Hype Cycle for Network Security, 2020

Published 30 June 2020 - ID G00441653 - 76 min read

By Analysts Pete Shoard

Initiatives: Infrastructure Security

Network security technologies protect IT systems, platforms and applications from attacks through prevention and immediate automatic response. Security and risk management leaders should employ these technologies where infrastructure may be at risk of compromise by external and internal threats.

Analysis

What You Need to Know

Network security technologies, such as enterprise firewalls, have been a foundational component of an organization's security strategy for many years. However, hybrid IT architectures that include both on-premises and cloud are becoming far more widely adopted; at the same time, attackers becoming more sophisticated and attacks more frequent. Because of these factors, the need for preventive security technologies that are highly agile and are compatible with a wide spectrum of the enterprises' IT infrastructure models is greater than ever before. Gartner has observed many traditional network security technologies reinvent themselves to meet this changed demand, expanding with adjacent preventive technologies to support hybrid IT architectures.

Organizations must set a strategy that will become our "new normal" in these uncharted waters, It remains true that no single security technology provides a complete prevention solution, and organizations still require a defense-in-depth approach. Therefore, a key requirement for setting an organizational network security strategy is to understand the available controls in the marketplace and ascertain if they remain relevant in hybrid and multicloud infrastructures. Security and risk management leaders are unable to prepare for every scenario. Therefore, they must make intelligent, risk-based decisions about which security technologies they may choose to defend their organization from threats and to maintain their day-to-day operations.

The Hype Cycle is an evolution of last year's "Hype Cycle for Threat-Facing Technologies, 2019." It contains details on a representative section of that Hype Cycle, focusing on technologies used by security leaders in organizations to mitigate and prevent threats, therefore reducing risk to their infrastructure. Security and risk management leaders focused on security strategy that aligns toward operational goals should read the other representative section offshoot of the "Hype Cycle for Threat-Facing Technologies, 2019," which is the "Hype Cycle for Security Operations, 2020."

The Hype Cycle

Network security technologies have evolved too slowly to meet the needs of modern organizations. They are often available in virtual and “as a service” formats, and meet the needs of organizations that continue to use more traditional IT infrastructure deployments. Data exploitation, leakage prevention and integrity management are also key features of security strategies where a more regimented and controllable boundary to networks is not present. The features of network security technologies focus on the prevention and protection of network infrastructure, cloud platforms and the transmission of data on these environments.

The network security landscape is mature and has little by way of direct Innovation Trigger-type solutions; much of the innovation in these markets is in functional consolidation and virtualization of core capability. This is seen in areas such as secure access service edge (SASE) and the continued evolution in long-term development areas such as firewall as a service (FWaaS). Much of the innovation and evolution have been slowed by resistance to change — not only in security departments, but also in infrastructure. Up until recently, the pace of adoption in network security technologies had resulted in slower mutations and favored “forklift” strategies for older-style network security technology implementations that are inefficient.

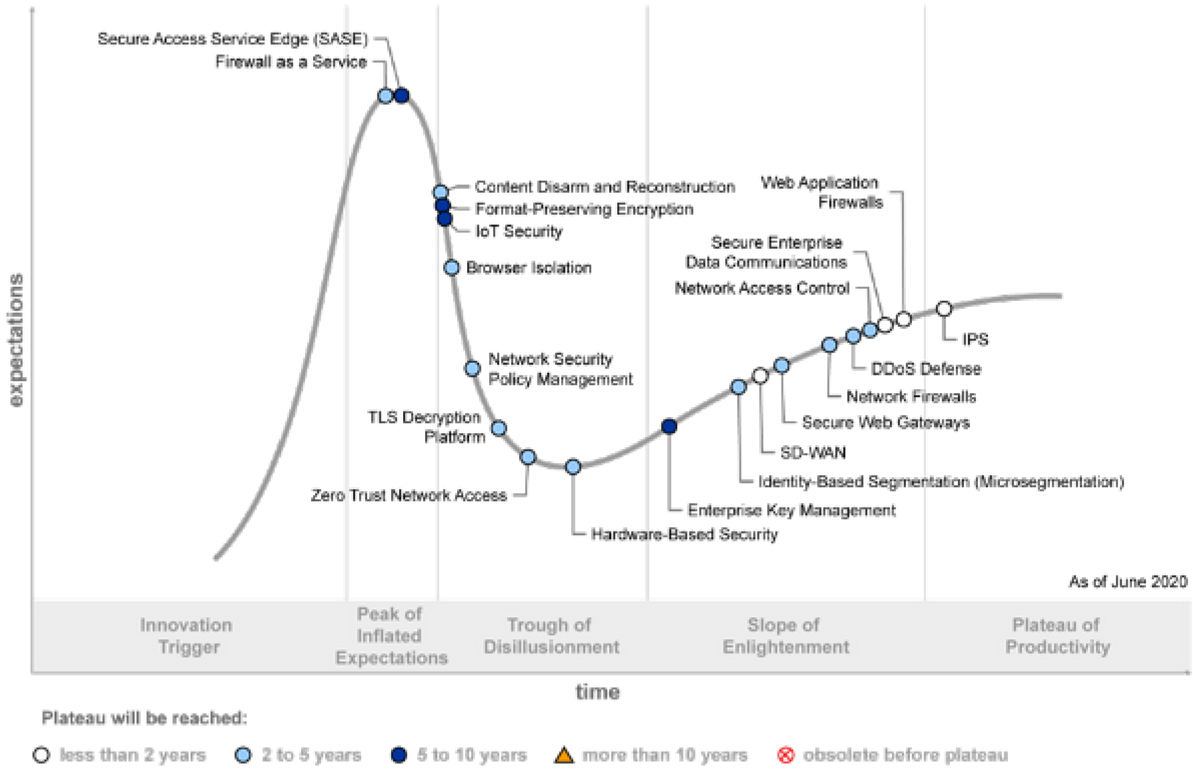
Nowadays, digital transformation dominates the IT architecture roadmaps of many organizations. This acceleration has encouraged the utilization of external management services or “as a service” applications within organizations that may not have traditionally considered outsourcing security, even if they are now outsourcing a large proportion of their IT estate. This acceptance of cloud solutions in wider IT is also influencing security technology pricing and consumption models to move toward a pay-as-you-use model. Furthermore, turnkey solutions are also increasingly in demand, with sales channels for prevention technologies are more frequently aligned with hosting providers and services such as Amazon, Google and Microsoft.

The need for specific security skills has not diminished in the management and operation of network security technologies, but simplification has been achieved through industry standardization and demands from end users in areas such as API integration. This simplification has meant that vendor specific skills are not as necessary; however, effective use of security budgeting and resourcing is still pertinent as the volumes of different types of IT technologies demand a growing number of prevention capabilities.

Network security strategy is often informed by assessments and consultative engagements carried out by specialist firms. It also regularly features as an informed and sometimes automated output of detection and response technologies and services. Technologies that use encryption as a core part of their solution have tended to evolve more slowly, with areas such as enterprise key management and hardware-based security expected to take between five and 10 years to reach the Plateau of Productivity. The vast majority of network security technologies evolve in line with the development of IT, and therefore will mature or be superseded in a much shorter time period than was previously the case.

Figure 1. Hype Cycle for Network Security, 2020

Hype Cycle for Network Security, 2020



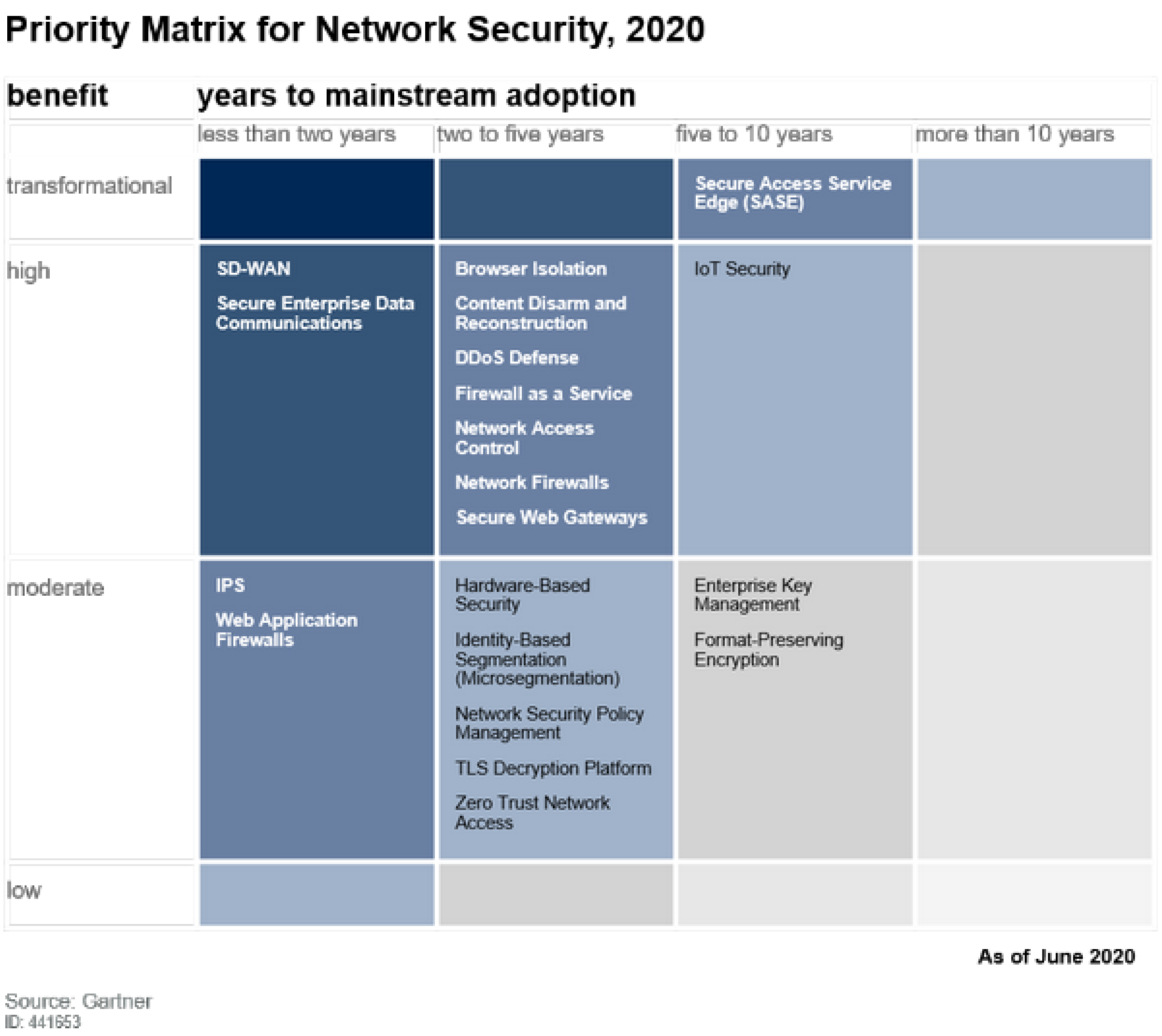
Source: Gartner
ID: 441653

The Priority Matrix

Network security technologies can provide a high level of benefit, as they can influence and enforce working policy, and enable significant changes in IT architecture where risk may have previously been identified as too high to allow adoption. However, these changes are rarely a reflection of the transformational results that they enable. Areas such as distributed denial of service (DDoS) and intrusion prevention systems (IPS) are driving benefit through them, continuing to require less interaction and becoming more autonomous, or sometimes supported by a wider network of vendor capability. These functions can therefore be delivered by less-experienced workers, and this decreases the time it takes for security technologies to reach mainstream adoption.

With the immense complexity in the typical enterprise environment, and digital transformation taking the front seat for many organizations, solutions are increasingly embedded into existing capabilities or infrastructure purchases. This is seen clearly in areas such as FWaaS. Furthermore, the importance of getting business done is also becoming a key feature of many security requirements. Simply blocking potentially bad things is not practicable or efficient in today's fast-moving society. Solutions such as content disarm and reconstruction (CDR) seek to address this type of issue, though not providing immense benefit on their own. But like many network security technologies, they are assisting the availability and functionality of technologies that are needed to continue business as usual. Many technologies in the network security space provide benefit through the consolidation of previous capability; this is true of SASE, and the benefits of that consolidation will be transformational to the security programs of businesses.

Figure 2. Priority Matrix for Network Security, 2020



Priority Matrix for Network Security, 2020

benefit	years to mainstream adoption			
	less than two years	two to five years	five to 10 years	more than 10 years
transformational			Secure Access Service Edge (SASE)	
high	SD-WAN Secure Enterprise Data Communications	Browser Isolation Content Disarm and Reconstruction DDoS Defense Firewall as a Service Network Access Control Network Firewalls Secure Web Gateways	IoT Security	
moderate	IPS Web Application Firewalls	Hardware-Based Security Identity-Based Segmentation (Microsegmentation) Network Security Policy Management TLS Decryption Platform Zero Trust Network Access	Enterprise Key Management Format-Preserving Encryption	
low				

As of June 2020

Source: Gartner
ID: 441653

Off the Hype Cycle

“IDPS” has been renamed “IPS,” or intrusion prevention systems, to better separate the distinction between detection technologies covered in the NDR market, versus prevention technologies that sit in-line of network traffic.

“NTA” has been renamed “NDR” and features on the “Hype Cycle for Security Operations, 2020.”

Several other profiles that previously appeared on the “Hype Cycle for Threat-Facing Technologies, 2019” have been realigned with their specific areas, such as Data Classification on the “Hype Cycle for Data Security, 2020.”

At the Peak

Firewall as a Service

Analysis By: Adam Hils

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 is primarily delivered as a multitenancy infrastructure that is shared among multiple enterprises. FWaaS can provide simpler, more flexible architecture by leveraging centralized policy management, multiple enterprise firewall features and traffic tunneling to partially or fully move security inspections to a cloud infrastructure.

Position and Adoption Speed Justification: The FWaaS concept awareness is growing within distributed organizations looking for a scalable solution to deliver secure site-to-site connectivity and direct internet presence. During COVID-19, the remote user use case is also driving interest. FWaaS vendors are deployed at a growing number of enterprise clients. FWaaS reaches the Peak of Inflated Expectations as more distributed organizations become aware of FWaaS when they evaluate cloud options to offload web security traffic.

Secure web gateways (SWGs) and web application firewalls (WAFs) delivered as cloud services are growing more quickly than their appliance-based equivalents. FWaaS has fast growth potential, but tunneling multiple protocols to the cloud infrastructure creates additional friction than when deploying single protocol cloud service (WAF, SWG). FWaaS vendors need to provide more than cost-effectiveness to convince enterprises to trust a cloud infrastructure as a core security component. A FWaaS must provide consistently good latency across all enterprise point of presence. Increasingly closer integration with software-defined WAN (SD-WAN) is aiding FWaaS development.

User Advice: Growing adoption of SD-WAN and hybrid WAN architectures is increasing interest in using FWaaS and we anticipate that trend to continue. Vendor choice for FWaaS and products have varying maturity levels. Organizations considering FWaaS should conduct extensive proofs of concept or limit the scope of an initial production deployment.

The appeal of simpler architecture and increased flexibility must materialize in faster deployment and easier maintenance. 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 and allow for a quick opt-out. Determine whether your organization is ready to move the entire security workload into the cloud, or if you need thicker local devices to perform some computation (such as HTTPS decryption) and address privacy concerns.

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 targeted at protecting mobile workers or companies whose applications are primarily cloud-hosted with no branch dependency on headquarters for applications. Another key action is to 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 mobile workforce, 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). If needed, verify the ability of the FWaaS provider to offer virtual instances dedicated to your enterprise, or other means used to ensure separations between the FWaaS customers.

Multifunction security platforms potentially compromise on the depth of security. Conduct an individual assessment of each key security component you plan to deploy and determine whether FWaaS provides unique security features, such as shared threat intelligence gathered from similar client organizations. Business continuity plans need to include the possibility of failure in the centralized FWaaS infrastructure.

Business Impact: FWaaS offers a significantly different architecture for branches or even single-site organizations. It also offers greater visibility through centralized policy, increased flexibility and reduced capital cosst by using a fully or partially hosted security workload.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Cato Networks; Check Point Software Technologies; Cisco; OmniNet; Open Systems; OPAQ Networks; Palo Alto Networks; Secucloud; Versa Networks; Zscaler

Recommended Reading: “Select the Right Strategy for Securing Web Access”

“Answers to Questions About 3 Emerging Security Technologies for Midsize Enterprises”

“Magic Quadrant for Network Firewalls”

“Magic Quadrant for WAN Edge Infrastructure”

Secure Access Service Edge (SASE)

Analysis By: Joe Skorupa; Neil MacDonald

Definition: Secure access service edge (SASE, pronounced “sassy”) delivers multiple capabilities such as SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA).

SASE supports branch office and remote worker access. SASE is delivered as a service, and based upon the identity of the device/entity, combined with real-time context and security/compliance policies. Identities can be associated with people, devices, IoT or edge computing locations.

Position and Adoption Speed Justification: 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. While the term originated in 2019, the architecture has been deployed by early adopters as early as 2017. By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.

By 2023, 20% of enterprises will have adopted SWG, CASB, ZTNA and branch FWaaS capabilities from the same vendor, up from less than 5% in 2019. However, today most implementations involve two vendors (SD-WAN + Network Security), although single vendor solutions are appearing. Dual-vendor deployments that have deep cross-vendor integration are highly functional and largely eliminate the need to deploy anything more than a L4 stateful firewall in the branch office. This will drive a new wave of consolidation as vendors struggle to invest to compete in this highly disruptive, rapidly evolving landscape.

SASE is in the early stages of market development but is being actively marketed and developed by the vendor community. Although the term is relatively new, the architectural approach (cloud if you can, on-premises if you must) has been deployed for at least two years. The inversion of networking and network security patterns as users, devices and services leave the traditional enterprise perimeter will transform the competitive landscape for network and network security as a service over the next decade, although the winners and losers will be apparent by 2022. True SASE services are cloud-native — dynamically scalable, globally accessible, typically microservices-based and multitenant. The breadth of services required to fulfill the broad use cases means very few vendors will offer a complete solution in 2020, although many already deliver a broad set of capabilities. Multiple incumbent networking and network security vendors are developing new or enhancing existing cloud-delivery-based capabilities.

User Advice: There have been more than a dozen SASE announcements over the past 12 months by vendors seeking to stake out their position in this extremely competitive market. There will be a great deal of slideware and marketecture, especially from incumbents that are ill-prepared for the cloud-based delivery as a service model and the investments required for distributed PoPs. This is a case where software architecture and implementation matters

When evaluating SASE offering, be sure to:

- Involve your CISO and lead network architect when evaluating offerings and roadmaps from incumbent and emerging vendors as SASE cuts across traditional technology boundaries.
- Leverage a WAN refresh, firewall refresh, VPN refresh or SD-WAN deployment to drive the redesign of your network and network security architectures.
- Strive for not more than two vendors to deliver all core services.
- Use cost-cutting initiatives in 2020 from MPLS offload to fund branch office and workforce transformation via adoption of SASE.
- Understand what capabilities you require in terms of networking and security, including latency, throughput, geographic coverage and endpoint types.
- Combine branch office and secure remote access in a single implementation, even if the transition will occur over an extended period.

- Avoid vendors that propose to deliver the broad set of services by linking a large number of products via virtual machine service chaining.
- Prioritize use cases where SASE drives measurable business value. Mobile workforce, contractor access and edge computing applications that are latency sensitive are three likely opportunities.

Some buyers will implement a well-integrated dual vendor best-of-breed strategy while others will select a single vendor approach. Expect resistance from team members that are wedded to appliance-based deployments.

Business Impact: SASE will enable I&O and security teams to deliver the rich set of secure networking and security services in a consistent and integrated manner to support the needs of digital business transformation, edge computing and workforce mobility. This will enable new digital business use cases (such as digital ecosystem and mobile workforce enablement) with increased ease of use, while at the same time reducing costs and complexity via vendor consolidation and dedicated circuit offload.

COVID-19 has highlighted the need for business continuity plans that include flexible, anywhere, anytime, secure remote access, at scale, even from untrusted devices. SASE's cloud-delivered set of services, including zero trust network access, is driving rapid adoption of SASE.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Akamai; Cato Networks; Cisco; Citrix; iboss; Netskope; Open Systems; Palo Alto Networks; VMware; Zscaler

Recommended Reading: "The Future of Network Security Is in the Cloud"

"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"

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

Sliding Into the Trough

Content Disarm and Reconstruction

Analysis By: Mark Harris; Neil MacDonald

Definition: 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 or company policy; and rebuilds a sanitized version. This near-real-time process is an effective approach to removing malware and other exploits from files. While sandboxing and almost all other techniques depend on detection of behaviors, CDR protects against exploits and weaponized content that have not been seen before.

Position and Adoption Speed Justification: Adoption of content disarm and reconstruction (CDR) is gradually increasing for sanitizing content when messaging, downloading, uploading or sharing files. Some secure email and web gateways, as well as content collaboration platforms, already include such capabilities. 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. In some organizations, CDR has replaced sandboxing. CDR also sees adoption in solutions for websites that allow the upload of content and that do not require originals (such as resumes or purchase orders). It also plays a defense-in-depth role for handling content with browser isolation solutions. CDR neutralizes all potentially malicious content, without requiring multiple antivirus scanning or sandboxing. We also expect CDR to be available as an optional add-on capability everywhere multiple antivirus scanning is deployed.

User Advice: Malicious content can be detected in advanced solutions using a gauntlet of signatures, static analysis and dynamic sandboxing analysis. However, malware is increasingly sandbox-aware and obfuscated such that these layers must constantly evolve to remain effective. CDR should be evaluated as an effective means of thwarting content-born attacks. However, the security value of CDR needs to be balanced with the business need for macro- or JavaScript-enabled content. The use of CDR can decrease document usability by stripping out active code that is intended for legitimate purposes. Better CDR solutions hold the original file in quarantine if its functionality is broken. Still, we expect CDR will ultimately be considered a best practice for general workforce members, with exceptions granted only for specific roles or users. Administrators should be able to manage an exception use case that allows specific users to receive content with embedded macros (for example, members of the sales organization can receive unprocessed Excel files). A remote viewer may be an alternative to CDR; however, there will always be cases where content needs to be moved local to the user and should be scanned and have CDR applied prior to allowing this.

Business Impact: CDR is an important layer in any organization's defense-in-depth and content protection strategies. Content can contain malicious code, links to malicious content (in the form of embedded URLs or scripts) or structural issues that trigger an exploit in a client application. CDR can eliminate one of the most common infection vectors that is hard to deal with in other ways. Scripts embedded in content can be highly obfuscated, which is a significant challenge for many anti-malware solutions that rely on static scanning. CDR is much faster than sandboxing, and therefore makes a good complementary solution. However, since CDR does not rely on detection, it can be challenging to demonstrate effectiveness without additional, retrospective analysis of content.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Check Point Software Technologies; Clearswift; Glasswall Solutions; Mimecast; OPSWAT; ReSec; Sasa Software; Symantec; Tresys; Votiro

Recommended Reading: "Market Guide for Email Security"

"Fighting Phishing — 2020 Foresight"

"5 Core Security Patterns to Protect Against Highly Evasive Attacks"

"Solution Comparison for Nine Secure Email Gateways"

"Magic Quadrant for Secure Web Gateways"

"Innovation Insight for Remote Browser Isolation"

Format-Preserving Encryption

Analysis By: Brian Lowans; Joerg Fritsch

Definition: Format-preserving encryption (FPE) is used to protect data at rest and in use, as well as when it's accessed through applications, while maintaining the original data length and structure. It's used to protect fields in an increasing number of relational database management systems (RDBMSs), data warehouses and NoSQL databases. 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.

Position and Adoption Speed Justification: 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.

User Advice: FPE is typically used across a variety of RDBMSs, data warehouses and NoSQL platforms, such as Hadoop, Cassandra and MongoDB. It 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 being stored or processed in cloud-based data warehouses and databases. However, it is still a blunt-force access control, and, when applied, it will protect data wherever it resides or accessed. Authorized users with application or database access privileges will have access to the data in clear text.

Hence, when implementing FPE, organizations should also consider tools to monitor and audit all user and administrator access to sensitive data, with database audit and protection tools (DAP). They should also use data loss prevention (DLP) to monitor data movement across endpoints. Any clear-text access to sensitive data may result in that data being stored in other data stores; hence, security policies must be coordinated across all data silos. A good security best practice is the segregation of duties (SOD) of database administrators (DBA) from security controls. DBAs should not be responsible for FPE, and should be managed as part of an enterprise key management (EKM) solution. The National Institute of Standards and Technology (NIST) published standard for FPE describes several algorithm modes within Special Publication 800-38G; however, only the FF1 mode has been approved. Some implementations of FF3 mode may still be accepted. When considering FPE, identify the following:

- What data fields need to be protected in accordance with perceived risks, threats and compliance requirements?
- Do the field lengths need to be maintained or protection only applied to part of a field?
- Should FPE be combined with DAP?
- What will be the adversarial impact of encryption on application functionality?
- Are transparent data encryption (TDE), tokenization or dynamic data masking (DDM) appropriate alternatives to FPE?
- How will FPE fit into an EKM approach?

The most common deployments focus on specific types of regulated data. FPE can replace the whole string within a field, or just a part of the field, to maximize functionality of applications, while maintaining anonymity and without requiring schema changes to databases. Some vendors offer FPE with added features of DDM, where the whole field can be decrypted on-the-fly and then part of a field can be masked on presentation to the application user to offer more flexible access policies.

Review how FPE interfaces with applications, and establish whether user identities can be employed to approve if fields are decrypted. Evaluate any impact on performance and functionality of applications accessing the database. Be aware that other security and database functionality, such as data discovery, can be affected.

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 and agile method to prevent unauthorized user access to data on-premises and, increasingly, in public cloud service platforms. This will help meet data protection and privacy regulations and data residency requirements to protect personal, health, credit card and financial data, as well as data breach disclosure regulations. FPE should be deployed to implement policy rules for user access in coordination with other security controls, according to Gartner's data security governance (DSG) framework.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Comforte; Dataguise; IBM; Informatica; Micro Focus; Oracle; PKWARE; Protegrity; SecuPi; Thales eSecurity

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"

"Market Guide for Data-Centric Audit and Protection"

"Prioritize Enterprisewide Encryption for Critical Datasets"

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

IoT Security

Analysis By: Barika Pace

Definition: Internet of Things (IoT) security works addresses software, hardware, network and data protection for digital initiatives involving IoT. The term is most often used in the context of business or marketing efforts, as opposed to cyber-physical systems security, which is a more descriptive and pragmatic term for security and risk practitioners. IoT security shares many of the same technologies and processes as IT, operational technology (OT) and physical security. IoT security provides safety, privacy and resilient for digital systems.

Position and Adoption Speed Justification: IoT security technologies and services are progressing but through the lens of a converging security ecosystem with end user and vendors seeking higher levels of integration with IT, OT and CPS solutions. IoT security continues to move at a modest pace. Areas such as digital trust, tamper-resistant device hardening techniques in hardware and firmware, secure cloud integration, remote access, device discovery, event detection and response systems, and improved consulting and system integration are contributing to the progress. Larger security providers continue to enter the market space and offer slightly higher levels of security product integration with IoT solutions. New IoT security technologies continue to emerge primarily as part of existing IT, OT and physical security technology refreshes. Increasing regulations (for example, GDPR and California's new SB-327 cybersecurity law) will continue to spur demand for

IoT security products and services over the years to come. Over the past year these regulations and compliance requirements have fueled adoption. While merges and acquisitions this past year left some end users slower to adopt, the past is expected to remain on track through this current period. Furthermore, as the threat landscape continues to evolve, IoT security is maturing rapidly to address and adapt to the new threats, thus leading it into the adolescent phase, as demonstrated by increasing maturity in areas of safety and reliability.

User Advice: Security and risk management leaders, including business executives, chief digital officers, chief risk officers, chief information security officers (CISOs) and CIOs, should:

- Establish proofs of concept to discover, classify and manage all connected devices to ascertain risk landscape, raise organizational awareness and create business value by onboarding visibility tools that can have dual purpose for operational team
- Determine design gaps in capability, skills and infrastructure
- Elevate IOT security requirements into their enterprise risk management efforts by adopting an integrated security strategy across IT, IOT and CPS.
- Account for data privacy concerns brought about by the increasing regulations for IoT devices that process personal data
- Record all IoT assets, from sensors to large industrial equipment, and create visibility into their IoT networks and topologies
- Include IoT security into the expanding scope of responsibility now and into the future
- Prepare for increasing regulations by focusing on safety and privacy in IoT designs that safeguard data, people and the environment
- Analyze regulatory exposure to IoT security requirements
- Work on developing in-house IoT security expertise, including coordination with environmental, health and safety subject matter experts
- Invest in digital risk management to properly plan for IoT security in digital transformation projects
- Change governance and oversight of IT and OT projects to accommodate specific digital risk concerns that lead to IoT security decisions
- Restructure skill sets and support resources (that is, organizational accountability and responsibility) to accommodate differences in deployment and operation of digital initiatives requiring secure IoT systems

- Incorporate regulatory compliance requirements for IoT technologies within existing IT, OT, CPS and physical security regulation tracking and management.

Business Impact: High-profile cyberattacks can create compromises in verticals such as telecommunications, government, transportation, energy and utilities, and healthcare. Initiatives such as connected homes, smart cities, connected automobiles and medical devices are vulnerable as well. Cyberattacks have driven early IoT security spend in these verticals and initiatives. Growing attention and pressure from different layers of government may lead to potential regulations. The effects of cyberattacks also highlight the overlapping safety regulation and general safety management impacts of IoT security. In the short term, IoT security will continue to be the No. 1 barrier to entry to the IoT. In the longer term, these emerging security technologies will enable the IoT.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Sample Vendors: 802 Secure; Armis; Darktrace; Forescout Technologies; Infineon Technologies; IOActive; Microsoft Azure; Prove & Run

Recommended Reading: “How to Secure the Enterprise Against the Internet of Things Onslaught”

“IoT Solutions Can’t Be Trusted and Must Be Separated From the Enterprise Network to Reduce Risk”

“Market Trends: IoT Edge Device Security, 2020”

“Market Insight: Tech CEOs Must Act Before Convergence Kills Your Stand-Alone OT/IoT Product Solution”

“Focus More on the Realities of Cyber-Physical Systems Security Than on the Concepts of IoT”

Browser Isolation

Analysis By: Neil MacDonald

Definition: Browser isolation is the strong separation of the browsing process from the end-user system to protect the system, its network and its resources from attacks that are carried out via the browser or to protect a sensitive application from a potentially compromised browser. Browser isolation is achieved using two main approaches: (1) remote browser isolation and (2) local browser isolation. At this time, the more mature of the two, with a larger number of vendor alternatives, is remote browser isolation.

Position and Adoption Speed Justification: Most organizations use URL filtering in the form of secure web gateways (SWGs) to protect their users and devices from the evils of the internet; and organizations have been slow to adopt browser isolation technologies. However, as demonstrated by the recent surge in ransomware, attacks still get through. Rather than allowing potentially hostile content in from the web, browser isolation strategies keep the session isolated (much like a suspicious package being opened by a remote-controlled robot).

There are two primary approaches:

- Remote browser isolation is conceptually like VDI; every browser session is remotely presented from a browser server and treated as if it might have been compromised. And, ideally, every session is reset back to a known good state from immutable templates when completed. With remote browser isolation, all webpages are rendered remotely, and an image or document object model of the website is sent to the user's local browser. Unlike VDI, nearly all remote browser solutions use Linux and containers to increase hardware densities and reduce licensing costs. Some vendors offer on-premises deployment options, while others are entirely cloud-based. Remote browser isolation capabilities are available from many point solution vendors and are also available as separately charged features from some larger security platform offerings such as secure email and web gateways; and, indeed, multiple acquisitions have already occurred. For example, Zscaler recently acquired Appsolate and McAfee acquired Light Point security. Further, we see RBI being a critical capability in the future delivery of a secure access service edge (SASE), supporting integration with SWG, CASB and ZTNA services. RBI also is used in the reverse direction when unmanaged devices are accessing sensitive data and applications. By controlling the browser used to access the application and data, this gives information security a critical control point when dealing with unmanaged and potentially compromised devices to add capabilities like sensitive data monitoring and protection from bot-based attacks.

- In contrast, local browser isolation attempts to isolate the browsing process from the rest of the end user's desktop using software-based isolation techniques such as running a separate VM, or using underlying hardware-based isolation. Microsoft released local browser isolation capabilities with Windows Defender Application Guard with Windows 10. There are a very small number of vendors that provide local browser isolation using this model and they are forced to offer compatibility with Microsoft's approach.

User Advice:

- Evaluate and pilot a browser isolation solution for specific high-risk users, such as finance, or use cases such as rendering email-based URLs, particularly if your organization is risk-averse.

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

- Start with a limited number of users and by selectively isolating a limited number of URLs, then expand the use cases.
- Focus on higher-risk individuals that are more likely to be targeted, such as in the executive office, research and development, or finance (for example, payment processing). Alternatively, focus on uncategorized URLs (which are inherently more risky) or those URLs with low reputation scores to isolate.
- Favor remote browser solutions that don't require a local agent or application to be installed, and instead use HTML5 to deliver remote sessions to the user's local modern browser for access. Evaluate different vendor approaches for rendering based on performance and bandwidth.
- Evaluate different vendor approaches for rendering based on performance, latency and bandwidth requirements.
- Design and implement a capability for content movement from the public internet into enterprise systems, but only after intensive scanning using multilayered threat detection techniques.
- Sign one- to two-year contracts only, because the market is in flux with downward pricing pressure.

Business Impact: Most attacks are delivered via the public internet either through 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. Through 2022, organizations that isolate high-risk internet browsing and access to URLs in email will experience a 70% reduction in attacks that compromise end-user systems. Notably, remote browser isolation can thwart ransomware attacks, blocking their ability to encrypt the users' files on their devices or in enterprise file shares, neither of which are directly accessible from the remote browser session.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Authentic8; Cyberinc; Ericom Software; Garrison; Hysolate; McAfee; Menlo Security; Proofpoint; Symantec; Zscaler

Recommended Reading: "Innovation Insight for Remote Browser Isolation"

"Magic Quadrant for Secure Web Gateways"

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

"The Future of Network Security Is in the Cloud"

Network Security Policy Management

Analysis By: Rajpreet Kaur; Adam Hils; John Watts

Definition: Network security policy management tools go beyond user policy administration interfaces that firewall vendors provide and offer support for hybrid environments. NSPM provides analytics and auditing for rule optimization, change management workflow, rule testing, compliance assessment, and visualization, often using a visual network map of devices and firewall access rules overlaid onto multiple network paths.

Position and Adoption Speed Justification: The growth in adoption of hybrid environments is challenging the security teams to maintain and have visibility of security policies across these environments. Since these controls are not only confined to traditional firewall controls but also include network security controls offered by cloud native vendors such as Amazon Web Services (AWS), Microsoft Azure, VMware, network security policy management (NSPM) tools close this gap by offering centralized visibility and control. Multivendor firewall rule management is mature within these tools. Other than network security policy management, maintaining security policies as per the compliance- and audit-based reporting is also a primary use case for adoption of these tools. The primary adoption driver varies. The NSPM tools are facing competition by other network security product vendors who are offering some level of overlapping features and capabilities by offering support for cloud native controls and trying to reduce management complexities.

User Advice: 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, 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. The primary components of these tools are: security policy management for multivendor firewalls and network security devices; change management system; risk and vulnerability analysis; application connectivity management.
- 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.
- Prepare a list of devices and tools being utilized in your environment based on your use case to check integration capabilities offered by NSPM vendors. This list should go beyond firewalls and routers to include vulnerability scanners, and SOAR, ITSM and DevOps tools.

Business Impact: As networks grow and expand into hybrid or multicloud environments, having visibility across these platforms is a growing challenge that makes it nearly impossible for network security operations teams to manage and maintain the right network security policies across these environments. The network security team requires more visibility into and control over native and third-party network security controls. These tools can be used to meet multiple use cases in an enterprise as well as service provider environments. Following are use cases which can be met by NSPM tools:

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

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: AlgoSec; FireMon; IBM; RedSeal; Skybox; SolarWinds; Tufin; Venustech

Recommended Reading: "Technology Insight for Network Security Policy Management"

TLS Decryption Platform

Analysis By: Adam Hils; Jeremy D'Hoinne

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

Position and Adoption Speed Justification: Gartner sees that the TLS decryption platforms are slowly maturing as organizations realize the importance and the complexity of building a TLS decryption strategy. Security and risk leaders are grappling with the issues raised by the growing amount of HTTPS traffic traversing their networks. Enterprises slow to adopt web traffic decryption best practices risk exposing their infrastructure to targeted malware campaigns and data loss. Evolutions of ransomware that leverage 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. Despite the widely acknowledged need for traffic visibility, Gartner has seen several important limitations that have restricted adoption.

An organization launching a decryption project will face challenges that can impact speed to adoption, including:

- **Organizational:** Decrypting HTTPS creates privacy challenges for monitored employees. Local regulations or enterprise culture might hinder the decryption project.
- **Technical:** The use of decryption architecture might degrade user experience, introducing poor performance and unexpected blocking of legitimate business applications. TLS 1.3 adds technical complications; for example, TLS 1.3 enforces Perfect Forward Secrecy (PFS) making off-box decryption and reencryption impossible using the original encryption key.
- **Budgetary:** The average cost per user of network security controls will rise because of the decryption costs, but the overall organizational perception of value is low. Some organizations choose to decrypt traffic instead within existing edge firewall, secure web gateway deployments or at the ADC level.

In addition, certificate pinning in many mobile applications prevents traffic decryption. If administrators are unable to drop traffic headed to these applications, they are forced to allow the traffic through uninspected, which limits efficacy.

User Advice: Security and risk management leaders should do the following:

- Monitor 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 privacy.
- Ensure that network traffic will be decrypted only once.
- Decide whether to decrypt with existing network security appliances or with dedicated decryption appliances.

- Check with the TLS decryption vendors about how they support TLS 1.3, and about how long they will support downgrades to TLS 1.2 where necessary.
- If the TLS decryption platform approach is selected:
- Ensure that the impact of decrypting traffic based on today's traffic and future growth is reflected in the network security budget.
- Maintain proper documentation of the decryption architecture and related process to prepare for audits.
- Ensure that decrypted traffic is segregated from clear-text traffic.
- Test the integration between the platforms and the security solutions that access the decrypted traffic.
- Review log policy for each part of the decryption infrastructure to avoid unwanted logging of confidential data and sensitive PII.

Business Impact: To solve visibility issues, this technology can be applied in organizations outside of some highly regulated nations. Sometimes decisions to decrypt widely must be coordinated with legal and human resources participation. Security and risk leaders implementing dedicated TLS decryption platform will get the better visibility necessary to protect organizational data and to let other security protections inspect the traffic. This technology is applicable to enterprises tolerant of adding another appliance to gain improved security. Midsize enterprises are more likely to leverage existing solutions to solve the visibility problems, even if they have to upgrade the capacity of those solutions to achieve necessary performance with TLS decryption offload.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: A10 Networks; Array Networks; ARA Networks; F5; Gigamon; Ixia; Symantec

Recommended Reading: "Market Guide for Network Traffic Analysis"

"Magic Quadrant for Secure Web Gateways"

"Magic Quadrant for Network Firewalls"

"Demystifying the Impact of TLS 1.3 on TLS Inspection"

Zero Trust Network Access

Analysis By: Steve Riley

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

Position and Adoption Speed Justification: ZTNA is a synthesis of concepts promulgated by the Cloud Security Alliance's software-defined perimeters (SDP) project, by Google's BeyondCorp vision, and in O'Reilly's *Zero Trust Networks* book. Early products on the market tended to focus on use cases involving access to web applications. Newer, more complete products work with a wider range of applications and protocols.

As more organizations suddenly find themselves transitioning to much more remote work, hardware-based VPNs exhibit limitations. ZTNA has piqued the interest of those seeking a more flexible alternative to VPNs and those seeking more precise access and session control to applications located on-premises and in the cloud. ZTNA vendors continue to attract venture capital funding. This, in turn, encourages new startups to enter an increasingly crowded market and seek ways to differentiate. Merger and acquisition (M&A) activity in this market is underway, with several startup vendors now having been acquired by larger networking, telecommunications and security vendors.

User Advice: Organizations should evaluate ZTNA for any of these use cases:

- Opening up applications and services to collaborative ecosystem applications, such as distribution channels, suppliers, contractors or retail outlets without requiring the use of a VPN or DMZ.
- Normalizing the user experience for application access — ZTNA eliminates the distinction between being on and off the corporate network.
- Application-specific access for IT contractors and remote or mobile employees as an alternative to VPN-based access.
- Extending access to an acquired organization during M&A activities, without having to configure site-to-site VPN and firewall rules. The merged companies can quickly and easily share applications without requiring the underlying networks and/or identity systems to be integrated.
- Enabling users on personal devices — ZTNA can improve security and simplify bring your own device (BYOD) programs by reducing full management requirements and enabling more-secure direct application access.
- Cloaking systems on hostile networks, such as systems facing the public internet used for collaboration.

- Carrying encryption all the way to the endpoints for scenarios where you don't trust the carrier or cloud provider.
- Permitting users in potentially dangerous areas of the world to interact with applications and data in ways that reduce or eliminate risk prone to originate in those areas.
- Securing access to enclaves of IoT devices if the device can support lightweight SDP agent or a virtual-appliance-based connector on the IoT network segment for connection.

Business Impact: The benefits of ZTNA are immediate. Similar to a traditional VPN, services brought within the ZTNA environment are no longer visible on the public internet and, thus, are shielded from attackers. In addition, ZTNA brings significant benefits in user experience, agility, adaptability and ease of policy management. For cloud-based ZTNA offerings, scalability and ease of adoption are additional benefits. ZTNA enables digital business transformation scenarios that are ill-suited to legacy access approaches. As a result of digital transformation efforts, most enterprises will have more applications, services and data outside their enterprises than inside. Cloud-based ZTNA services place the security controls where the users and applications are — in the cloud. Some of the larger ZTNA vendors have invested in dozens of points of presence worldwide for low-latency access.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Akamai; AppGate; Cato Networks; Cisco; Netskope; Perimeter 81; Proofpoint; Pulse Secure; SAIFE; Zscaler

Recommended Reading: "Market Guide for Zero Trust Network Access"

"Zero Trust Is an Initial Step on the Roadmap to CARTA"

"Solving the Challenges of Modern Remote Access"

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

"The Future of Network Security Is in the Cloud"

Hardware-Based Security

Analysis By: Neil MacDonald; Tony Harvey

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 monitoring and unencrypted memory handling.

Position and Adoption Speed Justification: Adoption is increasing and becoming mainstream, as hardware-based isolation capabilities are becoming standard in most hardware devices and cloud-based IaaS 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 has risen in the face of ongoing disclosures of new types of side-channel attacks. Another driver is the desire to use IaaS providers in potentially hostile parts of the world and protect these workloads from virtual machine and memory snapshotting. However, disillusionment remains as methods vary wildly among vendors, and some strong isolation capabilities such as Intel Software Guard Extensions (SGX) require applications to be rewritten and are incompatible with techniques used by AMD. Abstraction layers, such as Asylo, may help but add another layer of complexity and are not widely adopted.

Multiple implementations are appearing across vendors, OSs and chipsets:

- Samsung's Knox security hypervisor, where a supervisory process monitors the OS kernel for aberrant behavior. The supervisory process runs at a higher privilege level than the OS and cannot be compromised.

- Intel SGX provides a new privilege level for running code, which can be set up in a user-level process but excluded from operating system or hypervisor access. Multiple public cloud providers now support SGX including Alibaba Group, IBM and Microsoft.

- AMD has a similar set of technologies for protecting memory against physical and system software-based attacks: Secure Memory Encryption (SME), Transparent Secure Memory Encryption (TSME) and Secure Encrypted Virtualization (SEV).

- In 2018, Intel introduced chip-level Threat Detection Technology (TDT) that was further improved in 2019 and is now supported by multiple security offerings, including Microsoft Windows Defender.

- Microsoft uses hardware-based virtualization features in Windows 10 and Windows Server 2016 to create a protected code execution space for monitoring the OS and providing security features with Device Guard and Credential Guard.

- VMware built AppDefense — a way to monitor and protect applications from the hypervisor layer, outside of the workload, protected by virtualization-enabled hardware.

- Apple has developed and shipped its iOS Secure Enclave processor to protect sensitive operations and monitor kernel integrity.

- Google has developed a custom chip, Titan, for hardware-based root of trust and is deployed throughout their data centers. This chip binds a strong identity to each server, verifies the integrity of firmware and software, and creates a nonrepudiable audit trail of all changes to each machine.

- Amazon Web Services (AWS) uses a custom-designed Nitro Controller on its Nitro-based systems that includes a special micro-controller for security isolation and integrity measurements called the Nitro Security Chip. This becomes the foundation for its confidential computing offering called Nitro Enclaves, although this isolation uses the Nitro Hypervisor.

User Advice:

- Hardware-based security is strong, but may potentially still be broken by software flaws, or side-channel attacks such as Spectre and Meltdown. Patch and remain vigilant for unexpected breaches.
- Most systems will include hardware-rooted isolation and integrity capabilities by default. Make strong isolation of sensitive code and security controls a mandatory part of IT systems procurement, including IaaS.
- For systems under direct enterprise control, implement a BIOS-level patching strategy to deal with exposures that require BIOS-level remediation.
- For systems that move to public cloud infrastructure, evaluate the need for confidential computing capabilities only for the most critical applications to protect sensitive operations such as key management and sensitive intellectual property.
- Although the SGX approach is compatible with hypervisors, there may be unanticipated interactions. For example, it may not be possible to snapshot, suspend and restore a partition with a protected process. Understand limitations of hypervisor-based functionality before implementing SGX.
- Before activating Windows 10 virtualization-based security, check for compatibility issues with third-party approaches that also use virtualization techniques.
- Hypervisor-based approaches with security rooted in hardware virtualization techniques are another way to achieve similar levels of strong isolation (for example, Hysolate and Bitdefender have offerings that use this approach).
- None of these mechanisms are interoperable, so plan different strategies for different devices and server platforms.

Business Impact: If an operating system 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 require that operating system software and system management software be able to make use of it. Upgrading to most recent versions of software that can use hardware features and using cloud systems with advanced security, can materially increase system security.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Amazon Web Services (AWS); Apple; Bitdefender; Fortanix; Google; Hysolate; Intel; Microsoft; Samsung Electronics; VMware

Recommended Reading: “Market Guide for Cloud Workload Protection Platforms”

“How to Make Cloud More Secure Than Your Own Data Center”

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

“How to Mitigate Firmware Security Risks in Data Centers, and Public and Private Clouds”

“Key Management as a Service Exposes Different Risks to Data in Public Clouds”

Climbing the Slope

Enterprise Key Management

Analysis By: Brian Lowans; David Mahdi

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.

Position and Adoption Speed Justification: EKM is improving; however, there are still issues with compatibility, centralization and manageability. Cryptographic products that implement encryption or tokenization are a critical component of a data security strategy to meet growing data residency and privacy requirements, and prevent data breaches or theft due to hacking, malicious insiders and accidental disclosure.

User Advice: EKM products typically comply with the key management interoperability protocol (KMIP) standard, sponsored by the Organization for the Advancement of Structured Information Standards (OASIS). EKM can manage third-party cryptographic products that are compliant with KMIP, and many storage and backup solutions support KMIP. However, other vendor cryptographic products will need custom-made integrations, compounded by cloud-native KM solutions that typically use proprietary interfaces requiring integration with key management as a service solutions (KMaaS) or customized bring your own key (BYOK) integrations with each cloud service.

EKM can be deployed as a software or hardware appliance. It achieves a security-accredited standard under NIST FIPS 140-2, ranging from Level 1 (software lowest security) to a pure implementation as a hardware security module (HSM) achieving Level 4. EKM provides management of products that operate across structured and unstructured data storage platforms. Gartner finds that most vendors offering EKM and cryptographic products still prefer to rely on a protectionist strategy in which the cryptographic products use proprietary integration protocols and do not support KMIP, even though their EKM products do support KMIP.

This creates a barrier to the adoption of EKM across multiple vendor products that do not integrate. It also creates a time-consuming project if the vendor product is changed, because all data will need to be decrypted, then re-encrypted with the new product.

Cryptography is an important access control, and the EKM policies define the granularity of protection applied and linked to active directory. As such it provides a means to ensure access controls are applied more consistently across a variety of storage platforms. EKM should be applied as part of a broader set of security controls through the data security governance (DSG) framework, with products such as data-centric audit and protection (DCAP), data loss prevention (DLP), and identity and access management (IAM). An EKM policy must:

- Plan for disaster recovery situations throughout the key life cycle, including key backup, recovery, escrow processes or changes to algorithms.
- Enable consistent implementation of data security policies across different silos, such as databases, file shares, big data and public cloud environments.

The challenges of implementing an enterprisewide data security policy in the wake of incompatible vendor products and managing EKM through separate, business-focused security teams must be addressed. Focus on reducing the number of cryptographic products deployed by different vendors, while the market continues to evolve.

Some storage and self-encrypting-drive vendors (which do not offer EKM products) are complying with the KMIP standard. However, until bidirectional support becomes more commonplace, enterprises must select one of two strategies:

- Deploy products from more than one vendor across different silos — clients will gain the benefit of best-of-breed products, but this results in uncoordinated EKM and data access policies.
- Deploy a single vendor's product across multiple silos — this provides consistent EKM and data access policies, but will require operational or functional compromises.

Use the DSG framework to assess how EKM can be implemented with other complementary security products. This can help meet growing data residency and compliance requirements.

Ensure that the adoption of public cloud environments is part of the policy review and vendor selection processes.

Business Impact: Enterprises must develop a business-led, data security strategy that will lead to the appropriate selection of multiple, siloed KM products or a single EKM. Implement a consistent, enterprise-class strategy, thereby protecting data and achieving legal and regulatory compliance, while limiting risk in a demonstrable way, and reducing operational and capital costs.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: IBM; Micro Focus; PKWARE; Protegrity; QuintessenceLabs; StorMagic; Thales eSecurity; Townsend Security

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"

"Prioritize Enterprisewide Encryption for Critical Datasets"

"Key Management as a Service Exposes Different Risks to Data in Public Clouds"

"Better Safe Than Sorry: Preparing for Crypto-Agility"

Identity-Based Segmentation (Microsegmentation)

Analysis By: Adam Hils; Neil MacDonald; Jeremy D'Hoinne

Definition: Identity-based segmentation (also referred to as microsegmentation, zero trust network segmentation or logical segmentation) uses policy- and workload-identity-driven firewalling (typically software-based) or differentially encrypted network communications to isolate workloads, applications and processes in data centers, public cloud IaaS and containers. This includes workloads that span on-premises and multiple public cloud IaaS providers.

Position and Adoption Speed Justification: With more servers being virtualized or moving to infrastructure as a service, traditional firewall, intrusion prevention, and antivirus rarely 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 further segmentation and zero trust networking based approaches 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 complex, if not impossible, to apply. Further, 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 also has 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/service identities as the foundation for adaptive application segmentation policies. This is critical to enforce segmentation policies in the dynamic networking environments used within container-based environments.

User Advice: Security and risk management leaders should use the following guidelines when implementing identity-based segmentation:

- Don't oversegment. Oversegmentation is the leading cause of failure and an unnecessary expense for segmentation projects.
- Don't use IP addresses or network location as the foundation for segmentation policies. Use the identities of applications, workloads and services, either via logical tags, labels, fingerprints or stronger identity mechanisms such as certificates.
- Start with a network flow mapping project to understand application and server flows before undertaking the segmentation project. Leading microsegmentation vendors provide this capability to help enterprises on their journey to microsegmentation.
- 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 when segmenting. Consider the business processes and the value information being protected.
- Consider products with established security expertise, such as those from security vendors targeting this market. Isolation alone isn't segmentation: If mediated communication is needed between zones, this requires different functionality than merely keeping them apart.
- Architect for consistent segmentation policies across on-premises and public cloud IaaS; using approaches such as host-based controls or using the native APIs of the underlying cloud fabric. Alternatively, several vendors use virtual appliance or container-based approaches to provide this capability.
- Ensure that your segmentation strategy extends into containers and container networking environments.
- Plan for coexistence of traditional firewalls and microsegmentation approaches for at least the next five years and seek products that can support using both.

Business Impact: Identity-based segmentation is a form of zero trust networking and is used to reduce the "blast radius" if and when an attacker breaches the enterprise network by reducing the ability of the attacker to spread laterally. It also enables enterprises to enforce consistent segmentation policies across on-premises and cloud-based workloads, including workloads that host containers meeting compliance requirements. In addition, several solutions provide extensive visibility and visualization of flows for baselining and anomaly detection. For some specific scenarios, like PCI reduction of scope, microsegmentation can be used to avoid costly network reconfiguration.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Amazon Web Services; Cisco; Edgewise; GuardiCore; Illumio; Microsoft; Palo Alto Networks; ShieldX; vArmour; VMware

Recommended Reading: "Market Guide for Cloud Workload Protection Platforms"

"Zero Trust Is an Initial Step on the Roadmap to CARTA"

"Control Network Security Complexity, Inefficiencies and Security Failures by Minimizing Firewall Diversity"

"Solution Comparison for Microsegmentation Products"

SD-WAN

Analysis By: Andrew Lerner

Definition: Software-defined wide-area network (SD-WAN) products replace traditional branch routers. They provide several features: dynamic path selection, based on business or application policy; centralized policy and management of WAN edge devices; 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.

Position and Adoption Speed Justification: Rampant client interest in SD-WAN products continues, and we estimate that more than 25,000 customers have deployed SD-WAN products in production networks, which is over 600,000 branch locations. We expect continued rapid growth of SD-WAN deployments, and forecast vendor revenue to grow at a more than 23% compound annual growth rate (CAGR) for the next three years. In conjunction with a hybrid WAN topology, 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. Large numbers of vendors (several dozen) are competing in the market, including incumbent network and security vendors, startup vendors and smaller vendors with regional or vertical focus.

User Advice: Networking leaders should refresh their branch WAN equipment by implementing SD-WAN when they're migrating apps to the public cloud, building hybrid WANs, equipment is at end of life, or managed network service/MPLS contracts are up for renewal. Follow a comprehensive SD-WAN selection process by evaluating a diverse set of vendors and running a pilot. This is particularly important now, because not all offerings on the market are stable and scalable. 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).

Business Impact: The main purpose of emerging SD-WAN products is to 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 approach are substantial, compared with traditional, router-based WAN architectures, including reduced capital and operational expenditures (capex/opex) at the WAN edge, improved provisioning times, and the potential for enhanced branch availability.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Aryaka; Cato Networks; Cisco; Fortinet; Palo Alto Networks; Silver Peak; Versa Networks; VMware

Recommended Reading: "Technology Insight for SD-WAN"

"Magic Quadrant for WAN Edge Infrastructure"

"Solution Comparison for SD-WAN"

"Assessing the Strengths and Weaknesses of SD-WAN Technology"

Secure Web Gateways

Analysis By: Lawrence Orans; Peter Firstbrook; John Watts

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 on-premises appliances (hardware and virtual), cloud-based services or hybrid solutions (cloud and on-premises).

Position and Adoption Speed Justification: SWGs have progressed to the Slope of Enlightenment, as the trend toward cloud-based services continues to strengthen. Gartner's volume of inquiries for cloud-based SWG services outpaces the inquiry volume for appliance-based SWGs by a factor of more than four-to-one.

The market outlook for SWG is positive, and new competitors have emerged. CASB vendors Bitglass and Netskope have begun to offer SWG functionality. Palo Alto Networks is also emerging as a competitor with its firewall-based Prisma Access solution. And, Akamai has introduced a proxy-based SWG cloud service. In the midmarket, SWGs face some pressure from firewall vendors that offer basic URL filtering (not complete SWG functionality) as an optional feature. Cloud-based recursive DNS solutions have also become a popular solution with midmarket customers.

As highlighted by Gartner's SASE framework (see "The Future of Network Security Is in the Cloud"), enterprises continue to seek a broader menu of security services from their cloud security service providers. The SWG market continues to evolve as vendors add services such as CASB, zero trust network access (ZTNA), remote browser isolation (RBI) and others to their list of available offerings.

User Advice: Security and risk management leaders responsible for endpoint and network security should take a fresh look at the SWG market and not automatically renew traditional approaches. Critical capabilities to seek out include purpose-built cloud solutions, advanced threat protection (for example, sandboxing), and CASB services to control and monitor access to SaaS applications. Some cloud SWG services offer outbound firewall functionality. Also, many SWGs can now apply policy to SaaS applications (including shadow IT) by integrating with CASB solutions (the CASB services share their cloud application discovery and risk database with the SWG providers). ZTNA functionality (primarily implemented as an alternative to traditional VPNs) is another important feature to consider. Enterprises may adopt or change SWG providers to accommodate growth or improve risk posture by applying best-of-breed security to web traffic.

Business Impact: Secure web gateways provide an additional layer of protection against destructive attacks such as ransomware, 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). When the SWG service also includes a firewall-as-a-service option, it can be used to eliminate branch office firewalls. Also, cloud SWG services can provide protection for mobile users that are off the corporate network.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Cisco; ContentKeeper; Forcepoint; iboss; McAfee; Menlo Security; Netskope; Sangfor Technologies; Symantec; Zscaler

Recommended Reading: "Magic Quadrant for Secure Web Gateways"

"Critical Capabilities for Secure Web Gateways"

"How to Avoid Failures When Migrating to a Cloud-Based Secure Web Gateway"

"The Future of Network Security Is in the Cloud"

Network Firewalls

Analysis By: Rajpreet Kaur; Adam Hils

Definition: The network firewall market is composed primarily of firewalls offering bidirectional controls (both egress and ingress) for securing networks. These networks can be on-premises, hybrid (on-premises and cloud), public cloud or private cloud. The product has capability to support one or more firewall deployment use cases such as perimeter, SMBs, data center, cloud and distributed offices.

Position and Adoption Speed Justification: Network firewalls are not restricted to appliance only vendors anymore and extend to vendors offering virtual versions, firewall as a service (FWaaS), native IaaS firewall controls or distributed identity-based firewalls. While the basic features in network firewalls such as anti-malware, IPS, application control and URL filtering have been commoditized, network firewalls are constantly challenged with evolving environments and threat landscapes and have evolved from basic stateful inspection capabilities to protecting cloud workloads. Network firewalls are evolving toward network security platforms offering automation and integration capabilities with other security products such as EDR and NAC. The vendors are also providing better API integration capabilities to integrate with other security products in the network. Firewall vendors regularly introduce better-performing models to overcome performance issues and newer FWaaS offerings also overcome performance issues through elastic scalability. Gartner still sees SSL/TLS decryption as having major impact on the performance of the appliances. Firewall vendors are working toward offering mature threat detection and prevention capabilities beyond network sandboxing such as behavioral analytics, deep learning, deception techniques. Gartner observes network firewall vendors introducing extended detection and response (XDR) portals to help enterprises improve threat detection capabilities. The firewall market is also growing with new FWaaS offerings driven by the sudden move to remote work in 2020. Gartner observes network firewall vendors acquiring and introducing new security products which moved the position on the Hype Cycle from post-trough to preplateau this year, but these products are generally still poorly integrated which limits their value. Network firewall vendors have been slow in offering support for public cloud platforms and DevSecOps and clients report struggling with compatibility and support related to issues.

User Advice: Firewalls come with multiple features which are offered as software subscriptions. Carefully evaluate the feature which you require today as well as throughout the life cycle of the firewall to decide the subscriptions you will require. As the firewall vendors are growing the breadth of their security products portfolio, buyers can often get carried away to consolidate toward a single vendor for many of their security needs with the benefit of automation and ease of management as marketed by majority of vendors. Buying products from the same vendor does not guarantee automation and reduced complexities. Gartner highly recommends that if the primary requirement to consolidate toward a single vendor is automation, integration and ease of management, do not finalize the offering without evaluating the required features in your environment.

Business Impact: Network firewalls continue to be the baseline requirement to provide the initial set of preventative controls for an organization. Network firewalls market is evolving toward becoming a network security platform protecting hybrid environments and offering automation and integration capabilities with other security products playing a much bigger role in the overall security architecture. Firewall vendors are developing capabilities or acquiring other vendors to meet multiple different firewall use cases, such as WAN edge with SD-WAN capabilities, FWaaS, and protecting public cloud. Hence, onboarding a firewall vendor can help an enterprise consolidate toward a single vendor for their multiple security requirements.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Check Point Software Technologies; Cisco; Forcepoint; Fortinet; Hillstone Networks; Huawei; Juniper Networks; Palo Alto Networks

Recommended Reading: "Magic Quadrant for Network Firewalls"

"Next-Generation Firewall Hype Has Become an Obstacle for Enterprises"

"How to Maximize Value in Firewall Contract Negotiations"

DDoS Defense

Analysis By: Lawrence Orans; Rajpreet Kaur; Claudio Neiva

Definition: Distributed denial of service 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.

Position and Adoption Speed Justification: This year, distributed denial of service (DDoS) defense progresses slightly to the right along the Slope of Enlightenment. There have been no record-breaking DDoS attacks since a 1.7 Tbps attack in February 2018. In response to that attack, and in order to keep up with advances made by attackers, many DDoS mitigation providers continue to invest in their infrastructure (for example, many scrubbing center providers have added more scrubbing centers and more aggregate bandwidth in recent years). The shifting threat landscape requires that DDoS mitigation vendors continue to evolve their products and add additional detection techniques to thwart more complex and varied DDoS attacks. The good news is that today, enterprises have more choices than ever for DDoS mitigation services, as the three leading IaaS providers now have mature offerings. Nonetheless, DDoS attacks continue to be a serious threat to enterprises.

User Advice: DDoS mitigation services should be a standard part of business continuity/disaster recovery planning, and they should be included in all internet service procurements when the business depends on the availability of internet connectivity. Most enterprises should look at 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). To defend against complex, application-based attacks, a hybrid solution of local protection (on-premises DDoS appliances) and cloud-based mitigation services is a strong option. The content delivery network (CDN) approach to DDoS protection is also a strong approach, particularly when the organization is already using a CDN for content distribution to improve the performance of its website. However, the CDN approach only protects websites. It does not protect against attacks aimed at nonweb targets (for example, corporate firewalls, VPN servers and email servers). Another option for DDoS mitigation services comes from the IaaS providers. The leading IaaS providers (Amazon Web Services [AWS], Microsoft Azure and Google Cloud) all offer basic and advanced (fee-based) DDoS mitigation services.

Because of the increased awareness of DDoS attacks, more CSPs and hosters have entered the market for DDoS mitigation services. Some have built their own infrastructure, whereas others have partnered with specialty DDoS mitigation service providers. Still others have actually been offering services over many years, which has enabled them to develop strong expertise. Prospective customers should gauge the level of experience of CSPs and make sure that the price of their services reflects their level of experience.

Enterprises that are frequent targets of DDoS attacks should consider the “always on” option available from scrubbing center providers. With this model, the customer pays a premium of approximately 50% over the “on-demand” service, so that traffic always flows through the scrubbing center before it arrives at the customer’s website (or any destination that they are protecting). Enterprises should also note that the average attack size is approximately 15 Gbps (according to published reports from several DDoS mitigation providers).

The increased competition in the DDoS mitigation market has also led to more competitive pricing and pricing models. Many providers now offer packages that are more cost-effective because they include a fixed number of mitigations per year (as opposed to an unlimited mitigation model). Enterprises that are at less risk of being attacked frequently are good candidates for these new pricing models with a fixed number of mitigations. These enterprises should also consider the less expensive services from ISPs and hosters.

Business Impact: 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. Also, if the enterprise does not defend itself properly during an attack, its reputation could be negatively impacted. Thus, DDoS mitigation services are a highly valuable investment for every enterprise that needs to protect its web presence and its access to the internet.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

Sample Vendors: Akamai; AT&T; F5; Imperva; Link11; Neustar; Nexusguard; NETSCOUT (Arbor Networks); Radware; Verizon

Recommended Reading: "Market Guide for DDoS Mitigation Services"

"Solution Comparison for DDoS Cloud Scrubbing Centers"

"DDoS: A Comparison of Defense Approaches"

Network Access Control

Analysis By: Claudio Neiva

Definition: Gartner defines network access control (NAC) as technologies that enable organizations to implement policies for controlling access to corporate infrastructure by both user-oriented devices and cyber-physical devices such as Internet of Things (IoT) and operational technology (OT) devices. Policies may be based on authentication, endpoint configuration (posture) or users' role/identity.

Position and Adoption Speed Justification: NAC solutions are used to profile and identify wired and wireless devices and to assess their configuration and hygiene. For example, organizations may grant wireless local-area network (WLAN) access to tablets and smartphones, but use different context variables (e.g., location, time/date, day of the week or even type of device) to determine whether the permission will be only for internet access or limited access to the enterprise network.

Gartner continues to see the lack of visibility and the need to control devices connecting to the corporate network during client engagements. Alongside increased visibility, NAC use cases include management of access from an external contractor or guest, and management of non-user-oriented devices, such as IoT/OT, which, from specific verticals (e.g., medical and manufacturing) have shown a need for device detection and segmentation to maintain security and availability.

The following capabilities should be evaluated through NAC selections:

- Policy server
- Visibility and reporting
- Device security posture check
- Guest management and identity
- Integration with other solutions
- Total cost of ownership (TCO)

User Advice: NAC solutions should be implemented in phase to minimize user friction and network disruptions. Implement NAC to deliver visibility (for example, which devices are connected to your network) and control (allow or deny access) over your corporate network. Integrate with existing asset management solutions bidirectionally to help maintain an accurate list of devices connected to the organization. Before moving to enforcement mode, ensure that your governance decisions and NAC solution choices align with your environment.

Business Impact: NAC helps enterprises provide a flexible approach to securely support BYOD, guest, and contractor access policies, often leveraging integration with UEM solutions. NAC will enable enterprises to ensure that UEM is in use on mobile devices and to provide the appropriate level of network access for compliant and noncompliant endpoints. NAC also improves an enterprise's security posture by providing visibility and control of devices that are on its network.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Cisco; Extreme Networks; Forescout Technologies; Fortinet (Bradford Networks); HPE (Aruba); OpenCloud Factory; Portnox; Pulse Secure

Recommended Reading: "Toolkit: Sample RFP for Network Access Control"

"How to Implement Network Access Control in Three Phases"

"Predicts 2020: As IoT Use Proliferates, So Do Signs of Its Increasing Maturity and Growing Pains"

"How to Secure the Enterprise Against the Internet of Things Onslaught"

Secure Enterprise Data Communications

Analysis By: Rob Smith

Definition: Secure enterprise data communications solutions provide encrypted and authenticated "virtual" connections for networks and apps. It is a broad category that supports site-to-site bridging, as well as individual remote and mobile users, and relies typically on IPsec and Transport Layer Security (TLS) for confidentiality.

Position and Adoption Speed Justification: The recent surge in remote working has made virtual private network (VPN) one of the most important technologies in IT, as the need for remote work reached unprecedented levels. The VPN aspects of this profile are mostly mature with little change and are heading rapidly to plateau. For example, site-to-site secure connections based on traditional VPN are barely considered competitive. Although in extremely high demand, remote PC access methods have not changed noticeably for more than a decade. Remote-access VPN access has proved challenging, due to limited bandwidth and hardware constraints, forcing the push of infrastructure into the cloud. This means that secure browser apps and other apps using TLS under the hood become the de facto standard. Software-defined perimeter (SDP), software-defined WAN (SD-WAN) and cloud app providers are offering their own virtual privacy connections. Cloud access security brokers (CASBs) are creating the equivalent of the enterprise gateway in the cloud, complete with centralized identity management and managed encrypted connections to business user destinations. Zero-trust network access (ZTNA) is also a potential replacement for VPN, as users migrate to cloud applications and no longer need traditional on-premises access.

User Advice: Companies that find themselves needing to renegotiate legacy VPN contracts should take a careful look at the timing of their cloud strategies. In many cases, site-to-site and end-user VPNs will be short-term investments, which will be replaced by cloud services that include data-in-transit encryption. In other cases, the transition could take many years. As migration to the cloud is completed, legacy VPNs will serve decreasing needs for on-premises services and servers, while the main business processes are incrementally modernized, web-enabled and migrated to the cloud. Secure communications between apps and servers in the cloud context will increasingly be handled directly by the apps and will not be managed under legacy VPN configurations.

Business Impact: Enterprises are putting their business infrastructures in the cloud, while their endpoint business processes are, in many cases, still designed for local, on-premises services and company endpoints. Security and risk management (SRM) leaders should ensure that architectural changes preserve security, while minimizing impacts on usability. Cloud-first companies must conduct an end-of-life analysis of legacy secure communications needs before investing further in conventional solutions.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Check Point Software Technologies; Cisco Systems; F5; Microsoft; NetMotion Software; Palo Alto Networks; Pulse Secure

Recommended Reading: "Solving the Challenges of Modern Remote Access"

"Market Guide for Secure Enterprise Data Communications"

"Market Guide for Zero Trust Network Access"

"Recreate Desktop Security After Users Move to the Cloud"

Web Application Firewalls

Analysis By: Jeremy D'Hoinne; Adam Hils; John Watts

Definition: Web application firewall (WAF) is a technology deployed in-line to protect web applications and APIs. WAFs focus primarily on exploits, such as cross-site scripting (XSS) and SQL Injection, in commercial applications or custom-developed code. It may include protection from other attacks, such as session manipulation and logic abuse. Many WAFs include a combination of negative and positive security models. A combination of DDoS protection, WAF, bot mitigation and API protection is also known as Web Application and API Protection (WAAP).

Position and Adoption Speed Justification: WAF is moving closer to the plateau. Many organizations adopt a "cloud first" strategy when selecting a WAF solution to protect public facing applications. Web Application and API Protection (WAAP) services and WAF appliances will ultimately end as separate markets, with WAF appliances being more a specialized control. Today, organizations continue to compare both solutions for similar use cases, with some enterprises requiring hybrid management capabilities. Vendors might offer managed services for their WAAP and sometimes make it mandatory because their self-service user interface is not fully featured. WAAP are often bundled with content delivery networks (CDNs), bot mitigation, protection against distributed denial of service (DDoS) and API security. Leading cloud WAAP vendors have made progress in their ability to block malicious bot, often through the acquisition of a specialized vendor. API protection continues to lag behind other features. Progresses are slow and focused on recommending API policy based on predefined schema definitions. Mobile applications and the growing number of publicly exposed APIs create new development opportunities for WAFs. Gartner observes, though, that innovation continues to happen mostly outside of the traditional WAF vendor landscape.

In 2019, Many WAF vendors acquired bot mitigation solutions, in order to improve their capabilities in this area.

Unlike WAF appliances, WAAP are growing and take market shares, especially because of their ability to be easily deployed in front of the new, still small-scale digital business applications. Organizations moving critical web applications to the public cloud frequently select WAAP from WAF, CDN or from IaaS providers, to shield these applications. These solutions can be delivered and managed more flexible than a traditional virtual appliance.

Many enterprises use WAFs to protect their public-facing applications, with a minority of these projects being driven chiefly by compliance concerns. WAAP providers focus on security improvements, and CDN vendors integrate their WAAP with their edge security features. As network-only controls, delivered from the WAAP or from the WAF appliance might be not sufficient to ensure a good security and a low false positive rate, Gartner anticipates a growing need for in-client or in-server app controls. However, privacy concerns on the client, and deployment frictions on the server might slow down the progress toward more “self-defending” applications. Similarly, containerization of WAF and WAAP engines might gain in popularity because they provide more deployment flexibility directly within container workloads or as a sidecar container/sidecar proxy depending on the app architecture and infrastructure.

Because the responsibility for web application security is shared across several teams within organizations, the continued challenge of a fragmented buying center hampers adoption of WAF technology. Gartner observes that new business applications, often developed with agile methodologies (Mode 2 project), sometimes get a different WAF solution than the one protecting the critical services. This two-tier approach is unusual in security markets, where the benefits are rarely worth the burden of managing duplicate technologies.

User Advice: Enterprises should first decide on their preferred deployment option: cloud as a service, virtual appliance (deployed on-premises or on IaaS) or physical appliance. Prospective buyers should carefully evaluate expected benefits and challenges for WAAP. This includes simplicity and bundled protection with DDoS and bot mitigation and API security, deployment challenges, such as certificate management for TLS decryption, data privacy, attacks on origin Internet Protocol (IP) and limited control over configuration.

As more applications are API-driven and follow agile development principles, prospective buyers should evaluate WAF’s API protection features. WAFs might compete against API gateways, often as part of a full life cycle API management solution.

WAF themselves are increasingly API-driven. Enterprises should also investigate this capability, such as APIs provided for managing the WAF, to use for automated deployment in a DevOps environment if required.

Enterprises should carefully review how WAFs integrate with security monitoring tools, web access management (WAM), API gateways, bot management, content delivery network, distributed denial of service protection, online fraud detection and other components of the data center infrastructure.

Business Impact: WAFs provide specific protection for data center servers and hosted applications and prevent initial breaches that could give access to important data that often lives behind web applications.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Akamai; Amazon Web Services (AWS); Barracuda; Citrix; F5; Fortinet; Imperva; Radware; Rohde & Schwarz; Signal Sciences

Recommended Reading: "Magic Quadrant for Web Application Firewalls"

"Critical Capabilities for Cloud Web Application Firewalls Services"

"Defining Cloud Web Application and API Protection Services"

Entering the Plateau

IPS

Analysis By: Sam Evans; Craig Lawson; John Watts

Definition: Intrusion prevention system (IPS) technologies provide first-generation IPS capabilities (e.g., threat and vulnerability exploitation detection and blocking threats in-line), along with application awareness and full-stack visibility, user visibility, and context and content awareness, with some using advanced analytics like UEBA. Upgrade paths are also provided that integrate new information sources including threat intelligence, advanced threat detection, advanced analytics and network sandboxing.

Position and Adoption Speed Justification: IPS vendors have found increasing market acceptance as they've introduced support for public cloud and added UEBA analytics features on top of their existing IPS capabilities. Most stand-alone vendors have NGIPS offerings today, and are competing for market share based on the robustness of features. IPS will remain viable for clients that value best-of-breed in-line network threat detection, prevention, response and compliance use cases. Through 2020, growth will slowly continue within this market. IPS is still widely deployed and has seen significant innovation through the use of advanced analytics like machine learning to deliver UEBA capabilities. This is a welcome innovation to the IPS market.

User Advice: Network security administrators should consider replacing their internet-facing IPS with a stand-alone IPS appliance with NGIPS features that is deployed at the perimeter for threat prevention and internally for additional use cases. If you are unable to replace your existing IPS, then push your incumbent vendor to show you what NGIPS features it has incorporated, and to share its plans for introducing new features like advanced analytics. If you are replacing or installing a perimeter network firewall, then consider an NGFW that includes an NGIPS. IPS (deployed in-line or in detection-only mode) should be considered for internal deployment use cases, like preventing/detecting lateral movement and workstation compromise, advanced malware detection, virtual patching, public cloud and making use of advanced analytics using UEBA.

Business Impact: Like first-generation IPSs, NGIPSs improve network security by blocking attacks that are focused on exploiting vulnerabilities in the network and at endpoints, or by causing a denial of service. NGIPSs apply fuller stack inspection and new sources of intelligence to existing methods. All leading IPSs now have NGIPS features.

Using these techniques, IPS can help protect organizations against a range of costly threats that are network-borne.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

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

Recommended Reading: "Market Guide for Intrusion Detection and Prevention Systems"

Appendixes

Figure 3. Hype Cycle for Threat-Facing Technologies, 2019

Source: Gartner (July 2019)

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1: Hype Cycle Phases

Phase ↓	Definition ↓

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

Source: Gartner (June 2020)

Table 2: Benefit Ratings

Benefit Rating ↓	Definition ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise

Benefit Rating	Definition
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (June 2020)

Table 3: Maturity Levels

Maturity Level	Status	Products/Vendors
Embryonic	▪ In labs	▪ None
Emerging	▪ Commercialization by vendors ▪ Pilots and deployments by industry leaders	▪ First generation ▪ High price ▪ Much customization
Adolescent	▪ Maturing technology capabilities and process understanding ▪ Uptake beyond early adopters	▪ Second generation ▪ Less customization
Early mainstream	▪ Proven technology ▪ Vendors, technology and adoption rapidly evolving	▪ Third generation ▪ More out-of-box methodologies
Mature mainstream	▪ Robust technology ▪ Not much evolution in vendors or technology	▪ Several dominant vendors

Maturity Level	Status	Products/Vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (June 2020)

Document Revision History

Hype Cycle for Threat-Facing Technologies, 2019 - 12 July 2019

Hype Cycle for Threat-Facing Technologies, 2018 - 13 July 2018

Hype Cycle for Threat-Facing Technologies, 2017 - 17 July 2017

Hype Cycle for Infrastructure Protection, 2016 - 6 July 2016

Hype Cycle for Infrastructure Protection, 2015 - 11 August 2015

Hype Cycle for Infrastructure Protection, 2014 - 30 July 2014

Hype Cycle for Infrastructure Protection, 2013 - 31 July 2013

Hype Cycle for Infrastructure Protection, 2012 - 31 July 2012

Hype Cycle for Infrastructure Protection, 2011 - 10 August 2011

Hype Cycle for Infrastructure Protection, 2010 - 20 August 2010

Hype Cycle for Infrastructure Protection, 2009 - 28 July 2009

Hype Cycle for Infrastructure Protection, 2008 - 22 September 2008

Hype Cycle for Infrastructure Protection, 2006 - 10 July 2006

Recommended by the Author

Understanding Gartner's Hype Cycles

Market Guide for Network Detection and Response

Market Guide for Intrusion Detection and Prevention Systems

Magic Quadrant for Network Firewalls

Magic Quadrant for Secure Web Gateways

Magic Quadrant for Endpoint Protection Platforms

Recommended For You

Market Guide for Zero Trust Network Access

Market Guide for Email Security

Magic Quadrant for Network Firewalls

Critical Capabilities for Network Firewalls

Gartner Peer Insights ‘Voice of the Customer’: Email Security