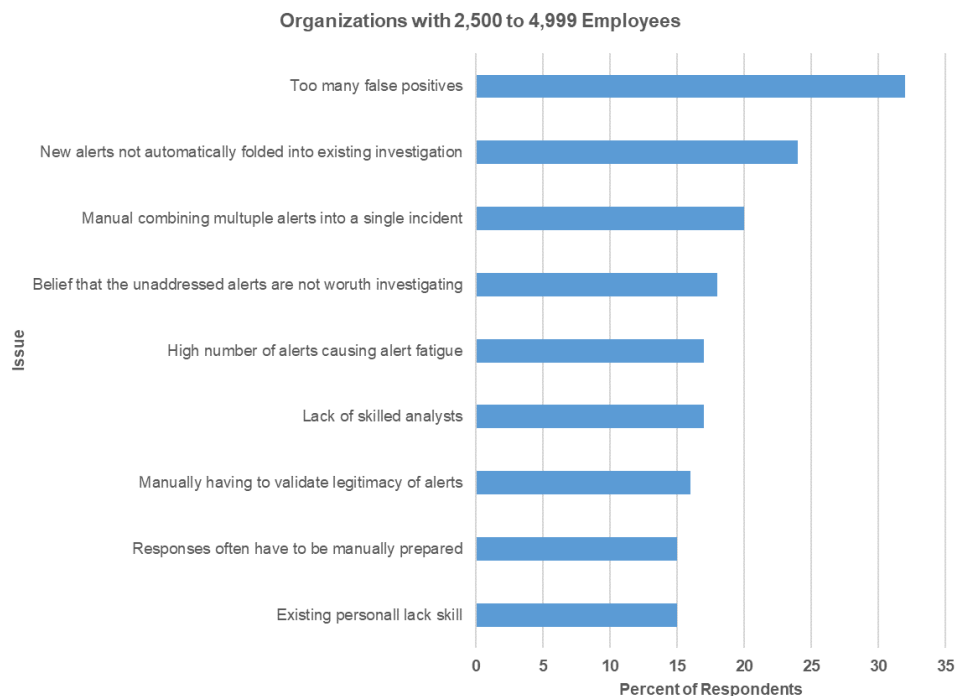
XDR solutions aim to deliver improved threat detection, prevention, and incident response. While EDR tools collect and monitor data from agents installed on endpoints, XDR platforms take a broader approach. They integrate, correlate, and contextualize data and alerts from multiple security components (network firewalls, endpoints, CASBs, IAM solution, cloud security stack, etc.). Once the telemetry is ingested into a data lake, advanced analytics correlates and streamlines alerts into specific active incidents for more accurate responses. XDR platforms can reduce the number of security tools and the sprawl of incident alerts while addressing the integration challenges of managing an extensive portfolio of best-of-breed security solutions. XDR solutions are SaaS-based and can be closed (only integrating with a vendor's other security solutions) or open (integrating with third-party security solutions via APIs).

Exhibit 147: XDR Components



Source: Gartner

Before XDR tools became available, security teams commonly used EDR solutions to draw telemetry from endpoints and security analytics solutions, such as SIEM, to better correlate alerts and more rapidly address security threats. The challenge of this approach is the significant investment in human resources and time needed to accurately tune and configure the tools and match SIEM data with EDR data. Consequently, SIEM deployments have been typically used by large enterprises that have highly qualified security operations teams and stricter compliance requirements. While XDR solutions still require hands-on oversight, their tightly integrated management console and broader analytics use cases they support can simplify deployments, eliminate the challenge of matching SIEM with EDR data, consolidate security tools, and lighten the load on small and mid-sized businesses that lack skilled security labor. In fact, Gartner estimates that by the end of 2028, 30% of organizations will deploy XDR to consolidate their security tools (vs. 5% today).

Exhibit 148: IDC Survey: What Prevents Security Teams from Investigating Alerts

Source: IDC

As opposed to SIEM tools, XDR solutions provide out-of-the-box integrations with a wide range of security tools. This supports rapid deployment and facilitates data transfer, ingestion, and collection in data lakes for advanced analysis, correlation, and contextualization. It's important to note that XDR solutions are generally built on EDR technology, commonly implemented on endpoints. This exposes XDR solutions to the most significant attack surface within an organization and provides them with the richest telemetry data sources for analysis and response.

While XDR solutions are promising, they are still in the early stages of development and maturity and often reflect various vendor approaches and core competencies. Most XDR solutions are still evolving and early in their maturation process. They also don't address use cases beyond threat detection and incident response. For example, enterprises that need to meet specific compliance and regulatory requirements for log retention still need to implement SIEM tools. As such, SIEM tools remain in high demand, especially with security operations teams in large enterprises with the resources and know-how to successfully stand and operate them. XDR tools are exceptionally well suited for companies with smaller security teams and less stringent compliance/regulatory requirements that can benefit from greater automation.

From a vendor perspective, the early entrants in the market were largely endpoint security vendors (like CrowdStrike, SentinelOne, and Trend Micro) applying analytics to the rich telemetry their EDR tools ingested. Over time, broader platform security vendors (like Palo Alto, Microsoft, and Cisco) that consolidate data and telemetry from multiple domains have also entered the market. We expect XDR vendors to partner closely and build integration ecosystems to broaden their telemetry collection capabilities, facilitating faster data ingestion and threat detection. Functional XDR solutions will need to integrate telemetry from network firewalls, CASBs, IAM solutions, and EDR solutions at a minimum. CrowdStrike's CrowdXDR alliance is an example of a developing ecosystem that standardizes data transfers among participating vendors for faster and efficient detection and remediation. It's important to note that we expect XDR vendors to add SIEM capabilities to address compliance related use cases required for large enterprise adoption. Cisco's acquisition of Splunk, CrowdStrike's acquisition of Humio, and Palo Alto's XSIAM solution are examples of this convergence. Last, we expect MDR vendors to expand their offerings to address Managed XDR (MXDR). We believe vendors with strong

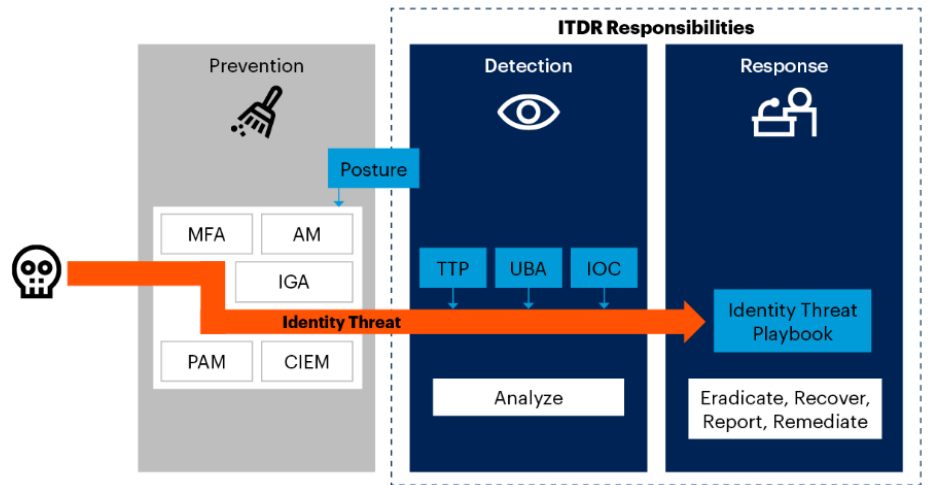
service capabilities have an advantage, especially with small and mid-sized customers that lack comprehensive security operations teams.

Identity Threat Detection & Response (ITDR)

The increase in identity-based attacks has created the need to secure user identities and passwords and the underlying access management infrastructure. Threat actors often attempt to forge SAML tokens from compromised service accounts to facilitate lateral movement. Rather than focusing on user authentication with traditional access management solutions, ITDR solutions act as an additional line of defense focused on securing and managing the underlying identity infrastructure (Okta, Active Directory, etc.).

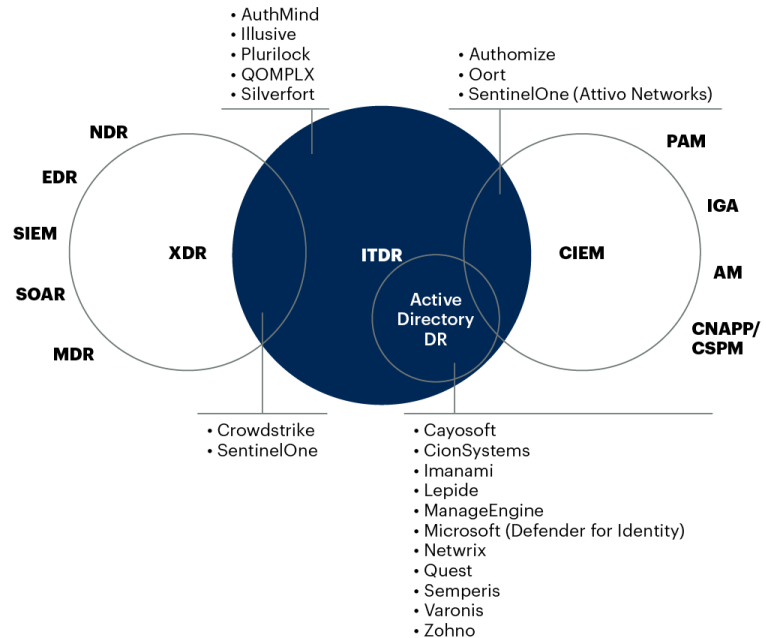
ITDR solutions enable security teams to map and identify all service and privileged accounts within their networks and analyze them for stale credentials that could be compromised. Once mapped, ITDR solutions ingest telemetry from identity security platforms to monitor authentication traffic and create a baseline of standard behavior to identify anomalous activity and unusual escalation of privileges. Solutions such as CrowdStrike’s Falcon Identity Protection can monitor authentication traffic in real-time, enabling customers to reduce the time between breach and detection. Once a breach is detected, ITDR tools alert SIEM or XDR solutions to trigger a response. Other ITDR capabilities include policy evaluation, configuration management, and threat intelligence.

Exhibit 149: ITDR Responsibilities



Source: Gartner

While the ITDR market is nascent, multiple vendors have entered, and competition is intensifying. Microsoft has emerged as an early leader with its Defender for Identity solution. However, Microsoft Defender for Identity only secures AD environments, and since most large enterprises use multiple identity security tools, we expect customers to leverage various ITDR vendors. Other notable vendors who have expanded into ITDR include CrowdStrike (via its acquisition of Preempt), SentinelOne (via its acquisition of Attivo Networks), and Tenable (via its acquisition of Alsid). The market has also seen interest from traditional IAM vendors, with Okta announcing its ITDR solution. While it is unclear who the longer-term winners in the market will be, we expect vendors with strong threat detection & response capabilities to hold an edge given the need to feed identity logs and signals to a SIEM or XDR to accomplish ITDR.

Exhibit 150: ITDR Market Overlap

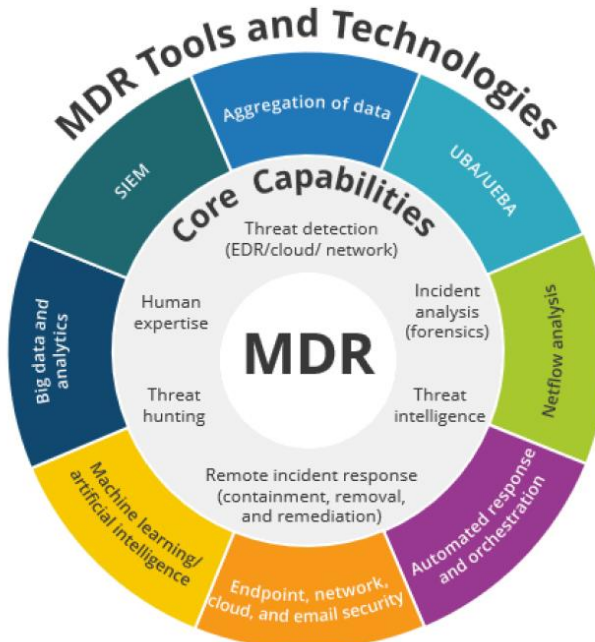
Source: Gartner

Managed Detection & Response (MDR)

In contrast to traditional EPP solutions, which run with minimal supervision after initial installation and configuration, EDR solutions require active monitoring, investigation, and analysis by trained security experts to respond to and remediate discovered threats appropriately. However, the shortage of skilled security professionals has made the implementation of EDR solutions challenging and pushed enterprises to look for MDR services from the EDR vendors themselves and third-party managed security service providers (MSSPs). MDR services combine the people, expertise, processes, and technologies needed to implement EDR capabilities, such as advanced detection and response, threat intelligence and monitoring, and alert triage.

MDR solutions are designed to reduce threat detection and response time by implementing remote 24/7/365 managed security operations center (SOC) capabilities. The services include log management, advanced analytics, threat intelligence, exposure management, digital forensics and incident response, and human expertise. And while MDR services have commonly addressed endpoint and network domains, they increasingly involve cloud services, SaaS, and custom applications. More advanced MDR services go beyond legacy remote-SOC services, collect and analyze telemetry data (logs, data, and contextual information), integrate with SIEM systems, provide contextual information (identity and user, threat exposure, etc.), customized threat hunting and threat detection, containment services, and remediation on behalf of the customer.

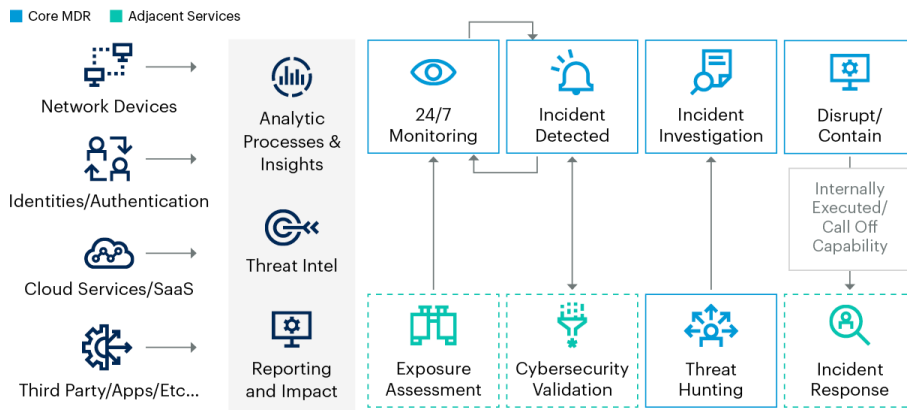
Exhibit 151: MDR Tools and Technologies



Source: IDC

MDR offers turnkey services designed to address a predefined technology stack, such as endpoints or network security, and it can be extended to protect cloud environments. Many MDR vendors offer services that include their proprietary technologies (like CrowdStrike’s Falcon Complete). In contrast, others are more open and manage third-party solutions already in the customer’s environment while providing the centralized back-end infrastructure to correlate and analyze data (like Artic Wolf). MDR services have also been extended to address cloud environments. For example, Arctic Wolf’s Cloud Detection & Response platform service offers 24/7 threat monitoring and incident response that helps under-resourced customers identify and mitigate threats across common IaaS and SaaS assets such as AWS, Microsoft 365, Google Workspace, Salesforce, and Box. Generally, MDR service providers differentiate with their ability to support robust data analysis, threat detection, and response capabilities, breadth of security capabilities, and quality of customer service and support. Given the growing value that MDR services deliver and the complexity of the threat landscape, Gartner estimates that by 2025, 60% of organizations will be actively using remote threat disruption and containment capabilities delivered by MDR providers, up from 30% today.

Exhibit 152: MDR Capabilities



Source: Gartner

We note a distinct difference between an MDR service and a managed-EDR or managed-XDR solution. Many of the latter solutions often lack high-touch, hands-on human engagement, a defining characteristic of a true MDR service. MDR customers often seek to leverage the services as an extension of their SOC. In contrast, managed point solutions are more limited in scope, focus more on eliminating the configuration work for the customer, and only come with a low-touch human component. MDR also differs from traditional MSP/MSSP offerings, which focus on managing security infrastructure (firewalls, networking hardware) rather than incident response use cases. We believe vendors who offer full 24/7 human engagement (i.e., CrowdStrike, Artic Wolf, eSentire) are better suited to address (capture share) solutions within the MDR market as they can alleviate key security pain points for organizations, especially small and medium-sized businesses that lack the skills, expertise, and human resources needed to deploy a modern security operations center. We expect such organizations to increasingly consider MDR services as their primary SOC and provide 24/7 protection and threat defense.

While MDR has largely been endpoint- and network-focused, many vendors have added capabilities to ingest telemetry data from beyond the endpoint (cloud infrastructure, SaaS applications, and identity solutions) as they look to deliver XDR. XDR can still be difficult to implement as it requires integrations and correlation work, presenting an attractive opportunity for existing MDR vendors. Some MDR vendors, such as CrowdStrike, have already released an XDR solution that leverages an alliance of integrations with other major security vendors. We expect more vendors to expand their platforms to offer native XDR and add integrations with leading security vendors. Last, we expect ITDR technology to become an MDR service as customers focus on securing identities vs. endpoints.

Considering various vendor approaches and some overlap between EDR, XDR, and MDR solutions, it is important to highlight their fundamental differences. The primary difference between EDR and XDR revolves around the scope of security tools addressed. EDR is strictly endpoint-focused, whereas XDR takes a comprehensive approach to managing multiple security tools across various domains (endpoint, network, and cloud). MDR and managed-XDR apply EDR and XDR technology through a service-based model that addresses customers who lack the resources to scale and operate EDR or XDR solutions.

Exhibit 153: EDR vs. MDR vs. XDR Comparison

EDR	MDR	XDR
Offers behavior-based detection engines	Allows organizations to outsource security tasks and ensure 24/7 coverage	Offers all capabilities of EDR but extends to broader systems for end-to-end protection
Can be deployed on-premises or in the cloud	Provides system-wide or targeted coverage	Can analyze internal and external traffic with machine learning-based technology
Centralized management console for all endpoints	Dedicated professionals who can provide manual threat hunting to uncover advanced threats	Offers rule and behavior-based detection engines
Focus exclusively on endpoints and endpoint dependencies	Capabilities dependent on vendor	Enables security orchestration across environments
Used to perform kill-chain analysis, threat quarantine, and automated remediation	Contractual services that reduce technical debt	Can quickly and easily scale to meet organizational need

Source: Oppenheimer & Co.

Endpoint Security Market Vendor Overview

Almost all legacy EPP vendors have introduced EDR solutions in recent years and vice versa. Also, given the complexity of managing EDR deployments, nearly all vendors have added MDR services to complement their solutions. As for XDR, while the technology is still nascent, several vendors have introduced XDR offerings and are working on

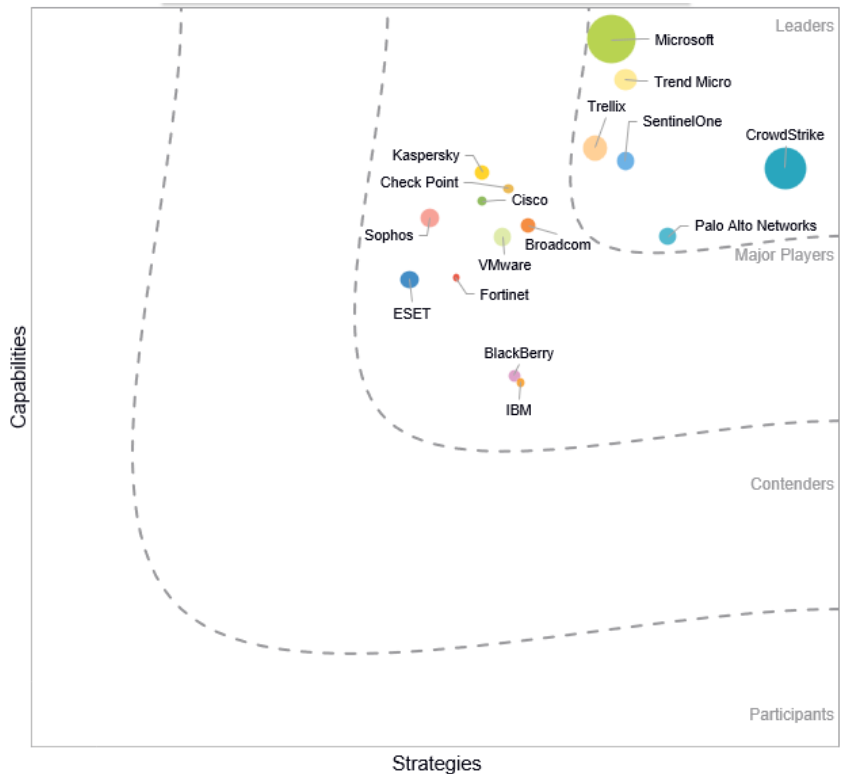
expanding the reach of their telemetry collection by adding integrations to third-party tools. Generally, all XDR solutions are relatively immature.

Exhibit 154: Gartner EPP Magic Quadrant



Source: Gartner

Exhibit 155: IDC 2024 Enterprise Endpoint Security MarketScape



Source: IDC

Exhibit 156: Forrester 2023 MDR New Wave



Source: Forrester (Q2 2023)

- Microsoft.** Defender for Endpoint (MDE) is Microsoft's comprehensive endpoint security solution, and it incorporates EPP, EDR, and threat-hunting capabilities, while Defender Antivirus of Windows OS is the company's EPP solution. Defender Antivirus is included in all of Microsoft's Enterprise plans. At the same time, MDE is only available in the more configured and expensive E5 plan, which also offers adjacent security solutions such as DLP, CASB, and email security. MDE offers seamless integrations with Microsoft's security solutions, allowing customers to create an effective XDR platform managed by a single cloud console. The underlying data lake enables deeper automation and unified threat hunting. Microsoft's endpoint security solutions are widely adopted globally, with strong adoption among enterprises looking to consolidate their security stack with a single vendor. Microsoft currently holds a leading position in XDR, given its broad reach across multiple security domains.
- CrowdStrike** offers a comprehensive endpoint protection platform with EPP, EDR, MDR, and XDR solutions. Its cloud-native platform is built on a single agent architecture that provides an easy-to-use management console and various modules for specific use cases, including Falcon Prevent (next-gen antivirus), Falcon Insight (EDR), Falcon Overwatch (threat hunting), FalconXDR, and Falcon Complete (MDR). The company also addresses log management and SIEM use cases with LogScale and offers modules for CWPP, CSPM, ASPM, and ITDR. Given the growing breadth of its product portfolio, CrowdStrike is firmly positioned to target customers looking to consolidate their security architecture. Its cloud-native, single-agent architecture enables frictionless expansion and helps customers alleviate agent bloat.
- SentinelOne** offers EPP, EDR, MDR, and XDR capabilities through its single-agent Singularity SaaS platform. Singularity Complete is the company's XDR platform, which layers behavioral AI on top of a fully-featured EDR solution to prevent known and unknown threats. SentinelOne Vigilance is the company's MDR and digital forensics and incident response (DFIR) service that builds off Sentinel's single-agent architecture to contextualize data flows. The company strengthened its capabilities

through its 2021 acquisition of log monitoring vendor Scalyr and expanded into the CWPP and ITDR segments.

- **Palo Alto Networks** offers EDR, XDR, and XMDR through its Cortex platform. The company's EDR solution uses a cloud-delivered agent to deliver antivirus, disk encryption, and vulnerability assessment capabilities. Cortex XDR ingests logs and telemetry from endpoints, networks, and cloud environments and then incorporates ML- and AI-driven analytics to deliver a comprehensive detection and response solution. Cortex also offers network traffic analysis (NTA) and user and entity behavior analytics (UEBA) capabilities. These capabilities fully integrate with Palo Alto's firewalls and cloud offerings to deliver endpoint attack prevention, alert triage, incident response, and threat hunting. Palo Alto also offers a managed XDR service, Cortex XMDR, which provides 24/7 coverage for resource-constrained customers.
- **Arctic Wolf** is a security operations provider that offers MDR, cloud detection & response (CDR), vulnerability and risk management, and CSPM solutions. The company currently focuses on small and medium-sized businesses that lack security expertise and detection & response capabilities. Its architecture is built on an open XDR architecture that allows customers to deploy customized detection and vertical-specific rules. Its platform relies on internally developed, proprietary sensors that collect logs from a customer's security technologies (firewalls, CASBs, endpoint protection tools) and IaaS (AWS, Azure, GCP) and SaaS (Office 365, Active Directory) applications. Arctic Wolf prices its offerings based on the number of endpoints protected and server sensors required. Unlike most competing managed security vendors, Arctic Wolf offers customers unlimited data collection and free 90-day log retention.
- **Cybereason** offers a comprehensive endpoint security portfolio with EPP, EDR, MDR, and XDR solutions. The company's EPP modules offer definition- and ML-based detection and use behavioral analysis and deception techniques to quickly detect and remediate malicious files. Its XDR solution extends EDR functionality to detect attacks on endpoints, the cloud, and the network. Cybereason is built on a cross-machine correlation engine that can automatically condense telemetry collected from multiple endpoints into one alert with a full attack story and root cause analysis. The platform integrates with leading security and infrastructure software vendors such as Okta, AWS, and G-Suite.
- **Vectra** offers an AI-enabled detection and response solution. The platform extracts metadata from network packets and logs across public cloud, SaaS, IAM, and data center environments and analyzes them with AI to detect attack methods in each domain. The company also leverages ML algorithms such as deep learning neural networks and hierarchical clustering. The Vectra platform can draw data from AWS, Azure, and hybrid cloud environments and offers native integrations with popular EDR (Carbon Black, SentinelOne, CrowdStrike), SIEM/SOAR (Splunk, Microsoft Sentinel, IBM QRadar), and ITSM (Jira, ServiceNow) solutions. Vectra also offers an MDR service called Vectra Sidekick.
- **eSentire** offers a suite of MDR, managed SOC services, and a comprehensive XDR platform. The company initially offered a Network Detection & Response (NDR) use case that was tailor-made for servicing hedge funds and other financial services customers. In 2017, eSentire expanded its portfolio and released its first MDR service, and later added an XDR-based service (called Atlas), which provides correlation of a wide range of telemetry (logs, cloud, network, endpoint) and offers 24/7 threat hunting with dedicated SOC analysts. The company also provides proprietary threat intelligence via a team of internal researchers. The company offers a multi-tiered pricing program and a specialized service to secure Microsoft environments.
- **Deepwatch** offers a comprehensive managed security platform, including MDR, threat hunting, EDR, and vulnerability management. The company takes a collaborative approach, leveraging customers' internal SOC teams to develop identity & asset risk profiles, map attack surfaces, and ensure effective security policies are in place. Once profiles are established, the platform prioritizes vulnerabilities based on

the customer's specific environment and priorities, reducing the volume of alerts. The company combines its platform with 24/7/365 security experts.

- **ReliaQuest** offers a managed-SOC solution centered on its GreyMatter platform, which automates detection, investigation, and response across cloud, endpoint, and on-premise applications. The platform leverages an XDR architecture, integrating and ingesting telemetry from leading third-party SIEM, EDR, and network security tools within a customer's environment. Once ingested, the platform leverages its proprietary Universal Translator to normalize telemetry data and provide visibility across a customer's toolset. The company also addresses Breach and Attack Simulation, Threat Intelligence, and Digital Risk Protection use cases.

Security Operations

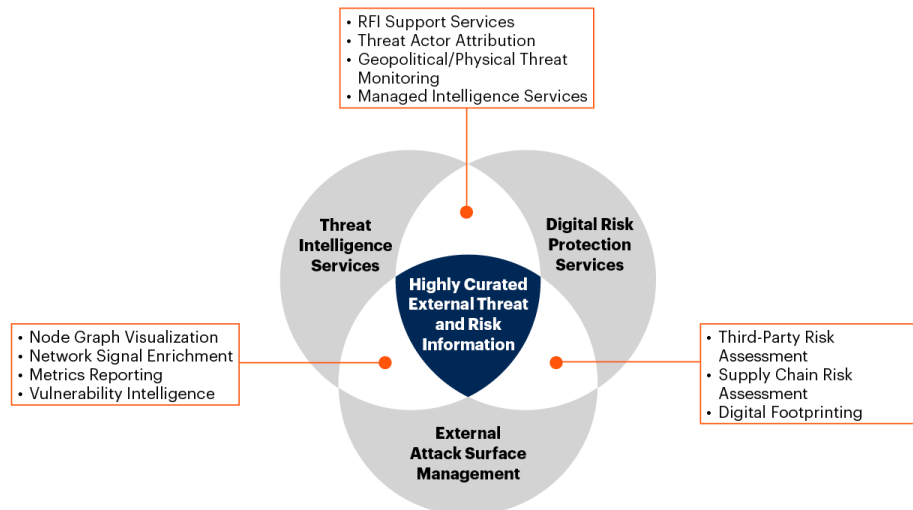
Threat Intelligence (TI)

TI solutions provide enterprises with knowledge, information, and data about global cybersecurity threats to better understand their identities, motivations, tactics, and methods. Security teams use this knowledge to prepare and improve their security posture and reduce the risk of a security breach. TI solutions utilize machine learning to automate data collection, disseminate intelligence, and integrate with the existing enterprise security stack to provide an improved and broader threat context (type of threat, attacker profile, motivation, etc.).

Data collection is critical for TI solutions. They gather raw data from various internal and external sources such as network log data, records of past incident responses, the open web, and the dark web (Internet sources that are not indexed by search engines and not accessible to the general public like medical and financial records, private forums, B2B networks, academic information, etc.). Once collected, the raw data is combed to identify threat data such as lists of threat actor profiles, indicators of compromise (IoCs), threat libraries and news, malicious IP addresses, URLs, and domains. Security teams then use the data for various use cases, such as attack emulation, detection engineering with SIEM tools, and incident response enrichment with SOAR tools.

With the high labor cost associated with analyzing TI data (labor-intensive), several vendors, such as Recorded Future, have introduced solutions with integrated machine learning capabilities to facilitate data collection and analysis, primarily when related to unstructured data. Nonetheless, it is important to note that given the breadth of information on the web, every TI vendor typically has access to data sources that others may not have access to. This has led to market fragmentation and growing enterprise reliance on multiple TI vendors to minimize threat blind spots.

Mature TI solutions have historically focused on feeding intelligence and data about threat actors and IoCs to SOC teams. More recently, solutions have expanded into adjacent areas to provide curated TI to identify IoCs within a customer's environment. Since then, we've seen TI vendors adding External Attack Surface Management (EASM) and Digital Risk Protection Services (DRPS), which focus on identifying and monitoring Internet-facing IT assets. By leveraging EASM and DRPS, TI vendors can map a customer's attack surface in detail and provide actionable intelligence specific to the customer's attack surface. We discuss EASM and DRPS in greater detail in our Attack Surface Management (ASM) section.

Exhibit 157: Threat Intelligence, DRPS, and EASM Overlap

Source: Gartner

Today, large enterprises broadly adopt TI solutions within their modern SOCs. Such organizations have sophisticated teams that require complex TI features and often collect knowledge from multiple sources. In contrast, small and mid-size organizations have yet to build out TI programs, given their limited SOC resources. We expect this base of customers to increasingly leverage managed TI services or solutions that offer machine learning-enabled automation (like Recorded Future). This user base represents a significant growth opportunity for TI vendors. In contrast to the traditional TI market, the DRPS and EASM market is relatively early in its adoption cycle, and we expect these solutions to see widespread demand from large to SMB customers.

Vendors from other security domains have also added TI capabilities to round out their solutions. Examples include Palo Alto, which added TI into its Cortex platform, and CrowdStrike, which introduced a separate TI module, Falcon intelligence. Importantly, vendors like CrowdStrike and Microsoft can source original threat intelligence from the telemetry gathered by their EDR agents. This is a competitive advantage to pure-play threat intelligence vendors who focus on aggregating intelligence from various external sources. Moving forward, we expect more platform vendors to add threat intelligence to their offerings and for smaller traditional TI vendors to be acquired and offered as an add-on capability in broader platforms. Recent examples of security vendors acquiring TI vendors include Rapid7's acquisition of IntSights (DRPS and attack surface management vendor) and Microsoft's acquisition of RiskIQ (threat intelligence and DRPS vendor). Last, we expect convergence between the TI, Vulnerability Management, and Attack Surface Management markets (discussed in the next section), considering their overlapping focus on identifying vulnerabilities within customer environments.

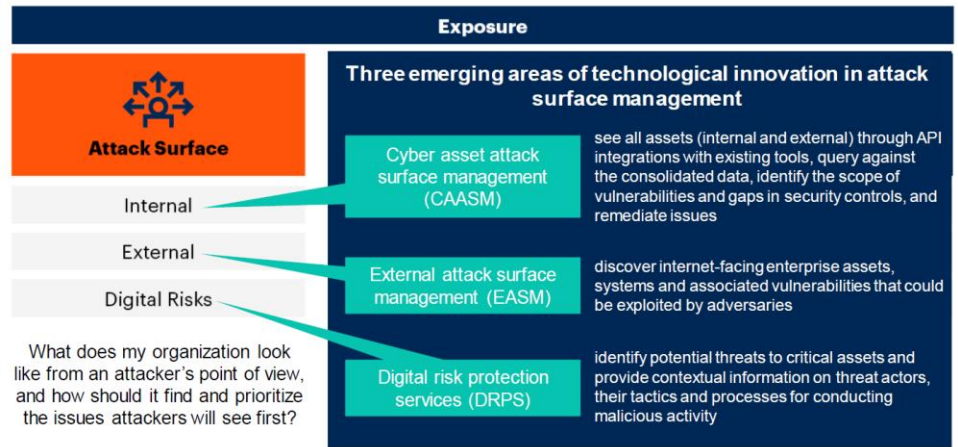
Attack Surface Management (ASM)

The growth in public cloud usage, adoption of hybrid-work models, and acceleration in digital transformation have led to an explosion in IT assets and widened the attack surface. IT teams often struggle to map their digital estate, including traditional internal assets (servers, on-premise applications), cloud assets, microservices, human & machine identities, IoT devices, SaaS applications, and external brand social media accounts. The added complexity from the explosion in assets has created gaps in security posture, leaving IT teams with no accurate visibility and knowledge of their actual IT footprint. Attack Surface Management tools address this growing challenge, facilitate, and automate the discovery and management process of all the assets mentioned above.

Historically, IT teams relied on vulnerability scanners to manage and secure their IT assets. However, these tools only scanned identified and known internal IT assets, leaving unknown and external assets exposed. ASM tools instead use a combination of technologies and services to continuously discover, inventory, and manage internal and external assets and reduce the exploitable attack surface. The ASM market consists of

three key components: (1) External Attack Surface Management (EASM), (2) Digital Risk Protection Services (DRPS), and (3) Cyber Asset Attack Surface Management (CAASM).

Exhibit 158: ASM Technologies



Source: Gartner

EASM includes professional services and technologies that give organizations visibility into their known and unknown, externally facing assets. These solutions ingest Internet data sources and automatically discover and map publicly facing assets such as IP domains, certificates, and services running in on-premises and cloud environments. Once inventoried, EASM tools analyze the assets to identify exploitable entry points (such as systems credential and public cloud misconfigurations and third-party software code vulnerabilities), providing security and IT teams with an external attacker's view of their IT footprint. EASM tools complement vulnerability assessment and CSPM tools that actively prioritize and remediate vulnerabilities and misconfigurations. Common use cases addressed by EASM tools include digital asset discovery and inventory, cloud security and data governance, data leakage protection, subsidiary risk assessment, and M&A risk assessment.

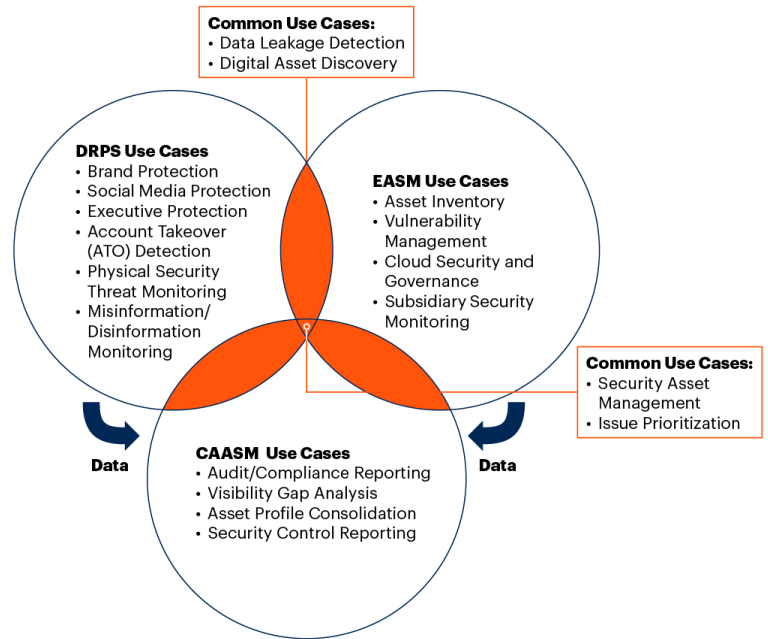
DRPS focuses on detecting and monitoring external digital assets like IP addresses, websites, brand assets (social media accounts), and digital identities of senior personnel (such as VIPs and C-Suite executives). DRPS solutions monitor social media platforms, marketplaces, and the dark web for vulnerabilities, such as fake profiles, compromised accounts, fake domains, rogue apps, and other misinformation. Once a vulnerability has been detected, DRPS can take down the account and remove sensitive or proprietary information such as credit card information and personally identifiable credentials. Unlike EASM tools, which are leveraged by security operations and IT teams, DRPS tools support business-centric use cases such as enterprise digital risk assessment and brand protection and are commonly used by business operations and brand marketing teams.

CAASM includes technologies that enable security teams to obtain continuous asset visibility throughout their internal environment. CAASM relies on API integrations to map internal assets, obtain data, and provide context surrounding the scope of vulnerabilities and gaps in security controls. CAASM tools enrich the data from these existing tools to provide security teams with a holistic view of their internal asset inventory, addressing compliance reporting, visibility gap analysis, asset consolidation, and security control reporting use cases. While CAASM sounds similar to EASM, they have a different focus. CAASM tools focus primarily on internal assets and utilize API integrations to conduct passive scans, whereas EASM tools focus on Internet-facing assets, many of which are unknown, and use a range of methods to scan the Internet actively.

While there may be significant overlap between DRPS, EASM, and CAASM capabilities, all three segments address different core use cases and are largely complementary. EASM offers operational focus for security teams engaged in vulnerability management, threat hunting, and governance. In contrast, DRPS is more often leveraged by business-centric users focused on digital risk assessment, compliance, and brand protection. EASM focuses on mapping and securing externally facing assets via various methods that scan

the Internet and serves as a source of record. In contrast, CAASM relies on API integrations with already deployed internal IT technologies and functions as a data aggregator. In fact, EASM tools often feed into CAASM to provide added visibility.

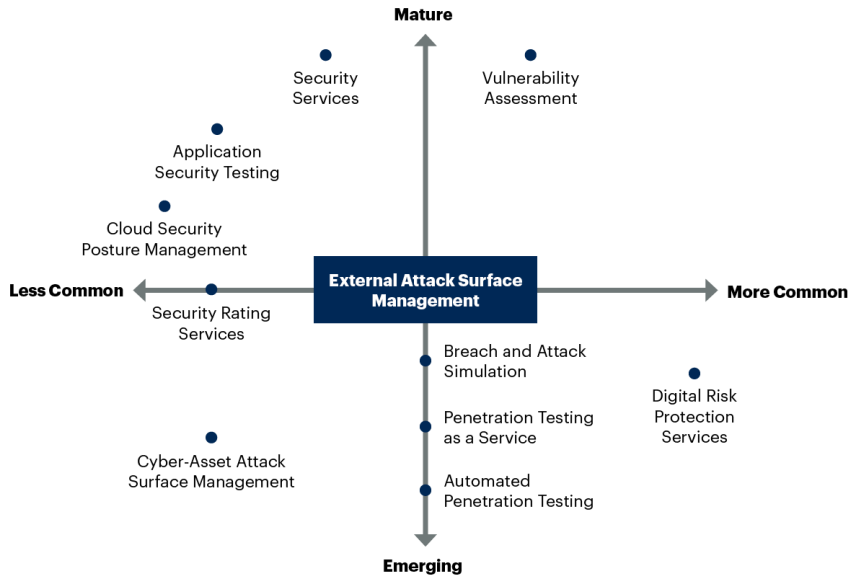
Exhibit 159: DRPS, EASM and CAASM Use Case Comparison



Source: Gartner

While vendors in the ASM market have focused on addressing one of the submarkets (EASM, DRPS, CAASM), the market has begun to converge. DRPS vendors (like LookingGlass [acquiring AlphaWave] and Recorded Future [acquiring Security Trails]) and CAASM vendors (like Axonius) have expanded by adding EASM to provide visibility into internal and externally-facing assets and delivering a single end-to-end ASM platform. While this process is still in the early stages of development, Gartner believes that by 2025, less than 10% of EASM vendors will be pure-play vendors and that by 2027, most ASM solutions will mature and bring EASM, DRPS, and CAASM into a single ASM platform.

Exhibit 160: EASM Consolidation

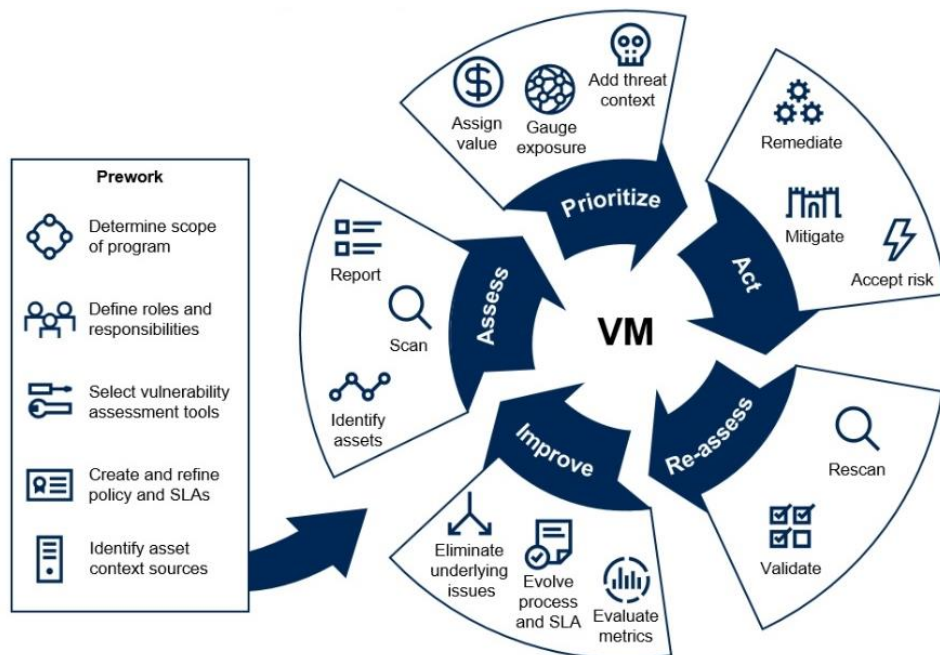


Source: Gartner

But the convergence has not stopped there. The ASM market is also blending with adjacent areas like Threat Intelligence, Vulnerability Management, and Cybersecurity Validation (Breach and Attack Simulation [BAS] and Automated Penetration Testing [APT]) to form a broader Exposure Management (EM) solution. Vendors like CrowdStrike (via its acquisition of Reposity), Tenable (via its acquisition of Bit Discovery), and Microsoft (via its acquisition of RiskIQ) have expanded into the ASM market to strengthen their ability to address Exposure Management use cases. Moving forward, we expect the larger vendors to continue to add ASM capabilities. In fact, according to Gartner, ~50% of the ASM market will be owned by vendors with more than \$1B in revenue by 2024.

Vulnerability Management (VM)

VM is an integral and often a required part of any organization's security posture. It addresses a broad set of capabilities and tools to identify, classify, prioritize, and mitigate software vulnerabilities. While Vulnerability Assessment (VA) tools historically stood at the core of VM, modern programs incorporate complementary tools such as Vulnerability Prioritization Technology (VPT), Breach and Attack Simulation (BAS), and Automated Penetration Testing. These complementary tools help organizations prioritize discovered vulnerabilities, test the efficacy of existing security controls, and identify new gaps with real-life exploits used by attackers.

Exhibit 161: The Vulnerability Management Lifecycle

Source: Gartner

VA tools have been commercially available for more than 20 years. They address security operations (vulnerability and security configuration assessments [SCA]), network asset and system visibility, and compliance (scanning requirements for regulatory/compliance standards) use cases. The tools use network- and host-based scanners and agents to scan servers, workstations, devices, and applications to discover vulnerabilities, known security gaps, and misconfigurations. The scanners assess devices from a credentialed (legitimate user) and uncredentialed (hacker) view and simulate attacks to see if they can be exploited. VA tools incorporate a broad range of capabilities, including vulnerability scanning (with an agent, virtual machine, or API), security configuration assessment, cloud security posture assessment, operational technology assessment, penetration testing, remediation prioritization, compliance reporting, ticketing, and behavioral monitoring.

VPT tools fill a gap in traditional VA tools. Rather than running assessment activity, VPT tools leverage telemetry generated by security testing technologies (VA, DAST, and SAST tools, for example), dynamic web application testing, penetration testing data, and network and endpoint security controls to identify and prioritize which vulnerabilities need to be remediated first. More sophisticated VPT solutions apply attack path mapping and ML analytics to generate granular remediation strategies and enable organizations to prioritize and focus on higher-risk scenarios. VPT solutions can consolidate and prioritize vulnerabilities into a centralized dashboard view for organizations that rely on standalone VA tools for agent and network scanning.

BAS tools complement VA tools by providing an attacker's view of the environment. They use agents and virtual machines to simulate common attack methods (MITRE, for example) to test the efficacy of existing security controls. BAS tools test configuration changes, identify vulnerabilities, and prioritize remediation actions for risky assets within the environment. While BAS tools incorporate limited VA functionality and can detect vulnerabilities without scanning an environment or ingesting VA telemetry, they don't focus on finding all vulnerabilities. Instead, they focus on the vulnerabilities that can be more reliably exploited and how to address them.

Automated penetration testing tools take this a step further and test IT infrastructure with real-life attack methods used by threat actors to identify vulnerabilities such as SQL injection, Cross-Site Scripting, Cross-Site Request Forgery, weak authentication, etc. While penetration testing is not new, it was historically delivered as a service by humans

and only conducted periodically, giving organizations only a point-in-time view of vulnerabilities. Automated penetration testing improves on this by leveraging a software-driven approach to test environments at frequent intervals without operational overhead. Leading vendors in the space, like Pentera, offer an agentless, software-delivered solution that provides persistent, low-touch testing, allowing security teams to continuously identify critical vulnerabilities and gaps in their security posture.

The VM market is dominated by three major vendors: Rapid7, Tenable, and Qualys. All offer VA scanning and prioritization, and attack simulation capabilities. The core VA scanning technology is very mature, and we believe these vendors have minimal technological differentiation. Instead, they differentiate with their GTM approach. Rapid7 primarily competes on cost and appeals to organizations focusing on compliance-related use cases. Qualys's solution spans the entire vulnerability management lifecycle and includes capabilities beyond traditional vulnerability assessment, such as IT asset inventory management, prioritization, and patch management. Last, Tenable focuses on providing feature-rich VA and VPT tools. Several MDR and EDR vendors, such as CrowdStrike, have also added VA capabilities, although these offerings are not robust and often can only implement agent-based scanning. This compares to the three major VA vendors, which offer virtual-machine-based scanning for IT assets that cannot run agents (i.e., firewalls, switches, routers).

We believe the VA market is evolving from a stand-alone solution to a feature within other security solutions such as CSPM, EDR, MDR, SIEM, DAST, and container security. In fact, all three major VA vendors have added CSPM and container security to their platforms to provide better coverage of assets running in the cloud and some form of ASM (EASM or CAASM). We expect the VA, TI, ASM, and security validation markets to converge to form a broader exposure management space that provides comprehensive security for internal and external assets. We expect this to continue as customers adopt cloud-based solutions and their digital asset inventory grows.

SIEM and SOAR

Over the past decade, the number of security tools deployed and managed has increased substantially, dramatically increasing the number of alerts security operations teams need to address. The explosion in alerts (as much as in the thousands in a given enterprise daily) can overwhelm security teams as they can take hours or days to resolve and deliver false positives or duplicate alerts. In response, security operations teams have turned to Security Information and Event Management (SIEM) and Security Orchestration Automation and Response (SOAR) solutions to gain a better contextual understanding of cyber-attacks, apply a more holistic approach to threat management (specifically threat detection and response), and address monitoring and compliance requirements while efficiently cutting through the deluge of alerts.

SIEM solutions enable configurable threat detection and security incident, investigation, and response through the collection, aggregation, and analysis of event data from a wide variety of sources such as security solutions (network firewalls, antivirus, VPN), network infrastructure (routers, switches, WAN), endpoints, servers, databases, SaaS applications, IaaS environments, and more. Once the primary data source, time-series-based log data, has been collected, it is aggregated and structured into a central console to identify, correlate, and categorize the data into meaningful alerts. SIEM tools have gone through several generations of change and evolved considerably to leverage a broader set of data sources, from simple log management use cases to real-time continuous security monitoring (of users, devices, etc.), external and internal threat discovery, incident investigation and response, policy enforcement, and compliance reporting and enforcement.

Modern SIEM solutions incorporate user and entity behavior analytics (UEBA), which uses machine learning to determine the baseline behavior of users and IT systems to identify anomalies. Combining UEBA with effective threat intelligence, behavior profiling, and analytics can improve threat detection. It is important to note that SIEM deployments tend to grow in scope over time as they incorporate more use cases, event sources, integrations with complementary technologies (such as EDR, SOAR), and behavioral analytics of third-party technologies.

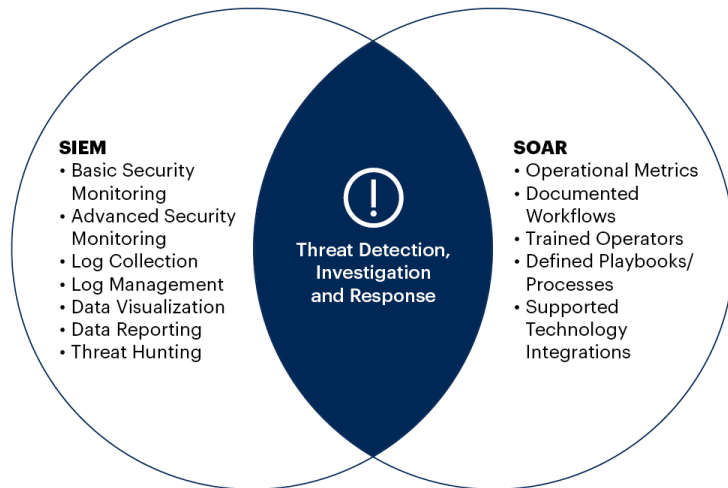
Exhibit 162: Top SIEM Use Cases



Source: IDC Survey (n = 259)

While SIEM tools offer great value, several challenges make their implementation difficult. First, it takes careful planning and extended tuning to set up a SIEM deployment that effectively reduces alert noise and separates everyday events from abnormal events. And this becomes more challenging as the number of use cases rises and deployments become more complex. Second, SIEM tools require close oversight from trained security professionals to maximize the value of the data collected and reduce false positives. This limits the implementation of SIEM solutions to large enterprises with trained and available security operations teams. Lastly, SIEM solutions are costly and require many resources (human, hardware, etc.).

Exhibit 163: SIEM vs. SOAR

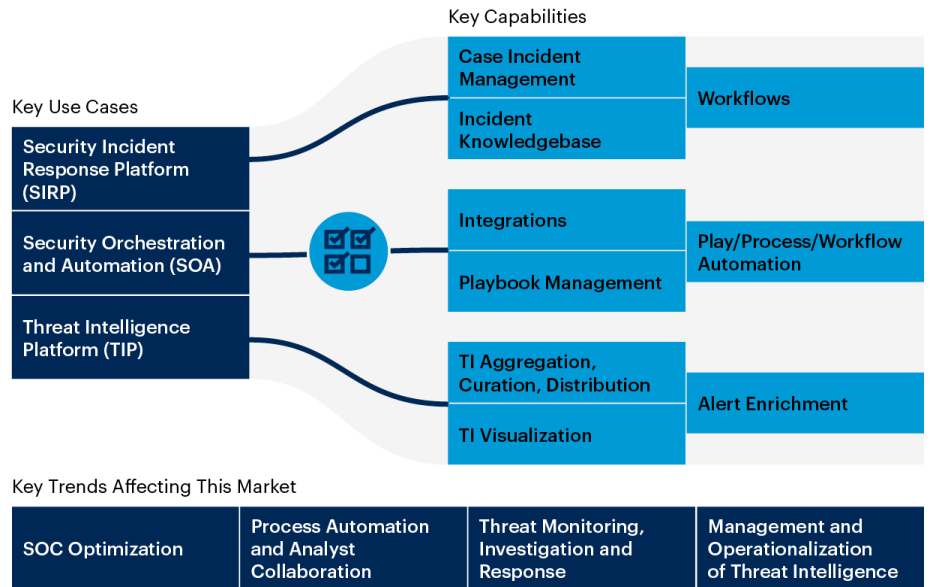


Source: Gartner

Security Orchestration Automation and Response (SOAR) tools extend the automation SIEM tools bring to managing alert volume to incident response. The SOAR market was formed through the convergence of three technologies: (1) Security Incident Response Platforms (SIRPs), (2) Security Orchestration and Automation (SOA), and (3) Threat Intelligence Platforms. They automate the collection of inputs from security tools (such as SIEM) with little to no human analysis and use predefined playbooks and incident

workflows for threat and vulnerability management, security incident response, incident triage, security operations automation, and compliance monitoring. They also store incident management data to support SOC investigations.

Exhibit 164: SOAR Capabilities



Source: Gartner

While SOAR solutions are part of the control plane for modern SOCs, they are still challenging to implement as fully automated, end-to-end incident workflow solutions. They are built with a monolithic architecture, limiting their ability to quickly scale usage up or down and require API integrations to connect to third-party tools, limiting their flexibility in connecting to modern cloud-native infrastructure like containers and Kubernetes clusters. As a result, SOAR solutions are more commonly deployed in large enterprises with sophisticated SOC teams that have resources and qualified professionals with deep knowledge across a range of domains to run and manage them.

Looking ahead, we expect the adoption of SaaS-based SIEM solutions to continue as customers shift to cloud architectures. We also expect SIEM vendors to embed SOAR capabilities into their offerings and for customers to rely on embedded automation capabilities within other tools such as SIEM, XDR, SEG, and ITSM, which have introduced easier-to-use automation capabilities, lowering the need for standalone SOAR tools. Additionally, observability, endpoint, and behavior analytics vendors seem likely to increasingly address SIEM/incident response use cases. Companies like Elastic and Datadog have released their own SIEM products to complement their log management capabilities, while EDR vendors like CrowdStrike and UEBA vendors like Exabeam have introduced cloud-based SIEM solutions.

SIEM vs. XDR

While they can address similar use cases, there are significant differences between SIEM and XDR solutions. SIEM solutions are geared toward security analytics and data normalization, need careful manual tuning, and are often prone to false positive or immaterial incident alerts. They also offer premier reporting and log retention capabilities, making them well-suited to address compliance and regulatory use cases.

XDR solutions ingest telemetry data into a data lake from various security domains (endpoints, networks, cloud) through APIs and come with native response capabilities. They leverage AI and behavioral analytics to prioritize high-risk alerts and offer automated remediation. At the same time, XDR solutions are not mature enough to address compliance and regulation requirements related to incident and log retention.

Consequently, SIEM solutions are best suited for large enterprises with large security teams and log management and compliance use cases. In contrast, XDR solutions are

best utilized as end-to-end detection and response platforms targeting small and mid-sized organizations with less sophisticated SOC teams and IT architectures.

Exhibit 165: SIEM vs. XDR

SIEM	XDR
Detection dependent on log data and alerts	Detection dependent on telemetry from multiple sources (endpoint, network, cloud)
Manual correlation of security events and telemetry	Automated correlation across multiple security tools
Investigation via querying and correlated alerts	Investigation via automated root cause analysis
Response capabilities via SOAR integration	Native response capabilities
Compliance and regulation use cases	Fast (within seconds) queries
SIEM-only queries take hours or days	Fast threat hunting
Slow threat hunting across different security tools	Flexible and scalable performance
Data normalization and analytics oriented	Easily integrates with existing security solutions

Source: Oppenheimer & Co.

Security Operations Market Vendor Overview

Below, we review several of the broader Security Operations market vendors.

Exhibit 166: Gartner SIEM Magic Quadrant



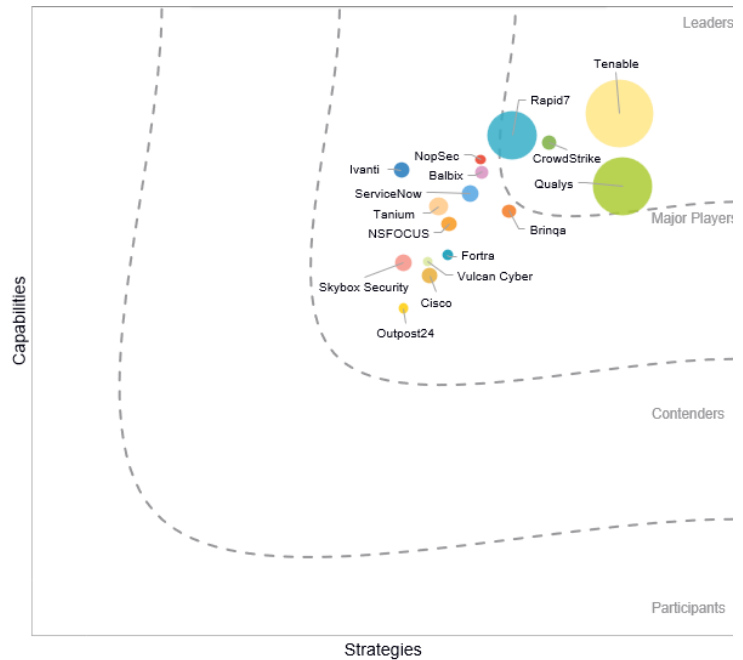
Source: Gartner

Exhibit 167: IDC 2022 SIEM Marketscape



Source: IDC

Exhibit 168: IDC 2023 VM Marketscape



Source: IDC

- Splunk** offers a comprehensive platform with SIEM, UEBA, and SOAR capabilities. Its products are broadly adopted among enterprises looking for a core SOC tool that supports third-party integrations. The company has utilized M&A to expand its capabilities from pure-play security into ITOps and Observability, including Victor Ops (incident management and response), Phantom Cyber (SOAR), Flowmill (network observability), Rigor (synthetic monitoring), Plumbr (APM), and SignalFX (observability for cloud-native technologies). Splunk offers an on-premises and a

cloud-based solution with various pricing models (data-ingestion-based, workload-based, tiered) that align with customer usage needs. The company's solutions are considered feature-rich but also expensive. In September 2023, Cisco announced a deal to acquire Splunk.

- **Elastic** offers a SIEM solution utilizing its proprietary search functionality as the back-end engine. Elastic's offering gives its customers a unique value proposition, allowing them to analyze the logs they already collect for observability and IT use cases. The platform offers customizable dashboards that are popular among its customers, with the ability to see both observability and security insights in one view as a strong selling point. Elastic has also expanded into endpoint security and cloud security via its acquisitions of Endgame and Cmd but primarily lands new security customers with its SIEM solution. Licensing is consumption-based and priced on the amount of compute and storage needed.
- **IBM's QRadar** is a popular solution in the SIEM market. The platform is known for filtering unwanted data, allowing customers to fine-tune their security-relevant data sources and reduce costs. QRadar also offers simplified analytics capabilities that enable users to search and filter for various analytic conditions. However, it lacks essential collaboration and orchestration features, often requiring customers to deploy QRadar SOAR solutions as an add-on. IBM has extended QRadar to cover XDR (QRadar XDR), offering threat detection and response. QRadar can be deployed on-premises or in the cloud and offers server- and capacity-based licensing models.
- **Microsoft** entered the SIEM market via its 2019 release of Azure Sentinel. The solution offers native integrations with Microsoft's extensive catalog of security and IT solutions (CASB, EDR, EPP, Office 365), making it a strong fit for customers heavily invested in the Microsoft ecosystem. Azure Sentinel is only offered as a SaaS-based solution with ingestion-based pricing, allowing customers to pay as they go or prepay for capacity. Microsoft has done an excellent job of accelerating the roadmap and quickly maturing the offering, in our view. It is now considered one of the best SIEM solutions in the market, given its rich ecosystem of integrated security products (i.e., CASB, Defender, AD).
- **Exabeam** offers a broad product portfolio that includes SIEM, UEBA, log management, and SOAR. Exabeam re-engineered its legacy single-tenant SIEM offering into a multi-tenant, cloud-native architecture that enables faster ingestion speed (more than 1 million events per second) and greater scale. These products can be purchased separately or as a platform that combines the capabilities of its entire product portfolio into a single cloud-native offering.
- **Securonix** offers a cloud-native security analytics and operations platform for complete security monitoring. The company's core products include (1) a SIEM solution that delivers log management, analytics, and response capabilities from a single management console; (2) a UEBA solution that uses machine learning and behavioral analytics to prioritize high-risk events; and (3) a cloud-native OpenXDR solution that leverages built-in connectors for real-time enrichment. Securonix also offers add-on products such as SOAR, NDR, and identity analytics. The company sells its products as a stand-alone solution and offers a unified platform that includes SIEM, UEBA, and SOAR. Securonix's platform can be consumed as SaaS or deployed on-premise.
- **Axonius** offers a cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security coverage gaps, and automatically validates and enforces security policies. The platform uses over 700 integrations with enterprise software tools to collect asset data, cross-correlate it, and generate a comprehensive and unique asset list. Its dashboard can notify security teams of missing or out-of-date security agents, misconfiguration issues, etc. The company's solution integrates with and automatically updates common configuration management databases (CMDB), and it can feed data into SOAR solutions to enrich response activity. Axonius's solutions are deployed as a single virtual appliance on-premise or in the cloud. The company offers its solution as a subscription and is priced based on the number of assets.

- **Recorded Future** is a threat intelligence (TI) and digital risk protection (DRPS) vendor. The company offers one of the broadest TI portfolios in the market, covering brand, SecOps, vulnerability, attack surface, and identity intelligence. Its large intelligence platform organizes and analyzes large amounts of data and uses AI and ML to correlate internal and external threats. Recorded Future also offers deep/dark web monitoring from its acquisition of Gemini Advisory. The platform addresses various use cases across exposure management, ransomware mitigation, and digital risk protection. The company provides easy integrations with popular SIEM/SOAR solutions (like Splunk). It sells its solution on a subscription basis and can be deployed on-premises or in the cloud.
- **SecurityScorecard** is a threat intelligence vendor that offers security scoring and services. The company provides organizations with an outside-in view of their security posture, identifying areas with a potential compromise. It collects data from publicly available commercial and open-source feeds across the Internet to identify common attack methods and known vulnerabilities. Once collected, the company cross-analyzes a customer's security posture against the data and assigns a security score. SecurityScorecard's solution addresses many use cases, including risk and compliance monitoring, M&A due diligence, and cyber insurance underwriting. The company also offers ratings for vendors within a customer's ecosystem to help them identify risks within their digital supply chains.
- **Code42** is a vulnerability and risk management vendor focused on reducing insider risk and IP theft. The company's Incydr is a cloud-native SaaS solution that monitors customer data to identify when files move outside a trusted environment. The solution relies on an endpoint-based agent that uses exfiltration detectors for IaaS (OneDrive, Google Drive, Box), email (Office 365 and Gmail), and SaaS (Salesforce) to guard against data and IP theft from internal employees. Incydr can also integrate with SIEM and SOAR tools to help streamline alert triage and remediate data leaks/theft. The platform can also integrate with IAM tools to create a watch list of employees who have exhibited risky behavior.
- **BlueVoyant** is a security operation vendor that offers third-party cyber risk management and DRPS services. The company takes a service-driven approach with unlimited takedown, making it potentially an attractive option for budget-constrained customers. Its DRPS service addresses various use cases, including digital brand protection, fraud campaign discovery, account takeover monitoring, data leakage detection, and EASM. The company maintains a strong presence within the financial services sector. It also offers MDR with strong integrations with Splunk and Microsoft 365. Pricing is attractive, and its DRPS service is sold on a module basis.
- **Armis Security** is an ASM vendor that offers a unified asset intelligence platform. The platform equips IT teams with visibility and contextual intelligence for various assets, including managed assets, unmanaged assets, IoT devices, applications, and cloud instances. The company offers four products: OT/IoT Security, Medical Device Security, Asset Management, and VPT. Armis profiles devices at network aggregation points to detect vulnerabilities, map relationships, and offer remediation capabilities. The platform is agentless, making it well-suited for covering IoT, and it can draw telemetry from endpoints by integrating with third-party EDR agents.
- **Claroty** offers visibility and threat detection for cyber-physical systems (CPS) connected to the Internet. These include physical devices such as programmable logic controllers (PLCs), building management systems (HVAC, elevators), IoT devices, medical devices, public infrastructure, and defense systems. Claroty's primary product, xDome, uses software agents and hardware collectors to map the CPS systems in a customer's environment. Once mapped, the platform correlates asset data with a database of vulnerabilities to generate a risk score. xDome also offers anomaly & threat detection by monitoring asset behavior and communication and monitoring for indicators of compromise. The company addresses customers in the industrial, healthcare, commercial, and public sector verticals.
- **Rapid7** is a security operations vendor that offers VM, SIEM, SOAR, and threat intelligence. The company has significantly expanded its product portfolio beyond core VM and now offers an integrated SOC platform. Its SIEM solution has gained

solid traction and is considered one of the most cost-effective offerings currently in the market according to industry analysts. Pricing for Rapid7's SIEM is consumption-based and based on the number of assets monitored.

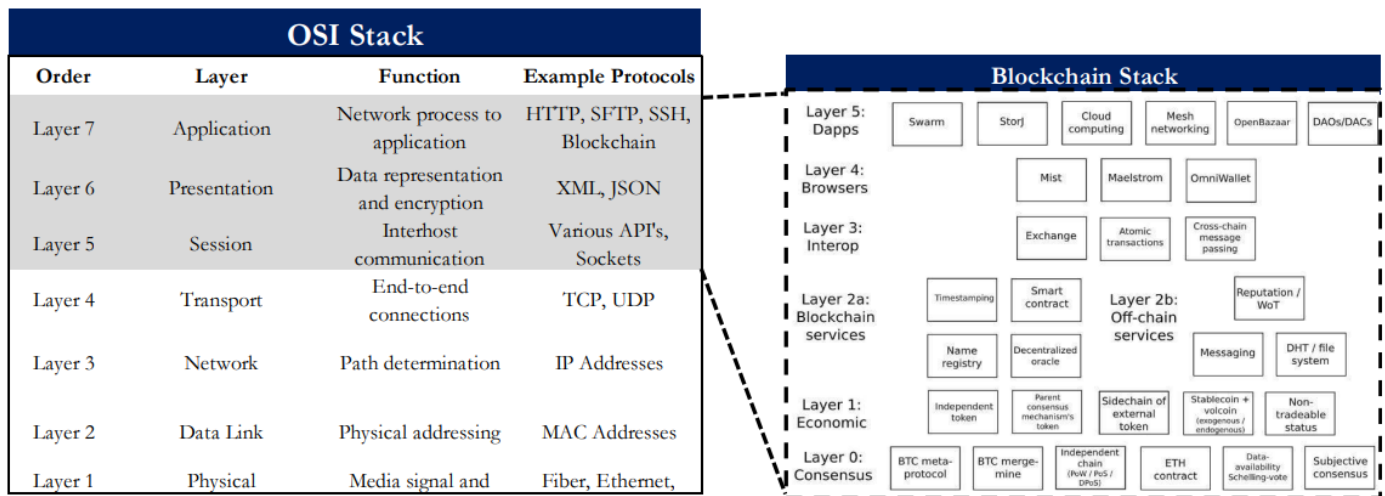
- Qualys** offers a security platform that includes vulnerability management, EDR, XDR, and cloud security. The company is one of the prominent three VA vendors. Its Vulnerability Management, Detection & Response (VMDR) platform is its most popular solution and enables IT teams to manage their assets and discover vulnerabilities. The solution overlays traditional VM capabilities with asset management, automation and orchestration, and threat detection and response. Qualys is well-known for addressing compliance-related use cases like policy compliance, PCI ASV compliance, file integrity monitoring, and configuration assessments. In recent years, the company has expanded its portfolio into higher growth security domains like EDR, XDR, CSPM, and attack surface management, offering these capabilities through a single agent.
- Tenable** is a VM vendor that offers traditional VA, ASM, CSPM, and application security capabilities. Its Tenable One platform is a SaaS-based platform that offers a comprehensive view of an organization's cyber risk exposure. It offers vulnerability coverage for various assets, including traditional IT systems, cloud resources, containers, web applications, and identity systems (i.e., Active Directory). The company expanded into EASM with the acquisition of Bit Discovery in 2022 and now offers EASM fully integrated with its vulnerability management platform.
- HackerOne** is a bug bounty vendor that connects enterprises with outsourced penetration testers. The company's network of hackers works to penetrate the target enterprise's infrastructure, and the hackers are paid a bounty if they are successful, with HackerOne receiving an annual upfront payment from their customers. HackerOne also offers ASM and cloud security solutions that leverage expertise from hackers to help organizations identify weak spots in their architecture.

Blockchain & Crypto Security

Blockchain Background

A "blockchain" is a digital distributed ledger technology (DLT) that generates an immutable record of transactions. The record (block) is stored across multiple participants (also known as nodes) on a peer-to-peer (P2P) network. The main characteristics of a blockchain are (1) no single central repository for storing the ledger information; (2) new transactions are added to the block once they meet a predefined preprogrammed criterion; and (3) each transaction block refers to the previous block, creating a chain, and uses secure cryptographic signatures. Blockchain leverages the Internet/Cloud and sits at the higher layers of the OSI stack, along with other protocols such as HTTP.

Exhibit 169: The OSI Stack and Blockchain



Source: Vitalik Buterin (On Silos), HPE, Wordfence.com, and Oppenheimer & Co.

Blockchain was introduced in January 2009 in a nine-page whitepaper published by Satoshi Nakamoto (alias) and served as the underlying technology behind a P2P electronic cash system, or “cryptocurrency,” called Bitcoin. Since then, other blockchains (and related ecosystems) have been created, including Ethereum, Hyperledger, NEO, EOS, Solana, Corda (technically a DLT but not a blockchain), etc., with Ethereum the predominant blockchain for launching cryptocurrency/tokens (in an Initial Coin Offering or ICO) and dApps (decentralized applications) across a variety of areas (DeFi or decentralized finance, non-fungible-tokens or NFTs, gaming, etc.). Part of the success of Ethereum can be attributed to the introduction of smart contracts or auto-executed programs on a blockchain. Smart contracts make blockchain applications look identical to web applications, although they are powered by decentralized, shared infrastructure instead of company-owned and managed servers.

Blockchains come in two flavors—permissioned or permissionless. A permissionless blockchain is fully decentralized and open to the general public to participate in as part of the consensus validation process (i.e., the step that creates the next block on the chain). This type of blockchain provides full transparency (but with anonymity) into the transactions on the chain, has no central authority, and often involves a digital asset or token as an incentive to participants who validate new blocks. In contrast, a permissioned blockchain is developed by a private entity or consortium and requires user approval to join the blockchain network. The transactions recorded on permissioned blockchains remove any anonymity from the participants and may involve digital assets or tokens (e.g., a private permissioned blockchain involving a bank consortium consisting of JP Morgan, Bank of America, etc.).

The benefits of a permissionless blockchain include broad decentralization, a high level of transaction transparency, and potential resilience to censorship and threat actors. On the downside, permissionless blockchains are less energy efficient, have difficulty scaling, and offer limited user privacy. In comparison, permissioned blockchain limits decentralization to approved participants, is highly customizable, offers strong privacy standards, and is more scalable vs. a permissionless blockchain due to the limited number of validation participants (nodes). The most significant drawbacks of permissioned blockchains are the limited level of decentralization and the lack of external oversight.

It should be noted that within permissioned, a blockchain can be public or private (i.e., with a select consortium of members). Unlike the original blockchain used for Bitcoin, which uses a proof-of-work (PoW) validation mechanism, a private permissioned system does *not* require a PoW to add a new block as it relies instead on an active and approved member list/service.

Exhibit 170: Permissioned vs. Permissionless Blockchains

Permissionless vs. permissioned blockchain

	Permissionless	Permissioned
OVERVIEW	Open network available for anyone to interact and participate in consensus validation. Fully decentralized across unknown parties.	Closed network. Designated parties interact and participate in consensus validation. Partially decentralized (i.e., distributed across known parties).
ALSO KNOWN AS	Public, trustless.	Private, permissioned sandbox.
KEY ATTRIBUTES	<ul style="list-style-type: none"> ■ Full transparency of transactions, based on open source protocols ■ Development via open source ■ Mostly anonymous, with some exceptions ■ Privacy depends on technological limitations or innovations ■ No central authority ■ Often involves digital asset or token for incentives 	<ul style="list-style-type: none"> ■ Controlled transparency, based on organizations' goals ■ Development via private entities ■ Not anonymous ■ Privacy depends on governance decisions ■ No single authority, but a private group authorizes decisions ■ May or may not involve digital assets or tokens
BENEFITS	<ul style="list-style-type: none"> ■ Broader decentralization, extending access across more network participants ■ Highly transparent, which is beneficial for speed and reconciliation across unknown parties ■ Censorship resistant, due to accessibility and participation across locations and nationalities ■ Security resilience, since attackers cannot target a single repository, and it is costly and difficult to corrupt 51% of the network 	<ul style="list-style-type: none"> ■ Incremental decentralization, but participation from multiple businesses helps mitigate risks of highly centralized models ■ Stronger information privacy because transaction information is only available based on permissions ■ Highly customizable to specific use cases through diverse configurations, modular components and hybrid integrations ■ Faster and more scalable, since fewer nodes manage transaction verification and consensus
PITFALLS	<ul style="list-style-type: none"> ■ Less energy efficient because network-wide transaction verification is resource-intensive ■ Slower and difficult to scale, as high volume can strain network-wide transaction verifications ■ Less user privacy and information control 	<ul style="list-style-type: none"> ■ Limited decentralization because a network with fewer participants increases risk of corruption or collusion ■ Risk of override, since owners and operators can control or change the rules of consensus, immutability, or mining ■ Less transparent to outside oversight, since participants are limited and operators determine privacy requirements
MARKET TRACTION	<ul style="list-style-type: none"> ■ Peer-to-peer ■ Business-to-consumer ■ Government-to-citizens 	<ul style="list-style-type: none"> ■ Business-to-business ■ Business-to-consumer ■ Governments-to-organizations

SOURCE: JESSICA GROOPMAN

© 2021 TECHTARGET. ALL RIGHTS RESERVED. TechTarget

Source: Jessica Groopman, TechTarget







Another recent development has been the move of the Ethereum blockchain platform (one of the most popular blockchains utilized for innovation by developers) from a PoW to a proof-of-stake (PoS) validation system (September 2022; also known as “The Merge”). This was done to improve transaction speed and reduce energy costs (PoW is energy-hungry and time-consuming). With the improvement in transaction latency and cost reduction, the Ethereum network hopes to accelerate the development of new and existing distributed applications (dApps) built on its blockchain platform (i.e., just as different SaaS providers can utilize the same operating platform/PaaS for their applications). Since the underlying blockchain platform must work in real-time and scale cost-efficiently for dApps to work effectively, the move to PoS is critical for the Ethereum blockchain platform’s long-term success.

Exhibit 171: Public vs. Private Blockchains

Public vs. Private Blockchains		
	Public	Private
Access	Open read/write access to database	Permissioned read and/or write access to database
Speed	Slower	Faster
Security	Consensus Algorithms (Proof-of-Work, Proof-of-Stake, dBFT)	Pre-approved participants
Identity	Anonymous/pseudonymous	Known identities
Privacy	Data publicly available	Privacy policy similar to traditional databases
Hosted	Globally on Nodes	Primarily on the cloud Azure/AWS
Number of Users	Millions/Billions	Dozens to several hundred
Cost To Use Network	Networks' Cryptocurrency, I.e. Ethereum converts Ether to "Gas" for network utilization	Dollars (AWS/Azure) for cloud usage and in some instances a cryptocurrency (I.e. EXP on Ripple).
Examples	Bitcoin, Ethereum, Neo	Ripple, Blockchain-as-a-service implemented for entities on Azure

Source: Steemit.com, Oppenheimer & Co.

Exhibit 172: Proof of Work (PoW) vs. Proof of Stake (PoS)

Proof of Work vs Proof of Stake		
	Proof of Work (Bitcoin Mining)	Proof of Stake (Ethereum's Future)
	The probability of mining a block is dependent on how much work is done by the miner	A user can mine (be a validator) depending on how many coins they stake (set aside in escrow)
	Payouts become smaller and smaller for bitcoin miners and there is less incentive to avoid a 51% attack	The PoS system of staking makes any 51% attack much more expensive if not impossible
	The transaction speed is slower and slower depending on the transaction fee	Transactions are very fast, and transaction costs come down significantly; PoS is more scalable
	The PoW system favors powerful miners and mining pools	PoS is fair and fast and can deliver finality (idea that transactions are final)
	Miners receive block rewards	Validators only receive transaction fees
	If a miner spends energy mining on the wrong chain (a 51% attack) or behaves badly, they simply lose the cost of the electricity and the opportunity cost of block rewards	If a validator acts badly, their stake is "slashed" or taken away, ensuring trust in the system

Source: Bitcointalk.org, Oppenheimer & Co.

Three properties are crucial for a successful blockchain implementation—scalability, decentralization, and security. However, achieving a simultaneous high degree of performance for all three vectors hasn't proven easy in real-world deployments. This led to a conjecture by Ethereum co-founder Vitalik Buterin, who claimed that blockchain systems could have at most two of these three critical properties optimized—a “blockchain trilemma.” This implies that a blockchain network can only optimize any two given factors

(such as decentralization and security) at the expense of the third (in this case, scalability).

In response, various blockchain-based solutions have propagated to improve scalability while maintaining the system's integrity (i.e., security) and decentralization. These enhancements can be characterized as Layer 1 or Layer 2 functionality.

- At the Layer 1 level of the blockchain (i.e., the main network in charge of the on-chain transactions), protocol improvements, such as the use of PoS (vs. PoW) and "sharding" (breaking up data sets and parallel processing), can improve scalability.
- At the Layer 2 level of the blockchain (i.e., the connected network for off-chain transactions that abstracts computationally heavy transactions away from Layer 1), a nested blockchain (Lightning, Plasma), state channels (off-chain smart contracts), and sidechains can address scalability challenges.




That said, it remains to be seen whether or not the aforementioned technological improvements in Layer 1 and 2 can completely overcome Buterin's proposition of a "blockchain trilemma."

The Blockchain Ecosystem

While the first widespread use of blockchain started with the cryptocurrency Bitcoin, we have seen exponential growth in the ecosystem and the number of use cases beyond cryptocurrency. Below, we delineate the different sections of the ecosystem and highlight major areas of innovation, such as the creation of Layer 2 (with the core blockchain network now called Layer 1), the use of state channels, sidechains, and smart contracts, and the expansion of blockchain into use cases such as NFTs and dApps (including DeFi).

- **Layer 1.** With the advent of Layer 2 (defined below), the core blockchain network and protocol are now referred to as Layer 1. At the base level, this includes the original blockchain, the type of consensus protocol (PoW, PoS, etc.), and the underlying infrastructure necessary to execute the blockchain. "On-chain" transactions are typically considered Layer 1. Historically, the slow transaction processing speed and high energy consumption have challenged blockchain scalability. However, these issues have recently been addressed through technological changes in the underlying protocol (e.g., Ethereum moving to PoS) and data sharding.
- **Layer 2.** Layer 2 is a secondary framework or protocol built on an existing blockchain platform (such as Lightning for Bitcoin and Plasma for Ethereum). This layer improves transaction speeds and capacity and delivers better scalability by moving the computation of transactions "off-chain" to save computing resources. This can also improve privacy, although security and compliance solutions must still be embedded carefully into the network to ensure integrity. Layer 2 innovation is still in its early days, and whether it can address the blockchain trilemma remains to be seen.

Exhibit 173: Blockchain Layer 1 vs. Layer 2

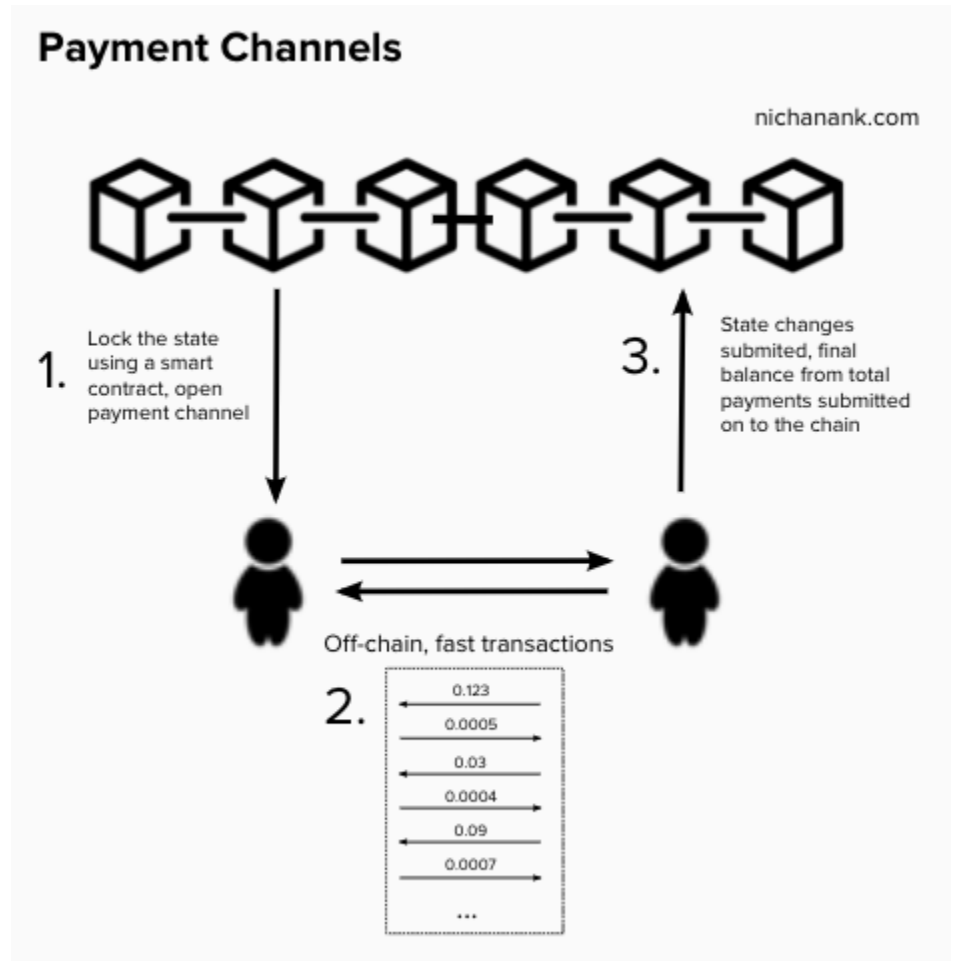
101 Blockchains BLOCKCHAIN LAYER 1 VS LAYER 2 - KEY DIFFERENCES		
Criteria	Layer 1	Layer 2
 Definition	Layer 1 scaling solutions are modifications in the base protocol of the blockchain network to achieve improved scalability.	Layer 2 scaling solutions involve the use of off-chain services or networks to improve scalability.
 Working	Changes in the base protocol, such as larger block sizes or new consensus mechanisms, can empower scalability.	Sharing the transaction ordering and processing workload with off-chain solutions improves scalability.
 Types	<ul style="list-style-type: none"> • Consensus protocol improvements • Sharding • Modifications in block size 	<ul style="list-style-type: none"> • Nested blockchains • Sidechains • State channels

Created by 101blockchains.com

Source: 101blockchains.com

- **State channels and sidechains** are types of Layer 2 scaling solutions that the blockchain community is exploring. The terms are sometimes used interchangeably, but each has pros and cons. A sidechain is a separate (“child”) blockchain that is attached to its main chain (“parent”), allowing for two-way movement between the side and main chain. State channels enable secure two-way transactions off the chain (“off-chain”) that are later recorded on-chain. As noted earlier, the availability of Layer 2 technologies, such as state channels and sidechains, can improve transaction speeds. Still, it remains to be seen whether they can fully solve the blockchain trilemma.

Exhibit 174: State Channels



Source: Nichanan Kesonpat (nichanank.com)

- **Smart contracts** are a way to automate agreements and transactions on the blockchain, thereby reducing human intervention and subsequent costs while improving latency. Technologically, smart contracts are self-executing contracts with pre-determined criteria built into the software code that acts as a trigger without third-party intermediary intervention. Smart contracts are considered the most promising and revolutionary technology within the blockchain community. They are expected to facilitate the proliferation of blockchain use cases in various end markets and verticals. Also, as noted earlier, most of the innovation around smart contracts is happening on the Ethereum platform. Smart contracts are also considered Layer 2 technology.

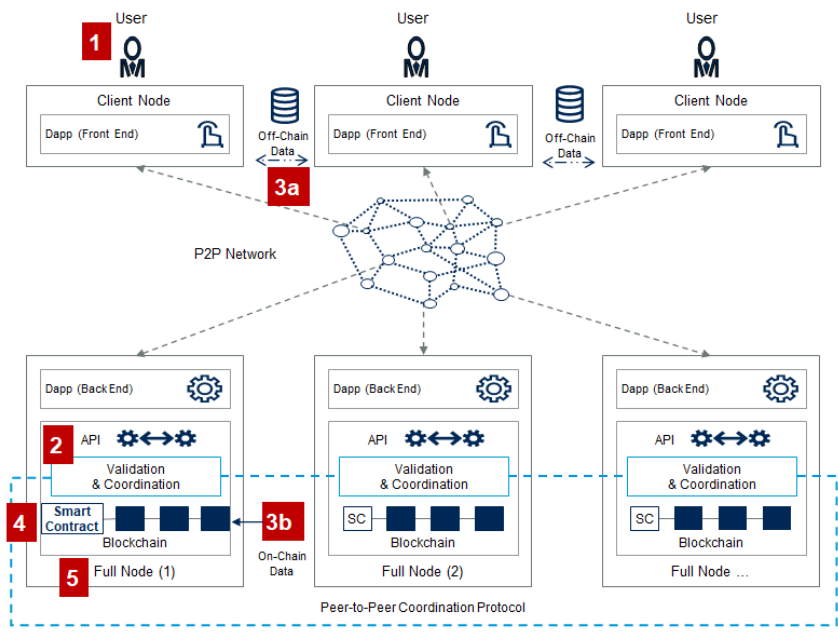
blocks. These payment requirements make it costly for threat actors to induce a DDoS attack or continuously spam the network. Nonetheless, some unique security challenges within the blockchain need to be addressed, such as 51% attacks, smart contract vulnerability, and permissioned node access in private blockchains.

As noted, most security threats and breaches related to a blockchain network resemble those currently in the non-blockchain data center and cloud infrastructures, such as endpoint, network, cloud, and application security. Assessing the combination of traditional security threat concerns and the unique challenges within the blockchain protocol, we identify five predominant threat vectors within the blockchain protocol and ecosystem—(1) end-user security, (2) interfaces such as APIs and oracles, (3) underlying data (on-chain and off-chain), (4) smart contracts, and (5) permissioned nodes.

Exhibit 176: Blockchain Security Threat Vectors

Top 5 Blockchain Security Threat Vectors Summarized

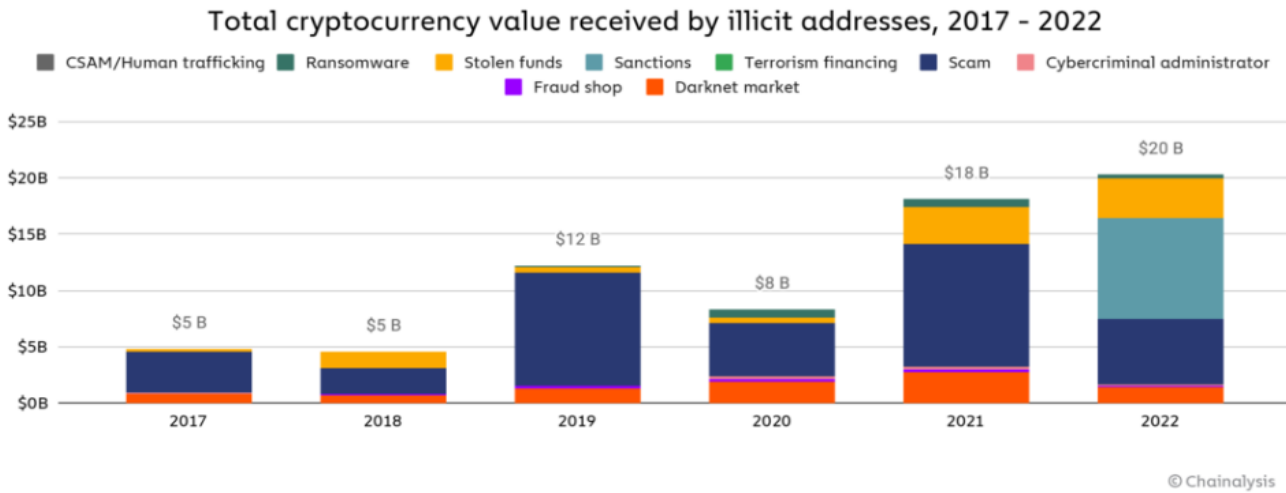
- 1. User:**
 - Weak Private key, Password mgt
 - Weak Endpoint security
 - Weak Identity Assurance**Risks:**
 - User Account Takeover
- 2. APIs, Oracles**
 - Bugs, exploits, invalid data**Risks:**
 - Incorrect Smart Contract Execution, Account Takeover
- 3. Off and on-chain data:**
 - Unprotected data
 - Lack of data integrity, confidentiality**Risks:**
 - Process failure, data compromise
- 4. Smart contracts**
 - Bugs, exploits, unauthorized execution**Risks:**
 - Theft, Manipulation
- 5. Permissioned nodes**
 - Insider threat, Data exposure, dApp exposure**Risks:**
 - Theft, Manipulation, Data Compromise



© 2020 Gartner, Inc.

Source: Gartner

Exhibit 177: Total Cryptocurrency Value Received by Illicit Addresses 2017-2022



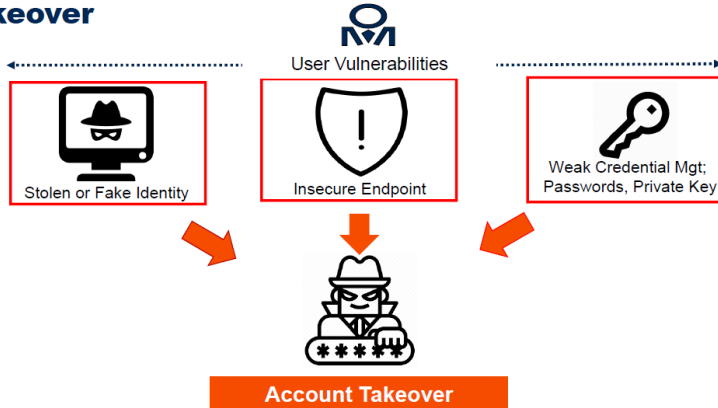
Source: Chainalysis

- 1. End-user security.** End-user vulnerabilities in blockchain environments are identical to traditional cybersecurity architectures, such as user identity authentication, endpoint vulnerabilities, and credential/password management. Such vulnerabilities are addressed with identity & access management (IAM) tools. Authentication at the endpoint (mobile devices, laptops, etc.) before access to wallets or exchange platforms can make the network more secure.

A unique (and relatively popular) aspect of end-user authentication within blockchains is the creation of private and public critical infrastructure (PKIs or tools used to create and manage keys used for encryption), which is a target for threat actors who attempt to steal keys by inserting malicious code into the PKI system. A few digital asset custodian companies (such as DigiCert) have developed countermeasures to offset the potential theft of digital assets from consumers. RSA has also recommended that PKIs be regularly analyzed using application security software such as SCA and SAST tools against key generation source codes and libraries and using DAST/IAST tools to analyze binaries.

Exhibit 178: User Vulnerabilities

Vector 1: User Vulnerabilities Lead to User Account Takeover

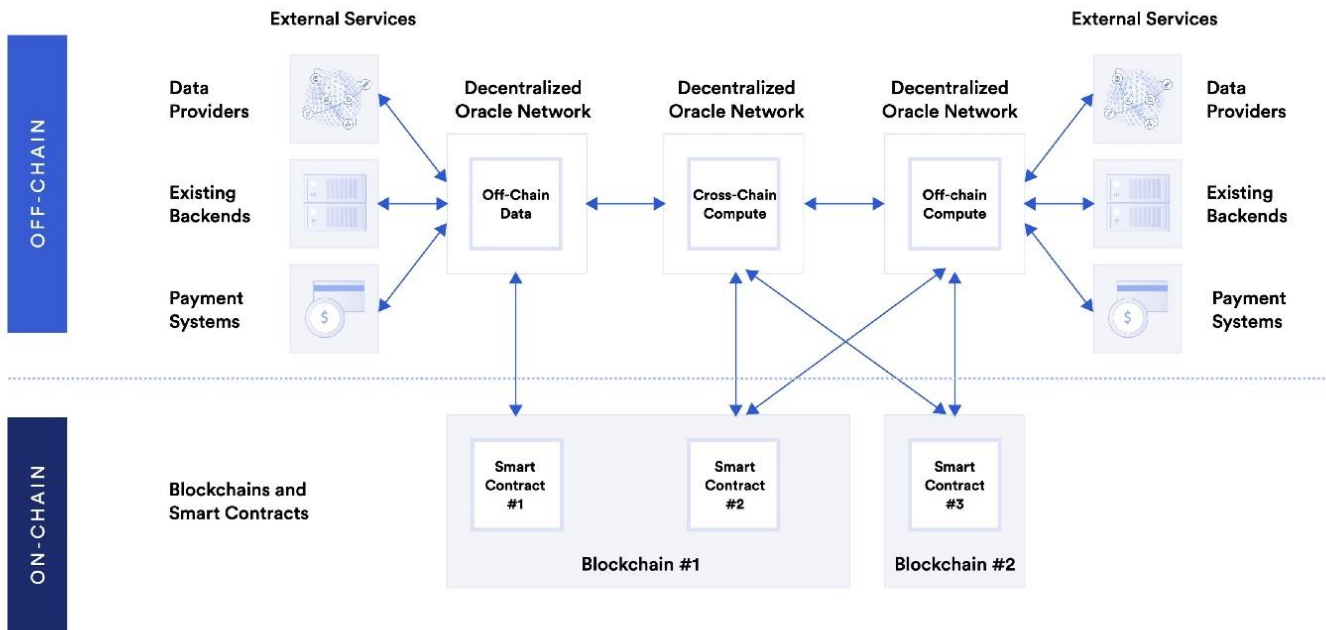


Source: Gartner

2. **APIs & Oracles.** Like traditional application software, APIs enable controlled interaction and communication between applications (HTTP, JSON, and XML). In a blockchain ecosystem, APIs may be used for wallets, payment processing, text query, etc. Blockchain ecosystems also use Oracles, or entities that connect blockchain platforms to external systems (such as existing data sources, legacy infrastructure, and advanced computational resources), allowing effective real-world expansion of smart contracts and dApps.

Threat actors attack APIs and attempt to manipulate pricing Oracles to create false exchange rates, which they can use for arbitrage opportunities. They can also try to develop malfunctions with the information feed source or steal a protocol's assets. While Oracle network providers, such as Chainlink and Band Protocol, secure their networks internally, traditional network and API security methods, such as firewalls, WAFs, and in-app API protection, can create a more robust and secure network.

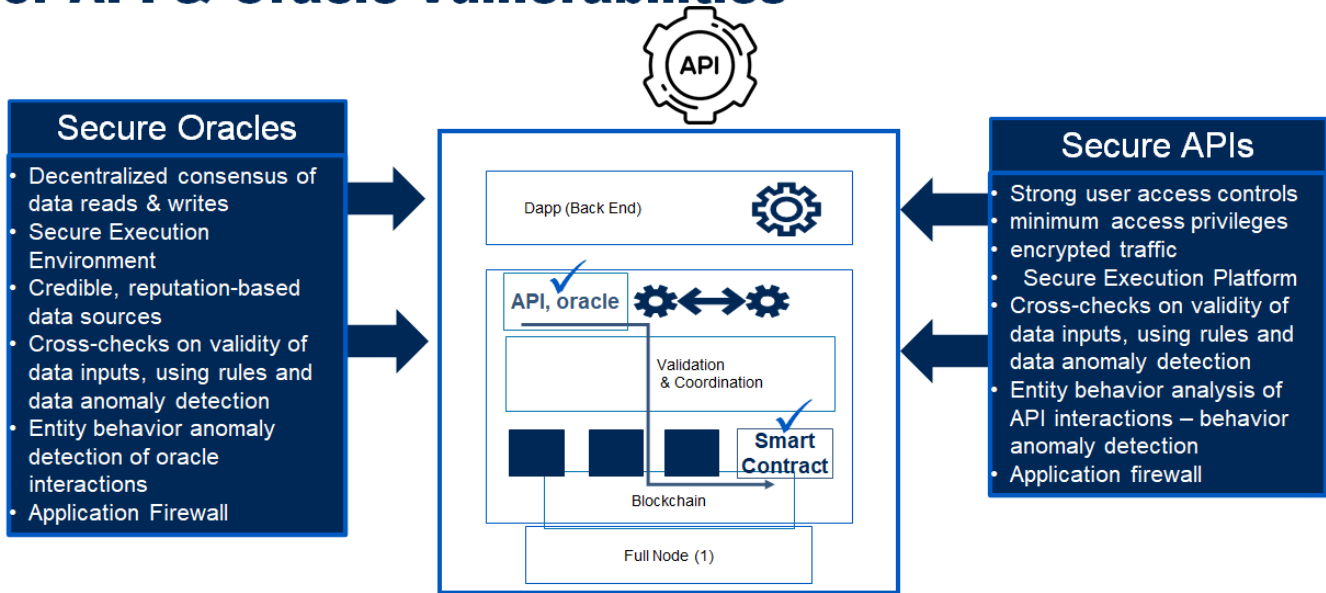
Exhibit 179: Blockchain Oracles in Smart Contracts



Source: Chainlink

Exhibit 180: API & Oracle Vulnerability Assessment

Vector 2: Complementary Layered Security Solutions for API & Oracle Vulnerabilities

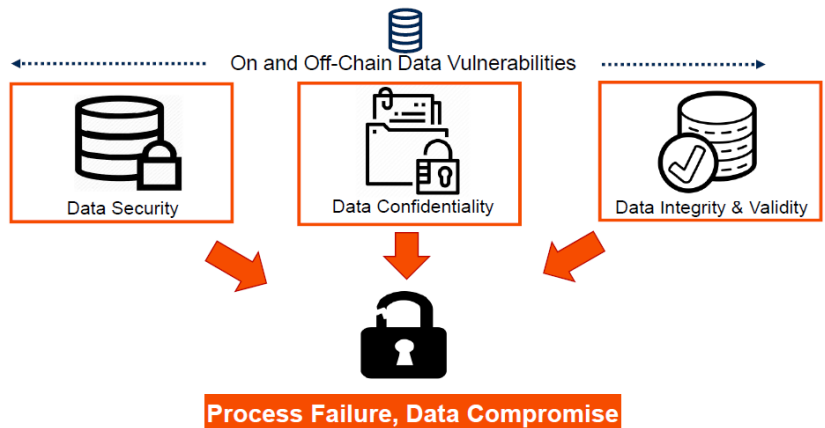


Source: Gartner

- Data.** Data vulnerabilities in blockchain relate to on-chain and off-chain data, including data security, confidentiality, and integrity. In addition to user-based breaches in data security (identity & access management), data vulnerability also exists within smart contracts and dApps, which utilize and store user information on a client node (off-chain) or a back-end infrastructure node (on-chain). Thus, from a security standpoint, there is an overlap with API/oracle, smart contract, and node vulnerability. Security technologies used here combine data loss prevention (DLP), API security, application security for smart contracts, vulnerability management (VM), and external attack surface management (EASM).

Exhibit 181: Off- and On-Chain Data Vulnerabilities

Vector 3: Unprotected Off- and On-Chain Data Leads to Process Failure and Data Compromise



Source: Gartner

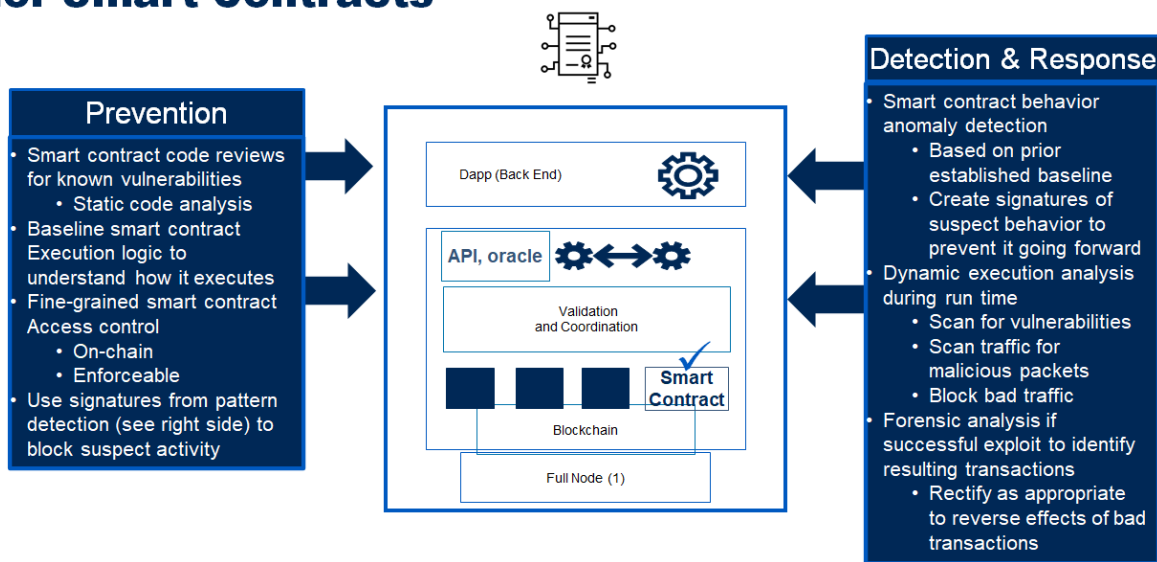
- Smart contracts.** Smart contracts are an attractive threat vector because assets can be easily locked up or taken off-chain when auto conditions are triggered, and reversing such immutable transactions requires consensus approval (>50%) to “hard

fork” the code and protocol. While some of the financial damage can be mitigated by creating intermediary escrow accounts (increases latency and impacts scalability), the issues with real-time execution remain.

To elaborate, threats and manipulation can come during smart contract creation (i.e., when the software code is created) when threat actors can introduce backdoors, malware, signatures, etc., into the contract itself, particularly if the smart contract utilizes open-source software (OSS). To mitigate security breaches within smart contracts, it is necessary to review and audit the underlying code, libraries, and dependencies using SCA tools, similar to mitigation strategies used during traditional software application development. Smart contract-specific cybersecurity vendors, such as AnChain.AI, ChainSecurity, and CertiK, have focused on auditing, monitoring, and KYC/AML onboarding, catering to the DeFi protocol.

Exhibit 182: Smart Contract Vulnerability Assessment

Vector 4: Complementary Layered Security Solutions for Smart Contracts



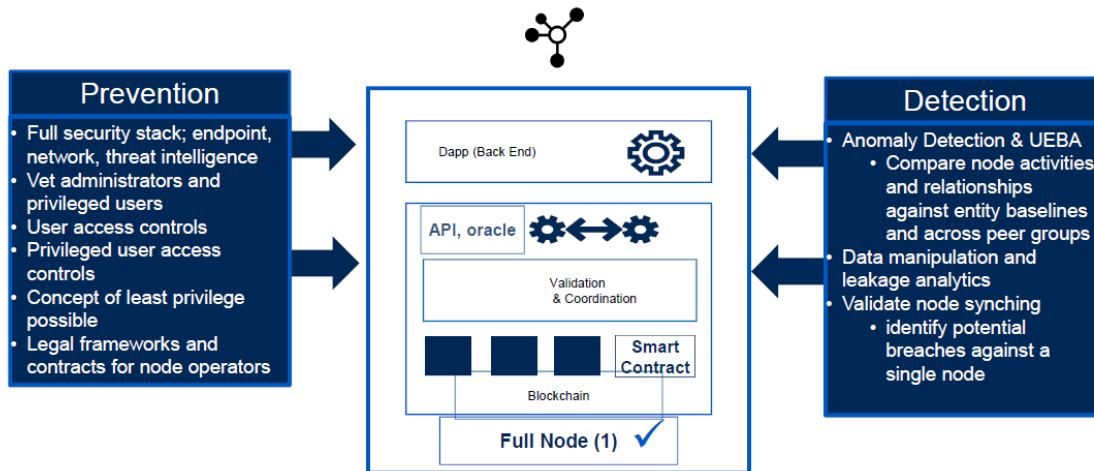
Source: Gartner

5. Permissioned nodes. The number of permissioned blockchains is relatively small compared to most permissionless protocols (although private blockchains are all inherently permissioned). By gaining access to a permissioned node (for example, Bank of America’s node access in a banking consortium on a private blockchain), threat actors can compromise, manipulate, or steal data and monetary funds. The attack methods here are identical to those on a server or infrastructure within a traditional network. They include blockchain-specific approaches such as 51% attack, other Sybil attacks (a 51% attack often utilizes Sybil [when a threat actor creates many false identities to gain a disproportionate influence on the underlying system]), and selfish mining. Threat mitigation strategies for permissioned nodes are similar to those for server and network end-point security and include firewalls, threat intelligence & monitoring, PAM, and user and entity behavior analysis (UEBA).

51% attacks. Blockchains validate additional blocks by achieving consensus (or above-50% agreement) within their P2P networks and showing PoW. In a 51% attack, a threat actor within the network can acquire control if they have above 50% “mining” power and can compute faster than other participants (tied to the PoW requirement). When successful, they can stop confirming new blocks (transactions) or add new (potentially fraudulent) ones. The move to PoS (from PoW) by Ethereum is expected to reduce the likelihood of 51% attacks since, in a PoS network, the threat actors would have to control 51% of the staked token/cryptocurrency, reducing the monetary value of their tokens by attacking the network (a financial disincentive for any such attacks).

Exhibit 183: Permissioned Node Vulnerability Assessment

Vector 5: Complementary Layered Security Solutions for Blockchain Nodes



Source: Gartner

In conclusion, blockchain is a relatively nascent technology that is evolving rapidly. Subsequently, its threat vectors continue to grow and expand exponentially as new and innovative technologies and features are added to the blockchain ecosystem. While inherent security benefits are embedded in blockchain technology (cryptographically secure data, audit trails, DDoS prevention, etc.), cybersecurity solutions must also be implemented to mitigate threat vectors and security breaches. To that end, we believe many existing cybersecurity solutions, such as firewalls, cloud workload security, application security (SCA, SAST, DAST/IAST), identity & access management, and threat intelligence, can be leveraged to address blockchain & crypto security. And they would need to be supplemented by novel security solutions that address specific gaps (such as Layer 2 functionality like smart contracts). As the market matures, we expect additional areas of vulnerability (and cybersecurity solutions) to come to the forefront and for existing and emerging vendors to address them.

Vendor Highlights

- **Chainalysis** is a blockchain data platform providing data, software, services, and research to governmental agencies, financial institutions, and cybersecurity companies. By analyzing data across its broad network, Chainalysis can identify and track ill-gotten cryptocurrency (while malicious actors attempt to launder the money), which can be used by financial institutions (in compliance and fraud detection) or law enforcement. To that end, the company has mapped out the cryptocurrency purchase and wallet portfolio histories for the last 8-10 years and then uses its graph database and a multitude of ML algorithms to build a risk profile across each wallet.

Glossary of Acronyms

ABAC	-	Attribute-Based Access Control
ACL	-	Access Control List
ADC	-	Application Delivery Controller
AI	-	Artificial Intelligence
AI-SPM	-	Artificial Intelligence Security Posture Management
AM	-	Access Management
API	-	Application Programming Interface
APISPM	-	API Security Posture Management
APM	-	Application Performance Monitoring
AppSec	-	Application Security
ARS	-	Application Runtime Security
APT	-	Automated Penetration Testing
ASIC	-	Application-Specific Integrated Circuit
ASM	-	Attack Surface Management
ASPM	-	Application Security Posture Management
AST	-	Application Security Testing
ATD	-	Advanced Threat Defense
ATO	-	Account Takeover
B2B	-	Business-to-Business
B2C	-	Business-to-Consumer
B2E	-	Business-to-Employee
BAS	-	Breach & Attack Simulation
bDSP	-	Broad-spectrum DSP
BEC	-	Business Email Compromise
BYOD	-	Bring Your Own Device
BYOI	-	Bring Your Own Identity
CAASM	-	Cyber Asset Attack Surface Management
CASB	-	Cloud Access Security Broker
CCPA	-	California Consumer Privacy Act of 2018
CDN	-	Content Delivery Network
CDR	-	Cloud Detection & Response
CI/CD	-	Continuous Integration/Continuous Delivery
CIAM	-	Customer Identity & Access Management
CIEM	-	Cloud Infrastructure Entitlement Management
CIO	-	Chief Information Officer

TECHNOLOGY / ANALYTICS, DATA, SECURITY, AND INFRASTRUCTURE SOFTWARE

CISO	-	Chief Information Security Officer
CLI	-	Command Line Interface
CNAPP	-	Cloud-Native Application Protection Platform
COPPA	-	Children's Online Privacy Protection Act
CPM	-	Consent and Preference Management
CPRA	-	California Privacy Rights Act
CPU	-	Central Processing Unit
CRM	-	Customer Relationship Management
CSP	-	Cloud Service Provider
CSPM	-	Cloud Security Posture Management
CTAP	-	Client to Authenticator Protocol
CVA	-	Correlated Vulnerability Assessment
CVE	-	Common Vulnerabilities & Exposures
CWPP	-	Cloud Workload Protection Platform
DAG	-	Data Access Governance
DAST	-	Dynamic Application Security Testing
DDoS	-	Distributed Denial-of-Service
DevOps	-	Development & Operations
DevSecOps	-	Development, Security, & Operations
DLP	-	Data Loss Prevention
DMARC	-	Domain-based Message Authentication, Reporting, & Conformance
DNS	-	Domain Name System
DOM	-	Document Object Model
DoS	-	Denial-of-Service
DPI	-	Deep Packet Inspection
DPO	-	Data Protection Officer
DRPS	-	Digital Risk Protection Service
DSAR	-	Data Subject Access Request
DSP	-	Data Security Platform
DSPM	-	Data Security Posture Management
EASM	-	External Attack Surface Management
EDLP	-	Enterprise Data Loss Prevention
EDR	-	Endpoint Detection & Response
EM	-	Exposure Management
EPP	-	Endpoint Protection Platform
FCRA	-	Fair Credit Reporting Act

FIM	-	Federated Identity Management
FTP	-	File Transfer Protocol
FWaaS	-	Firewall-as-a-Service
FWTK	-	Firewall Toolkit
GAI	-	Generative Artificial Intelligence
GDPR	-	General Data Protection Regulation
GRC	-	Governance Risk and Compliance
HIPAA	-	Health Insurance Portability & Accountability Act of 1996
HTML	-	HyperText Markup Language
HTTP	-	HyperText Transfer Protocol
IaaS	-	Infrastructure-as-a-Service
IaC	-	Infrastructure-as-Code
IAG	-	Identity & Access Governance
IAM	-	Identity & Access Management
IAMaaS	-	IAM-as-a-Service
IAST	-	Interactive Application Security Testing
ICES	-	Integrated Cloud Email Security
ID	-	Identity Document
IDaaS	-	Identity-as-a-Service
IDLP	-	Integrated Data Loss Prevention
IdP	-	Identity Provider
IDPS	-	Intrusion Detection & Prevention System
IDS	-	Intrusion Detection System
IGA	-	Identity Governance & Administration
IoC	-	Indicator of Compromise
IoT	-	Internet-of-Things
IP	-	Internet Protocol
IPS	-	Intrusion Prevention System
IPSec	-	Internet Protocol Security
ITSM	-	IT Service Management
JIT	-	Just-In-Time
JSON	-	JavaScript Object Notation
JTO	-	Journey Time Orchestration
K8s	-	Kubernetes
KSPM	-	Kubernetes Security Posture Management
LAN	-	Local Area Network

TECHNOLOGY / ANALYTICS, DATA, SECURITY, AND INFRASTRUCTURE SOFTWARE

LGPD	-	Lei Geral de Protecao de Dados Pessoais
LLM	-	Large Language Model
LTE	-	Long-Term Evolution
MAST	-	Mobile Application Security Testing
MDR	-	Managed Detection & Response
MFA	-	Multi-Factor Authentication
MITM	-	Man-In-The-Middle
MITRE ATT&CK	-	MITRE Adversarial Tactics, Techniques, & Common Knowledge
ML	-	Machine Learning
MPLS	-	Multi-Protocol Label Switching
MSSP	-	Managed Security Service Provider
MX	-	Mail Exchange
MXDR	-	Managed Extended Detection & Response
NGFW	-	Next-Generation Firewall
NICE	-	National Initiative for Cybersecurity Education
NLP	-	Natural Language Processing
NLU	-	Natural Language Understanding
NVD	-	National Vulnerability Database
OIDC	-	OpenID Connect
OOTB	-	Out-Of-The-Box
OS	-	Operating System
OSI	-	Open Systems Interconnection
OSS	-	Open-Source Software
OSVDB	-	Open Source Vulnerability Database
OTP	-	One Time Password
OWASP	-	Open Web Application Security Project
PaaS	-	Platform-as-a-Service
PAM	-	Privileged Access Management
PASM	-	Privileged Account & Sessions Management
PDPA	-	Personal Data Protection Act
PDPB	-	Personal Data Protection Bill
PEDM	-	Privileged Elevation & Delegation Management
PIM	-	Privileged Identity Management
PIN	-	Personal Identification Number
PIPL	-	Personal Information Protection Law
POP	-	Post Office Protocol

PPM	-	Privileged Password Management
PSM	-	Privileged Session Management
QA	-	Quality Assurance
RaaS	-	Ransomware-as-a-Service
RASP	-	Runtime Application Self-Protection
RBAC	-	Role-Based Access Control
RBI	-	Remote Browser Isolation
RFID	-	Radio Frequency Identification
SaaS	-	Software-as-a-Service
SAML	-	Security Assertion Markup Language
SAR	-	Subject Access Request
SASE	-	Secure Access Service Edge
SAST	-	Static Application Security Testing
SBOM	-	Software Bill-of-Materials
SCA	-	Software Composition Analysis
SDK	-	Software Development Kit
SDLC	-	Software Development Lifecycle
SDN	-	Software-Defined Networking
SDP	-	Software-Defined Perimeter
SD-WAN	-	Software-Defined Wide Area Network
SECaaS	-	Security-as-a-Service
SEG	-	Secure Email Gateway
SIEM	-	Security Information & Event Management
SIRP	-	Security Incident Response Platform
SMTP	-	Simple Mail Transfer Protocol
SOA	-	Security Orchestration & Automation
SOAR	-	Security Orchestration, Automation, & Response
SOC	-	Security Operations Center
SOD	-	Segregation Of Duties
SOX	-	Sarbanes-Oxley Act
SQL	-	Structured Query Language
SQLi	-	SQL Injection
SRR	-	Subject Rights Request
SSCS	-	Software Supply Chain Security
SSE	-	Security Service Edge
SSL	-	Secure Sockets Layer

TECHNOLOGY / ANALYTICS, DATA, SECURITY, AND INFRASTRUCTURE SOFTWARE

SSO	-	Single Sign-On
SSPM	-	SaaS Security Posture Management
SWG	-	Secure Web Gateway
TCO	-	Total Cost of Ownership
TCP	-	Transmission Control Protocol
TI	-	Threat Intelligence
TIP	-	Threat Intelligence Platform
TLS	-	Transport Layer Security
TRiSM	-	Trust Risk and Security Management
UAP	-	User Administration & Provisioning
UBA	-	User Behavior Analytics
UDP	-	User Datagram Protocol
UEBA	-	User & Entity Behavior Analytics
UI	-	User Interface
URL	-	Uniform Resource Locator
UX	-	User Experience
VA	-	Vulnerability Assessment
VLAN	-	Virtual Local Area Network
VM	-	Virtual Machine
VPN	-	Virtual Private Network
VPT	-	Vulnerability Prioritization Technology
WAAP	-	Web Application & API Protection
WAF	-	Web Application Firewall
WAN	-	Wide Area Network
WFH	-	Work-From-Home
XDR	-	Extended Detection & Response
XML	-	Extensible Markup Language
XSS	-	Cross-Site Scripting
ZSP	-	Zero Standing Privileges
ZTNA	-	Zero Trust Network Access

Disclosure Appendix

Oppenheimer & Co. Inc. does and seeks to do business with companies covered in its research reports. As a result, investors should be aware that the firm may have a conflict of interest that could affect the objectivity of this report. Investors should consider this report as only a single factor in making their investment decision.

Analyst Certification - The author certifies that this research report accurately states his/her personal views about the subject securities, which are reflected in the ratings as well as in the substance of this report. The author certifies that no part of his/her compensation was, is, or will be directly or indirectly related to the specific recommendations or views contained in this research report.

Potential Conflicts of Interest:

Equity research analysts employed by Oppenheimer & Co. Inc. are compensated from revenues generated by the firm including the Oppenheimer & Co. Inc. Investment Banking Department. Research analysts do not receive compensation based upon revenues from specific investment banking transactions. Oppenheimer & Co. Inc. generally prohibits any research analyst and any member of his or her household from executing trades in the securities of a company that such research analyst covers. Additionally, Oppenheimer & Co. Inc. generally prohibits any research analyst from serving as an officer, director or advisory board member of a company that such analyst covers. In addition to 1% ownership positions in covered companies that are required to be specifically disclosed in this report, Oppenheimer & Co. Inc. may have a long position of less than 1% or a short position or deal as principal in the securities discussed herein, related securities or in options, futures or other derivative instruments based thereon. Recipients of this report are advised that any or all of the foregoing arrangements, as well as more specific disclosures set forth below, may at times give rise to potential conflicts of interest.

All price targets displayed in the chart above are for a 12- to- 18-month period. Prior to March 30, 2004, Oppenheimer & Co. Inc. used 6-, 12-, 12- to 18-, and 12- to 24-month price targets and ranges. For more information about target price histories, please write to Oppenheimer & Co. Inc., 85 Broad Street, New York, NY 10004, Attention: Equity Research Department, Business Manager.

Oppenheimer & Co. Inc. Rating System as of January 14th, 2008:

Outperform(O) - Stock expected to outperform the S&P 500 within the next 12-18 months.

Perform (P) - Stock expected to perform in line with the S&P 500 within the next 12-18 months.

Underperform (U) - Stock expected to underperform the S&P 500 within the next 12-18 months.

Not Rated (NR) - Oppenheimer & Co. Inc. does not maintain coverage of the stock or is restricted from doing so due to a potential conflict of interest.

Oppenheimer & Co. Inc. Rating System prior to January 14th, 2008:

Buy - anticipates appreciation of 10% or more within the next 12 months, and/or a total return of 10% including dividend payments, and/or the ability of the shares to perform better than the leading stock market averages or stocks within its particular industry sector.

Neutral - anticipates that the shares will trade at or near their current price and generally in line with the leading market averages due to a perceived absence of strong dynamics that would cause volatility either to the upside or downside, and/or will perform less well than higher rated companies within its peer group. Our readers should be aware that when a rating change occurs to Neutral from Buy, aggressive trading accounts might decide to liquidate their positions to employ the funds elsewhere.

Sell - anticipates that the shares will depreciate 10% or more in price within the next 12 months, due to fundamental weakness perceived in the company or for valuation reasons, or are expected to perform significantly worse than equities within the peer group.

Distribution of Ratings/IB Services Firmwide				
Rating	IB Serv/Past 12 Mos.			
	Count	Percent	Count	Percent
OUTPERFORM [O]	426	62.28	196	46.01
PERFORM [P]	257	37.57	99	38.52
UNDERPERFORM [U]	1	0.15	0	0.00

Although the investment recommendations within the three-tiered, relative stock rating system utilized by Oppenheimer & Co. Inc. do not correlate to buy, hold and sell recommendations, for the purposes of complying with FINRA rules, Oppenheimer & Co. Inc. has assigned buy ratings to securities rated Outperform, hold ratings to securities rated Perform, and sell ratings to securities rated Underperform.

Note: Stocks trading under \$5 can be considered speculative and appropriate for risk tolerant investors.

Additional Information Available

Company-Specific Disclosures: Important disclosures, including price charts, are available for compendium reports and all Oppenheimer & Co. Inc.-covered companies by logging on to <https://www.oppenheimer.com/client-login.aspx> or writing to Oppenheimer & Co. Inc., 85 Broad Street, New York, NY 10004, Attention: Equity Research Department, Business Manager.

Other Disclosures

This report is issued and approved for distribution by Oppenheimer & Co. Inc. Oppenheimer & Co. Inc. transacts business on all principal exchanges and is a member of SIPC. This report is provided, for informational purposes only, to institutional and retail investor clients of Oppenheimer & Co. Inc. and does not constitute an offer or solicitation to buy or sell any securities discussed herein in any jurisdiction where such offer or solicitation would be prohibited. The securities mentioned in this report may not be suitable for all types of investors. This report does not take into account the investment objectives, financial situation or specific needs of any particular client of Oppenheimer & Co. Inc. Recipients should consider this report as only a single factor in making an investment decision and should not rely solely on investment recommendations contained herein, if any, as a substitution for the exercise of independent judgment of the merits and risks of investments. The analyst writing the report is not a person or company with actual, implied or apparent authority to act on behalf of any issuer mentioned in the report. Before making an investment decision with respect to any security recommended in this report, the recipient should consider whether such recommendation is appropriate given the recipient's particular investment needs, objectives and financial circumstances. We recommend that investors independently evaluate particular investments and strategies, and encourage investors to seek the advice of a financial advisor. Oppenheimer & Co. Inc. will not treat non-client recipients as its clients solely by virtue of their receiving this report. Past performance is not a guarantee of future results, and no representation or warranty, express or implied, is made regarding future performance of any security mentioned in this report. The price of the securities mentioned in this report and the income they produce may fluctuate and/or be adversely affected by exchange rates, and investors may realize losses on investments in such securities, including the loss of investment principal. Oppenheimer & Co. Inc. accepts no liability for any loss arising from the use of information contained in this report, except to the extent that liability may arise under specific statutes or regulations applicable to Oppenheimer & Co. Inc. All information, opinions and statistical data contained in this report were obtained or derived from public sources believed to be reliable, but Oppenheimer & Co. Inc. does not represent that any such information, opinion or statistical data is accurate or complete (with the exception of information contained in the Important Disclosures section of this report provided by Oppenheimer & Co. Inc. or individual research analysts), and they should not be relied upon as such. All estimates, opinions and recommendations expressed herein constitute judgments as of the date of this report and are subject to change without notice. Nothing in this report constitutes legal, accounting or tax advice. Since the levels and bases of taxation can change, any reference in this report to the impact of taxation should not be construed as offering tax advice on the tax consequences of investments. As with any investment having potential tax implications, clients should consult with their own independent tax adviser. This report may provide addresses of, or contain hyperlinks to, Internet web sites. Oppenheimer & Co. Inc. has not reviewed the linked Internet web site of any third party and takes no responsibility for the contents thereof. Each such address or hyperlink is provided solely for the recipient's convenience and information, and the content of linked third party web sites is not in any way incorporated into this document. Recipients who choose to access such third-party web sites or follow such hyperlinks do so at their own risk.

This research is distributed in the UK and elsewhere throughout Europe, as third party research by Oppenheimer Europe Ltd, which is authorized and regulated by the Financial Conduct Authority (FCA). This research is for information purposes only and is not to be construed as a solicitation or an offer to purchase or sell investments or related financial instruments. This research is for distribution only to persons who are eligible counterparties or professional clients. It is not intended to be distributed or passed on, directly or indirectly, to any other class of persons. In particular, this material is not for distribution to, and should not be relied upon by, retail clients, as defined under the rules of the FCA. Neither the FCA's protection rules nor compensation scheme may be applied. <https://opco2.bluematrix.com/sellside/MAR.action>

Distribution in Hong Kong: This report is prepared for professional investors and is being distributed in Hong Kong by Oppenheimer Investments Asia Limited (OIAL) to persons whose business involves the acquisition, disposal or holding of securities, whether as principal or agent. OIAL, an affiliate of Oppenheimer & Co. Inc., is regulated by the Securities and Futures Commission for the conduct of dealing in securities and advising on securities. For professional investors in Hong Kong, please contact researchasia@opco.com for all matters and queries relating to this report.

ESG Scores: ESG scores from Refinitiv are designed to transparently and objectively measure a company's relative ESG performance, commitment and effectiveness, based on company-reported data. This covers 10 main themes including emissions, environmental product innovation, human rights, shareholders and so on. Ratings are available on close to 10,000 companies globally, with time-series data going back to 2002. The percentile rank scores are simple to understand and transparent. They are benchmarked against The Refinitiv Business Classifications (TRBC – Industry Group) for all environmental and social categories, as well as the controversies score. They are also measured against the country of incorporation for all governance categories.

Please note that all ESG ratings are independent of Oppenheimer stock ratings. They are intended to provide supplemental information regarding ESG for our covered companies. ESG ratings do not have any impact on the stock rating.

This report or any portion hereof may not be reprinted, sold, or redistributed without the written consent of Oppenheimer & Co. Inc. Copyright © Oppenheimer & Co. Inc. 2024.