# Hype Cycle for Workload and Network Security, 2023

Published 31 July 2023 - ID G00792335 - 98 min read

By Analyst(s): Charlie Winckless, Feng Gao

Security platform consolidation, zero trust strategies and generative AI are key developments for this Hype Cycle. Security and risk management leaders should consolidate security platforms and adopt suitable emerging technologies to boost efficiency and gain wider security visibility.

## Analysis

### What You Need to Know

The desire for less complexity, simplified operations and greater efficiency continues to drive cybersecurity consolidation, according to the 2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey. More than half the participants in this survey were pursuing vendor consolidation to increase the efficacy of security solutions, while just over one-third (35%) saw cost reduction as a primary motivation. Gartner sees strong consolidation efforts in multiple workload and network security areas, including the pairing of security service edge (SSE) and secure access service edge (SASE) platforms for (largely) outbound user traffic, and the use of cloud-native application protection platforms (CNAPPs) for cloud workloads and applications.

Developing a zero trust approach remains important for many of Gartner's clients, and new technologies to support a zero trust mindset continue to emerge. Of these, generative cybersecurity AI has been subject to a great deal of hype in 2023. Organizations are extremely interested in the possible impacts — positive and negative — of generative AI, especially this technology's potential to help their (often short-staffed) security teams work with increasingly complex environments.

Security and risk management leaders must select the right enabling security technologies for their organization to continuously support cybersecurity consolidation and a zero trust strategy without missing the opportunities that arise from emerging technologies like generative cybersecurity AI.

## The Hype Cycle

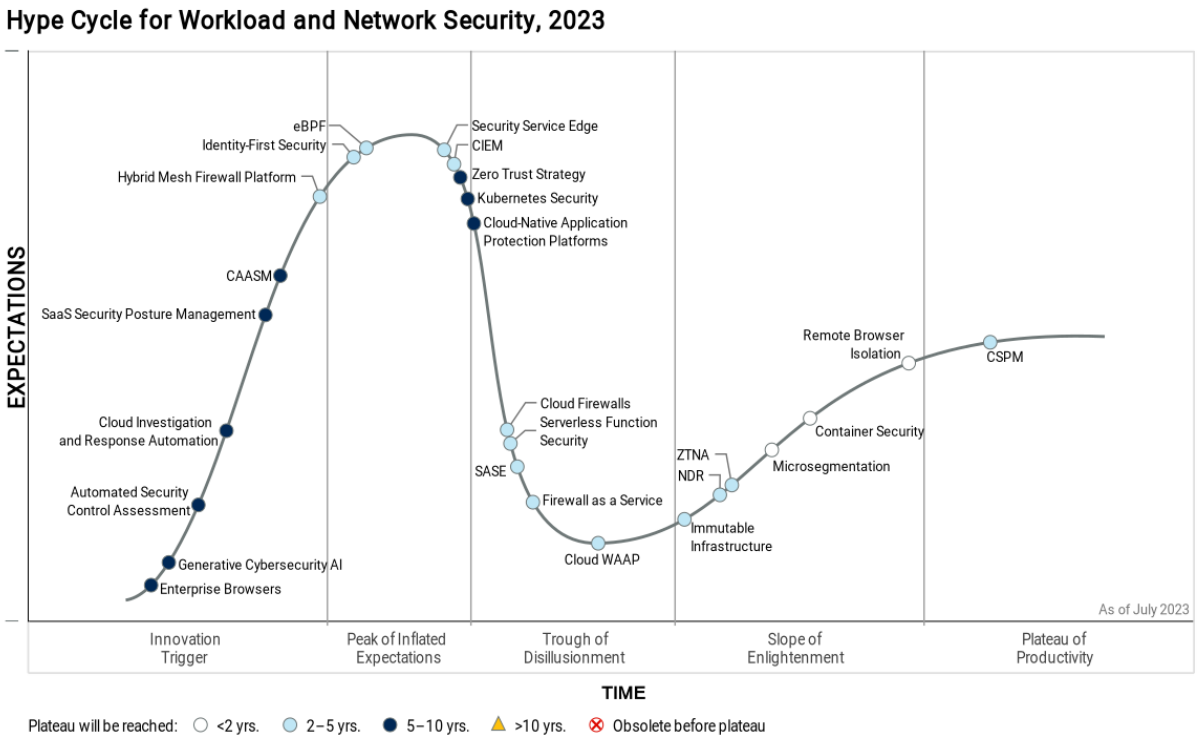
This Hype Cycle reflects the continuing trend toward converged platforms and strong interest in zero trust strategies, as well as emerging cloud security technologies, generative AI and more.

Several technologies have been retired from the Hype Cycle this year, due to their maturation and to increased consolidation at the edge and in the cloud (for a full list, see the Off the Hype Cycle section). For instance, most organizations are replacing secure web gateways, cloud access security brokers (CASBs) and many of their remote access solutions with converged security service edge (SSE) platforms, and CNAPPs are incorporating the mature cloud workload protection platforms (CWPPs). Adoption of ZTNA (and emerging interest in universal ZTNA) and the hybrid workforce has reduced interest in (and hype about) network access control, and ZTNA remains a starting point for many zero trust architecture efforts. Additionally, cloud adoption and, again, the hybrid workforce are furthering the expansion of highly mature network firewalls into cloud firewalls and nascent firewall-as-a-service products. They are also prompting network security policy management to develop in the direction of cloud security posture management (CSPM) and CNAPPs.

Several emerging technologies appear in this Hype Cycle:

- Generative AI has attracted a great deal of hype this year, which has triggered the inclusion of generative cybersecurity AI.
- Coping with complex configuration requirements remains a big challenge in both cloud and on-premises environments, and is best addressed with automation. As a result, automated security control assessment (ASCA) tools are emerging to verify the configuration of products in hybrid environments.
- Desire for a reliable method of ascertaining the severity of security events in the cloud has led to cloud investigation and response automation (CIRA) products.
- Extended Berkeley Packet Filter (eBPF) techniques are becoming the new norm for Linux security and are now widely used in Linux workload protection.

Figure 1: Hype Cycle for Workload and Network Security, 2023




## The Priority Matrix

Convergence is driving the transformational innovations of SASE and SSE as networking and security teams seek to simplify their operations, improve visibility to user access to resources regardless of user and device location, and implement dynamic zero trust policies for front-end, user and device access. SASE and SSE have already subsumed many other innovations, and we expect remote browser isolation also to be largely a feature of these platforms in the next two years. Many vendors offer elements of a SASE framework, which means organizations must prioritize their use cases and contract expirations when selecting a vendor (or two coupled vendors).

Microsegmentation is maturing quickly, but remains difficult to deploy at scale. Move past the evaluation phase by narrowing your scope to fewer, critical workloads running behind strong macrosegmentation controls and work directly with application teams to verify connections before enforcing policy. Iterate to support additional workloads after addressing the most critical.

CSPM is on the Plateau of Productivity and of high benefit. Expect CSPM products to add cloud infrastructure entitlement management (CIEM) functionality, and increasingly to become part of consolidated CNAPP platforms. Look for CSPM products that offer runtime visibility, either through integration with mature CWPP platforms, eBPF integration, or the use of side-scanning techniques.

### Table 1: Priority Matrix for Workload and Network Security, 2023

(Enlarged table in Appendix)

| *Benefit* | *Years to Mainstream Adoption* | | | |
|---|---|---|---|---|
| ↓ | ***Less Than 2 Years*** ↓ | ***2 - 5 Years*** ↓ | ***5 - 10 Years*** ↓ | ***More Than 10 Years*** ↓ |
| Transformational | | SASE<br>Security Service Edge | Generative<br>Cybersecurity AI | |
| High | Microsegmentation | Cloud WAAP<br>CSPM<br>Hybrid Mesh Firewall Platform<br>Identity-First Security | Cloud-Native Application Protection Platforms<br>Zero Trust Strategy | |
| Moderate | Container Security | CIEM<br>Cloud Firewalls<br>eBPF<br>Firewall as a Service<br>Immutable Infrastructure<br>NDR<br>Serverless Function Security<br>ZTNA | Automated Security Control Assessment<br>CAASM<br>Cloud Investigation and Response Automation<br>Enterprise Browsers<br>Kubernetes Security<br>SaaS Security Posture Management | |
| Low | Remote Browser Isolation | | | |

Source: Gartner (July 2023)

## Off the Hype Cycle

- CASBs are now mature. Recent innovations have been largely subsumed by SSE platforms.
- CWPPs in their stand-alone form are mature and have reached the Plateau of Productivity. Gartner is also seeing CWPPs delivered as components of CNAPPs.
- The single entry for container and Kubernetes security on last year's Hype Cycle has been replaced by separate (though closely related) entries for container security and Kubernetes security, due to differing levels of maturity, adoption, and client interest.
- Distributed denial of service (DDoS) mitigation platforms continue to be widely adopted because of the growing number of DDoS attacks. DDoS mitigation is still available as a stand-alone offering. There are also platform-based offerings. The market for DDoS mitigation is mature, with service providers offering tiered pricing models.
- Hardware-based security solutions have attained maturity.
- Network access control (NAC) is a fully mature technology. Major vendors are incrementally improving products and expanding NAC to handle cyber-physical systems' security or integrating NAC with ZTNA as part of universal ZTNA products. Many organizations implement NAC to improve visibility and control for devices on local networks, often as a result of an audit, using well-known protocols. This poses well-documented technical challenges, for which there are, however, workarounds.
- Network firewalls are an important network security control, the market for which is fully mature, with all the vendors offering similar capabilities. The rise of hybrid environments and workforces is fueling demand for cloud firewalls, firewall as a service (FWaaS) and hybrid mesh firewall products that support emerging use cases.
- Network security policy management (NSPM) has reached full maturity. Emerging cloud use cases increasingly favor CSPM tools and CNAPPs.
- Secure web gateways are fully mature. Recent innovations have been largely subsumed by SSE platforms.

## On the Rise

### Enterprise Browsers

**Analysis By:** Dan Ayoub

**Benefit Rating:** Moderate

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Definition:**

Enterprise browsers and extensions deliver security services for policy enforcement, visibility, and productivity through a managed web browser or plug-in extensions. Many products in this category provide lightweight features and benefits similar to those found in SWG, CASB, ZTNA, RBI, VDI, and VPN products. Enterprise browsers are complementary to existing security solutions, and have seen early success providing access and posture assessment security to unmanaged devices.

**Why This Is Important**

Enterprise browsers represent a new way of delivering security services and receiving real-time intelligence from existing security agents layered into the OS. Today, many of these products are able to deliver some important features and benefits of other security products; however, trade-offs still remain. This gap is expected to close over time as the category becomes more mature and more partners enter the ecosystem.

**Business Impact**

Existing security products will continue to provide enterprises with increasingly sophisticated levels of protection, access control and reporting analytics. However, many of these products will extend functionality to support browsers via strategic partnerships, integrations or browser extensions. Enterprise browsers are not likely to replace existing security controls throughout the enterprise, but rather extend the reach of these tools for additional use-case coverage.

**Drivers**

- Enterprise browsers are embracing the new remote-work paradigm to consolidate secure remote access for contractors, suppliers and branch locations relying on nonstandardized equipment.

- Existing security solutions often struggle to support unmanaged devices. This is an area where enterprise browsers have found early traction in the market, by providing an acceptable level of secure remote access that is able to maintain a mostly familiar end-user experience.
- Small and midsize organizations are also expected to be early adopters of this technology. Organizations with simpler environments and requirements may see early opportunities to displace existing or add new security controls with an enterprise browser as a cheaper, centrally managed option that immediately raises their maturity level.
- Many security vendors already offer integration with browsers via extensions, while others have sought strategic partnerships and integrations with browser manufacturers. Enterprise browsers represent a new way of delivering security services to an organization, which extend the edge of traditional network security solutions.
- Enterprise browser vendors are increasing integration with security controls, such as data loss prevention (DLP), configuration management, logging and integration with security information and event management (SIEM)/extended detection and response (XDR) platforms, identity protection, phishing protection, security service edge (SSE) functions, and monitoring for malicious activity across downloads and extensions.

### Obstacles

- Free browsers are ubiquitous, to the point that organizations must have specific use cases to justify the purchase of a separate browser. These justifications will become easier to identify as enterprises begin to realize the extensible and flexible enterprise security and management potential of the browser. However, it is unlikely most companies will dedicate budget to an enterprise browser without the ability to offset that spend elsewhere.
- Larger organizations with mature cybersecurity and infrastructure operations may find it impractical to reduce the complexity of their existing environments with enterprise browsers, though specific use cases may exist to justify a relatively small purchase (such as providing Day 1 access for new organizations gained through mergers and acquisitions, contractor access management, or as layered security controls on top of fragile critical infrastructure).

### User Recommendations

- Recognize that placing all security controls at the endpoint (or in this case, browser) is a flawed strategy. Browser-based integrations may make sense in some circumstances, but having multiple points of integration will be required.
- Focus on hybrid offerings that are able to leverage browsers to securely deliver access to workforce productivity tools.
- Exercise caution when reviewing messaging and promises from vendors in this space, as specialized infrastructure (proxy, gateway, etc.) may still be required to address certain use cases.
- Expect an increasing number of security and productivity tool capabilities to be incorporated over time. However, the technology is still in the early stages of adoption, so individual vendor roadmaps will be driven by early market success.

### Sample Vendors

Check Point Software Technologies; Ermes Cyber Security; Google; Island; Microsoft; Perception Point; Seraphic Security; SlashNext; SURF Security; Talon Cyber Security

### Gartner Recommended Reading

Emerging Tech: Security — The Future of Enterprise Browsers

## Automated Security Control Assessment

**Analysis By:** Evgeny Mirolyubov, Jeremy D'Hoinne

**Benefit Rating:** Moderate

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

### Definition:

ASCA processes and technologies focus on the analysis and remediation of misconfigurations in security controls (e.g., endpoint protection, network firewall, identity, email security, and security information and event management), which improves enterprise security posture. ASCA can be a stand-alone tool or a capability of other security products, such as firewalls, identity threat detection and response, network security policy management, and cloud infrastructure entitlement management.

### Why This Is Important

Automated security control assessment (ASCA) technologies reduce an organization's attack surface caused by security configuration drift, poor defaults, exessive tuning to reduce false positive rates, and high administration staff turnover. ASCA improves the security posture by verifying the proper, consistent configuration of security controls, rather than simply verifying the existence of controls.

### Business Impact

Organizations implementing ASCA processes and technologies enhance staff efficiency, minimize the impact of human errors and improve resilience in the face of organizational churn. ASCA reduces security control configuration gaps that unnecessarily expose the organization to otherwise preventable attacks.

### Drivers

- The volume of misconfigurations in security controls continues to grow with the increased complexity of environments, emerging threat vectors, the proliferation of new security tools and the high turnover of administration staff, leading to a more exposed attack surface.
- Specific organizational use cases and objectives require the preservation of complex heterogeneous infrastructure and security architectures, instead of pursuing simplification through vendor consolidation.
- The optimization of configurations of enterprise security controls cannot rely exclusively on manual periodic configuration reviews; siloed, tool-centric approaches; or occasional penetration tests.
- Continuously assessing and remediating security controls configurations in accordance with the highest-risk exposures is an effective risk mitigation strategy, ultimately reducing the attack surface.

### Obstacles

- Lack of support for niche vendor and security control assessments makes ASCA tools less valuable for large, complex organizations with specialized point solutions.
- Overlaps with existing tools and vendors that are looking to accomplish similar goals in individual silos, such as tools for network firewall or cloud configuration assessments.
- The slow pace of remediation, paired with continuous assessments, may cause findings to pile up without proper automation and a triage process that considers business context.
- Lack of mature processes to optimize security controls configurations end to end.
- Budget increases to invest in people, technologies and, possibly, managed services needed to respond to an accelerated list of configuration issues discovered by ASCA tools.

### User Recommendations

- Reduce complexity by pursuing security vendor consolidation or considering alternatives, such as “policy as code” to manage security configurations.
- Establish processes to evaluate enterprise security controls, including planning, assessing, remediating and validating expected configurations.
- Evaluate incumbent security providers for ASCA capabilities, including continuous configuration monitoring and alerting about the impact of configuration changes on security protection, operations and productivity.
- Assess ASCA providers’ capabilities, including the breadth of coverage for your enterprise security controls, cross-control configuration analysis quality and integration of input from cybersecurity validation tools, such as BAS and VA.

### Sample Vendors

Absolute Software; CardinalOps; Veriti; XM Cyber

### Generative Cybersecurity AI

**Analysis By:** Jeremy D'Hoinne, Avivah Litan, Mark Horvath, Wilco van Ginkel

**Benefit Rating:** Transformational

**Market Penetration:** Less than 1% of target audience

**Maturity:** Embryonic

**Definition:**

Generative cybersecurity AI technologies generate new derived versions of security-related and other relevant content, strategies, designs and methods by learning from large repositories of original source data. Generative cybersecurity AI can be delivered as a public or privately hosted cloud service or embedded with security management interfaces. It can also integrate with software agents to take action.

**Why This Is Important**

Enterprises witness many applications leveraging foundation models that can read multimodal objects (such as sensory data and images), following the first applications based on large language models (LLMs).

Cybersecurity technology providers can exploit generative cybersecurity AI to improve existing workflows, be a proxy of existing analytics, and generate security configuration or realistic attack data. Soon, applications will include autonomous agents, which can work using high-level guidance without a need for frequent prompting.

**Business Impact**

Existing vendors and new startups will add generative cybersecurity AI, expanding or replacing features. They will start implementing it with resource-intensive tasks, such as incident response, exposure or risk management, or code analysis.

Organizations will benefit from generative cybersecurity AI as it can improve efficiency and shorten response times to cybersecurity risks and threats. The pace of adoption will vary across industries and geographies due to security and privacy concerns.

**Drivers**

- ChatGPT is one of the most hyped and fastest-adopted AI technologies ever. It relies on generative AI foundation models, which are largely trained on massive internet datasets.
- Security operations center (SOC) teams cannot keep up with the deluge of security alerts they must constantly review, and are missing key threat indicators in the data.
- Risk analysts need to speed up risk assessments, and be more agile and adaptable through increased automation and prepopulation of risk data in context.
- Organizations continue to experience skill shortages and look for opportunities to automate resource-intensive cybersecurity tasks. Use cases for the application of generative AI include: synthesizing and analyzing threat intelligence; generating remediation suggestions for application security, cloud misconfigurations and configuration changes to adjust to threats; generating scripts and codes generation; implementing secure code agents; identifying and graphing key security events in logging systems; conducting risk and compliance identification and analysis; automating the first steps in incident response; tuning of security configuration adjustment; creating general best practice guidance.
- Generative cybersecurity AI augments existing continuous threat exposure management (CTEM) programs by better aggregating, analyzing and prioritizing inputs. It also generates realistic scenarios for validation.
- Generative AI offerings include the ability to fine-tune models, develop applications using prompt engineering and integrate with prepackaged tools and plugins through APIs. These possibilities open up a path for providers to add generative cybersecurity AI.
- Microsoft has already demonstrated a preview version of its security co-pilot feature, which is expected to drive competitors to embed similar approaches.
- Security program performance solutions and activities can solve their increasing demand for business alignment. Further, they can perform scenario planning for budget (re)allocation, and efficiency and effectiveness indicators and corrections.

**Obstacles**

- The cybersecurity industry is already plagued with false positives. Early examples of “hallucinations” and inaccurate responses will cause organizations to be cautious about adoption or limit the scope of their usage.
- Best practices and tooling to implement responsible AI, privacy, trust, security and safety for generative AI applications do not fully exist yet.
- Privacy and intellectual property concerns could prevent sharing and usage of business- and threat-related data, reducing the accuracy of generative cybersecurity AI outputs.
- As generative AI is still emerging, establishing the trust required for its wider adoption will take time. This is especially true for the skill augmentation use cases, as you would need the skills you are supposed to augment, in order to ensure the recommendations are good.
- Uncertainty on laws and regulations related to generative AI may slow down adoption in some industries, for example regulated industries in EU countries subject to GDPR compliance.

### User Recommendations

- Pick initial use cases carefully. First implementations might have a higher error rate than more mature techniques already in place.
- Monitor the addition of generative AI features from your existing providers and beware of “generative AI washing.” Don’t pay a premium before obtaining measurable results.
- Choose fine-tuned models that align with the relevant security use case or fine-tune in-house models from base models offered by the providers.
- Refrain from sharing sensitive and confidential data with hosted models until verifiable privacy assurances are provided by the host.
- Apply AI security frameworks, such as AI TRiSM. Work with your legal team on data privacy and copyright issues.
- Implement a documented approval workflow for allowing new generative cybersecurity AI experiments.
- Make it mandatory from a policy standpoint that any content (that is, configuration or code) generated by an AI is fully documented, peer-reviewed by humans and tested before it is implemented. If not possible, consider any AI-generated content as “Draft Only” when used for critical use cases.

### Gartner Recommended Reading

4 Ways Generative AI Will Impact CISOs and Their Teams

Innovation Insight for Generative AI

Market Guide for AI Trust, Risk and Security Management

## Cloud Investigation and Response Automation

**Analysis By:** Neil MacDonald

**Benefit Rating:** Moderate

**Market Penetration:** Less than 1% of target audience

**Maturity:** Emerging

**Definition:**

CIRA offerings automate the collection of forensics data and assist with the automated response to cloud incidents, such as a breach. Collecting this information spans multiple clouds, account boundaries and types of resources, many of which are highly dynamic, requiring new cloud-native approaches.

**Why This Is Important**

Legal and regulatory requirements for preservation of digital evidence for forensics is common across many industries in the event of a breach. This capability must be available for cloud-based resources. Cloud investigation and response automation (CIRA) offerings provide a highly automated, cloud-neutral way of providing this capability with a deep understanding of cloud artifacts, log sources and telemetry to capture.

**Business Impact**

Most organizations have manual procedures and processes for the collection and preservation of digital evidence in the event of a breach to meet legal and regulatory requirements. CIRA offerings streamline this through automation and normalization of collection processes across multiple public clouds with built-in knowledge of what artifacts to capture, helping to leverage limited cloud security resources.

**Drivers**

- Many enterprises have legal/regulatory obligations and their own requirements for evidence preservation in the event of a breach.
- All cloud infrastructure is programmatic, lending itself to automation of the collection of logs and other digital artifacts in the event of a breach.
- Most enterprises have a shortage of skilled cloud security professionals, making automation a critical requirement for cloud security offerings.
- CIRA offerings include out-of-the-box knowledge of what to collect and how to collect it, accelerating the time to adopt.
- The hyperscale providers themselves will offer built-in CIRA capabilities — albeit specific to their own clouds. Third-party CIRA offerings standardize the collection across clouds.

### Obstacles

- Many organizations manually collect incident response information or write their own scripts to gather the evidence required and don't see the need for CIRA.
- Most tools don't capture the memory of running systems or require the deployment of additional agents to achieve this, yet this is often a requirement for forensics.
- Legacy forensics vendors will add capabilities to address their cloud forensics gaps, and potential customers may wait for this rather than pursue a point solution.
- Modern security information and event management (SIEM), security orchestration, automation and response (SOAR), and extended detection and response (XDR) platforms will add CIRA capabilities over time, and potential customers may wait for this rather than pursue a point solution.
- Cloud security posture management (CSPM) and cloud-native application protection platforms (CNAPPs) will likely also address cloud detection and response use cases and include CIRA capabilities, offsetting the need for a point solution.
- No vendor yet offers deep support for private clouds built on VMware; VMware Cloud on Amazon Web Services (AWS), Microsoft Azure VMware Solution or Google Cloud VMware Engine; or OpenStack.

### User Recommendations

Users considering a CIRA capability should:

- Extend and standardize their incident response capabilities to cloud-based resources
- Favor the use of a third-party tool over manual collection, especially when multiple clouds are involved
- Have a plan for the capture and preservation of memory footprints of systems where detailed forensics are required
- Investigate the use of management agents or OSS agents such as VARC to gather memory images for critical systems if required
- Ensure the offering addresses the unique requirements of container and Kubernetes-based environments
- Ensure the offering gathers details on serverless function executions, permissions and access as no agent-based visibility is possible

- Ensure the offering provides a rich set of automated response options
- Favor SIEM/SOAR, CSPM, CDR or XDR platforms that offer a roadmap for multicloud CIRA capabilities without requiring the purchase of a third-party solution

**Sample Vendors**

Amazon Web Services; Binalyze; Cado Security; Command Zero; Gem; Magnet Forensics; Mitiga; OpenText

**Gartner Recommended Reading**

Emerging Tech: Security — Cloud Investigation and Response Automation Offers Transformation Opportunities

Emerging Technologies: Future of Cloud-Native Security Operations

Market Guide for Cloud-Native Application Protection Platforms

Market Guide for Digital Forensics and Incident Response Retainer Services

Toolkit: Cybersecurity Incident Response Plan

**SaaS Security Posture Management**

**Analysis By:** Charlie Winckless

**Benefit Rating:** Moderate

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Adolescent

**Definition:**

SaaS security posture management (SSPM) continuously assesses the security risk and manages the security posture of SaaS applications. SSPM tools offer a range of capabilities, such as reporting on and suggesting improvements to native SaaS security settings, managing identity permissions, and identifying interconnected SaaS applications. Some tools also provide a comparison against industry frameworks, data visibility and democratized or fully automated remediation.

### Why This Is Important

SaaS is the delivery model for many critical enterprise applications, leading to large amounts of sensitive information being stored outside the traditional controls of the corporate network. These applications and their interconnections (commonly to other SaaS applications) are increasingly complicated to configure and manage security, an issue compounded by the fact that everyone is different. SSPM platforms provide consistent and automated visibility into the security of SaaS applications

### Business Impact

SaaS usage is both widespread and growing in Gartner clients. Security service edge (SSE) vendors provide protection of sensitive data and user access at the network layer, but are often blind to complex configuration errors and SaaS-to-SaaS communication. SSPM tools reduce exposure to common SaaS risks by continuously scanning for and reducing configuration mistakes, suspicious SaaS-to-SaaS communications, and overly scoped permissions.

### Drivers

- As more valuable data is processed using SaaS, attackers will increasingly target these applications to breach sensitive data. The primary source of cloud breaches is a failure in configuration or theft of a token. It is extremely rare for it to be an underlying flaw in the platform.
- SaaS's rising popularity, complexity and interconnectedness have created blind spots (for example, an unprotected connected application might be able to access data with minimum restrictions) and control gaps (particularly regarding SaaS configuration) in ever-more critical applications. Traditional controls and even SSE controls cannot manage and mitigate these gaps effectively. In such cases, SSPM tools provide the necessary visibility and protection.
- Regulation is becoming increasingly strict, imposing large penalties for data breaches. Regulators are starting to show concern about SaaS applications such as Cybersecurity and Infrastructure Security Agency (CISA)'s reference architecture for SaaS, Secure Cloud Business Applications (SCuBA).
- SaaS is not simple as a service. Trying to control SaaS via manual processes does not scale. Increased automation of configuration validation and remediation is necessary for effective control.

### Obstacles

- There is increased overlap and consolidation of SSPM features and functions within SSE platforms and few organizations wish to have another console to govern another set of clouds.
- Many enterprises lack focus on SaaS security and lack any role responsible for SaaS security and therefore a buyer for SSPM. Acquisition and configuration of SaaS often reside within the business.
- Most current SSPM tools lack discovery capabilities, so rely on alternative tools (such as SSEs or next-generation firewalls) to identify the SaaS applications in use across the enterprise, or assume they are integrated into an enterprise identity provider.
- SSPM tools rely heavily on robust APIs from the SaaS provider for visibility into configuration and identity permissions. While many SaaS apps provide APIs, little standardization exists and most smaller vendors have limited or no API-based visibility.

### User Recommendations

- Evaluate the current SSPM-like capabilities of existing tools, particularly if you have an SSE or SMP. If they provide sufficient visibility and management of SaaS native controls, use them. Don't buy yet another product and invest tactically when you decide to purchase to address any identified shortcomings.
- Prefer SSPM tools with broad capabilities, not ones that focus just on interconnection, or just on configuration.
- Configure the SSPM tool to crawl through each new release of governed SaaS applications to discover new functions and potential attack surfaces, such as exposed APIs, to maintain full visibility and compliance.
- Pressure vendors in established cloud security and management markets to broaden their capabilities to offer SSPM capabilities, including automation for SaaS control with a specific focus on SSE and SMP providers.
- Establish shorter-term contracts if SSPM is needed to address a gap.

### Sample Vendors

Adaptive Shield; AppOmni; Axonius; Microsoft; Netskope; Obsidian; Palo Alto Networks; Suridata.ai; Valence

**Gartner Recommended Reading**

Tool: Framework for Developing SaaS Security Policy

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Market Guide for SaaS Management Platforms

Quick Answer: Cloud, Kubernetes, SaaS — What's the Best Security Posture Management for Your Cloud?

## CAASM

**Analysis By:** John Watts, Mitchell Schneider, Neil MacDonald

**Benefit Rating:** Moderate

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

**Definition:**

Cyber asset attack surface management (CAASM) is focused on enabling security teams to overcome asset visibility and exposure challenges. It enables organizations to see all assets (internal and external), primarily through API integrations with existing tools, query consolidated data, identify the scope of vulnerabilities and gaps in security controls, and remediate issues.

**Why This Is Important**

CAASM aggregates asset visibility from other products that collect a subset of assets, such as endpoints, servers and devices. By consolidating internal and external cyberassets, users can query to find coverage gaps and misconfigurations for security tools such as vulnerability assessment and endpoint detection and response (EDR) tools. CAASM provides mostly passive data collection via API integrations, replacing time-consuming manual processes to collect and reconcile asset information.

### Business Impact

CAASM enables security teams to improve basic security hygiene by finding security controls gaps, security posture, and asset exposures across all digital assets. Organizations that deploy CAASM reduce dependencies on homegrown systems and manual collection processes, and remediate gaps either manually or via automated workflows. Organizations visualize security tool coverage, support attack surface management (ASM) processes, and correct systems of record that may have stale or missing data.

### Drivers

- Full visibility into any asset owned by the organization collected through existing tools to improve the understanding of an organization's potential attack surface and existing security control gaps.
- Quicker audit compliance reporting through more accurate, current, and comprehensive asset and security control reports.
- Consolidation of existing products that collect asset and exposure information into a single normalized view, to reduce operational overhead of manual processes and dependencies on homegrown applications.
- Access to consolidated asset views for multiple individuals and teams across an organization and integrations with other systems of record for current state visibility.
- Lower resistance to data collection from, and better security visibility into, "shadow IT" organizations, installed third-party systems and line-of-business applications over which the IT department lacks governance and control. Security teams need visibility in these places, whereas the IT department may not.
- Help IT teams improve the accuracy of their existing CMDB through periodic updates of assets and attributes missed by CMDB reconciliation processes.

**Obstacles**

- Resistance to “yet another” tool — there are increasing overlaps with CAASM vendors and adjacent tools that provide some asset inventory and reporting.
- Not all vendors have capabilities to identify and integrate with every required system for visibility and vulnerability information.
- Vendor response actions to prioritized issues may be limited to opening tickets or invoking a script.
- Products licensed per asset consumed become cost-prohibitive for very large organizations.
- The scalability of a single instance may be limited for extremely large environments, in terms of both data collection and usability.
- Tools that can be integrated with a CAASM product either do not exist (due, for example, to the lack of an API) or may be prevented from integrating by the teams that own them.
- Reconciliation processes that conflict with source systems may not be resolved easily within CAASM vendor tooling.

### User Recommendations

- Take advantage of proof-of-concept opportunities, and free versions of products and subscriptions, in order to “try before you buy,” as CAASM products are nondisruptive and easy to deploy.
- Given the immaturity of the market, sign no more than a one year contract.
- Favor vendors that can combine inside-out and outside-in asset visibility capabilities or partner with EASM providers.
- Favor vendors that understand all asset types beyond traditional asset categories such as granular software assets, users, and IoT/OT systems to extend to more use cases.
- Inventory all available APIs that can be integrated with the CAASM product you are considering, and ensure you have read-only or low-privilege user accounts available to integrate.
- Ask your incumbent security vendors if they have a roadmap to provide CAASM functionality in future.

### Sample Vendors

Armis; Axonius; Brinqa; Encore; JupiterOne; Noetic Cyber; Northstar.io; Ordr; Panaseer; Sevco Security

### Gartner Recommended Reading

Innovation Insight for Attack Surface Management

Implement a Continuous Threat Exposure Management (CTEM) Program

Competitive Landscape: External Attack Surface Management

Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management

## Hybrid Mesh Firewall Platform

**Analysis By:** Rajpreet Kaur, Adam Hils, Feng Gao

**Benefit Rating:** High

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Emerging

**Definition:**

A hybrid mesh firewall (HMF) platform is a centralized policy management plane supporting hybrid environments through different firewall enforcement types by integrating with native cloud and on-premises network security controls along with other adjacent security technologies. The management plane is primarily a cloud-delivered service connected to on-premises, cloud and as-a-service firewall enforcement points from a single vendor.

**Why This Is Important**

Security and risk management leaders are struggling with the need to implement firewall controls in multiple environments leading to a lack of centralized implementation, management and visibility. Hybrid mesh firewall platforms offer multiple firewall enforcement types (e.g., hardware, virtual, cloud-native, firewall as a service [FWaaS]) from the same vendor, which can be deployed and managed from a centralized management interface.

**Business Impact**

Hybrid mesh firewall platforms help enterprises align with the cybersecurity mesh architecture (CSMA) concept for their firewall requirement. It allows you to consolidate into a firewall platform from a single vendor across multiple environments supporting consolidated policy management. It can support multiple firewall use cases such as data center, cloud, work from home, roaming users, branch offices and enterprise networks.

### Drivers

- Cloud-hosted workloads often have radically different “agile” deployment pipelines that preclude the use of traditional firewall controls. This requires firewall controls for agile deployed workloads and containers or serverless compute offering automation and seamless integration to support this evolving use case.
- Growing adoption of zero trust architecture has also changed the firewall selection criteria, as enterprises have moved beyond adding a point firewall solution toward a platform, which can help them use the firewalls across multiple use cases.
- Remote and hybrid working has accelerated the adoption of FWaaS and preference from the same firewall vendor.
- Adoption of Internet of Things (IoT) devices is changing the interconnectivity requirement and the need to secure them.
- There is a need for centralized visibility and control across multiple firewall enforcements.
- Use of best-of-breed firewall players for evolving use cases is leading to added complexity and management overhead.

### Obstacles

- The features and automation promised by the vendor don’t always work as advertised.
- On-premises firewalls present deployment and maintenance issues when combined with current hybrid and remote working models. They require different firewall enforcement points without an additional management overhead for the administrators.
- Network security teams lack skills and resources to configure and run the firewalls for emerging use cases such as DevSecOps, distributed connectivity for hybrid environments leading to integration and support challenges.
- Multiple different enforcement types are leading to different pricing models, leading to pricing and licensing complexity as the traditional models are no longer relevant.
- Not all vendors offer mature enforcement types for all the firewall use cases; as a result, teams are bound to adopt best-of-breed stand-alone offerings.

### User Recommendations

- Integrate hybrid mesh firewalls with your zero trust strategy, as most existing controls such as hardware-based firewalls will not be fully retired in the mid to long term, driving complexity that HMF helps simplify.
- Always evaluate the automation and integration needs for the specific use case, such as DevSecOps being run in the environment.
- Demand transparent contracts from the reseller/vendor. Refuse to sign a contract that doesn't clearly highlight the part numbers and components involved in it.
- Closely verify the requirement for all the software subscriptions. You might not need all of the subscriptions that the vendors try to sell.

### Sample Vendors

Barracuda; Check Point Software Technologies; Cisco; Forcepoint; Fortinet; H3C; Huawei; Juniper; Palo Alto Networks; SonicWall

### Gartner Recommended Reading

Magic Quadrant for Network Firewalls

Quick Answer: Demystifying Network Firewall Pricing Models to Build an Effective Sourcing Strategy

Tool: Competitive Evaluation of Network Firewalls

## At the Peak

### eBPF

**Analysis By:** Simon Richard

**Benefit Rating:** Moderate

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

#### Definition:

Extended Berkeley Packet Filter (eBPF) is an enhancement to the Linux operating system kernel that allows specific instruction sets to run (sandboxed) inside the kernel. It allows companies to add features to Linux without changing kernel source code or requiring kernel modules.

#### Why This Is Important

eBPF increases the extensibility of Linux. It allows users to create hooks that are triggered by Linux kernel events. This offers a safer and simpler way to add capabilities, such as performance, security and visibility, in Linux. Technology vendors like ISVs and cloud providers use eBPF to avoid kernel-level modules, which carry inherent risks. eBPF is used in production at scale by hyperscalers, including AWS, Facebook and Netflix, and content delivery networks (CDN) such as Cloudflare.

#### Business Impact

eBPF improves observability, security and performance for applications. However, most enterprises will not use eBPF directly. Technology vendors do use eBPF as an underpinning technology in their products and services to improve the performance and safety of programs that run on Linux. eBPF allows extremely technically savvy organizations to safely and quickly make changes to Linux, compared to using alternative approaches, such as Linux kernel modules or upstreaming to the Linux distribution.

#### Drivers

- eBPF usage is driven by hyperscalers using it to deliver more efficient cloud offerings, as well as networking, monitoring and security vendors that use it in their products.

- Hyperscalers use eBPF to remediate kernel vulnerabilities without patching to address Day 0 vulnerabilities, and to more efficiently handle distributed denial of service (DDoS) attacks.
- Organizations are looking to accelerate the development speed of software that runs on Linux via avoidance of the requirement for upstream inclusion into the Linux distribution.
- Organizations are looking to improve the performance, security and monitoring capabilities of software running on Linux.
- eBPF is popular among technologically advanced companies, including technology vendors and hyperscalers, because it provides a standardized interface, supported kernel portability and requires less in-depth kernel programming knowledge.
- eBPF helps overcome scale and visibility limitations of iptables, which is the default networking stack in Linux. eBPF helps optimize and customize Linux network packet handling by processing them earlier in the cycle.
- Vendors are increasingly using eBPF in their career network infrastructure (CNI) software to improve performance, security and network visibility.

### Obstacles

- While it is realistic for technology vendors and hyperscalers, most enterprises lack the expertise and skills necessary to build and integrate eBPF-based functions.
- Most enterprises do not have the awareness, need or risk tolerance to tackle Linux kernel challenges directly.
- Many older Linux kernels don’t support eBPF, or only partially support the latest features.
- Security and system reliability concerns will severely limit what organizations are willing to deploy using eBPF, as poorly written eBPF programs can directly impact the operation of the Linux kernel.
- Integration challenges and backward compatibility with existing non-eBPF-enabled products.

### User Recommendations

- Migrate to more modern platforms for organizations that are still using Linux distributions with limited or no eBPF support.
- Seek eBBF-based Kubernetes CNI solutions when scale, performance, visibility and security are top of mind.
- Use Linux variants that provide eBPF support to enable network performance, visibility and security products.
- Explore whether eBPF can meaningfully address the organization's performance or visibility challenges by supporting technologically advanced enterprises.
- Invest in eBPF to improve performance and visibility, to avoid falling behind competitors, for networking and network security vendors.

**Sample Vendors**

Aqua; Cloudflare; Isovalent; New Relic; Splunk; Sysdig; Tigera

**Gartner Recommended Reading**

Cool Vendors in Cloud Networking

Using Emerging Service Connectivity Technology to Optimize Microservice Application Networking

**Identity-First Security**

**Analysis By:** Paul Rabinovich

**Benefit Rating:** High

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Definition:**

Identity-first security is an approach to security design that makes identity-based controls the foundational element of an organization's protection architecture. It marks a fundamental shift from perimeter-based controls that have become obsolete because of the decentralization of assets, users and devices. Effective identity-first security relies on context-based access policies that are continuous and consistent.

### Why This Is Important

All organizations are operating in a challenging and escalating threat environment. Users and resources are no longer confined to the corporate network, and the corporate network itself cannot be trusted. Identity-first security strategies make identity a cornerstone of security. It shifts the control plane for security from the network (and the physical perimeter) to identity-based controls.

### Business Impact

Identity-first security was introduced because the traditional network security model could no longer protect modern organizations. By embracing an identity-first security mindset, organizations can drastically improve their security posture and mitigate security incidents. However, this approach requires a culture shift followed by investments in new tools, processes, policies and architectures.

### Drivers

- With the advent of cloud services, digital supply chains and remote access, the perimeter has become porous. A typical organization's attack surface dramatically expanded to include assets and users outside of the corporate network.
- Hybrid and remote work are here to stay. Gartner predicts that by 2026, 75% of workers will continue to split time between home and office locations. Both company-owned and employee-owned devices may hold company data and must be protected.
- External access to organizations' applications and data is now common. Enterprises need to collaborate with partners, vendors and suppliers, support API-based access to their information and interact with their customers through digital channels.
- Digital supply chain risks continue to rise. Some organizations share infrastructure with third parties such as managed service providers.
- Identity-first security is a key enabler of zero trust architectures (ZTAs), which depend on identity (and context) for assessing risk.
- An identity-first approach strengthens security by relying on the following core principles (the "3 Cs"): designing *consistent* identity and access management (IAM) policies for all digital assets regardless of their location, using *contextual* data when evaluating access risk, and applying adaptive controls *continuously*, both at login time and throughout user sessions.

### Obstacles

- Identity-first security requires a fundamental rethinking of an organization's approach to its protection architecture. One cannot buy an enterprisewide identity-first security product and be done with it. Legacy systems are the biggest barrier to implementing identity-first security. Most software-delivered applications were written on the assumption that they would run in a closed — and benign — environment. Older IAM tools do not natively support anywhere computing, standards-based single sign-on, unmanaged devices and access by external users.
- IAM maturity at many organizations is insufficient to meet the demands of identity-first security such as handling of new types of identity (e.g., machines), new entitlements and advanced controls (e.g., adaptive access).
- Institutional inertia: One of the key principles of the zero trust model is "assume compromise — even on internal networks," but not all organizations recognize this threat or sufficiently invest in its mitigation.

### User Recommendations

- Inventory all applications and services and identify where and how they rely on implicit trust. Assess risk and, for those applications and services where existing risk exceeds the organization's risk tolerance, evaluate alternative identity-first security-based architectures and tools that can support them.
- Adopt the three principles (the "3 Cs") of identity-first security. Incorporate contextual data such as risk and recognition signals into your IAM infrastructure, and establish capabilities to share and propagate them across security controls.
- Evaluate the use of device and workload identities to enable more granular access policies and support application-to-application access use cases.
- Ensure that the IAM team effectively communicates with business stakeholders, security teams, infrastructure and operations (I&O), cloud and DevOps as the newly introduced IAM controls will impact both end users and IT personnel.

### Gartner Recommended Reading

Identity-First Security Maximizes Cybersecurity Effectiveness

Improve IAM Architecture by Embracing 10 Identity Fabric Principles

Predicts 2023: Zero Trust Moves Past Marketing Hype Into Reality

Quick Answer: How to Explain Zero Trust to Technology Executives

The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)

### Security Service Edge

**Analysis By:** Charlie Winckless, John Watts

**Benefit Rating:** Transformational

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

#### Definition:

Security service edge (SSE) secures access to the web, cloud services and private applications. Capabilities include adaptive access control, data security, visibility and control. Further capabilities include an advanced threat defense and acceptable use control enforced by network-based and API-based integrations. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.

#### Why This Is Important

SSE improves organizational flexibility to secure the usage of web and cloud services, and remote work. SSE offerings are the convergence of security functions (at least, secure web gateways [SWGs], cloud access security brokers [CASBs] and zero trust network access [ZTNA]) to reduce complexity and improve user experience. They are delivered from the cloud. When organizations are pursuing a secure access service edge (SASE) architecture, SSE is paired with software-defined WAN (SD-WAN) to simplify networking and security operations.

#### Business Impact

Hybrid work is continuing to drive the adoption of public cloud services, especially of SaaS applications. Both hybrid work and the adoption of public cloud services remain business enablers for most Gartner clients. SSE allows the organization to support anytime-anywhere workers by using a cloud-centric approach to enforce a security policy when accessing the web, cloud services and private applications. Simultaneously, SSE reduces the administrative complexity of running multiple products.

**Drivers**

- Organizations need to secure user, application and enterprise data that is distributed, decentralized and requires secure remote access.
- For many enterprises, a significant amount of critical data is now hosted in SaaS. Therefore, there is a need to perform data loss prevention (DLP) on data that is located in, going to, and leaving these SaaS platforms.
- SSE enables flexible and primarily cloud-based security for users and devices without being tied to on-premises network infrastructure and connectivity. The same security outcome is delivered to users regardless of their location or connectivity.
- Administrators can have enhanced visibility on user traffic and a single configuration and monitoring location for this traffic.
- SSE allows organizations to implement a posture based on identity and context at the edge.
- By consolidating vendors, organizations reduce complexity, costs and the number of vendors used to enforce security policy. Using a single SSE platform rather than multiple point offerings, they can both reduce complexity and reduce gaps in security coverage.
- Sensitive data inspection and malware inspection can be done in parallel across all channels of access. SSE allows doing both inspections in parallel, leading to a better performance and more consistent configuration than doing them separately.
- An adaptive access can take into account more input signals and be more consistently enforced, regardless of the application location or type.
- Organizations look for deeper security capabilities when building a SASE architecture compared to vendors that may have a minimal set of security features as part of their SD-WAN offering.
- Tight integrations that exist between discrete SD-WAN and SSE vendors allow interoperability without requiring a single-vendor approach.

**Obstacles**

- As the market is being formed by the convergence of capabilities, vendors may be strong in certain capabilities and weak in others. Vendors may also lack overall tight integration between SSE capabilities or with SD-WAN vendors.
- Not all vendors provide sufficiently sensitive data identification and protection to manage business risks.
- Some vendors have focused less on SaaS security and integrations. However, businesses increasingly need this visibility and protection.
- Being cloud-centric, SSE typically doesn't address every need supported by on-premises controls such as internal firewalling.
- Organizations are concerned about uptime or availability of services that they depend on for their business. This is compounded by weak SLAs from some vendors.
- Not all vendors provide all features locally in all geographies, resulting in performance or availability issues.
- Switching costs from incumbent vendors or timing of contract expirations prohibit near-term consolidation.
- Migrating from a VPN will increase costs.

### User Recommendations

- Exploit the converged market, consolidate vendors, and cut complexity and costs as contracts renew for SWGs, CASBs and VPNs by replacing them with a ZTNA approach.
- Approach SSE consolidation identifying which elements you may already have in place (for example, existing cloud-based CASB or SWG). Develop a shortlist of vendors based on your use cases regarding secure end-user requirements, the cloud services you use, and the data you need to protect.
- Inventory your equipment and contracts to implement a multiyear phaseout of on-premises perimeter and branch security hardware in favor of the cloud-based delivery of SSE.
- Global enterprises should validate that remote offices have acceptable performance and features with selected vendors. Vendor point of presence (POP) locations and service support are key.
- Actively engage with initiatives for branch office transformation, SD-WAN and Multiprotocol Label Switching (MPLS) offload to integrate cloud-based SSE into the scope of project planning.

### Sample Vendors

Broadcom; Cisco; Cloudflare; Forcepoint; iboss; Lookout; Netskope; Palo Alto Networks; Skyhigh Security; Zscaler

### Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Adopt Security Service Edge (SSE) to Replace Stand-Alone SWG, CASB and ZTNA Products

## CIEM

**Analysis By:** Henrique Teixeira

**Benefit Rating:** Moderate

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Emerging

**Definition:**

Cloud infrastructure entitlement management (CIEM) capabilities help enterprises manage cloud access risks via administration-time preventive controls for the governance of entitlements in hybrid and multicloud infrastructure as a service (IaaS) and platform as a service (PaaS). They use analytics, machine learning (ML) and other methods to discover anomalies in account entitlements, such as accumulation of privileges, and dormant and unnecessary permissions.

**Why This Is Important**

Multicloud entitlement management is challenging, given the rapid increase in the number and complexity of entitlements, and the inconsistent cloud provider approaches to their definition and configuration. This challenge is getting worse given the proliferation of machine identities, which are orders of magnitude more numerous than human identities in cloud infrastructure. Managing cloud entitlements continues to be a responsibility of the client organization alone.

**Business Impact**

CIEM can help organizations to:

- Reduce the risk of misconfiguration by simplifying the effort to manage entitlements in multiple clouds.
- Reduce cloud attack surface and access risks posed by excessive permissions of machine identities.
- Improve agility in DevSecOps use cases by giving visibility to unnecessary developer privileges without disrupting developer flows.
- Extend privileged access management (PAM) use cases with easy-to-apply least privilege approaches.
- Simplify compliance with regulations like SOX and GDPR.

**Drivers**

- Cloud infrastructure and platform services (CIPS) providers keep adding more services, which in turn leads to a rapid increase in the number and complexity of entitlements to be managed.
- The proliferation of machine identities led to a volume of entitlements which is now orders of magnitude bigger than the number of human entitlements. It is estimated that the percentage of dormant machine identities has doubled in the last two years.
- CIEM has become a useful example of applied identity analytics for security posture management, and an enabler of the identity fabric immunity (see Top Trends in Cybersecurity 2023).
- CIEM capabilities that were originally only available from pure-play vendors, are now also being made available as optional modules embedded in cloud security posture management (CSPM) and converged cloud-native application protection platforms (CNAPP). In the identity and access management (IAM) space, a number of PAM vendors and a few identity governance and administration (IGA) vendors have developed or integrated CIEM functionality in their products. Cloud providers — except for Microsoft — have not invested in multicloud permission management capabilities.
- More mature CIEM providers have started to expand their scope beyond IaaS and PaaS, into SaaS, Kubernetes, access management (AM) tools and other identity providers (IdPs).
- Some CIEM providers have added more traditional IAM capabilities and configuration management, such as lightweight user and entitlement life cycle management, via integrations with Jira and ServiceNow for access requests and remediation.
- Some CIEM providers have broadened their scope into identity threat detection and response (ITDR), and security posture dashboards.

### Obstacles

- Per its original definition, CIEM is meant to address risks of multicloud permissions in CIPS only. More mature CIEM providers are expanding into SaaS, and AM targets, and adding PAM, CSPM or ITDR features. However, vendors and customers are still experiencing early challenges in understanding what CIEM can provide today, and what this technology may become in the future.
- CIEM has two possible buying centers in the organization — IAM or cloud security — which need to align. The uncertainty about which of these two areas should be accountable for the CIEM initiative can delay adoption.

### User Recommendations

- Adopt a pragmatic approach to evaluate CIEM functionality that starts with basic actionable intelligence to remove dormant entitlements.
- Use CIEM to manage entitlements of machine identities as well as for people.
- Maximize CIEMs value by capitalizing on its analytics capabilities to optimize posture management after removing unnecessary entitlements. Leading CIEM capabilities enforce least-privilege policies and remediate violations.
- Check if existing or prospective PAM, IGA and cloud security vendors offer CIEM capabilities to avoid redundant investments. Inversely, if choosing a CIEM stand-alone product, check how it may save you money by bundling CSPM, CNAPP and ITDR features.
- Use CIEM as part of a broader IAM and cloud security strategy to supplement IGA, PAM and CSPM technologies. CIEM will add identity visibility.

### Sample Vendors

Authomize; Britive; Ermetic; Microsoft; SailPoint; Sonrai Security

### Gartner Recommended Reading

Innovation Insight: Cloud Infrastructure Entitlement Management

Top Trends in Cybersecurity 2023

Emerging Tech: CIEM Is Required for Cloud Security and IAM Providers to Compete

Quick Answer: Cloud, Kubernetes, SaaS — What's the Best Security Posture Management for Your Cloud?

Magic Quadrant for Privileged Access Management

### Zero Trust Strategy

**Analysis By:** John Watts, Thomas Lintemuth

**Benefit Rating:** High

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Definition:**

Zero trust strategy constitutes a set of core principles and program-level activities that establish contextual-based adaptive access controls. It replaces implicit trust with explicit adaptive trust aligned with a calculated risk of access to the sensitivity of the asset. Chief information security officers (CISOs) typically define and own a zero trust strategy, and execute zero trust initiatives to achieve a risk-optimized security posture for their organizations.

**Why This Is Important**

A zero trust strategy reduces the risk of attackers abusing implicit trust in environments that achieve lateral movement, employ available exploits and gain privilege escalation to gain their objectives. It matches the level of security controls to the sensitivity of the resource to improve end-user experience. Also, it limits an attacker's ability to bypass static controls by establishing continuous trust assessments.

**Business Impact**

A zero trust strategy establishes strategic objectives based on cybersecurity principles to improve organizations' end-user experience and reduce the risk of certain cybersecurity threats. This is done by replacing legacy perimeter security approaches with fine-grained access controls. A zero trust strategy limits the impact of incidents when they occur and enables the digital transformation of businesses by installing flexible security controls closer to the assets that need protection.

### Drivers

- The excessive hype in the information security community about the zero trust strategy is leading to higher sector visibility across organizations, even for nonsecurity leaders.
- The strategic response to security incidents where attackers abuse the excessive trust extended to user accounts, devices and workloads result in ransomware and data-exfiltration incidents.
- The desire to improve end-user experience with more adaptive controls. Also, the need to reduce the burden for access to less critical resources while requiring more context for more sensitive resources.
- The strategy to reduce the attack surface and limit scan and exploit attacks is cloaking existing networks and applications from discovery.
- The desire to deemphasize user and device location as a single, weak proxy for trust.

### Obstacles

- The hype from vendors around zero trust often overpromises and underdelivers on their ability to achieve the vision of an organization's zero trust strategy.
- Organizational resistance to zero trust is interpreted as having no trust in employees.
- The isolated strategic development within the CISO group lacks context and conflicts with other organizational goals.
- The required involvement and availability from business-domain stakeholders and technical staff limit the use of outsourced strategy development to overcome skill and resource constraints.
- External constraints, such as technical debt and integration of multiple technologies from different security vendors, limit the strategic scope and require more resources for implementation than organizations can anticipate.
- Misaligned outcome expectations of a zero trust strategy lead organizations to replace existing security controls rather than augment them.

### User Recommendations

- Establish an identity-first strategy as part of an identity and access management (IAM) program. Mature identity practices are a prerequisite to a zero trust strategy.
- Make the zero trust strategy part of a wider vision for cybersecurity. Integrate it with other cybersecurity strategies such as data, endpoint, and application security.
- Collaborate with stakeholders from security and nonsecurity functions to avoid confusion from varied interpretations of the term zero trust.
- Align the zero trust strategy to business initiatives, like digital transformation.
- Prioritize and rationalize investments defined by a zero trust strategy using zero-trust architecture development to define the scope and desired future end state.
- Build a set of outcome-driven metrics to measure the current risk and track the progress of risk reduction over time.

### Gartner Recommended Reading

2023 Strategic Roadmap for Zero Trust Security Program Implementation

Treat Cybersecurity as a Business Decision to Minimize Cyber Risk

## Kubernetes Security

**Analysis By:** Charlie Winckless, Thomas Lintemuth

**Benefit Rating:** Moderate

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

**Definition:**

Kubernetes security refers to the implementation of security processes, testing and controls for the Kubernetes container orchestration platform. It operates in close conjunction with individual container security, but focuses on Kubernetes configuration and admission control.

### Why This Is Important

Kubernetes expands the potential attack surface for an organization, as it provides the capabilities to deploy, scale, monitor and manage container infrastructures. This increase in attack surface and the broad adoption of Kubernetes by developers — and in managed cloud environments — means security teams need tools to provide visibility and control in these environments. Unsecure Kubernetes can expose containers and its ecosystem to various attacks.

### Business Impact

Kubernetes is the most common container orchestration platform, and is in many ways a de facto standard. Kubernetes involves significant complexities in terms of access control and RBAC, container name spaces, Kubernetes networking, segmentation, admission control and other configuration, requiring automated tools that work closely with container security systems to protect the environment. Kubernetes security tools help address these potential exposures.

### Drivers

- Developer adoption of containers and Kubernentes has been driven by their fit to DevOps style microservices. This adoption has expanded the attack surface, forcing security teams to use different tools and approaches to address orchestration exposures.
- Container as a service (CaaS) offerings built on Kubernetes, such as Amazon Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS) and Google Kubernetes Engine (GKE), are on the rise. These require security integrations to provide coverage.
- Security and risk management leaders must address the security of their container orchestration — primarily Kubernetes — to mitigate misconfigurations and overly permissive access.
- Container environments spread the attack surface across many containers, each of which is a unique network endpoint. East-west traffic is vastly increased, and the value of segmentation is correspondingly higher. Kubernetes security solutions can address these segmentation requirements.
- Shift-left and general container security is bolstered by effective use of admission control to limit the deployment of malicious or vulnerable container images.
- Cloud-native application protection platforms are incorporating kubernetes security capabilities.

**Obstacles**

- Kubernetes security blurs the line between application security, infrastructure security and container security, creating overlap in vendors, offerings and responsibilities within the organization.
- Kubernetes security alone cannot address the overall security of a containerised application. Multiple other attack points exist.
- Kubernetes is often just one part of an architecture that also includes PaaS, and even serverless functions. Teams struggle to understand the whole system in these cases — not just the Kubernetes risks.
- While Kubernetes is widely adopted for container orchestration, other orchestration platforms do exist and may not be supported by the same products as Kubernetes.
- Unless the Kubernetes security solution is designed to provide minimal friction for developers, their adoption will be at best, resisted and, at worst, actively circumvented.

### User Recommendations

- Use and enforce admission controls to prevent vulnerable or malicious containers from being deployed into your environment. Use these as a guard rail for your developers.
- Ensure that your tools support validating the Kubernetes orchestration environment for proper patch levels and correct and compliant configuration, both in development and in production.
- Ensure that the Kubernetes tools you adopt have the ability to do more than forward logs, and to support both native Kubernetes and Kubernetes-based CaaS options.
- Enforce least privilege and minimal access — avoid wildcard permissions and use name spaces to reduce permission access. Use RBAC for all users and service accounts.
- Use an industry standard baseline like the CIS benchmarks and automate scanning of your environment to ensure continuous compliance.
- Address Kubernetes networking risks by adopting tools that support network policy controls.
- Collaborate with engineering teams to implement security controls that require application context.

### Sample Vendors

Aqua Security; ARMO; Lacework; Orca; Palo Alto Networks; Red Hat; Sysdig; Trend Micro; Wiz

### Gartner Recommended Reading

Market Guide for Cloud Workload Protection Platforms

How to Make Cloud More Secure Than Your Own Data Center

Guidance Framework for Securing Kubernetes

Container Supply Chain: 10 Security Vulnerabilities and How to Address Them

## Sliding into the Trough

### Cloud-Native Application Protection Platforms

**Analysis By:** Neil MacDonald, Charlie Winckless

**Benefit Rating:** High

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

**Definition:**

Cloud-native application protection platforms (CNAPPs) are an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production. CNAPPs consolidate a large number of previously siloed capabilities, including container scanning, cloud security posture management, infrastructure as code scanning, cloud infrastructure entitlements management and runtime workload protection.

**Why This Is Important**

Comprehensively securing cloud-native applications requires the use of multiple tools from multiple vendors that are rarely well-integrated. This lack of integration and automation slows developers down and creates fragmented visibility of risk and friction. CNAPP offerings allow an organization to use a single integrated offering to protect the entire life cycle of a cloud-native application.

**Business Impact**

Cloud-native application protection platforms consolidate disparate fragmented security testing and protection tools that increase cost and complexity for IT. Using a CNAPP offering will improve developer and security professional efficacy. It will also reduce complexity and costs while maintaining development agility and improving the developer's experience.

**Drivers**

CNAPPs:

- Reduce the chance of misconfiguration, mistake or mismanagement as cloud-native applications are rapidly developed, released into production and iterated.

- Converge and reduce the number of tools and vendors involved in the continuous integration/continuous delivery (CI/CD) pipeline.
- Reduce the complexity and costs associated with creating secure and compliant cloud-native applications.
- Facilitate the reporting and auditing of cloud security posture/status.
- Improve developer acceptance with security-scanning capabilities that seamlessly integrate into their development pipelines and tooling.
- Place an emphasis on scanning proactively in development and rely less on runtime protection, which is well-suited for container as a service and serverless function environments.

### Obstacles

- Cloud workload protection platform (CWPP) vendors that are good at runtime protection aren't necessarily good at integrating into development and vice versa.
- Cloud-native workloads in the form of containers and serverless functions don't require heavyweight runtime protection capabilities.
- There is no single CNAPP offering that does everything. Convergence of capabilities will occur, but will take place over several years.
- Organizations may have siloed purchases of application security testing tooling that is chosen by a different team that manages the runtime protection of workloads. Even at runtime, a separate team may be responsible for web application protection.
- Organizational immaturity in terms of cloud-native application development may inhibit adoption and fragment buying motions.
- Buying centers and influencers are shifting to newer roles such as DevOps architects and cloud security engineering, requiring information security teams to coordinate with these users.

### User Recommendations

- Sign contracts of only one to two years because the market for CNAPP is changing rapidly.

- Solicit CWPP vendors to scan containers in development and add cloud security posture management (CSPM) capabilities, including infrastructure-as-code scanning.
- Select integrated offerings with flexible licensing models that allow you to only pay for the capabilities your organization is prepared to use.
- Evaluate the CSPM vendor's ability to add scan of Kubernetes security posture management (KSPM) as well as provide runtime Kubernetes protection capabilities.
- Consolidate open-source software (OSS) vulnerability scanning and software composition analysis through integrations or replacement within a CNAPP offering.
- Scan containers proactively in development for all types of vulnerabilities, not just vulnerable components, including hard-coded secrets, malware and Kubernetes misconfiguration.

### Sample Vendors

Aqua Security; Cisco; Lacework; Microsoft; Orca Security; Palo Alto Networks; Rapid7; Sysdig; Trend Micro; Wiz

### Gartner Recommended Reading

Market Guide for Cloud-Native Application Protection Platforms

How to Select DevSecOps Tools for Secure Software Delivery

How to Make Cloud More Secure Than Your Own Data Center

## Serverless Function Security

**Analysis By:** Charlie Winckless

**Benefit Rating:** Moderate

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

**Definition:**

Serverless function (also referred to as “function PaaS”) security technologies are designed to address the unique security and compliance requirements of serverless function protection. Comprehensive solutions start with proactive vulnerability and configuration scanning in development, entitlement and access checking — typically combined with lightweight runtime protection and behavioral analysis.

**Why This Is Important**

Serverless functions are available in all hyperscale platforms, and may be included in cloud-native applications as a simple and scalable way to enable an event-driven microservices architecture. These services appeal to developers, but present risks from both vulnerable code and environment misconfiguration while being hard to protect with traditional controls due to their serverless nature.

**Business Impact**

By ensuring the security and compliance of the serverless functions they create, information security organizations can securely enable the developer-driven adoption of these technologies without slowing down the same developers. In the longer term, serverless functions have the potential to improve overall enterprise security profiles by migrating responsibility for significant elements of the attack surface to the hyperscaler, rather than the enterprise.

**Drivers**

- Driven by developers, adoption of serverless functions is increasing across hyperscalers.
- Serverless functions have a differentiated attack surface driving the need for security capabilities, such as software composition analysis, vulnerability scanning, API security, correct and compliant serverless PaaS configuration.
- When new types of attacks emerge against function PaaS, serverless function security is uniquely positioned to help organizations detect and respond to those attacks, as it provides visibility and security controls into the PaaS environment.
- Cloud permissions are extremely complex, and serverless function security allows for automatic detection and remediation of overly permissioned functions that increase risk.

### Obstacles

- In most cases, information security is blind to the use of serverless functions and unaware of the risks they pose. Additionally, few attacks have been clearly documented on serverless code, meaning that any perceived risk is low for the effort and money invested.
- Serverless function security must have minimal friction for developers to avoid its adoption being disrupted by the developer community.
- At runtime, since serverless functions live for a matter of seconds or minutes, the need for additional runtime security other than monitoring is minimal. Very few options are available, short of injecting or wrapping serverless functions with runtime protection code.
- Serverless security tools are still maturing, and standards for secure deployment across multiple platforms are yet to be defined.

### User Recommendations

- Engage with cloud-native development teams on the scope of serverless function usage and planned usages. Run a discovery project to see if serverless code is in use that you aren't aware of.
- Scan for vulnerabilities, vulnerable open-source code and misconfiguration automatically during development, as you would for any static application code.
- Require your cloud security posture management (CSPM) tool to provide risk visibility and configuration/permissions management of the entire IaaS configuration, including serverless.
- Adopt a least-privilege security posture, including serverless function permissions and network connectivity. Automate discovery of over-privileged use of serverless functions and reduce this to the least possible.
- Require an API gateway or event broker for invocation, providing a visibility and control point.
- Require your cloud workload protection platform (CWPP) or CSPM vendor to offer serverless function security and compliance capabilities — either now or as a roadmap item.

### Sample Vendors

Amazon Web Services; Aqua Security; Check Point Software Technologies; Contrast Security; Palo Alto Networks; Rapid7; Snyk; Sysdig; Trend Micro

### Gartner Recommended Reading

Market Guide for Cloud-Native Application Protection Platforms

5 Things You Must Absolutely Get Right for Secure IaaS and PaaS

How to Make Cloud More Secure Than Your Own Data Center

## Cloud Firewalls

**Analysis By:** Adam Hils, Rajpreet Kaur, Feng Gao

**Benefit Rating:** Moderate

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

### Definition:

A cloud network firewall offers bidirectional, stateful traffic inspection (both egress and ingress) for securing different types of public clouds. They can be deployed as cloud-native from the cloud infrastructure vendor, as a separate virtual instance or in containers. Container firewalls can also secure interconnections between containers within or between clouds.

### Why This Is Important

Cloud firewalls apply to both public and private clouds. They are critical for securing ingress and egress traffic, and can potentially offer additional attached security capabilities such as intrusion prevention system (IPS) and URL filtering. Security and risk management (SRM) leaders are tasked with securing these varied environments, and cloud firewalls are foundational to cloud security strategy.

### Business Impact

- Security provided by infrastructure as a service (IaaS) firewalls enables organizations to support both digital transformation and compliance requirements.
- Workloads are increasingly moving from on-premises to the cloud, and there should be a similar amount of security and access control in the cloud.
- Cloud firewalls are key to strategic hybrid data center initiatives.

### Drivers

- The cloud firewall market will grow in parallel with the IaaS market.
- SRM leaders who desire to have more advanced security firewall features (IPS and web filtering, for example) often choose to use a more advanced cloud-native option or a third-party best-of-breed solution for better security outcomes.
- Some IaaS vendors have teamed with third-party firewall vendors in joint development projects to instrument advanced security capabilities into the native infrastructure, improving security without adding the operational friction that a third-party firewall often does.
- SRM leaders often use third-party firewall virtual appliance solutions to unify firewall policy management across hybrid networks. In this case, the network security team has a “single source of truth” in one firewall management console and one policy, reducing management complexity.
- As container firewalls become more capable, security-conscious DevOps teams are selecting firewalls built specifically to secure the interconnection between containers within or between clouds.

### Obstacles

- Several IaaS providers offer ingress/egress gateway firewalls for each virtual private cloud by default. Organizations deploying IaaS have native, basic firewall capabilities upon cloud deployment, presenting an obstacle to third-party cloud firewalls.
- The basic built-in cloud-native firewalls sometimes lack security features such as IPS and URL filtering. SRM leaders therefore hesitate to deploy critical workloads behind basic security tools.
- For SRM leaders choosing to use cloud-native firewalls, multiple clouds mean multiple management consoles, increasing management complexity and staffing pressure. Third-party firewalls can create significant operational drag, rendering them suboptimal for cloud architects and application developers.
- Some organizations in heavily regulated industries and regions are hesitant to move to the cloud. Implementing container firewalls requires changing the cloud container architecture.

### User Recommendations

- Align your cloud firewall strategy with the organization's overall digital transformation strategy. As critical infrastructure moves to the cloud, plan for firewalls appropriate to risk level and potential operational complexity.
- When a third-party firewall makes sense, use the same brand of firewall as one used in on-premises environments for consistency in policy management.
- Use a cloud firewall provider that partners closely with the cloud service provider (CSP), or a third party that offers detailed architecture guidance to achieve optimal integrations with the CSP.
- For a purely ingress/egress use case, firewall as a service (FWaaS) may be a suitable alternative approach.

### Sample Vendors

Amazon Web Services; Aviatrix; Check Point Software Technologies; Cisco; Fortinet; Google; Microsoft; Palo Alto Networks; Sophos

## SASE

**Analysis By:** Neil MacDonald, Andrew Lerner

**Benefit Rating:** Transformational

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Definition:**

Secure access service edge (SASE) delivers converged network and security capabilities, including SD-WAN, SWG, CASB, firewall and zero trust network access (ZTNA). SASE supports branch office, remote worker and on-premises secure access use cases. SASE is primarily delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies.

**Why This Is Important**

SASE is a key enabler of modern digital business transformation, including work from anywhere and the adoption of edge computing and cloud-delivered applications. It increases visibility, agility, performance, resilience and security. SASE also dramatically simplifies the delivery and operation of critical network and security services mainly via a cloud-delivered model. SASE reduces the number of vendors required for secure access to one or two explicitly partnered vendors.

**Business Impact**

SASE enables:

- Digital business use cases (such as branch office transformation and hybrid workforce enablement) with increased ease of use while reducing costs and complexity via vendor consolidation and dedicated circuit offload.
- Infrastructure and operations and security teams to deliver a rich set of networking and network security services in a consistent and integrated manner to support the needs of digital business transformation, edge computing and work from anywhere.

Drivers

- Digital business transformation including the adoption of cloud-based services by mobile workforces, edge computing and business continuity plans that must include a flexible, anywhere, anytime, secure, identity-based logical perimeter model of SASE.
- The need to flexibly support digital business transformation efforts with a zero trust security architecture while managing complexity is a significant factor for the adoption of SASE, primarily delivered as a cloud-based service.
- For IT, SASE can reduce the deployment time for new users, locations, applications and devices.
- For information security, SASE enables a single way to set policy enforcement consistently across all types of access — internet, web applications and private applications, reducing the attack surface and shortening remediation times.
- Enterprise desire to simplify network and network security deployments via the reduction of policy engines and management consoles.

Obstacles

- **Organizational silos, existing investments and skills gaps:** A full SASE implementation requires a coordinated and cohesive approach across security and networking teams, which is challenging given refresh/renewal cycles, silos and existing staff expertise.
- **Organizational bias and regulatory requirements for on-premises deployment:** Some customers have an aversion to the cloud and want to maintain control.
- **Global coverage:** SASE depends upon cloud delivery, and a vendor's cloud footprint may prevent deployments in certain geographies, such as China, Africa, South America and the Middle East.
- **SASE maturity:** SASE capabilities vary widely. Sensitive data visibility and control is often a high-priority capability, but it is difficult for many SASE vendors to address. While your preferred single vendor may lack the capabilities you require, two-vendor partnerships can be a viable approach.

### User Recommendations

- Involve the security architect and network architect when evaluating offerings and roadmaps from the incumbent and emerging vendors to ensure an integrated approach.
- Leverage WAN, firewall, VPN hardware refresh cycles or software-defined WAN (SD-WAN) deployments to update network and network security architectures.
- Explore single-vendor SASE, dual-vendor SASE and managed SASE options when investing, but avoid deploying SASE with more than two vendors, regardless of vendor marketing for all core services to minimize complexity and improve performance.
- Use vendor combinations — when selecting a dual-vendor solution — that have explicit integration including turnkey automation and visibility, and ideally management and data plane integration.
- Combine branch office and remote access in a single implementation to ensure consistent policies and minimize the number of vendors required.
- Leverage branch office transformation and dedicated circuit offload projects to adopt SASE.

### Sample Vendors

Cato Networks; Cisco Systems; Cloudflare; Forcepoint; Fortinet; Juniper Networks; Netskope; Palo Alto Networks; Versa Networks; Zscaler

### Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Market Guide for Single-Vendor SASE

The Future of Network Security Is in the Cloud

Magic Quadrant for SD-WAN

Magic Quadrant for Security Service Edge

## Firewall as a Service

**Analysis By:** Adam Hils, Rajpreet Kaur

**Benefit Rating:** Moderate

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

**Definition:**

Firewall as a service (FWaaS) is a multifunction security gateway delivered as a cloud-based service, often to protect small branch offices and mobile users. FWaaS can provide a simpler, more flexible architecture using centralized policy management, multiple enterprise firewall features and traffic tunneling to move network security inspections partially or fully to a cloud service.

**Why This Is Important**

Hybrid working is here to stay, and growing adoption of software-defined WAN (SD-WAN) and hybrid WAN architectures is increasing interest in using FWaaS to help secure small branches and securely enable hybrid work. We expect this trend to continue. FWaaS offerings are of varying levels of maturity.

**Business Impact**

- FWaaS offers significantly different architecture for small branches or single-site organizations. It offers visibility with centralized policy, flexibility and the reduced capital costs associated with a fully or partially hosted security workload.
- FWaaS enables inspection of web and nonweb protocols, providing more outbound protocol coverage.
- FWaaS changes budgetary considerations as organizations move from capital to operational spending.
- Organizations with hybrid workforces will find FWaaS helps them work securely in a widely distributed network.

### Drivers

- Organizations rearchitecting their networks by implementing SD-WAN technology sometimes want FWaaS to secure outbound network traffic. FWaaS can also support inbound traffic use cases.
- FWaaS is a component of most SD-WANs and security service edge (SSE) offerings, which makes it part of the secure access service edge (SASE) framework sometimes offered as part of a larger SASE architecture.
- Hybrid mesh firewall architecture may include FWaaS.
- FWaaS can decrypt outbound traffic for inspection on a large scale. Alternative hardware or virtual branch firewalls often lack the performance to do this.
- The continuing move toward hybrid working necessitates bringing security services closer to workers in order to minimize latency.

### Obstacles

- Network firewall hardware appliances comprise the largest security equipment market. The appliance approach has been predominant, and many organizations use appliances effectively and efficiently. Many organizations lack compelling reasons to change to a new form factor.
- Security teams find some FWaaS solutions difficult to implement and manage. New FWaaS deployments often require professional services engagements.
- Over 80% of outbound traffic in organizations uses HTTP and HTTPS. Cloud-based SSE services can protect and inspect this traffic at scale to offload existing hardware firewalls. This makes it much easier and less costly to extend investments in existing firewall hardware than to rearchitect the edge to forward all traffic to a FWaaS.
- FWaaS licensing is based on per-user per-year subscription pricing. This can be more expensive for large organizations with high user counts than hardware-based solutions that may have lower subscription costs, and that can be deployed and used beyond their capital depreciation life span.

### User Recommendations

- Verify that the additional hop to FWaaS infrastructure does not create unacceptable latency for some of your sites, and look at models that limit initial investment until acceptable latency is proven. Simpler architecture and increased flexibility must materialize in faster deployment and easier maintenance.
- Determine whether your organization is ready to move its entire security workload to the cloud, or whether you need thicker local devices to address privacy concerns and perform some on-premises segmentation or virtual LAN trunking.
- Assess how FWaaS might impact your branch architecture. Current FWaaS offerings offer mostly outbound security or protect mobile workers or companies that are primarily cloud-hosted. Consider maintaining on-premises firewalls for data center use cases.
- Evaluate the strength of the cloud service in three key respects: data center locations, points of presence and SLAs.
- Determine whether the complexity of an FWaaS project will necessitate a professional services engagement for initial setup and configuration.

### Sample Vendors

Barracuda; Cato Networks; Check Point Software Technologies; Cisco; Fortinet; Juniper Networks; Palo Alto Networks; Versa Networks

### Gartner Recommended Reading

Magic Quadrant for Network Firewalls

Critical Capabilities for Network Firewalls

Select the Right Strategy for Securing Web Access

## Cloud WAAP

**Analysis By:** Aaron McQuaid, Rajpreet Kaur, Dale Koeppen

**Benefit Rating:** High

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Mature mainstream

**Definition:**

Cloud web application and API protection (WAAP) is a technology that mitigates runtime attacks exemplified by the Open Web Application Security Project (OWASP) Top 10 web application security vulnerabilities. Capabilities include web application firewall (WAF), distributed denial of service (DDoS) protection, bot management and API security. Innovation is driven by the need to defend against an expanding attack surface caused by growth in the number of web applications and APIs.

**Why This Is Important**

Organizations with web applications and APIs hosted on-premises or as infrastructure as a service (IaaS) often buy cloud WAAP solutions from security vendors to shield applications and APIs. They can be more flexible to deliver and manage than traditional virtual appliances, because they're easily deployed. Combined with continuous integration/delivery (CI/CD) pipelines, the proliferation of microservices architectures is causing API use to grow rapidly, increasing the need for WAAP.

**Business Impact**

Public web applications and APIs are high-risk targets. Modern applications are web-based and built with microservices architectures. APIs enable microservices to communicate with each other and with public-facing services, so it is important to protect them. Cloud WAAP solutions are easier to consume than their appliance counterparts. Cloud WAAP is highly scalable; it provides centralized management, centralized visibility and stronger integration with hyperscalers.

### Drivers

- There is a proliferation of web-based applications and APIs. Modern software development has moved from monolithic application design toward microservices architectures. A microservices-based design decomposes a single monolithic application into several loosely coupled, independent software instances (typically containerized). These instances communicate with each other via APIs and externally via APIs or web-based protocols.
- There is evidence of an increasing number of Layer 7 application layer denial of service (DoS) attacks that require robust application layer security.
- Adversary groups continue to use and improve automated credential stuffing attacks. Bots are increasingly being leveraged in these attacks.
- The adoption of cloud-native architectures is shifting buyers from traditional appliance models to cloud-delivered services. The burden of deploying and managing a discrete set of appliances at every physical location is mitigated by adopting a cloud-delivered service with a common cloud-based management interface.

### Obstacles

- **Privacy-related:** Compliance requirements can be issues for organizations. Some don't trust cloud decryption to log application traffic and host-related secrets. This is likely to become less pronounced as cloud adoption continues to gain acceptance.
- **Complexity:** Expanding features sets for WAAP are leading many organizations to adopt managed security services, which may increase costs.
- **Cost:** WAAP offerings that are part of an existing ADC might appear less expensive for organizations that don't want to redesign their solutions.
- **Application fit:** Organizations with on-premises applications might not see the value in cloud WAAP deployments or favor a unified management approach, where they use hosted virtual appliances to keep the same centralized console for on-premises and cloud-hosted applications.
- **Geographic presence:** Insufficient, regional point of presence (POP) density could lead to adoption of virtual or on-premises appliances.

### User Recommendations

- Align your WAAP strategy with your future application architecture by adopting a cloud-first policy via the “follow the app” principle, when deciding from among an on-premises WAF appliance, a cloud WAAP or a distributed WAAP.
- Carefully evaluate the pros and cons of cloud WAAP. This includes simplicity of consumption, data privacy, DDoS protection, bot mitigation and API security, as well as deployment challenges, such as certificate management for transport layer security (TLS) inspection.
- Continue to improve your stance against bots and automated attacks by measuring the efficacy of existing controls and adding new techniques when needed.
- Implement products with automated API discovery and anomaly detection. Many WAAP solutions do not yet offer best-of-breed API security capabilities; compare them with offerings from dedicated API security vendors.
- Evaluate integrations with API gateways that help with API management when looking for consolidation of API management and API security.

### Sample Vendors

Akamai; Barracuda; Cloudflare; F5; Fastly; Fortinet; Imperva; Radware; ThreatX

### Gartner Recommended Reading

Magic Quadrant for Web Application Firewalls

Critical Capabilities for Cloud Web Application and API Protection

## Climbing the Slope

### Immutable Infrastructure

**Analysis By:** Neil MacDonald, Tony Harvey

**Benefit Rating:** Moderate

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Early mainstream

#### Definition:

Immutable infrastructure is a process pattern (not a technology) in which the system and application infrastructure, once deployed, are never updated in place. Instead, when changes are required, the infrastructure and applications are simply updated and redeployed through the CI/CD pipeline.

#### Why This Is Important

Immutable infrastructure ensures the system and application environment, once deployed, remains in a predictable, known-good-configuration state. It simplifies change management, supports faster and safer upgrades, reduces operational errors, improves security, and simplifies troubleshooting. It also enables rapid replication of environments for disaster recovery, geographic redundancy or testing. This approach is easier to adopt with cloud-native applications.

#### Business Impact

Taking an immutable approach to workload and application management simplifies automated problem resolution by reducing the options for corrective action to, essentially, just one — repair the application or image in the development pipeline and rerelease. The result is an improved security posture and a reduced attack surface with fewer vulnerabilities and a faster time to remediate when new issues are identified.

#### Drivers

- Linux containers and Kubernetes are being widely adopted. Containers improve the practicality of implementing immutable infrastructure due to their lightweight nature, which supports rapid deployment and replacement.

- The GitOps deployment pattern, which emphasizes continuously synchronizing the running state to the software repository, has become an effective way to implement immutable infrastructure in Kubernetes-based, containerized environments.
- Infrastructure as code (IaC) tools (including first-party cloud provider IaC tools) have increasingly integrated configuration drift detection and correction, improving the practicality of implementing immutable infrastructure across an application's entire stack and environment.
- Interest in zero-trust and other advanced security postures where immutable infrastructure can be used to proactively regenerate workloads in production from a known good state (assuming compromise), a concept referred to as "systematic workload reprovisioning."
- For cloud-native application development projects, immutable infrastructure simplifies change management, supports faster and safer upgrades, reduces operational errors, improves security, and simplifies troubleshooting.

### Obstacles

- The use of immutable infrastructure requires a strict operational discipline that many organizations haven't yet achieved, or have achieved for only a subset of applications.
- IT administrators are reluctant to give up the ability to directly modify or patch runtime systems.
- Applying the immutable infrastructure pattern is most easily done for stateless components. Stateful components, especially data stores, represent special cases that must be handled with care.
- Implementing immutable infrastructure requires a mature automation framework, up-to-date blueprints and bills of materials, and confidence in your ability to arbitrarily recreate components without negative effects on user experience or loss of state.
- Many enterprise applications are stateful applications deployed on virtual machines. These applications are oftentimes commercial off-the-shelf and are not designed for fully automated installation when redeployed.

### User Recommendations

- Reduce or eliminate configuration drift by establishing a policy that no software, including the OS, is ever patched in production. Updates must be made to individual components, versioned in a source-code-control repository, then redeployed.
- Prevent unauthorized change by turning off all administrative access to production compute resources. Examples of this might include not permitting Secure Shell or Remote Desktop Protocol access.
- Adopt immutable infrastructure principles with cloud-native applications first. Cloud-native workloads are more suitable than traditional on-premises workloads.
- Treat scripts, recipes and other codes used for infrastructure automation similar to the application source code itself, as this mandates good software engineering discipline.
- Include immutable infrastructure scripts, recipes, codes and images in your backup and ransomware recovery plans as they will be your primary source to rebuild your infrastructure after an infection.

**Sample Vendors**

Amazon Web Services; Google; HashiCorp; Microsoft; Perforce; Progress; Red Hat; Snyk; Turbot; VMware

**Gartner Recommended Reading**

Comparing DevOps Architecture to Automate Infrastructure and Operations for Software Development

2022 Strategic Roadmap for Compute Infrastructure

To Automate Your Automation, Apply Agile and DevOps Practices to Infrastructure and Operations

Innovation Insight for Continuous Infrastructure Automation

Market Guide for Cloud-Native Application Protection Platforms

**NDR**

**Analysis By:** Jeremy D'Hoinne, Nat Smith, Thomas Lintemuth

**Benefit Rating:** Moderate

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

**Definition:**

Network detection and response (NDR) products detect abnormal system behaviors by applying behavioral analytics to network traffic. They continuously analyze raw network packets or traffic metadata for both internal (east-west) and "public" (north-south) networks. NDR can be delivered as hardware and software sensor, and software or increasingly SaaS management console. Organizations rely on NDR to detect and contain postbreach activity, such as ransomware, or insider's malicious activity.

**Why This Is Important**

NDR focuses on detecting abnormal behaviors, with less emphasis on signature-based controls detecting known threats. NDR is effective in detecting weak signals and previously unknown behavior from traffic on networks such as lateral movement or data exfiltration. NDR solutions expand to hybrid networks, adding new detections. Automated response capabilities, provided natively or through integration remain important, but incident response workflow automation becomes an increasing area of focus.

**Business Impact**

NDR solutions provide visibility into network activities to spot anomalies. The machine learning algorithms that are at the core of many NDR products help to detect anomalies in traffic that are often missed by other detection techniques. The automated response capabilities help to offload some of the workload for incident responders. NDR products also help incident responders with their threat hunting by providing useful context and drill-down capabilities.

### Drivers

- Detecting postbreach activity: NDR complements traditional preventative controls by detecting activities based on deviations from baseline. This allows the security team to investigate insider's activities resulting from breaches without relying on having observed a previous occurrence of the same activity.
- Low risk — high reward: Implementing NDR products is a low-risk project because the sensors are positioned out-of-band, so they don't represent a point of failure or a "speed bump" for network traffic. Enterprises that implement NDR products as a proof of concept (POC) often report high degrees of satisfaction because the tools provide much-needed visibility into network traffic and enable even small teams to spot anomalies.
- Monitoring cloud traffic: A growing number of NDR vendors offer the ability to monitor IaaS traffic and M365 by leveraging available APIs from the cloud providers. Organizations expanding their cloud presence use NDR to avoid creating gaps in their ability to monitor interactions between their systems.

### Obstacles

- Enterprises with a lower maturity security operation program might struggle to justify the expense for a technology that cannot simply be evaluated by counting the number of alerts it triggers.
- The response features of the NDR products are more rarely deployed or narrowed down to specific use cases, such as ransomware, due to a risk of false positives. Many organizations postpone their implementation until they understand how to use the NDR tool better.
- NDR is expanding to support more detections in the cloud but have yet to prove they are the right tool for the use case.
- False positives are inevitable with any behavioral-based detection tool. NDR tools might require fine-tuning of the configuration to reduce the amount of false positives, especially in early days of the deployment. This explains why response capabilities are more rarely deployed initially.
- NDR increasingly competes for budget with consolidated platforms such as SIEM and extended detection and response (XDR).

### User Recommendations

- Develop a strong understanding of the overall traffic patterns and specific traffic patterns in your enterprise network to gain maximum value from NDR.
- Carefully plan sensor types and deployment locations so that the most relevant network traffic can be analyzed. Proper positioning of the NDR sensors is critically important to limit the number of false positives and control the cost of the deployment.
- Tune out false positives in the implementation phase (false positives may be triggered by vulnerability scanners, shadow IT applications and other factors that may be specific to your environment).
- Plan for ongoing tuning as new detection models are deployed from the vendor.
- Select sensor capturing capacity that is sized appropriately for your network.

### Sample Vendors

Cisco; Corelight; Darktrace; ExtraHop; Fortinet; IronNet; MixMode; Plixer; Trend Micro; Vectra

### Gartner Recommended Reading

Market Guide for Network Detection and Response

Emerging Tech: Top Use Cases for Network Detection and Response

## ZTNA

**Analysis By:** John Watts, Thomas Lintemuth

**Benefit Rating:** Moderate

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

**Definition:**

Gartner defines zero trust network access (ZTNA) as products and services that create an identity- and context-based, logical-access boundary that encompasses an enterprise user and an internally hosted application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a collection of named entities, limiting lateral movement in the network.

**Why This Is Important**

ZTNA is a key technology for enabling dynamic user-to-application segmentation through a trust broker to enforce a security policy that allows organizations to hide private applications and services and enforce a least-privilege access model for applications. It reduces the surface area for attack by creating individualized “virtual perimeters” that encompass only the user, the device and the application.

**Business Impact**

ZTNA logically separates the source user/device from the destination application to mitigate full network access and reduce the attack surface within the organization. This improves user experience (UX) and remote access flexibility while enabling dynamic, granular user-to-application segmentation through simplified policy management. Cloud-based ZTNA offerings improved scalability and ease of adoption for secure remote access.

### Drivers

- The rise of zero trust initiatives within organizations has led to the need for more precise access and session control in on-premises and cloud applications.
- There is an increasing need to modernize and simplify traditional VPN deployments that were optimized for static user locations connecting to data center environments rather than applications, services and data located outside an enterprise.
- Cloud-based ZTNA services are needed to augment on-premises remote access methods to offload hardware-based solutions when hybrid work demand exceeds hardware capacity.
- Some organizations need to acquire the ability to observe application access patterns before enforcing granular controls.
- Some organizations have a need to connect third parties such as suppliers, vendors and contractors to applications securely without exposing their entire networks over VPNs, or to connect the applications to the internet for access.
- Organizations that undergo mergers and acquisitions need to be able to extend application access to acquired companies without deploying endpoints or interconnecting their corporate networks.

### Obstacles

- **Cost:** ZTNA is typically licensed per named user on a per-user/per-year basis at a price roughly twice or three times that of traditional VPNs.
- **Limited support:** Not all products support all applications. For example, some client-based ZTNA solutions do not support UDP applications, and clientless ZTNA solutions typically only support web, Remote Desktop Protocol (RDP) and Secure Shell (SSH) protocols. Some vendors market VPN as a service (VPNaaS) as ZTNA, but lack support for some zero trust posture capabilities.
- **Adoption limited to VPN replacement:** Cloud-based trust brokers may not extend policy enforcement points on-premises, limiting use cases compared to universal ZTNA offerings.
- **Granularity of access policy:** Organizations must map application access for users, but many lack this understanding and end up with access rules which are either too granular or not granular enough.

### User Recommendations

- Enable application and service specific access with clientless ZTNA rather than full tunnel network access intended for extended workforce, “bring your own device” (BYOD) users, mergers and acquisitions, and B2B end users.
- Align ZTNA vendor choice with security service edge (SSE) vendor choice to support unified security controls for hybrid workers and remote branches and ZTNA policies with the organization’s zero trust strategy. Measure risk reduction using outcome-driven metrics.
- Demand universal ZTNA capabilities from vendors offering secure remote access to unify access control policies both on- and off-premises with added Internet of Things (IoT) support to replace legacy network access control (NAC) or software-defined network (SDN) implementations.
- Cloak systems, such as traditional VPN concentrators and collaboration systems exposed to the internet, from scan-and-exploit threats, and permit users to only interact with limited applications and data to reduce risk.

### Sample Vendors

Appgate; Cisco; Fortinet; Google; Microsoft; Netskope; Palo Alto Networks; Zscaler

### Gartner Recommended Reading

Market Guide for Zero Trust Network Access

How to Select the Right ZTNA Offering

7 Effective Steps for Implementing Zero Trust Network Access

2023 Strategic Roadmap for Zero Trust Security Program Implementation

2022 Strategic Roadmap for SASE Convergence

## Microsegmentation

**Analysis By:** Adam Hils, Rajpreet Kaur, Jeremy D'Hoinne

**Benefit Rating:** High

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Early mainstream

**Definition:**

Microsegmentation — also referred to as identity-based segmentation or zero trust network segmentation — can create more granular and dynamic access policies than traditional network segmentation, which is limited to internet protocol/virtual LAN (IP/VLAN) circuits.

**Why This Is Important**

Once a system is breached, attackers move laterally (including in ransomware attacks), which can cause serious damage. Microsegmentation seeks to limit the propagation of such attacks. It can greatly reduce the initial attack surface as well.

**Business Impact**

Microsegmentation can mitigate the risk and impact of cyberattacks. It is a form of zero trust networking that controls the access between workloads and is used to limit lateral movement, if and when an attacker breaches the enterprise network. Microsegmentation also enables enterprises to enforce consistent segmentation policies across on-premises and cloud-based workloads, including those that host containers.

**Drivers**

- As servers are being virtualized, containerized or moved to infrastructure as a service (IaaS), existing safeguards such as traditional firewalls, intrusion prevention solutions and antivirus software struggle to follow the fast pace of deployment for new assets. This leaves the enterprise vulnerable to attackers gaining a foothold and then moving laterally within enterprise networks. This has created increased interest in visibility and granular segmentation for east-west traffic between applications, servers and services in modern data centers.
- Zero trust is becoming a requirement in data center design, and microsegmentation is a practical way to accomplish this.
- The increasingly dynamic nature of data center workloads makes traditional network-centric segmentation strategies difficult to manage at scale, if not impossible to apply.
- Some microsegmentation products provide rich application communication mapping and visualization, allowing data center teams to identify which communication paths are valid and secure.
- The shift to microservices container architectures for applications has also increased the amount of east-west traffic and further restricted the ability of network-centric firewalls to provide this segmentation.
- The extension of data centers into IaaS has placed a focus on software-based approaches for segmentation — in many cases, using the built-in segmentation capabilities of cloud providers.
- Growing interest in zero trust networking approaches has also increased interest in using application and service identities as the foundation for adaptive application segmentation policies. This is critical to enforcing segmentation policies in the dynamic networking environments used within container-based environments.

### Obstacles

- Complexity — If not planned and scoped correctly, microsegmentation projects can lose organizational support before completion.
- Lack of knowledge — Security and risk leaders don't know which applications should be communicating with others, sowing doubt in automatically generated protection rules.
- Legacy network firewalls — Some data centers have network firewalls for broader east-west traffic segmentation, which is adequate for some organizations. Traditional firewalls can also present operational challenges to some identity-based segmentation solutions when policies overlap or conflict.
- Organizational dynamics — Cloud-centric organizations employing DevOps may value agility more than security, believing that any additional security controls will introduce operational friction.
- Expense — Full microsegmentation can come at a high price. Many organizations consider microsegmentation to be a net new budget item.

### User Recommendations

- Select zones to microsegment based on the highest risk. Oversegmentation is the leading cause of failure and an unnecessary expense for segmentation projects.
- Seek a solution that maps application communication paths and makes policy recommendations, using AI to make policy recommendations.
- Do not use IP addresses or network location as the foundation for east-west segmentation policies. Use the identities of applications, workloads and services — either via logical tags, labels, fingerprints or stronger identity mechanisms.
- Use the microsegmentation style (network overlay, host-based, cloud-native, API-based) that covers both the location of the workloads (on-premises, hybrid and IaaS) and the type of environment in which workloads are hosted (containers and virtual machines).
- Target the most critical assets and segment them first.
- Plan for coexistence of traditional firewalls and microsegmentation approaches for the next five years, and seek products that can support both.

### Sample Vendors

Akamai Technologies; Aqua Security Software; Cisco; ColorTokens; Fortinet; Illumio; Palo Alto Networks; VMware; Zero Networks; Zscaler

### Gartner Recommended Reading

2023 Strategic Roadmap for Zero Trust Security Program Implementation

### Container Security

**Analysis By:** Charlie Winckless, Michael Warrilow, Thomas Lintemuth

**Benefit Rating:** Moderate

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

### Definition:

Container security refers to the technologies and processes, testing, and controls in container-based environments. Full-life-cycle container security starts in development by assessing the risk or trust of the container's contents, secrets management and configuration of container instances. This extends into production with runtime container segmentation, threat protection and access control.

### Why This Is Important

By enabling greater speed and agility to streamline development, container-based applications have become mainstream. Rapid adoption of orchestration platforms, such as Kubernetes, has left traditional vendors and some security teams without appropriate tools to ensure secure application deployment. Container security requires a life cycle approach, starting with scanning of containers in development and protection of containers at runtime.

### Business Impact

Containers are not inherently insecure, but they are being deployed insecurely with known vulnerabilities and configuration issues. Without proper controls, developers can introduce vulnerabilities into development and, subsequently, production environments. This can expose organizations to avoidable risk. Furthermore, security has been slow to embrace secure container development practices and tools, leaving organizations unaware of potential risks and unprepared to respond to attacks.

### Drivers

- Developer adoption of containers and Kubernetes has shifted threats from traditional environments to containerized ones, forcing security teams to use different tools and approaches to address these new threats.
- Container-as-a-service (CaaS) offerings, such as Amazon Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS) and Google Kubernetes Engine (GKE), are on the rise. These require security integrations to provide coverage for the clusters and containers they host.
- With rising adoption of containers, security and risk management leaders need to address container-related security issues around vulnerabilities, visibility, compromise, and compliance. This would help meet the needs of digital business and application modernization.
- Multiple point solutions can now integrate transparently into the continuous integration/continuous delivery pipeline and DevOps practices, to proactively scan containers for security and compliance issues. However, organizations must carefully manage these point solutions to minimize the complexity they introduce.
- Microservices architectures are proliferating and driving container deployments in DevOps processes, which causes some of the responsibility for securing the environment to shift left to developers. DevOps pipeline integrations provide opportunities to secure against supply chain and other development risks in these environments.

### Obstacles

- Container security must start in development, yet many security vendors and enterprises treat container security as a runtime-only problem. Worse, some vendors are simply placing an agent on a container, forwarding logs and calling this “container security.”
- If container image governance policies are not introduced early on, applying standards becomes increasingly difficult, as different software product teams start to implement their own processes for building container images.
- Organizations and teams may resist the use of active runtime container security for fear of disrupting applications and business.

### User Recommendations

- Create and maintain a minimum set of hardened and immutable container images as the basis for all container workloads. In doing so, prioritize the use of a container-optimized operating system distribution.
- Scan containers in development for configuration and vulnerability issues of all code types, before deploying to production. Integrate with admission controllers to prevent these vulnerable containers being deployed.
- Take advantage of continuous scanning provided by code repositories and cloud providers.
- Use automated tools to analyze the processes expected to run in containers, along with their behaviors. Use this information to replace signature-based deny-listing with allow-listing-based lockdown.
- Require container security solutions to explicitly support and integrate with your container management tooling and/or Kubernetes.
- Design single-purpose containers and clear tagging mechanisms to track data sensitivity.

### Sample Vendors

Aqua Security; Lacework; Palo Alto Networks; Red Hat; Snyk; SUSE, Sysdig; Tigera; Trend Micro; Uptycs

### Gartner Recommended Reading

Container Supply Chain: 10 Security Vulnerabilities and How to Address Them

Market Guide for Cloud-Native Application Protection Platforms

## Remote Browser Isolation

**Analysis By:** John Watts, Neil MacDonald

**Benefit Rating:** Low

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

**Definition:**

Remote browser isolation (RBI) separates the rendering of untrusted content (typically from the internet) from users and their devices, or separates sensitive applications and data from an untrusted device. When used to protect from untrusted content, RBI significantly reduces the chance of a breach, as a large number of attacks have shifted to users and endpoints. When used to protect sensitive data and applications from unmanaged devices, RBI helps to reduce risks associated with BYOD.

**Why This Is Important**

Browser isolation keeps the session between an endpoint and the web services it is accessing segregated, reducing the risk of malware and data loss. When an endpoint is accessing web content, RBI prevents web-delivered malware from being delivered directly to the endpoint. RBI also works in the reverse direction. In use cases such as SaaS access via a cloud access security broker (CASB) or internal application access via zero-trust network access (ZTNA), it protects sensitive data and applications from attack by an unmanaged and potentially infected device.

**Business Impact**

Today, most attacks are delivered via the public internet, either through exploits delivered by web browsing or via emailed links that trick users into visiting malicious sites. Connecting the browser from the end user's desktop to another browser running in a separate location improves the efficacy of existing security tools. RBI protection can also extend to protect private and SaaS applications accessed from unmanaged devices, thus reducing the threat of data exfiltration.

### Drivers

- Many organizations desire to establish an adaptive zero-trust posture by using isolation as a policy action within security service edge (SSE) for forward proxy, reverse proxy and private applications.
- There is often a need to apply malware protection and data protection to both managed and unmanaged devices.
- Isolation of websites is a more efficient means of improving security than relying on slow, static blocklists to stop targeted attacks.
- Allowing isolated access to uncategorized sites, rather than blocking them, can reduce user friction.
- Email-based URLs that resolve externally can be isolated to prevent phishing attacks on employees.

### Obstacles

- End users often cite a poor experience when RBI is deployed for all sites, leading some organizations to limit RBI to only certain categories of sites.
- Few stand-alone RBI vendors remain in the market, which limits choices, as most RBI options are now included as features of secure access service edge (SASE) and SSE platforms.
- Localizing the browsing experience for cloud-based, multitenant RBI requires IP address assignments to be regionally combined with either VPN exit points or local points of presence.
- RBI is an additional layer of defense at additional cost, as it rarely fully replaces other security controls.
- Most RBI offerings are software-based and cloud-delivered, limiting options for organizations looking for an on-premises, hardware-based isolation option.
- RBI does not protect against infected content that is permitted to download to the endpoint. Mechanisms like file antivirus and sandboxing, conversion to PDF, remote viewers and content disarm and reconstruction (CDR) are required.

### User Recommendations

- Evaluate and pilot an RBI solution for specific high-risk users (such as finance teams) or use cases (such as rendering email-based URLs), particularly if your organization is risk-averse.
- Evaluate RBI as a feature of your existing SASE/SSE provider and determine how it can be used to improve the efficacy of the solution. Roll out RBI incrementally for threat protection. Start by deploying to a limited number of high-value target users and by selectively isolating a limited number of URLs. Then, expand the use cases.
- Evaluate different vendor approaches for rendering (e.g., pixel streaming, DOM reconstruction or graphics rendering) based on performance, latency and bandwidth requirements.
- Use RBI to isolate files for read-only viewing. However, when downloads are required, use CDR or best-in-class file scanning to prevent malware.

### Sample Vendors

Authentic8; Broadcom; Cloudflare; Forcepoint; Garrison; Menlo Security; Netskope; Proofpoint; Skyhigh Security; Zscaler

### Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Market Guide for Single-Vendor SASE

## Entering the Plateau

### CSPM

**Analysis By:** Neil MacDonald, Charlie Winckless

**Benefit Rating:** High

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

#### Definition:

Cloud security posture management (CSPM) offerings continuously manage IaaS and PaaS security posture through prevention, detection and response to cloud infrastructure risks. The core of CSPM offerings applies common compliance frameworks, regulatory requirements and enterprise policies to proactively and reactively discover and assess risk/trust of cloud services' configuration and security settings. If an issue is identified, remediation options (automated or human-driven) are provided.

#### Why This Is Important

The complexity of modern IaaS/PaaS environments makes validating secure configuration extremely difficult. Even simple misconfiguration issues, such as open-storage objects, represent significant and often unidentified risk. The speed and scale of modern cloud deployments compound the impact of misconfiguration, and they make it effectively impossible to address cloud risk without automation. This is an urgent problem and one that is driving rapid growth and maturation in this category.

#### Business Impact

CSPM offerings provide business and security leaders assurance that their cloud services are implemented in a secure and compliant fashion, despite the speed, complexity, dynamics, and scale of IaaS and PaaS deployments. For enterprises that have a multicloud strategy, CSPM offerings provide a single way to implement and monitor security and compliance guardrails across multiple IaaS and PaaS providers.

#### Drivers

- Multiple mature offerings are now available from established vendors.
- Hyperscalers offer built-in CSPM capabilities suitable for single-cloud deployments with limited multicloud support.

- Most cloud-native application protection platforms (CNAPPs), cloud workload protection platforms (CWPPs) and security service edge (SSE) vendors now offer CSPM capabilities as a result of acquisitions or open-source integration.
- CSPM tools offer an abstraction layer that allows for consistent policy management across multiple clouds.
- There are several open-source software options, with enterprise offerings available.
- Most emerging CSPM platforms leverage graph and relationship mapping technologies that enable rich risk prioritization, attack path simulation, detection and forensic use cases.
- Most vendors now offer full-stack risk visibility with an understanding of vulnerabilities within the workload itself, typically achieved by taking a snapshot of the running workload.

**Obstacles**

- The market for CSPM is maturing and consolidating.
- Emerging CNAPP offerings subsume CSPM capabilities and offer a longer-term more integrated approach.
- The market is increasingly looking for tooling that shifts left and offers infrastructure-as-code scanning capabilities. Not all vendors offer this, or they offer only a limited set of infrastructure-as-code scripting languages.
- CSPM capabilities are available in many adjacent markets, making it difficult for end users to select the best approach.
- There is no standard way to remediate issues identified, and approaches vary.
- Organizations are reluctant to enable automated remediation from SaaS-based CSPM offerings (that require read/write access) and prefer remediation within the context and control of their own cloud service provider tenancy.

**User Recommendations**

- Investigate and see if you already have suitable CSPM capabilities from your IaaS provider, CWPP vendor, SSE/cloud access security broker vendor and IT operations team. The IaaS provider might have sufficient CSPM capabilities built in, and the IT operations team may have purchased a cloud management platform for billing/utilization, but many also have suitable CSPM capabilities.
- Treat investments as tactical if a point solution is used. Limit contracts to one to two years as the market matures and further consolidates.
- Evaluate the CSPM provider's cloud infrastructure entitlement management capabilities as an alternative to purchasing a stand-alone solution for this.
- Extend scanning into development, including infrastructure-as-code scanning.
- Evaluate and compare the response options when an out-of-compliance configuration is encountered, including alerting and automated remediation alternatives.
- Evaluate emerging CNAPP offerings that include integrated CSPM capabilities.

### Sample Vendors

Check Point Software Technologies; Lacework; Orca Security; Palo Alto Networks; Rapid7; Sonrai Security; Tenable; Trend Micro; Wiz; Zscaler

### Gartner Recommended Reading

Market Guide for Cloud-Native Application Protection Platforms

Solution Criteria for Cloud Security Posture Management (CSPM)

Emerging Tech: Security — Adoption Growth Insights for Cloud Workload Protection Platforms

## Appendixes

See the previous Hype Cycle: Hype Cycle for Workload and Network Security, 2022

## Hype Cycle Phases, Benefit Ratings and Maturity Levels

### Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

| Phase | Definition |
|---|---|
| *Innovation Trigger* | A breakthrough, public demonstration, product launch or other event generates significant media and industry interest. |
| *Peak of Inflated Expectations* | During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers. |
| *Trough of Disillusionment* | Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales. |
| *Slope of Enlightenment* | Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process. |
| *Plateau of Productivity* | The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase. |
| *Years to Mainstream Adoption* | The time required for the innovation to reach the Plateau of Productivity. |

Source: Gartner (July 2023)

### Table 3: Benefit Ratings

| *Benefit Rating* ↓ | *Definition* ↓ |
|---|---|
| *Transformational* | Enables new ways of doing business across industries that will result in major shifts in industry dynamics |
| *High* | Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise |
| *Moderate* | Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise |
| *Low* | Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings |
| | |

Source: Gartner (July 2023)

### Table 4: Maturity Levels

(Enlarged table in Appendix)

| Maturity Levels | Status | Products/Vendors |
|---|---|---|
| *Embryonic* | In labs | None |
| *Emerging* | Commercialization by vendors<br>Pilots and deployments by industry leaders | First generation<br>High price<br>Much customization |
| *Adolescent* | Maturing technology capabilities and process understanding<br>Uptake beyond early adopters | Second generation<br>Less customization |
| *Early mainstream* | Proven technology<br>Vendors, technology and adoption rapidly evolving | Third generation<br>More out-of-box methodologies |
| *Mature mainstream* | Robust technology<br>Not much evolution in vendors or technology | Several dominant vendors |
| *Legacy* | Not appropriate for new developments<br>Cost of migration constrains replacement | Maintenance revenue focus |
| *Obsolete* | Rarely used | Used/resale market only |

Source: Gartner (July 2023)

## Evidence

**2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey:** This survey was conducted to determine how many organizations are pursuing vendor consolidation efforts; what the primary drivers are for consolidation; the expected or realized benefits of vendor consolidation; and how those that are consolidating are prioritizing their consolidation efforts. Another key aim of the survey was to collect objective data on extended detection and response (XDR) and SASE for consolidation of megatrend analysis.

The survey was conducted online, from March through April 2022, among 418 respondents from North America (n = 277; the U.S. and Canada), Asia/Pacific (n = 37; Australia and Singapore) and EMEA (n = 104; France, Germany and the U.K.).

Results were from respondents whose organizations generated $50 million or more in enterprisewide revenue in 2021. They came from industries including manufacturing, communications and media, IT, government, education, retail, wholesale trade, banking and financial services, insurance, healthcare, services, transportation, the utilities sector, natural resources, and pharmaceuticals, biotechnology and life sciences.

Respondents were screened for job title, company size, job responsibilities (including information security/cybersecurity and IT roles), and primary involvement in information security.

*Disclaimer: The results of this survey do not represent global findings or the market as a whole. They reflect the sentiments of the respondents and companies surveyed.*

## Document Revision History

Hype Cycle for Workload and Network Security, 2022 - 18 July 2022

---

## Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Market Guide for Cloud-Native Application Protection Platforms

Innovation Insight for Attack Surface Management

Magic Quadrant for Security Service Edge

---

## Table 1: Priority Matrix for Workload and Network Security, 2023

| *Benefit* ↓ | *Years to Mainstream Adoption* | | | |
|---|---|---|---|---|
| | *Less Than 2 Years* ↓ | *2 - 5 Years* ↓ | *5 - 10 Years* ↓ | *More Than 10 Years* ↓ |
| Transformational | | SASE<br>Security Service Edge | Generative Cybersecurity AI | |
| High | Microsegmentation | Cloud WAAP<br>CSPM<br>Hybrid Mesh Firewall Platform<br>Identity-First Security | Cloud-Native Application Protection Platforms<br>Zero Trust Strategy | |
| Moderate | Container Security | CIEM<br>Cloud Firewalls<br>eBPF<br>Firewall as a Service<br>Immutable Infrastructure<br>NDR<br>Serverless Function Security<br>ZTNA | Automated Security Control Assessment<br>CAASM<br>Cloud Investigation and Response Automation<br>Enterprise Browsers<br>Kubernetes Security<br>SaaS Security Posture Management | |
| Low | Remote Browser Isolation | | | |

Source: Gartner (July 2023)

## Table 2: Hype Cycle Phases

| *Phase* | *Definition* |
|---|---|
| *Innovation Trigger* | A breakthrough, public demonstration, product launch or other event generates significant media and industry interest. |
| *Peak of Inflated Expectations* | During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers. |
| *Trough of Disillusionment* | Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales. |
| *Slope of Enlightenment* | Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process. |
| *Plateau of Productivity* | The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase. |
| *Years to Mainstream Adoption* | The time required for the innovation to reach the Plateau of Productivity. |

| Phase ↓ | Definition ↓ |
| --- | --- |

Source: Gartner (July 2023)

### Table 3: Benefit Ratings

| Benefit Rating ↓ | Definition ↓ |
| --- | --- |
| *Transformational* | Enables new ways of doing business across industries that will result in major shifts in industry dynamics |
| *High* | Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise |
| *Moderate* | Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise |
| *Low* | Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings |

Source: Gartner (July 2023)

## Table 4: Maturity Levels

| *Maturity Levels* ↓ | *Status* ↓ | *Products/Vendors* ↓ |
|---|---|---|
| *Embryonic* | In labs | None |
| *Emerging* | Commercialization by vendors<br>Pilots and deployments by industry leaders | First generation<br>High price<br>Much customization |
| *Adolescent* | Maturing technology capabilities and process understanding<br>Uptake beyond early adopters | Second generation<br>Less customization |
| *Early mainstream* | Proven technology<br>Vendors, technology and adoption rapidly evolving | Third generation<br>More out-of-box methodologies |
| *Mature mainstream* | Robust technology<br>Not much evolution in vendors or technology | Several dominant vendors |
| *Legacy* | Not appropriate for new developments<br>Cost of migration constrains replacement | Maintenance revenue focus |
| *Obsolete* | Rarely used | Used/resale market only |

Source: Gartner (July 2023)