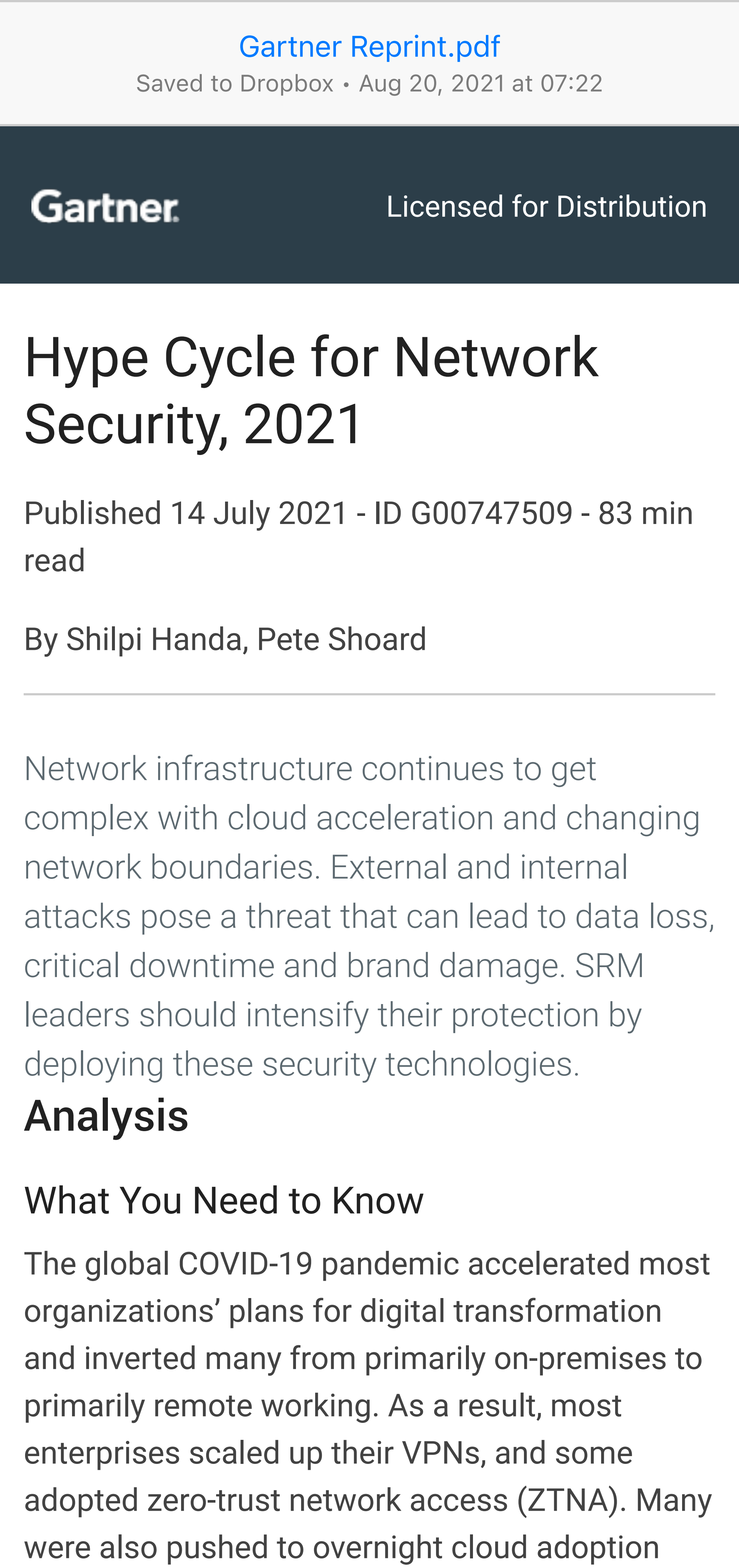


Gartner
Licensed for Distribution

Hype Cycle for Network Security, 2021

Published 14 July 2021 - ID G00747509 - 83 min read

By Shilpi Handa, Pete Shoard

Network infrastructure continues to get complex with cloud acceleration and changing network boundaries. External and internal attacks pose a threat that can lead to data loss, critical downtime and brand damage. SRM leaders should intensify their protection by deploying these security technologies.

Analysis

What You Need to Know

The global COVID-19 pandemic accelerated most organizations’ plans for digital transformation and inverted many from primarily on-premises to primarily remote working. As a result, most enterprises scaled up their VPNs, and some adopted zero-trust network access (ZTNA). Many were also pushed to overnight cloud adoption and digitalization. Traditional network security technologies supported this by expanding their cloud-delivered services with adjacent preventive technologies to protect assets and to support mobile workforces.

Rapid scaling and the need to enhance the user experience of remote workers played an important role in the adoption and consolidation of cloud-based network security controls which contributed to trends of SASE, ZTNA, etc. With vendors consolidating multiple network security controls, it is important to understand when to choose consolidated vs stand-alone products based on your use cases. Security controls still vary from vendor to vendor, and you need to understand the available controls in the marketplace and ascertain if they secure hybrid clouds, digital infrastructure, remote workforce and other business security and risk goals when setting an organizational network security strategy. SRM leaders must make intelligent, risk-based and cost-effective decisions about the security technologies they choose to defend their organizations.

The Hype Cycle

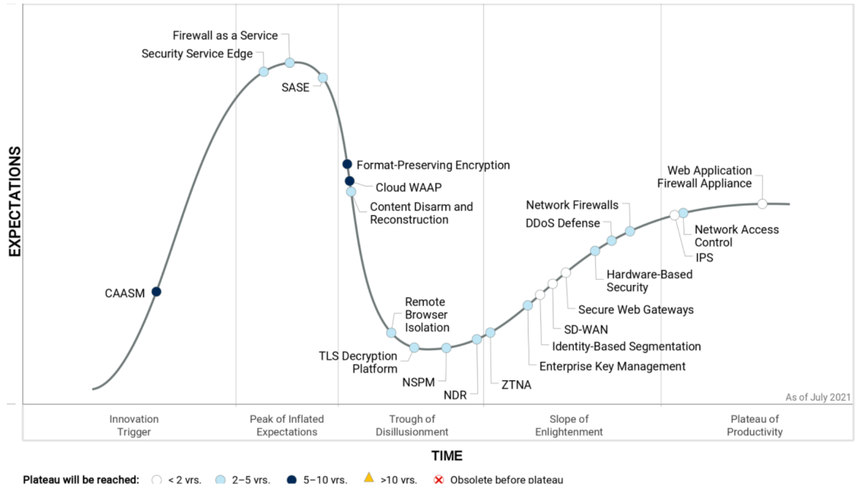
The network security market is mature with technologies moving in sync with infrastructure and cloud innovation. The innovation in network security technologies, mostly therefore, is not presented independently, but as upgrades and enhancements to existing solutions and markets. However, two new areas — namely secure access service edge (SASE) services and cyber asset attack surface management (CAASM) — have been added to the Hype Cycle this year. While SASE services are an extension of the SASE market, CAASM focuses on asset visibility for vulnerability management.

Remote workforce strategies have brought technology and deployment consolidation into focus, and this can be seen in areas such as secure access service edge (SASE) and its associated technologies such as secure web gateway (SWG), zero-trust network access (ZTNA) and cloud access security broker (CASB).

COVID-19 pushed a lot of organizations to digitize rapidly, and these organizations were pressed to expand public-facing applications and APIs to support digital business initiatives. This increased the pace of adoption for network and application protection technologies such as cloud WAAP including API protection and bot mitigation. Gartner also observed a significant drift toward cloud-delivered application protection and consolidation of content delivery, application, API, and bot security as opposed to on-premises web application firewalls (WAFs).

Identifying and retaining the right cybersecurity resources has always been a challenge, even more for organizations that host technologies in-house, and this year was no different. Incident responders looked at tools such as network detection and response (NDR) with automated response capabilities, which are advantageous in such scenarios .The machine learning algorithms that are at the core of many NDR products can help to detect anomalous network traffic. Policy management was another important area for security and risk managers this year. This was primarily aimed at reducing complexity around policy management. Network security policy management (NSPM) technology focuses on simplifying policy management across firewalls in hybrid environments. Vendors of network security technology strive to reduce policy complexity across the portfolio and third-party integrations. Increasing interest in identity-based segmentation technologies can also be attributed to easy policy identification and management.

Figure 1: Hype Cycle for Network Security, 2021



Gartner

Source: Gartner

Downloadable graphic: Hype Cycle for Network Security, 2021

The Priority Matrix

In today's hybrid business environments, network security controls need to be tied to the infrastructure's changing forms and yet need to maintain its uniformity and manageability. This is more evident from the fact that many large security vendors are improving their administration by building integrated management themes across their portfolios. Network security technology vendors have also started working toward removing data silos, and today bet big on data intelligence lakes built from their various customer touchpoints, to support threat detection and response.

Some of the most beneficial changes this year have been in the area of SASE. By pursuing a consolidation strategy in network security, it increases ease of use of network security tools, and reduces complexity with modular tools and licensing. SASE security services is an extension into a single-vendor, cloud-centric converged capability.

The adoption of some technologies is becoming more mainstream. This includes hardware-based security, which is becoming standard in most hardware devices and cloud-based IaaS offerings. As IPSs mature, they are becoming a feature of NGFW and FWaaS. Network Access Control continues to mature as most organizations benefit from increased visibility and control of devices on the local network. Virtual Private Network became even more important last year due to the remote workforce requirements of organizations but there has not been much innovation in the technology. Zero-trust network access (ZTNA) is a potential replacement for mainstream VPN, as organizations look to implement zero trust networking strategies within their environment. With an increase in cloud delivered security, FWaaS saw traction this year more so because businesses wanted to overcome the bottleneck of on-prem infrastructure due to remote workforce surge.

A new area of focus is Cyber Asset Attack Surface Management (CAASM), it is an emerging technology focused on enabling security teams to solve persistent asset visibility and vulnerability challenges. It enables organizations to gather all assets both internal and external through API integrations, query them, and remediate security control and vulnerability gaps.

Table 1: Priority Matrix for Network Security, 2021

Enlarge Table

Benefit	Years to Mainstream Adop	
	Less Than 2 Years	2 - 5 Y
Transformational		SASE

High	SD-WAN Secure Web Gateways Web Application Firewall Appliance	Conte Disar Reco DDoS NDR Netw Acces Contr Netw Firew NSPM Remo Brow

Source: Gartner (July 2021)

Off the Hype Cycle

Three profiles have graduated or retired. WAF has been separated into WAF Appliances and Cloud WAAP to better align with the market adoption and trends. IoT Security has changed focus to a development-centric approach and therefore no longer aligns with the aims and capabilities associated with security operations. Secure Enterprise Data Communications, while still relevant to network security, has matured off of the Hype Cycle as it has been superseded by modern remote access solutions such as ZTNA.

On the Rise

CAASM

Analysis By: John Watts, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition

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

Why This Is Important

CAASM expands beyond the limited scope of products that focus on a subset of assets such as endpoints, servers, devices or applications. By consolidating into a single repository, users can query to find gaps in coverage for external attack surface management (EASM) and endpoint detection and response (EDR) tools. CAASM provides passive data collection by using API integrations, replacing manual and timeconsuming processes to collect and reconcile asset information.

Business Impact

CAASM enables security teams to improve basic security hygiene by ensuring security controls, security posture and asset exposure are understood and remediated across the environment. Organizations that deploy CAASM reduce dependencies on homegrown systems and manual collection processes, and remediate gaps manually or through automated workflows. In addition, such organizations can visualize security tool coverage and correct source systems of record that may have stale or missing data.

Drivers

- Full visibility into all assets under an organization’s control to understand attack surface area and any existing security control gaps.
- Quicker audit compliance reporting through more accurate, current and comprehensive asset and security control reports.
- Consolidation of various existing products already collecting asset information into a single normalized view, reducing the need for manual processes or dependencies on

homegrown applications.

- Access to consolidated asset views for multiple teams across the organization such as enterprise architects, vulnerability management teams and IT administrators, who can benefit from viewing and querying consolidated asset inventories.

- Lower resistance to collect data and gain security visibility from shadow IT organizations, installed third-party systems and line-of-business applications where IT lacks governance and control. Security teams need visibility in these places while IT may not.

Obstacles

- Resistance to “yet another” tool — Organizations with adjacent products that provide asset visibility may be challenged to justify the cost and addition of CAASM.

- Products may be licensed per asset consumed and become cost-prohibitive for very large organizations with millions of assets under management.

- Scalability of a single instance may be limited for extremely large environments, both for data collection as well as usability of the tool with excessive data points.

- Tools that can be integrated with a CAASM either do not exist (e.g., lacking API) or are blocked for integration by teams who own the existing tools.

- Reconciliation processes that conflict with source systems can cause confusion and frustration if the source system of record is not allowed to be corrected when errors are found.

User Recommendations

- Take advantage of POCs or free versions of products to try before you buy. Products are nondisruptive and easy to deploy, limiting the risk of purchasing a CAASM product and then needing to retire or replace it with another vendor.

- Determine the primary use cases you want to solve with CAASM such as achieving more comprehensive visibility into assets, auto remediation of security gaps, updating sources of records or easing compliance reporting burdens.

- Inventory all available APIs that can be integrated with the CAASM product and make sure you have user accounts available to integrate.

- Extend usage beyond core security teams to multiple users including compliance teams, threat hunters, vulnerability management teams and system administrators.

- Inquire with incumbent security vendors to understand what visibility they currently provide into assets and if they have a roadmap to provide CAASM functionality in the future.

Sample Vendors

AirTrack Software; Axonius; Brinqa; JupiterOne; Panaseer; Sevco Security

At the Peak

Security Service Edge

Analysis By: Neil MacDonald, John Watts

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition

Security service edge (SSE) secures access to the web, cloud services and private applications. Capabilities include access control, threat protection, data security, security monitoring and acceptable use control enforced by network-based and API-based integration. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.

Why This Is Important

The overall SASE market convergence is driven by the increasing usage of cloud services, combined with a shift to remote work. SSE offerings reduce complexity and improve user experience by consolidating multiple disparate security capabilities (e.g., secure web gateways [SWGs]; cloud access security brokers [CASBs]; zero trust network access [ZTNA]; remote browser isolation [RBI]; and firewall as a service [FWaaS]) into a single-vendor, cloud-centric converged capability.

Business Impact

The shift to remote work and the adoption of public cloud services was underway and further accelerated by COVID-19. SSE allows the organization to support the anywhere, anytime workers using a cloud-centric approach for the enforcement of security policy. SSE offers immediate opportunities to reduce complexity, costs and the number of vendors.

Drivers

- Users, applications, and enterprise data are everywhere. Old data center-centric security architectures/products need adjustment. SASE offerings are the necessary adjustment.

- Organizations choose SSE when looking to add flexible cloud-based network security for users and devices without tying it to their choice of network infrastructure (e.g., if the organization has already deployed SD-WAN).

- SSE tends to have more mature security features, appealing to buyers looking for deeper security capabilities as compared to some SD-WAN vendors that only recently added a minimal set of security features to their offering.

- Zero-trust, least-privileged access based on identity and context is a core capability of leading SSE offerings.

- By consolidating vendors, organizations can reduce complexity, costs and the number of consoles used to define security policy. This also helps to eliminate risk created by gaps in coverage or inconsistencies with the use of multiple disparate offerings.

- Sensitive data inspection and malware inspection can be made consistent and in parallel across all channels of access — SaaS, internet and private applications — with better performance than doing this separately.

- Organizations improve user experience by providing exactly the same secured experience remotely, in a branch or in the main office.

Obstacles

- Some organizations want to strategically combine and unify their secure access strategy using SD-WAN and SSE from a single vendor rather than relying on two separate vendors.

- Most leading SD-WAN vendors now have a set of SSE services natively or through partnerships, placing competitive pressure on SSE vendors to add basic SD-WAN capabilities.

- Because the market is being formed by convergence of capabilities, most vendors are better in a single category and have gaps in other categories. Further, some vendors don't yet have a complete suite of SSE services (e.g., they are missing FWaaS or other security services).

- Some vendors are weak in sensitive data identification and protection, and this capability is critical for risk- and context-based access decisions.

- Being cloud-centric, SSE typically doesn’t address the need for on-premises (e.g., file servers) and endpoint DLP.

- Not all vendors will commit to performance SLAs on all services.

User Recommendations

- Consolidate vendors, and cut complexity and costs as contracts renew for SWGs, CASBs and VPNs (replacing with a ZTNA approach). Leverage a converged market that emerges by combining these services.

- Inventory equipment and contracts to implement a multiyear phase out of on-premises perimeter and branch security hardware in favor of cloud-based delivery of SSE. Target consolidation of on-premises equipment ideally to a single appliance.

- Actively engage with initiatives for branch office transformation, SD-WAN and Multiprotocol Label Switching (MPLS) offload in order to integrate cloud-based SSE into the scope of project planning.

Sample Vendors

Bitglass; Broadcom (Symantec); Forcepoint; iboss; McAfee; Menlo Security; Netskope; Palo Alto Networks; Versa; VMware; Zscaler

Gartner Recommended Reading

2021 Strategic Roadmap for SASE Convergence

Magic Quadrant for Secure Web Gateways

Magic Quadrant for Cloud Access Security Brokers

Critical Capabilities for Cloud Access Security Brokers

Market Guide for Zero Trust Network Access

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 intended to protect small branch offices and mobile users. FWaaS can provide simpler, more flexible architecture using centralized policy management, multiple enterprise firewall features and traffic tunneling to partially or fully move security inspections to a cloud infrastructure.

Why This Is Important

The uptick in remote work, and growing adoption of SD-WAN and hybrid WAN architectures are increasing interest in using FWaaS. We anticipate that this trend will continue. FWaaS offerings are of varying levels of maturity. Organizations considering FWaaS should conduct extensive proofs of concept or limit the scope of an initial production deployment.

Business Impact

The main business impacts are:

- FWaaS offers a significantly different architecture for branches or even single-site organizations. It offers greater visibility through centralized policy, increased flexibility and reduced capital costs associated with using a fully or partially hosted security workload.

- As with other as a service (aaS) security offerings, FWaaS changes budgetary considerations as organizations move from capital to operational spending.

- Organizations with workforces that may stay remote will find that FWaaS helps them work securely in a widely-distributed network.

Drivers

- Organizations rearchitecting their networks by implementing SD-WAN often want FWaaS to secure outbound network traffic.

- Firewall as a Service is a core component of the security access service edge (SASE) framework often offered as part of a larger SASE security service.

- FWaaS can decrypt outbound traffic for inspection at scale. Alternative branch firewalls often lack the performance to do this.

- The move toward remote work in 2020 and 2021 necessitates bringing security services closer to the workers to minimize latency.

Obstacles

- Network firewall appliances comprise the largest security equipment market in security and risk. The appliance approach has been predominant for decades, and many organizations use them effectively and efficiently.

- Security and risk leaders find some FWaaS solutions difficult to implement and manage.

- Over 75% of outbound traffic in organizations is HTTP and HTTPS traffic. Cloud-based secure web gateway (SWG) services can protect and inspect this traffic at scale to offload existing hardware-based firewalls. This makes it much easier to extend investments in existing firewall hardware without completely rearchitecting 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 compared to hardware-based solutions, which may have lower subscription costs and can be deployed and used beyond their capital depreciation life span.

User Recommendations

- Verify that the additional hop to the FWaaS infrastructure does not create unacceptable latency for some of your sites and look at business models that limit initial investment until limited latency is proven. The appeal of simpler architecture and increased flexibility must materialize in faster deployment and easier maintenance.

- Determine whether your organization is ready to move the entire security workload into the cloud, or if you need thicker local devices to address privacy concerns and perform some on-premises computation (such as segmentation or VLAN trunking).

- Assess how FWaaS might impact your branch architecture, especially your ability to maintain and easily manage multiple network segments. Current FWaaS offerings are mostly outbound security for now, or they are targeted at protecting mobile workers or companies whose applications are primarily cloud-hosted with no branch dependency on headquarters for applications.

- Evaluate the strength of the cloud service on three key aspects — data center locations, points of presence and SLA. Ensure that the FWaaS provider has sufficient points of presence for your remote workforce. Ensure that they have data centers close to branch offices and a strong SLA for availability and latency (e.g., 99.999% uptime and no more than 100ms of latency).

- Conduct an individual assessment of each key as-a-service security component that you plan to deploy and determine whether FWaaS provides unique security features, such as shared threat intelligence gathered from similar client organizations.

- Include the possibility of failure in the centralized FWaaS infrastructure in business continuity plans.

Sample Vendors

Aryaka; Barracuda; Cato; Check Point Software Technologies; Cisco; Palo Alto Networks; Versa; Zscaler

Gartner Recommended Reading

Magic Quadrant for Network Firewalls

Critical Capabilities for Network Firewalls

Select the Right Strategy for Securing Web Access

SASE

Analysis By: Joe Skorupa, Neil MacDonald

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition

Secure access service edge (SASE) delivers multiple converged network and security as a service capabilities, such as SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA). SASE supports branch office, remote worker and on-premises general internet security use cases. SASE is 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, resilience and security. SASE also dramatically simplifies the delivery and operation of critical network and network security services mainly via a cloud-delivered model. SASE can reduce the number of vendors required for secure access from four to six today to one to two over the next several years.

Business Impact

SASE enables:

- New digital business use cases (such as digital ecosystem and mobile 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

- SASE is driven by enterprise digital business transformation: the adoption of cloud-based services by distributed and mobile workforces, edge computing and business continuity plans that must include flexible, anywhere, anytime, secure remote access and use of the internet and cloud services.

- The need to flexibly support digital business transformation efforts with a zero trust security architecture while keeping complexity manageable is a significant factor for the adoption of SASE, primarily delivered as a cloud-based service (see The Future of Network Security Is in the Cloud). The COVID-19 pandemic accelerated these trends.

- For IT, SASE can reduce the deployment time for new users, locations, applications and devices as well as reduce attack surface and shorten remediation times by as much as 95%.

- Network security models based on data center perimeter security are ill-suited to address the dynamic needs of a modern digital business and its distributed digital workforce. This is forcing a transformation of the legacy perimeter into a set of cloud-based, converged capabilities created when and where an enterprise needs them — that is, a dynamically created, policy-based secure access service edge, or SASE.

Obstacles

- **Organizational silos, existing investments and skills gaps**: A full SASE implementation requires a coordinated and cohesive approach across network security and networking teams.

- **Organizational bias and regulatory requirements that drive continued 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, Russia and the Middle East, where vendors may have limited cloud presence.

- **SASE security services maturity:** For the next several years, SASE capabilities will vary widely. Sensitive-data visibility and control is often a high-priority capability, but it is difficult for most SASE vendors to address. Your preferred vendor may lack the capabilities you require but two-vendor partnerships can be a viable approach.

User Recommendations

- Involve the CISO and network architect when evaluating offerings and roadmaps from incumbent and emerging vendors to ensure an integrated approach.

- Leverage WAN, firewall, VPN refresh or SD-WAN to update network and network security architectures.

- Strive for not more than two vendors for all core services to minimize complexity and improve performance.

- Identify required capabilities for networking and security, including latency, throughput, geographic coverage and endpoint types to develop evaluation criteria.

- Focus on vendors that include CASB if DLP is a priority. They have the most experience in this area.

- Combine branch office and remote access in a single implementation to ensure consistent policies and minimize the numbers of vendors required. Deploy ZTNA to augment or replace legacy VPN to limit investment in legacy technology.

- Consolidate vendors to cut complexity and cost as contracts renew.

- Leverage branch office transformation and MPLS offload to adopt SASE for security services.

Sample Vendors

Cato Networks; Fortinet; Palo Alto Networks; Versa Networks; VMware; Zscaler

Gartner Recommended Reading

2021 Strategic Roadmap for SASE Convergence

Market Guide for Zero Trust Network Access

The Future of Network Security Is in the Cloud

Magic Quadrant for WAN Edge Infrastructure

Magic Quadrant for Cloud Access Security Brokers

Market Guide for Zero Trust Network Access

Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge

Sliding into the Trough

Format-Preserving Encryption

Analysis By: Brian Lowans, Joerg Fritsch

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition

Format-preserving encryption is used to protect data at rest and in use, and when it’s accessed through applications, while maintaining the original data length and format. It’s used to protect fields in a growing number of databases and document types on-premises and on public cloud services. FPE is an important anonymization technique for data protection and privacy, minimizing the risks of hacking or insider threats, and compliance requirements to control access by administrators and users.

Why This Is Important

FPE can be used to protect data at the point of ingestion, storage in a database or access through applications. It is increasingly being deployed to protect data stored or processed across a variety of databases and selected document types on-premises or on cloud service platforms (CSP). However, it is still a blunt-force access control, and, when applied, it will protect data wherever it resides or accessed.

Business Impact

The NIST standard for FPE has enabled its acceptance by organizations to address evolving compliance and threat landscapes without having to extensively modify databases or applications. It provides a strong, agile method to prevent unauthorized user access to data on-premises and in public CSPs. This helps meet data protection and privacy regulations and data residency requirements to protect personal, health, credit card and financial data, and to adhere to data breach disclosure regulations.

Drivers

- Adoption is increasing due to the fast-growing need to provide data protection and privacy, in compliance with legislation such as the General Data Protection Regulation (GDPR).

- Organizations increasingly need to analyze data, while keeping it anonymized.

- The ability to mix the implementation of FPE with data masking is also increasing its dynamic adoption for different use cases.

Obstacles

- Security is frequently not coordinated across all data silos, resulting in alternative clear-text access to sensitive data in other data stores not secured with FPE.

- Conflict of interest could be an issue; for example, database administrators or application owners that have been loaded with security responsibilities without thinking about the proper segregation of duties (SOD) of database administrators (DBA) from security controls.

- Encryption keys not managed by resilient life cycle best practices and enterprise key management (EKM) could lead to the loss of larger amounts of data if the encryption keys are lost.

User Recommendations

- Deploy FPE to implement policy rules for user access in coordination with other security controls, according to Gartner's data security governance (DSG) framework.

- Review how FPE interacts with applications, and establish whether user identities can be employed to approve where fields are decrypted.

- Evaluate the impact on performance and functionality of applications accessing the database.

- Be aware that application and database functionality, such as sorting, can be affected.

- Monitor and audit all user and administrator access to sensitive data, even when FPE is deployed.

- Augment the data security strategy with data loss prevention (DLP) where feasible to monitor data movement across endpoints after it has been accessed from a database.

Sample Vendors

Baffle; comforte; IBM; Micro Focus; Oracle; PKWARE; Prime Factors; Protegrity; SecuPi; Thales

Gartner Recommended Reading

Use the Data Security Governance Framework to Balance Business Needs and Risks

Develop an Enterprisewide Encryption Key Management Strategy or Lose the Data

Protecting PII and PHI With Data Masking, Format-Preserving Encryption and Tokenization

Select the Right Key Management as a Service to Mitigate Data Security and Privacy Risks in the Cloud

Better Safe Than Sorry: Preparing for Crypto-Agility

Cloud WAAP

Analysis By: Jeremy D'Hoinne, Adam Hils, John Watts, Rajpreet Kaur, Shilpi Handa

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition

Cloud web application and API protection (WAAP) products are cloud-delivered multifunction web application security products, integrating at least four core features: web application firewall, DDoS protection, bot management and API protection. WAAP is an evolution of the role of the web application firewall, driven by enterprises' need to better defend against multiple threat vectors while significantly growing their number of publicly exposed web applications and APIs.

Why This Is Important

Organizations moving critical web applications to the public cloud frequently select cloud WAAP solutions from WAF, CDN or infrastructure-as-a-service (IaaS) providers to shield these applications. These solutions can be delivered and managed more flexibly than a traditional virtual appliance due to their ability to be easily deployed. Cloud WAAP roadmaps are dynamic and continue to improve their detection capabilities and the maturity of their management and monitoring consoles.

Business Impact

Public-facing web applications are at high risk of breach. As more and more critical business processes and sensitive data are hosted on these applications, protecting them becomes paramount. Cloud WAAP solutions can also be deployed more easily and managed more efficiently than their WAF appliance counterparts. The value of cloud WAAP goes beyond the bundling approach, with potential benefits from the global visibility provided by cloud deployment.

Drivers

Cloud WAAP simplifies the deployment of runtime application security controls in front of one or many applications. For smaller organizations, compliance requirements represent a primary driver for deploying WAAP in front of public-facing applications. Digital natives, B2C verticals (e.g., retail) and global organizations deploy cloud WAAP to protect assets that they consider critical. In addition to the web application firewall, they value the three other core features of cloud WAAP:

- **Protection against denial of service:** This is important to avoid denial of service attacks, which could impact the business and hurt the brand.

- **Bot mitigation:** This is especially important for the online retail, gaming and travel industries, but all verticals gain from better understanding the impact of automated traffic on their applications.

- **API protection:** Security teams might not have full visibility on it, but a growing share of web application traffic is API-driven. Dedicated controls are required to protect API, and some cloud WAAP providers are focusing on this issue.

Obstacles

The most frequent obstacles facing organizations selecting a cloud WAAP solution are:

- **Privacy-related:** Compliance requirements or fear of legal issues or complex project approval can be issues for organizations. Some organizations don’t trust the cloud to decrypt and log the application traffic and host related secrets.

- **Due to existing applications:** Some organizations face issues because of an existing on-premises or hybrid web application deployment. They prioritize unified management and monitoring, or don’t want to embark on a new learning curve when they are satisfied with their existing products.

- **Cost:** WAAP as a feature of an ADC might be less costly than a cloud WAAP solution, especially when including the cost of switching to a new architecture.

- **Regional support:** The availability of skilled and experienced support teams might vary for the more recent cloud WAAP products in regions not well supported by vendors, or when no PoPs are located near the organization’s origin servers.

User Recommendations

Prospective buyers should:

- Build their application security strategy for the present and the future of their application architecture by applying a cloud-first strategy or “follow the app” principle when deciding between on-premises WAF appliance and cloud WAAP.

- Carefully evaluate the expected benefits and challenges of cloud WAAP. This includes simplicity, data privacy, DDoS protection, bot mitigation and API security, as well as deployment challenges such as certificate management for TLS decryption.

- Continue to improve their stance against bots and other automated attacks by measuring the efficacy of existing controls and adding new techniques when results decline.

- Implement products with automated API discovery and anomaly detection. Note that many WAAP solutions do not yet offer best-of-breed API security capabilities; compare them with offerings from dedicated API security vendors.

- Consider integrations with API gateways or vendors that provide gateways which help with

API management.

Sample Vendors

Akamai; Barracuda Networks; 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

Content Disarm and Reconstruction

Analysis By: Mark Harris, Neil MacDonald

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition

Content disarm and reconstruction (CDR), also referred to as "content sanitization," breaks down files into their discrete components, strips away anything that doesn't conform to that file type's original specification/ISO standard, removes any content that could be malicious (macros, links, embedded objects), and rebuilds a sanitized version.

Why This Is Important

CDR protects against exploits and weaponized content without the need for lengthy dynamic analysis or traditional content inspection techniques (such as signatures) for identifying malicious content. This is particularly useful where files are crossing organizational boundaries such as email, web and file content sharing sites.

Business Impact

CDR is an important layer in any organization's defense-in-depth and content protection strategies. It:

- Significantly reduces the risk of malicious content entering an organization, for example, via email, by removing active content such as macros, which is one of the most common infection vectors and hard to deal with in other ways.
- Is much faster than sandboxing, and therefore makes a good complementary solution.

Drivers

- Remote working has increased the need to ensure files and documents are sanitized before being shared internally, driving adoption of CDR.

- CDR sanitizes content when files are crossing data boundaries. Some examples are email attachments, web downloads, users uploading content like application forms, resumes or CVs, and sharing or receiving documents from other untrusted sources.

- Some secure email and web gateways as well as content collaboration platforms already include such capabilities, either built in-house, OEM’d or at additional cost via a third-party license, which is helping to drive adoption.

- The speed of CDR complements dynamic analysis in sandboxes, which is notoriously slow. As a result, users can see a sanitized attachment immediately and can request the original after an integrated sandbox has finished its processing.

- CDR neutralizes all potentially malicious content, without requiring multiple rounds of antivirus scanning or sandboxing.

- CDR serves as a strong and low-latency alternative to sandboxing and multi-AV in all malware prevention scenarios where files (typically Office, PDF and multimedia) move from an untrusted to a trusted environment.

Obstacles

- The use of CDR can decrease document usability by stripping out active code that is intended for legitimate purposes. Some solutions hold the original file in quarantine if its functionality is broken, in addition to more granular control over what is removed, but this can decrease the value CDR provides.

- Since CDR does not rely on detection, it can be challenging to demonstrate effectiveness without additional, retrospective analysis of content.

- Most CDRs do not identify malicious actors or malicious intent. Such information can be useful in understanding the organizational risk posture.

- Awareness of CDR technology is still low, inhibiting broader adoption.

- CDR is only useful for specific file types.

User Recommendations

- Protect against inbound threats from malicious documents by considering CDR as part of your email and web security strategy.

- Use CDR as an alternative to sandboxing and multi-AV scanning, to ensure files and documents shared or received from untrusted sources are free of malware.

- Use CDR in conjunction with sandboxing solutions to allow sanitized documents to be available immediately while the sandbox analysis completes.

- Use CDR to sanitize content in high-security environments, to ensure tracked changes, internal comments, etc., are removed before sharing.

Sample Vendors

Check Point Software Technologies; Fortinet; Glasswall; HelpSystems; OPSWAT; Sasa Software; Votiro

Gartner Recommended Reading

Market Guide for Email Security5 Core Security Patterns to Protect Against Highly Evasive AttacksMagic Quadrant for Secure Web Gateways

Remote Browser Isolation

Analysis By: Neil MacDonald, John Watts

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition

Remote browser isolation (RBI) separates the handling 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 an organization’s attack surface, as a large number of attacks have shifted to users and endpoints. When used to protect sensitive data and applications from untrusted devices, RBI helps to reduce risk when BYOD is used.

Why This Is Important

SWGs are useful, but attacks will get through. Rather than letting in potentially hostile content from the internet to be executed on the endpoint via a web browser, browser isolation strategies keep the session isolated (similar to VDI, but for the browser session). RBI also works in the reverse direction, protecting sensitive data and applications from attack by an unmanaged and potentially infected device in use cases such as SaaS access via a CASB or internal application access via ZTNA.

Business Impact

Most attacks are delivered via the public internet, through either web browsing or emailed links that trick the user into visiting malicious sites. Simply removing (or, more strongly, isolating) the browser from the end user’s desktop significantly improves enterprise security posture, including protection from ransomware attacks. RBI protection can also extend to internal private applications and SaaS applications from unmanaged devices and thus reduce the threat of data exfiltration.

Drivers

- Static signatures of bad sites in the form of URL blocklists can fail and are too slow to stop targeted attacks.

- Blocking uncategorized sites can hurt the end-user experiences.

- The shift to remote work accelerated by COVID-19 has increased the usage of unmanaged devices. RBI provides a way to introduce a control point for unmanaged devices for things such as sensitive data protection, and CASBs and ZTNA offerings are using RBI for exactly that.

- Email-based URLs that resolve externally are often used to phish employees. Isolating these can reduce successful phishing attacks.

- SASE has combined a set of access capabilities from the cloud, including SWG, CASB and ZTNA. RBI adds value in all these SASE use cases and is becoming a common feature of these products.

- RBI is cheaper than using VDI for isolation if the only application being isolated is the browser.

Obstacles

- User experience is the single greatest obstacle to adoption. Standardization on Chromium as the rendering engine helps with most issues; however, concerns remain about latency and bandwidth impacts on the user experience.

- Localization of the browsing experience requires IP address assignments to be regionally combined with either VPN exit points or local POPs.

- RBI potentially has a high cost. Someone has to pay for the CPU and bandwidth costs necessary for the remote rendering if RBI is delivered as a cloud-based service.

- Most RBI offerings are software-based and delivered from the cloud. Some companies will prefer to run the RBI solution themselves. Further, some defense and intelligence scenarios may benefit from stronger isolation of a hardware-based RBI approach versus software-based.

User Recommendations

- Evaluate and pilot a browser isolation 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.

- Pressure your SWG, CASB, ZTNA and/or SEG vendor to provide RBI as an optional defense-in-depth protection option.

- For threat protection, start with 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 based on performance and bandwidth.

- Evaluate different vendor approaches for rendering (e.g., pixel streaming, vector-based) based on performance, latency and bandwidth requirements.

- Design and implement a capability for moving content from the public internet into enterprise systems, but only after intensive scanning using multilayered threat detection techniques.
- Sign one- to two-year contracts only; the market is in flux, with downward pricing pressure.

Sample Vendors

Authentic8; Cloudflare; Ericom; Forcepoint (Cyberinc); Garrison; McAfee; Menlo Security; Proofpoint; Symantec (Broadcom); Zscaler

Gartner Recommended Reading

2021 Strategic Roadmap for SASE Convergence

Magic Quadrant for Secure Web Gateways

Magic Quadrant for Cloud Access Security Brokers

Quick Answer: Cost-Effectively Scaling Secure Access While Preparing for a Remote Workforce

Quick Answer: How to Securely Enable Access for Unmanaged Devices

The Future of Network Security Is in the Cloud

TLS Decryption Platform

Analysis By: Adam Hils, Jeremy D'Hoinne

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition

Transport Layer Security (TLS) decryption platform is a dedicated appliance (in-line or out-of-band) used to decrypt and pass TLS traffic to other traffic-processing technologies. It makes the decrypted traffic available to multiple stand-alone security inspection solutions, then encrypts the traffic before the traffic proceeds to its final destination. TLS decryption platform can be used to decrypt inbound and outbound traffic.

Why This Is Important

As an ever-greater percentage of inbound and outbound traffic is encrypted, security and risk management leaders must consider how to gain visibility into potentially malicious traffic.

Business Impact

This technology can solve visibility issues in organizations outside of highly regulated nations. In nations with data privacy and data sovereignty laws, decisions to decrypt must be coordinated with legal and HR. Enterprises tolerant of additional appliances can use a dedicated TLS decryption platform for greater visibility necessary to protect their data and let other security tools inspect traffic. Midsize enterprises are likely to leverage existing solutions to solve visibility problems.

Drivers

- TLS decryption platforms are maturing as organizations realize the importance and complexity of building a TLS decryption strategy.

- Specialized TLS decryption platforms are being adopted as security and risk management leaders are grappling with issues raised by the growing amount of HTTPS traffic traversing their networks. Traditional IPS and anti-malware solutions can’t detect encrypted threats. Without a systematic decryption strategy, enterprises risk data loss by exposing their infrastructure to targeted malware campaigns.

- Ransomware that leverages encryption for malware delivery and command-and-control communications will have higher financial costs because of longer dwell time before detection. The value of network security controls will decrease because of encrypted web traffic blindness, further driving adoption of TLS decryption platforms.

- TLS decryption solutions are now able to fully support decryption of TLS 1.3 traffic.

Obstacles

- Local regulations or enterprise culture might hinder the decryption project as decrypting HTTPS creates privacy challenges for monitored employees.

- Decryption architecture might degrade user experience, introducing poor performance and unexpected blocking of legitimate business applications (e.g., TLS 1.3 enforces perfect forward secrecy [PFS], making off-box decryption and encryption impossible using the original encryption key).

- Decryption costs increase the average cost per user but organizational perception of value is still low, so some organizations choose to decrypt traffic within the existing edge firewall, secure web gateway deployments or at the application delivery controller (ADC) level.

- Cloud proxies can decrypt web-bound traffic at a scale impossible for appliance-based decryption solutions. In addition, network detection and response (NDR) solutions can either decrypt internal traffic themselves or detect malicious traffic without decryption.

- Some solutions provide threat detection inside encrypted traffic without first decrypting it (e.g., Cisco's Encrypted Traffic Analytics [ETA], part of its Stealthwatch solution).

User Recommendations

- Track the mix of traffic within the organization to estimate the impact of encrypted traffic on network security controls.

- Check with business leaders to see what the organization's tolerance is for outbound TLS decryption.

- Assess organizational and regulatory constraints to ensure compliance with privacy laws.

- Decide whether to decrypt with existing network security appliances, with a cloud-based proxy or with dedicated decryption appliances.

- Review log policy for each part of the decryption infrastructure to avoid unwanted logging of confidential data and sensitive PII, and ensure encryption keys are stored and managed in a secure way.

Sample Vendors

A10 Networks; Array Networks; Broadcom; Gigamon; Keysight

NSPM

Analysis By: Rajpreet Kaur, John Watts, Adam Hils

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition

Network security policy management (NSPM) tools offer centralized network security policy management, orchestration and auditing capabilities which go beyond firewall rules, and extend to hybrid environments, hence simplifying the management of network security policies across environments.

Why This Is Important

The NSPM tools can play an important role by offering centralized visibility and policy workflow management in a hybrid network security architecture. NSPM provides analytics and auditing for rule optimization, change management workflow, rule testing, application connectivity, compliance assessment and visualization, often using a visual network map of network security devices and firewall access rules overlaid onto multiple network paths.

Business Impact

As enterprises adopt hybrid environments, these tools can offer centralized management and visibility across platforms capable of integrating with different technologies and native policies using APIs. The API-based integration can also be used to achieve security automation with CI/CD pipelines. These tools already have an established market in management of multiple firewalls, continuous audit and compliance of network security policies and related use cases as defined below.

Drivers

- As the networks have evolved and the majority of the enterprises today are running across hybrid environments, it is making network security architecture more complicated than ever. With stand-alone network security vendors and native security policies, to multiple teams trying to automate their processes, network security has never been more overwhelming. NSPM tools can help simplify by offering centralized management of network security policies across these hybrid environments. This, in turn, helps the network security teams work toward achieving segmentation using the API integration capabilities with different vendors/technologies in the network security architecture.

- While the above mentioned is the primary driver today, following are adoption drivers:

- Centralized management of multiple/multibrand firewall rules
- Visibility and management of network security policies across hybrid networks and multicloud environments
- API-based segmentation
- Continuous audit and compliance of security policies
- Change management and automation of network security operations
- Migration of firewalls
- Continuous network security risk analysis and vulnerability assessment
- Application connectivity management
- DevSecOps

Obstacles

- **End user perception:** As the primary use case of NSPM tools has been management of firewall rules and auditing, the end users fail to recognize the border scope of features these tools offer beyond traditional use cases.

- **Integration challenges:** Since the foundation of NSPM tools is integration with multiple different vendor products and APIs, end users often complain they bump into integration issues when the integrated products undergo a firmware upgrade.

- **Overlapping markets:** As vendors are trying to offer multiple different overlapping features, the NSPM market capabilities overlap with markets such as CSPM, firewall-centralized managers and vulnerability management.

- **Cloud support:** NSPM vendors have failed to offer mature features to support multicloud environments, compared to CSPMs with limited support for limited vendors. The vendors now wait for the demand from their end-user installed base to develop the support or feature.

User Recommendations

NSPM tools have potential to meet multiple network security and application management use cases. NSPM tools have extended visibility into, and security policy management capabilities for, public and private cloud platforms such as VMware NSX, Amazon Web Services (AWS), Microsoft Azure and occasionally OpenStack. Users are advised to:

- Identify the primary and initial use case to address as the main requirement before shortlisting vendors. NSPM tools come with multiple subscriptions and associated cost.

- Identify and evaluate the API integration capability NSPM platforms offer to achieve centralized visibility and control across environments including the native network security controls implemented.

- Avoid finalizing any NSPM tool purchase without conducting a proper evaluation of the primary and adjacent use cases. Evaluation factors must include support for different network security products with their current firmware version.

Sample Vendors

AlgoSec; FireMon; Tufin; Skybox Security; SolarWinds

Gartner Recommended Reading

Technology Insight for Network Security Policy Management

NDR

Analysis By: Lawrence Orans, Jeremy D'Hoinne

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition

Network detection and response (NDR) technology uses a combination of machine learning, rule-based detection and advanced analytics to detect suspicious activities on enterprise networks. NDR tools analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NDR tools detect abnormal traffic patterns, they raise alerts. NDR solutions monitor north-south and east-west traffic. These tools also provide threat hunting capabilities.

Why This Is Important

NDR is very effective in detecting suspicious traffic on networks, such as lateral movement or data exfiltration. It focuses on detecting abnormal behaviors, with less emphasis on more traditional signature-based controls, detecting known threats. NDR solutions also provide response capabilities. Responses can be automated (for example, sending commands to a firewall to drop packets) or manual (providing tools for incident responders to search through metadata for forensic analysis).

Business Impact

NDR solutions provide visibility into network traffic. The machine learning algorithms that are at the core of many NDR products help to detect anomalous traffic that is often missed by other detection techniques. The optional automated response capabilities help to offload some of the workload for incident responders. The threat hunting functionality provides valuable tools for incident responders.

Drivers

- **Low Risk — High Reward —** Implementing NDR tools is a low risk project, since the sensors are positioned out-of-band (they are not in the line of traffic, so they don’t represent a point of failure or a “speed bump” for network traffic). Enterprises that implement NDR solutions as a proof of concept (POC) often report high degrees of satisfaction, because the tools provide much needed visibility into network traffic. The POC projects often result in the customer buying the solution, because they see value in the traffic visibility.

- **Encrypted Traffic Analysis —** As the volume of encrypted traffic grows, it becomes more challenging for traditional network security tools to analyze it. Multiple security research reports from leading vendors show growth in the frequency of instances where malware is delivered in an encrypted traffic stream. In the NDR market, vendors offer at least one of these three techniques for detecting anomalies in encrypted traffic. **JA3 signatures:** JA3 is a method of fingerprinting the handshake between a client and a server. By comparing handshakes in live traffic to the handshake patterns of commonly used applications, vendors can detect suspicious traffic. Nearly all NDR vendors support this technique. **Message lengths and time intervals between messages:** Monitoring this information is a proven technique for detecting suspicious traffic without decrypting it. Some vendors support this capability. **Traffic decryption:** Decrypting traffic so that it can be analyzed for malware is the most accurate technique, but only a few vendors support this capability.

- **Securing SaaS Applications —** Some NDR vendors offer the ability to monitor traffic destined for Microsoft 365 and other popular SaaS applications. These tools are good at detecting brute force login attempts and other suspicious behavior. Good CASB tools offer this functionality and more, but NDR vendors can add value where the customer does not already own CASB technology.

Obstacles

- NDR competes for budget with endpoint detection and response (EDR), increasingly extended detection and response (XDR) and sometimes user analytics, depending on the threat vectors that the prospective customers try to mitigate.

- 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 recent and still evolving.

- Smaller organizations do not have the staff to support and operate a detection-only tool, but struggle to accept a fully automated response.

- False positives — they are inevitable with any behavioral-based detection tool. But NDR tools, once tuned, do not exhibit a chronic problem in this area and tend to trigger a relatively low volume of alerts.

User Recommendations

- Develop a strong understanding of the overall traffic patterns and specific protocol patterns in your enterprise network to gain maximum value from NDR.

- Carefully plan sensor deployment so that the most relevant network traffic can be analyzed. Proper positioning of the NDR sensors is critically important.

- 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).

- Select sensors that are sized appropriately for your network. Some vendors offer sensors that support up to 100 Gbps of line rate capture, whereas other vendors’ sensors can only scale up to 10 Gbps.

Sample Vendors

Arista Networks; Cisco; Darktrace; ExtraHop; Fidelis Cybersecurity; FireEye; Gigamon; Plixer; Vectra; VMware

Gartner Recommended Reading

Market Guide for Network Detection and Response

Climbing the Slope

ZTNA

Analysis By: John Watts, Lawrence Orans, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition

Zero trust network access (ZTNA) creates an identity- and context-based logical access boundary around applications. Applications are hidden from discovery and access is restricted via a trust broker to a set of named entities. The broker verifies identity, context and policy adherence of specified participants and devices before allowing access, and prohibits lateral movement in the network. This removes public visibility of applications and significantly reduces the attack surface area.

Why This Is Important

ZTNA is a key technology for enabling user-to-application segmentation through a trust broker, to enforce a security policy that allows organizations to hide private applications and services and enforces a least-privilege access model for applications. It is a synthesis of concepts in the Cloud Security Alliance’s Software-Defined Perimeter (SDP) guide, Google’s BeyondCorp vision and O’Reilly’s Zero Trust Networks book.

Business Impact

ZTNA yields immediate benefits by shielding services from attackers. In contrast to basic VPN products, ZTNA removes full network access and improves user experience, flexibility and adaptability. It enables more granular user-to-application segmentation through simplified policy management. Cloud-based ZTNA offerings improve scalability and ease of adoption. Early products on the market focused on web applications, but have expanded to work with a wider range of applications and protocols.

Drivers

- The need to support digital business transformation scenarios ill-suited to legacy access approaches, such as access to applications, services and data located outside the enterprise.

- Need for flexibility to quickly expand capacity as the sudden shift to remote work in 2020, with the onset of the COVID-19 pandemic, strained legacy on-premises VPN infrastructure.

- The rise of zero trust initiatives within organizations, which resulted in the need for more precise access and session control in on-premises and cloud applications.

- A desire for vendor consolidation, to remove point solutions and adopt more products from vendors with SASE frameworks, resulting in ZTNA additions to existing SWG or CASB services.

- A need to connect third parties such as suppliers, vendors and contractors to applications securely without exposing the network over VPN, or to connect the application to the internet for access.

- Mergers and acquisitions enabled by the ability to extend application access to acquired companies preclosure without needing to deploy endpoints or connect networks directly between the two companies.

Obstacles

- Cost: ZTNA is typically licensed per named user on a per user per year basis and may cost more than traditional VPNs.

- Limited support: Not all products support all applications. For example, some only support web, RDP and SSH protocols.

- Agent or agentless ZTNA: Some providers only offer one way to consume ZTNA. This limits applicable use cases.

- Weak identity management: Organizations with no federated identity support in the cloud find limitations with use cases as many providers rely on third-party identity providers for user authentication.

- Lack of on-premises trust brokers: Cloud-based trust brokers work well for remote access, but may not be preferred to extend the same policies on-premises. While providers exist that have both cloud and on-premises trust brokers, they are far and few between.

- Limited knowledge of acceptable application access rights for users: Organizations must map the correct application accesses upfront to get full benefit of ZTNA.

User Recommendations

- Open applications and services without requiring the use of a VPN or DMZ.
- Normalize the user experience for application access both on and off the corporate network.
- Implement application-specific access for employees and IT contractors as an alternative to VPN-based access.
- Extend access to systems prior to a merger, without having to configure site-to-site VPN and firewall rules.
- Allow access on personal devices by reducing full bring your own device (BYOD) management requirements and enabling more secure direct application access.
- Cloak systems from hostile networks, such as collaboration systems exposed to the internet.
- Permit users in potentially dangerous areas of the world to interact with applications and data to reduce or eliminate risk.

- Secure access to enclaves of Internet of Things (IoT) devices if the device can support a lightweight SDP agent or a virtual-appliance-based connector on the IoT network segment for connection.

Sample Vendors

Akamai; Appgate; Cato Networks; Ivanti; Netskope; Perimeter 81; Proofpoint; SAIFE; Zscaler

Gartner Recommended Reading

Market Guide for Zero Trust Network Access

Solving the Challenges of Modern Remote Access

Quick Answer: Cost Effectively Scaling Secure Access While Preparing for a Remote Workforce

Quick Answer: How to Securely Enable Access for Unmanaged Devices

2021 Strategic Roadmap for SASE Convergence

Enterprise Key Management

Analysis By: Brian Lowans, David Mahdi, Joerg Fritsch

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition

Enterprise key management (EKM) provides a single, centralized software or hardware appliance for multiple symmetric encryption- or tokenization-based cryptographic solutions. Critically, it enforces consistent data access policies across different structured and unstructured storage platforms, on-premises and in public cloud services. It facilitates key distribution and secure key storage, and maintains consistent key life cycle management.

Why This Is Important

Cryptographic products that implement encryption or tokenization are critical components of a data security strategy to solve for growing data residency risks, meet privacy requirements and prevent data breaches/theft due to hacking, malicious insiders or accidental disclosure. Cryptographic products require EKM to provide consistent key life cycle management to help mitigate these risks and reduce the risks of accidental shredding of data in case keys are lost.

Business Impact

EKM can enable an enterprise strategy, while limiting risk as well as reducing operational and capital costs. Enterprises can purchase specialized products that cryptographically protect data across various on-premises and multicloud data repositories and processes, as well as native platform cryptographic products. This will result in many independent key management consoles that do not integrate, and increase the risk of a security or compliance incident.

Drivers

- Cryptography is important for access control and EKM policies define the granularity of protection applied, typically linked to active directory.

- EKM is a means to ensure access controls are applied consistently across a variety of storage platforms. This is done by enabling cryptography to protect the data in storage only, protect individual files, or protect fields stored within or accessed from SQL and NoSQL platforms.

- Increasingly, EKM can also be deployed with privacy-enhanced computation technologies.

- EKM is increasingly required to enforce enterprisewide data security governance (DSG) policies that complement a broader set of product controls, such as database activity monitoring (DAM), data access governance (DAG), data loss prevention (DLP) and identity and access management (IAM).

- EKM is increasingly evolving to provide an enterprisewide plan for disaster recovery situations throughout the key life cycle, including key backup, recovery, escrow processes or changes to algorithms.

- There is a growing need to provide consistent implementation of encryption-based data access policies across different silos, such as databases, file shares, big data and multicloud environments.

- The use of a single EKM product greatly simplifies the ability to provide consistent key management policies and data access policies across disparate data silos and multicloud architectures.

- EKM reduces the number of vendors and native key management products in use, if storage and self-encrypting-drive vendors (that do not offer EKM products) are complying with the Key Management Interoperability Protocol (KMIP) standards.

Obstacles

- EKM products typically comply with KMIP standards sponsored by OASIS. However, cryptography products typically do not comply with KMIP. This means that cryptography products cannot be managed by a different vendor's EKM.

- A number of storage platforms provide their own native encryption offering that may require custom integration to vendor EKM solutions. This makes implementation of EKM a huge challenge in the wake of many incompatible products and disparate native platform encryption offerings managed by a variety of nonsecurity administrators.

User Recommendations

- Focus on reducing the number of cryptographic products deployed by different vendors.

- Ensure your EKM capabilities can manage third-party cryptography or native products compliant with KMIP.

- Ascertain your vendors support cloud-native key management solutions, which use proprietary interfaces requiring integration with key management as a service (KMaaS) solutions using customized bring your own key (BYOK) integrations with each cloud service.

- Assess whether EKM should be deployed as a software or a hardware appliance. It can achieve a security-accredited standard under NIST FIPS 140-2, ranging from Level 1 (software lowest security) to Level 3 or 4 (pure implementation or integration to a hardware security module).

- Review each vendor's EKM ability carefully to operate across various structured and unstructured data storage platforms that require protection.

- Be careful when selecting EKM and cryptographic products from multiple vendors. EKM vendors rely on a protectionist strategy and their products do not typically integrate with other vendors' cryptographic products.

Sample Vendors

Fortanix; IBM; Micro Focus; PKWARE; Protegrity; QuintessenceLabs; StorMagic; Thales

Gartner Recommended Reading

Use the Data Security Governance Framework to Balance Business Needs and Risks

Develop an Enterprisewide Encryption Key Management Strategy or Lose the Data

Select the Right Key Management as a Service to Mitigate Data Security and Privacy Risks in the Cloud

Identity-Based Segmentation

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

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition

Identity-based segmentation (also referred to as microsegmentation, zero-trust network segmentation or logical segmentation) can create more granular and dynamic policies than traditional network segmentation, which is limited to IP/VLAN circuits. “Identity-based” refers to workload identity, not user identity.

Why This Is Important

Certain attacks — such as ransomware attacks — can cause serious damage if allowed to spread laterally. Identity-based segmentation seeks to limit the propagation of such attacks.

Business Impact

Identity-based segmentation can reduce the risk and impact of cyberattacks. Identity-based segmentation is a form of zero-trust networking and is used to reduce the damage if and when an attacker breaches the enterprise network. This is done by reducing the ability of the attacker to spread laterally. Identity-based segmentation also enables enterprises to enforce consistent segmentation policies across on-premises and cloud-based workloads, including workloads that host containers that meet compliance requirements.

Drivers

- As more servers are being virtualized or moved to infrastructure as a service (IaaS), traditional firewall, intrusion prevention, and antivirus are rarely able 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.

- The increasingly dynamic nature of data center workloads makes traditional network-centric segmentation strategies operationally complex, if not impossible to apply.

- Some identity-based segmentation solutions provide rich application communication mapping, allowing data center teams to identify where 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 complicated the ability of network-centric firewalls to provide this segmentation.

- The extension of data centers into public cloud has also placed a focus on software-based approaches for segmentation — in many cases, using the built-in segmentation capabilities of the 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

The most frequent obstacles to identity-based segmentation are:

- Complexity: If not planned and scoped correctly, identity-based segmentation 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 firewall 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.
- 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 identity-based segmentation to be a net new budget item.

User Recommendations

- Use a network flow mapping project to understand application and server flows.

- Start small and iterate with basic policies. Oversegmentation is the leading cause of failure and an unnecessary expense for segmentation projects.

- 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 ID-based segmentation style (agent-, network- or hypervisor-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).

- Apply continuous adaptive segmentation. Start with new assets, then close existing gaps. Identify quick wins, and mix zoning governing principles when needed.

- Adopt a risk-based approach and look beyond technical considerations.

- Consider products with established security expertise. Isolation alone isn't segmentation. If mediated communication is needed between zones, different functionality is required.

- Plan for coexistence of traditional firewalls and ID-based segmentation approaches for the next five years, and seek products that can support using both.

Sample Vendors

Amazon Web Services; Cisco; ColorTokens; Guardicore; Illumio; Microsoft; Palo Alto Networks; vArmour; VMware; Zscaler

Gartner Recommended Reading

Three Styles of Identity-Based Segmentation

SD-WAN

Analysis By: Andrew Lerner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition

Software-defined wide-area network (SD-WAN) products replace traditional branch routers. They provide dynamic path selection based on business or application policy, centralized policy and management of appliances, VPN, and zero-touch configuration. SD-WAN products are WAN transport/carrier-agnostic, and can create secure paths across multiple WAN connections. SD-WAN products can be hardware- or software-based, and managed directly by enterprises or embedded in a managed service offering.

Why This Is Important

SD-WAN improves site availability, cost and performance for enterprise WANs, and is aligned with the broader shift of applications to public cloud workloads. There is high client interest in SD-WAN products, and we estimate that more than 50,000 customers have deployed SD-WAN products in production networks. Further, we expect continued rapid growth of SD-WAN deployments, and forecast vendor revenue to grow at a more than 20% compound annual growth rate (CAGR) for the next three years.

Business Impact

SD-WAN products create simpler and more cost-effective branch office WANs that map to modern application and cloud architectures.

These products are significantly faster, easier to deploy and more manageable than traditional, router-based solutions. The benefits of an SD-WAN include reduced capital and operational expenditures (capex/opex) at the WAN edge, reduced device provisioning times, easier alignment with applications, and enhanced branch availability, compared with traditional routers.

Drivers

- Digitalization and cloud adoption are driving more applications out of private data centers and to public Internet, including SaaS and public cloud providers.

- In conjunction with hybrid or all-internet WAN topologies, SD-WAN improves availability, cost and performance for enterprise WANs.

- Organizations moving to hybrid or internet-only WAN transport are driven toward SD-WAN products because of their improved path-selection functionality and manageability.

- Several dozen vendors are competing in the market, including incumbent network and security vendors, startup vendors and smaller vendors with a regional or vertical focus. These vendors are aggressively pushing SD-WAN products and services to enterprises.

Obstacles

- Inability to get out of an existing equipment or service provider contract.
- WAN architecture is not hybrid and/or branch locations have only a single connection.
- Lack of budget.
- Closure of remote locations due to broader business reasons.
- Lack of cloud adoption, which reduces the benefits of hybrid WAN architectures.
- Limited need for increased branch availability.
- Inability to utilize the internet as transport, often due to compliance or security concerns, or lack of reliable connectivity.
- Existing WAN edge products (firewalls/routers) are good enough to meet business requirements.

User Recommendations

- Refresh your branch WAN equipment by implementing SD-WAN when you're migrating apps to the public cloud, building hybrid WANs, equipment is at end of life, or managed network service/MPLS contracts are renewing.

- Follow a thorough SD-WAN selection process by shortlisting a diverse set of vendors/providers and running a pilot.

- Include network security teams in the design, planning and implementation, because SD-WAN-enabled hybrid WANs directly affect placement of security controls, such as firewalls and secure web gateways (SWGs). SD-WAN should be designed in conjunction with a SASE architecture.

Sample Vendors

Cisco; Citrix; Fortinet; Hewlett Packard Enterprise (HPE); Palo Alto Networks; Versa Networks; VMware

Gartner Recommended Reading

Magic Quadrant for WAN Edge Infrastructure

Critical Capabilities for WAN Edge Infrastructure

Magic Quadrant for Network Services, Global

Toolkit: RFP Template for Managed and DIY SD-WAN Products and Services

2021 Strategic Roadmap for SASE Convergence

Secure Web Gateways

Analysis By: Lawrence Orans, John Watts

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition

Secure web gateways (SWGs) utilize URL filtering, advanced threat defense (ATD) and malware detection to protect organizations and enforce internet policy compliance. SWGs are delivered as cloud-based services, hybrid (cloud and on-premises), or as on-premises solutions only.

Why This Is Important

Because SWGs are positioned between the user and the internet, they offer valuable protection from internet-born malware. Also, the SWG dashboards and reporting tools provide visibility into users' behavior on the internet. This functionality is important to detect and investigate if an employee has violated the organization's internet usage policy.

Business Impact

Secure web gateways provide an additional layer of protection against destructive attacks, and enable safer and more efficient adoption of cloud-based services. Cloud-delivered SWGs can also reduce branch office networking costs by using commodity internet access (instead of backhauling web traffic over MPLS links to a centralized data center) and eliminating branch office firewalls. Cloud SWG services can also provide protection for mobile users that are off the corporate network.

Drivers

- The rapid adoption of SaaS and remote work is driving enterprises to migrate from on-premises appliance-based SWGs to cloud-delivered SWG services.

- The traditional WAN architecture of backhauling all traffic from remote offices to a centralized data center, where the firewall and other physical security appliances are positioned, is outdated in the SaaS era.

- Today, enterprises want to send traffic directly from the remote office to SaaS apps and other destinations on the internet.

- The new WAN architecture (direct to the internet) requires a cloud-based security stack (the SWG is the foundation) that is positioned between the user and the internet.

- As enterprises consume more and more cloud-based security services, they are increasingly looking to consolidate security vendors.

- Operationally, it is very challenging to manage multiple cloud security services. For example, if you have three cloud security services, each will likely require its own endpoint agent and its own network tunnel to direct traffic from the laptop to the cloud service.

- It's much easier to subscribe to a single cloud security service that provides multiple security services (the most common services are SWG, cloud access security broker [CASB] and zero trust network access [ZTNA]).

- Additional security services include firewalls as a service (to apply policies to all ports and protocols), data loss prevention, sandboxing and remote browser isolation.

- SWG vendors and CASB vendors are encroaching on each other's turf and are adding additional security services to address the threat of vendor consolidation.

Obstacles

- Firewall vendors that offer low-cost basic URL filtering (not complete SWG functionality) often compete against SWG vendors.

- Cloud-based recursive DNS solutions have also become a popular solution with mid-market customers, as they offer cost-effective security protection.

- Some of the DNS services use selective proxying — they proxy traffic destined for suspicious websites (typically, about 10-15% of the traffic is proxied).

- Because the DNS services don't proxy all of the traffic all of the time, they offer inferior security protection when compared to services that use the full proxy model.

- Some industry verticals that are cloud averse have resisted migrating their on-premises SWGs to the cloud. This is particularly true in the financial services and healthcare verticals.

- The Middle East region has been slow to migrate on-premises proxies to the cloud.

User Recommendations

- Take a fresh look at the SWG Market as opposed to automatically renewing traditional approaches.

- Seek out critical capabilities such as purpose-built cloud solutions, advanced threat protection (for example, sandboxing), and CASB services to control and monitor access to SaaS and data center applications.

- Replace branch office firewalls with cloud-based outbound firewall services.

- Examine ZTNA functionality (primarily implemented as an alternative to traditional virtual private networks [VPNs]), as it is available as a feature from leading SWG vendors.

Sample Vendors

Cisco; ContentKeeper; Forcepoint; iboss; McAfee; Menlo Security; Netskope; Sangfor Technologies; Symantec (Broadcom); Zscaler

Gartner Recommended Reading

Magic Quadrant for Secure Web Gateways

Critical Capabilities for Cloud-Based Secure Web Gateways

Using Secure Web Gateway Technologies to Protect Users and Endpoints

Hardware-Based Security

Analysis By: Neil MacDonald, Tony Harvey

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition

Hardware-based security uses chip-level techniques for the protection of critical security controls and processes in host systems independent of OS integrity. Typical control isolation includes encryption key handling, secrets protection, secure I/O, process isolation/monitoring and encrypted memory handling.

Why This Is Important

Adoption is increasing as hardware-based isolation capabilities are becoming standard in most hardware devices and cloud-based IaaS offerings, including emerging confidential computing offerings. These approaches strongly isolate parts of the system (and typically its security controls) from a breach of the application or OS. Interest in strong isolation techniques is rising in the face of ongoing disclosures of new types of side-channel attacks and requirements for cloud and data sovereignty.

Business Impact

If an OS is compromised, its security controls can be disabled and sensitive data in memory stolen; hardware-based security can prevent this. Hardware-based security can significantly reduce attack surfaces across computing devices, but these capabilities require support from operating system software and system management software. Upgrading to more recent versions of software and cloud providers, which use hardware-based security features, can materially increase system security.

Drivers

- The desire to extend trust from the hardware level of a system through the OS to applications and workloads, including containers that run above it. This root of trust needs a strong foundation in hardware.

- Software-based isolation of security controls is inevitably fallible and will be attacked, increasing interest in protection approaches rooted in hardware.

- The desire to use IaaS providers in potentially hostile parts of the world and protect these workloads from OS compromise or virtual machine and memory snapshotting is increasing.

- Most hardware platforms for servers and mobile devices, including Android and iOS devices, now include hardware-based isolation capabilities.

- Requirements for data sovereignty enabled by public cloud confidential computing offerings are driving demand for isolation approaches rooted in hardware.

Obstacles

- In public clouds, enterprises don’t have access to the underlying hardware and must rely on hardware-based attestations provided by the CSP.

- Approaches to hardware-based confidential computing vary across microprocessor vendors, complicating application deployment using these techniques. No single approach covers all use cases. Abstraction layers, such as Asylo, may help but add another layer of complexity and are not widely adopted.

- Hardware-based security is strong, but may potentially still be broken by software flaws or side-channel attacks such as Spectre and Meltdown.

User Recommendations

- Patch and remain vigilant for unexpected breaches. For systems under direct enterprise control, implement a BIOS-level patching strategy to deal with exposures that require BIOS-level remediation.

- Make strong isolation of sensitive code and security controls a mandatory part of IT systems procurement, including IaaS.

- Evaluate the need for confidential computing capabilities only for the most critical applications in systems that move to public cloud infrastructure, to protect sensitive operations such as key management and sensitive intellectual property.

- Check for compatibility issues with third-party approaches that also use virtualization techniques, before activating Windows 10 virtualization-based security.

- Explore the use of hypervisor-based approaches with security rooted in hardware virtualization techniques as another way to achieve similar levels of strong isolation.

- Plan different strategies for different devices and server platforms as none of these mechanisms are interoperable.

Sample Vendors

Amazon Web Services (AWS); AMD; Apple; Bitdefender; Fortanix; Google; Hysolate; Intel; Microsoft; Samsung Electronics

Gartner Recommended Reading

Market Guide for Cloud Workload Protection Platforms

How to Make Cloud More Secure Than Your Own Data Center

Select the Right Key Management as a Service to Mitigate Data Security and Privacy Risks in the Cloud

Security Leaders Need to Do Seven Things to Deal With Spectre/Meltdown

DDoS Defense

Analysis By: Lawrence Orans, Claudio Neiva, Rajpreet Kaur

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

Definition

Distributed denial of service (DDoS) attacks use multiple techniques to disrupt business use of the internet or to extort payment from businesses to stop the attacks. DDoS defense products and services detect and mitigate such attacks.

Why This Is Important

Any website can be targeted by DDoS attackers. Attackers will sometimes target nonweb resources (such as firewalls) to disrupt users' access to the internet. DDoS mitigation services are highly effective in mitigating these attacks. For example, a good DDoS mitigation provider will restore access to a company's website, even during a large-scale attack. Enterprises that lack DDoS mitigation services could face an extended outage and could incur heavy financial losses in the event of an attack.

Business Impact

Most enterprises fall into one of two risk categories for DDoS attacks:

- High-risk enterprises are targeted on a daily or near-daily basis. Sometimes the attacks are sophisticated, which requires these enterprises to invest in best-in-class DDoS mitigation services.
- Low-risk enterprises are attacked

intermittently, possibly every 12 to 18 months. These attacks are typically unsophisticated and can be mitigated by commodity-class DDoS mitigation services.

Drivers

- The fear of a highly disruptive DDoS attack drives enterprises to adopt DDoS mitigation services.

- Enterprises seeking DDoS mitigation services that are “good enough” (to protect against typical DDoS attacks) have driven more ISPs and hosting companies to enter the market.

- Leading infrastructure as a service (IaaS) providers have expanded their DDoS mitigation offerings to include more robust, fee-based services.

- The wide availability of DDoS stressers (aka DDoS booters) is an important factor in the increasing number of attacks, thereby driving the adoption of DDoS mitigation services. These low-cost DDoS stresser services (many available for $25 per month or lower) make it easy for nontechnical individuals to launch a DDoS attack.

Obstacles

- Cost is the biggest obstacle to the adoption of DDoS mitigation services. Prices vary widely, depending upon the provider of the service. The fee-based IaaS offering is typically $3,000 per month, whereas fees for the scrubbing center services can easily exceed $10,000 per month; pricing is based on bandwidth — higher the committed information rate (CIR), higher the fee. The pricing for ISP-based services is typically 15% of the cost of the bandwidth; this fee is usually less than the scrubbing center option.

- Even the lower-cost ISP services are a significant obstacle for many enterprises.

- Complacency also impedes the adoption of DDoS mitigation services. Many enterprises choose to forgo DDoS mitigation services, hoping that they will not experience a DDoS attack. For most enterprises though, forgoing DDoS mitigation services is a high-risk gamble, given the growing spread of DDoS attacks.

User Recommendations

- Make DDoS mitigation services a standard part of business continuity or disaster recovery planning. They should be included in all internet service procurements when the business depends on the availability of internet connectivity.

- Evaluate detection and mitigation services that are available from communications service providers (CSPs), hosters or DDoS-security-as-a-service specialists (for example, “scrubbing center” providers).

- Adopt a content delivery network (CDN) approach to DDoS protection when the organization is already using a CDN for content distribution to improve the performance of its website. The CDN approach, however, only protects websites. It does not protect against attacks aimed at nonweb targets (for example, corporate firewalls, VPN servers and email servers).

- Evaluate the basic and advanced (fee-based) DDoS mitigation services of leading IaaS providers.

Sample Vendors

Akamai; AT&T; F5; Imperva; Link11; NETSCOUT SYSTEMS; Neustar; Nexusguard; Radware; Verizon Communications

Gartner Recommended Reading

Market Guide for DDoS Mitigation Services

DDoS: A Comparison of Defense Approaches

Network Firewalls

Analysis By: Rajpreet Kaur, Adam Hils

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition

The network firewall market primarily offers bidirectional controls (both egress and ingress) for securing networks and users. These networks can be on-premises, hybrid (on-premises and cloud), public cloud or private cloud. The product can support one or more firewall deployment use cases such as perimeter, SMBs, data center, cloud and distributed offices.

Why This Is Important

Despite being established and long-standing, the network firewall market has experienced constant change as the networks evolve. The market is expanding with CSPs, SASE and SD-WAN vendors introducing their native firewall offerings. The market is constantly overseeing multiple strategic acquisitions to make vendor offerings stronger to support multiple deployment use cases while often lacking mature integration between the product lines.

Business Impact

- Network firewalls continue to remain the most important security control in the network environment, keeping the business resources secure.

- They have a potential to support multiple deployment use cases as employees work from home and businesses adopt multicloud, while maintaining on-premises data centers.

- Businesses are working toward rearchitecting their infrastructure, and firewall vendor selection will play a critical role.

Drivers

- Primary growth in the market comes from renewal, but the evolving infrastructure is poised to drive even faster growth. The majority of enterprises today are hybrid, which can include on-premises data center, private cloud and multiple public clouds. All of these environments require a firewall, and this expands the scope and size of the market.

- Vendors are making acquisitions and developing related technology to thrive in all of these environments. As a result, network firewalls will gradually evolve into network security platforms by offering support for multiple use cases beyond traditional use cases such as containers, FWaaS, identity-based segmentation, multifactor authentication, SD-WAN, zero trust network access (ZTNA) and SASE across hybrid environments. These platforms must offer centralized management and mature integration to simplify the network security management and offer automation, especially with DevOps tools.

- The network firewall market is expanding beyond traditional firewall players with infrastructure vendors offering native firewall features and non-network vendors offering SASE and identity-based segmentation. This has expanded the scope of the market, leading to acquisitions and multiple feature updates. The vendors are working toward building stronger features to compete in multiple use cases.

- With employees working from home and adoption of cloud, the threat landscape continues to evolve, which is driving the firewall vendors to offer more use-case-focused threat detection and prevention capabilities such as stronger authentication, TLS decryption and mature public cloud integration.

Obstacles

- The biggest challenge this market is facing is to support hybrid environments while reducing the complexities to manage policies across them.
- Gartner still finds vendors in catch-up mode and clients struggling to secure their hybrid environment. This is due to a lack of integration capabilities with modern automation tools in the ecosystem and failure to offer centralized management of different firewall offerings vendors have to secure hybrid environments.
- Vendors are acquiring other vendors to support different firewall deployment use cases and build stronger advanced threat detection prevention and cloud security features. Thus, the firewall software and support cost is inflating, increasing the total cost of ownership of running firewalls across different environments, which is not healthy and an emerging caution.
- Traditional firewall vendors will soon face a strong pricing challenge from infrastructure vendors offering native firewall capabilities as they mature their offerings.

User Recommendations

- Keep in mind the emerging use cases of firewall deployments such as cloud firewall, FWaaS and identity-based segmentation where vendors can have use-case-based limitations; hence, you should thoroughly evaluate the offerings before buying them.

- Clients can either consolidate toward a single vendor based on the use cases that belong to them and the maturity of the vendor offering or adopt best-of-breed vendors who are mature in emerging use cases such as pure-play SASE vendors and native firewall offerings by infrastructure vendors.

- Always evaluate the TCO for five years while considering the firewall vendor — software and support costs are inflating on a yearly basis.

- Make sure the vendor offers full clarity on how the cost of enterprise license agreement (ELA) is evaluated, as vendors tend to offer bulk costs that are often confusing and might not necessarily save money.

- Always consider the vendor’s roadmap in case you want to expand a firewall’s deployment beyond traditional use cases.

Sample Vendors

Alibaba Cloud; Amazon Web Services; Barracuda Networks; Check Point Software Technologies; Cisco Systems; Forcepoint; Fortinet; H3C; Hillstone Networks; Huawei; Juniper Networks; Microsoft; Palo Alto Networks; Sangfor Technologies; SonicWALL; Sophos; Venustech; WatchGuard Technologies

Gartner Recommended Reading

Magic Quadrant for Network Firewalls

Critical Capabilities for Network Firewalls

Solution Comparison for Network Firewalls

How the Shift From Firewall Appliances to Hybrid Cloud Firewalling Will Change Selection Criteria

Entering the Plateau

IPS

Analysis By: Aaron McQuaid

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition

Intrusion prevention system (IPS) technologies provide threat detection, threat blocking, application awareness, application visibility, user visibility, and context and content awareness for networks. IPS systems support the integration of new information sources including threat intelligence, advanced threat detection, advanced analytics and network sandboxing. IPS is deployed in-line for active real-time blocking while IDS is deployed out-of-band for alerting and monitoring.

Why This Is Important

IPS has become part of the standard corporate security stack. Their deployment is widespread and will continue to be so in the near term. Enterprise organizations use IPS systems to detect and block advanced persistent threats and other malware. IPS integration with security orchestration, automation and response (SOAR) and security information and event management (SIEM) tools form a critical solution for SOC analysts, threat hunters, and incident response teams.

Business Impact

IPS improves network security by blocking attacks that are focused on exploiting vulnerabilities, or by preventing denial of service attacks. IPS systems apply deep packet inspection to real-time network traffic for detection and in-line blocking of known exploits via the use of signatures, protocol anomaly detection, and threat intelligence feeds. For unknown malware (zero day exploits) IPS systems provide some protection via the use of heuristics and file sandboxing.

Drivers

- Stand-alone IPS deployments have remained flat while integration of IPS services inside other form factors such as the network firewall and internet based secure web gateway (SWG) services has increased in recent years. IPS services will become increasingly ubiquitous in different form factors over the near to midterm.

- Stand-alone IDS deployments have also remained flat with greater focus on network detection and response (NDR) platforms gaining increased market acceptance.

- The ability to create custom signatures on most IPS platforms enables support for virtual patching, emerging threats and for threat hunting use cases. Virtual patching is a technique where a known vulnerability in a specific endpoint system is mitigated on the IPS instead of on the endpoint itself. This technique provides flexibility for endpoint teams when it becomes impractical to patch the endpoint in a timely manner.

- IPS systems are being deployed on internal networks to provide inspection services for east/west traffic. This is used as a compensating control for the “flat network” problem and can be utilized as a temporary solution while larger identity-based segmentation (microsegmentation) projects are being completed.

- IDS and IPS systems are critical tools in the network attack detection and response functions. SOC teams rely on IDS or IPS systems to accomplish their basic job functions as well as support advanced use cases like threat hunting.

Obstacles

- False positives are occasionally an issue, operationally the larger problem can be from the sheer volume of alerting that this technology can generate if end users aren’t careful on how they are tuned.

- Tuning — Clients are advised to tune their solutions to align with better pragmatic outcomes such as the vulnerabilities they have and the vulnerabilities that are being exploited in the wild. IPS remains a solution that Gartner regularly see’s as either having too many signatures turned on in the case of stand-alone IPS appliances and too little turned on in firewall based IPS.

- Encryption — Today the vast majority of user traffic is encrypted and most IPS systems are not able to detect malicious traffic if the attack payload is hidden by encryption.

- Device placement/flow ingestion — historically IPS systems have been point solutions based on a physical appliance which implied that only a single point on the network could be inspected. Today the ability to deploy virtual sensors in conjunction with an external packet broker provides greater flexibility.

User Recommendations

- Tune policy and device configuration to find the right balance between security efficacy and business agility.

- Implement a decryption solution so that the IPS can inspect traffic in the clear. Either a native option or the use of packet brokers and application delivery controllers are popular options. This is critical for the efficacy of any IPS solution since upward of 80% of traffic is encrypted in environments today.

- Leverage native decryption on a stand-alone IPS or a Firewall with IPS included in the software stack for smaller deployments.

- For larger enterprises it is recommended that physical TAPs in conjunction with a packet broker be used for IPS systems. For IDS deployments we recommend that enterprise clients utilize mirrored packet flows sourced from a Packet Broker.

Sample Vendors

Alert Logic; Cisco; FireEye; Fortinet; Lastline; McAfee; NSFOCUS; Trend Micro; Vectra; Venustech

Gartner Recommended Reading

Market Guide for Intrusion Detection and Prevention Systems

Network Access Control

Analysis By: Claudio Neiva

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition

Network access control (NAC) enables organizations to implement policies and control access to corporate infrastructure by both user devices and cyber physical devices such as the Internet of Things (IoT) and operational technology (OT) devices. Policies may be based on authentication, endpoint configuration (posture) or users' role/identity. NAC can also implement postconnect policies based on integration with other security products.

Why This Is Important

Visibility and control for access to an organization's local IT infrastructure remain part of the protection strategy to reduce the attack surface. However, the cyber-physical system (CPS) for IoT and OT devices drives specific sectors, such as manufacturing, critical infrastructure and health, to consider CPS-centric security technologies to increase NAC.

Business Impact

The NAC market is considered mature with slow growth and acquisition of existing vendors (i.e., Pulse Secure and Inverse). In addition, the primary use case for implementing NAC is visibility and access control of equipment in the local infrastructure of the organization. NAC represents an important tool to apply segmentation and isolation of endpoints that may represent a risk to the entire infrastructure.

Drivers

- Preconnect or postconnect authentication approach. The preconnect authentication can be thought of as a “guilty until proven innocent” model (“default deny”); whereas postconnect authentication can be considered an “innocent until proven guilty” model (“default allow”).

- Visibility into on-premises infrastructure connected devices with the goal of implementing access policies. This includes commonly used devices (such as a workstation, laptop, printer, IP phone, IP camera, access points and IoT devices like OT devices, medical devices and building automation).

- Management of corporate network access for different types of users and devices, such as employees, contractors, consultants and guests, using either corporate-owned or user-provided endpoints.

- Ability to analyze compliance with a minimum security posture at the endpoint and provision of a quarantine network for devices not in compliance via Change of Authorization (CoA). If not compliant, that device is only allowed access to a quarantine VLAN until those items are remediated.

- Interoperability with other security solutions. Integration with other solutions can happen in two ways: customization through open APIs or the use of built-in integration.

Obstacles

- NAC's focus is primarily as an on-premises control for devices and users, and can be expensive and difficult to implement at scale across an organization.

- NAC uniquely satisfies multiple security use cases for user and device security on the corporate network. However, depending on the organization's need, a combination of different solutions such as ZTNA, unified endpoint management (UEM) and CPS-specific security products might provide the same features and benefits as an NAC provider.

- Future security roadmaps may dictate implementation of a secure access service edge (SASE) framework that includes ZTNA products. ZTNA addresses some narrow NAC use cases for user-to-application segmentation and may influence the overall scope of an NAC implementation when considering both remote and on-premises security authentication and authorization policies for devices and users.

User Recommendations

- Focus on vendors that target organizations of your size and complexity and, in some instances, industry vertical or region. Because NAC is a mature market, many vendors are clearly aligned regarding small and midsize businesses and large-enterprise opportunities or specialize in certain industry verticals and regions such as Europe and Southeast Asia.

- Perform an initial network inventory before selecting an NAC vendor. This will influence your decision based on the capabilities of your network switches and routers, as well as help with budgeting since many NAC vendors license based on the number of IP addresses protected.

- Determine which UEM solutions are already installed on the network to identify providers that have direct integration with existing UEM solutions.

- Implement NAC to deliver visibility and control over your corporate network. Integrate with existing asset management solutions bidirectionally to help maintain an accurate list of devices connected to the organization.

Sample Vendors

Akamai; Auconet; Cisco; CommScope; Extreme; Forescout Technologies; Fortinet; Hewlett Packard Enterprise; InfoExpress; Ivanti; macmon secure; Open Cloud Factory; OPSWAT; Portnox

Gartner Recommended Reading

Market Guide for Network Access Control

Toolkit: Sample RFP for Network Access Control

Solution Path for Evolving to Next-Generation Enterprise Networks

Web Application Firewall Appliance

Analysis By: Shilpi Handa, Jeremy D'Hoinne

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition

Web application firewall (WAF) is a technology deployed in-line to protect web applications and APIs. WAF appliances focus primarily on exploits, such as cross-site scripting (XSS) and SQL injection, in commercial applications or custom-developed code. They may include protection from other attacks, such as session manipulation and logic abuse.

Why This Is Important

Organizations deploy WAF appliances to protect their traditional corporate websites, B2C and B2B web applications, as well as a growing number of API-driven applications. Large B2C applications face a higher risk of automated attacks coming from bots. Some organizations opt to host websites powered by third-party content management systems, which frequently include various vulnerabilities that might expose them to data leakage. WAF appliances are also important from a compliance perspective.

Business Impact

WAFs are used to:

- Protect data center servers and hosted applications.
- Prevent attacks that could give access to important data that often lives behind web applications.
- Provide documentation and features to support compliance requirements, such as PCI and GDPR.

Drivers

WAF appliances are quickly reaching the Plateau of Productivity. Cloud-delivered web application and API protection (WAAP) is leading the race for most of the “cloud first” strategy organizations, and COVID-19 has added velocity to its swift adoption. WAF appliances are largely adopted for specialized control and customized policy and rules development. WAF appliances remain the deployment of choice for organizations with existing deployments in the EMEA and Asia/Pacific region and for organizations that are heavily regulated and need data to reside in-house.

Obstacles

WAF appliances will see further competition this year as WAAP service providers have started to strengthen their offerings of API protection and bot mitigation and have increased the number of POPs.

The major obstacles are:

- Deploying and maintaining WAF appliances in-house is resource intensive and some organizations find this challenging
- Most WAF vendors are making R&D investment into their cloud offerings leaving many appliances lagging behind when it comes to new and advanced features

User Recommendations

Enterprises deciding on deployment options should keep in mind that:

- Appliances provide more control, and they are not dependent on the service provider’s management and maintenance of technology.

- Appliances give an option to have customized policies and in-depth rules.

- Appliances benefit customers with data privacy concerns with more control over WAF deployment location, log storage, access and retention.

- An appliance’s bot mitigation, DDoS and API protection features might not have parity with cloud options. Understanding the difference is important for specific use cases.

- WAFs are increasingly API-driven and DevOps environments favor WAFs that expose APIs to facilitate automated deployment.

- Seeking information on WAF integration with other security controls is important for increased visibility and efficiency. For example integration with security monitoring tools, web access management (WAM), API gateways, bot management, content delivery network, DDoS and online fraud detection.

Sample Vendors

Akamai; Barracuda Networks; Citrix; F5; Fortinet; Imperva; Radware

Gartner Recommended Reading

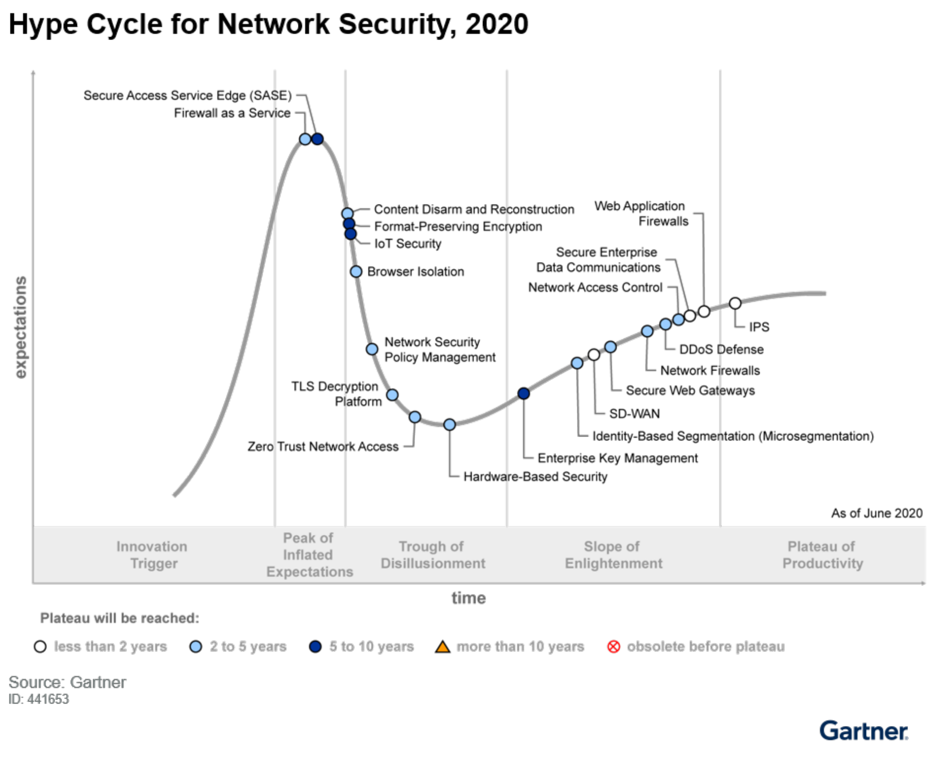
Magic Quadrant for Web Application Firewalls

Critical Capabilities for Cloud Web Application Firewalls Services

Defining Cloud Web Application and API Protection Services

Appendixes

Figure 2. Hype Cycle for Network Security, 2020



Source: Gartner (June 2020)

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

Enlarge Table

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	Because the innovation

Source: Gartner (July 2021)

Table 3: Benefit Ratings

Enlarge Table

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

Source: Gartner (July 2021)

Table 4: Maturity Levels

Enlarge Table

Maturity Levels	*Status*	*Produ*
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First g High p Much

Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Secon Less c
Early mainstream	Proven technology Vendors, technology and	Third More metho

Source: Gartner (July 2021)

Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."