Hype Cycle for Threat-Facing Technologies, 2017

Published: 17 July 2017 **ID:** G00313843

Analyst(s): Greg Young

Threat-facing technologies protect IT infrastructure, including networks, hosts and things. Driven by persistent threats and technology changes, most of the evolution of the technologies on this Hype Cycle is concerned with the cloud, analytics and advanced threats.

Table of Contents

List of Tables

List of Figures

Analysis

What You Need to Know

In 2017, the threat level to enterprise IT remains at blistering levels, with daily accounts in the press of large breaches and attacks being the new normal. No single safeguard will protect against all possible attacks, and enterprises are unlikely to be able to deploy all of the possible technologies and service defenses presented in this Hype Cycle, so difficult choices must be made. This Hype Cycle can be a useful visual guide in assessing the security technology and security service choices that are available to protect enterprises' IT infrastructures and resources against threats. Formerly known as the Hype Cycle for Infrastructure Protection, the name has been changed to better reflect that, although infrastructure is key, what we protect today goes beyond this to include data and all IT. The underlying goal is to protect against threats.

Threat-facing technologies are segmented according to the infrastructure component being protected: the network, host system data or applications. Technology or services alone cannot provide effective infrastructure protection. Effective processes, as well as adequate deployment and operations staffing, are also required. Inadequate processes and staffing are a frequent cause of ineffective infrastructure protection technology and service deployments, and the worldwide shortage of security professionals should be a weighted factor in selecting or retiring any infrastructure protection.

The structure of enterprise IT organizations remains the greatest barrier to single-vendor solutions, and this will not change because there are necessary and good reasons for specialization and segregation of duties. However, there is the increasing opportunity for intelligence exchange between products and services to assist in correlation and to provide context, rather than for a single solution that protects all infrastructure components. However, interoperability is limited at present, and no "mega-convergence" of safeguards is coming. This Hype Cycle illustrates that the primary receptors of intelligence from other technologies and services are those on or near the plateau, such as security information and event management (SIEM), firewalls and intrusion prevention systems (IPSs). Management consoles are mostly proprietary to single vendors.

Enterprises have been obligated to counter new threats, primarily with additional technology and service deployments, because incumbent security vendors have been slow to add new features or integrate acquired products. This puts pressure on security budgets. The idea of all-cloud, all-virtual, or single-vendor security remains a myth. Most enterprises' IT is a hybrid of cloud and noncloud, and security is the same.

The Hype Cycle

Gartner subdivides IT security into three macrodomains:

- Identity and access management (IAM) — "letting the good guys in"
- Business continuity and governance — "keeping the wheels on"
- Threat-facing technologies — "keeping the bad guys out"

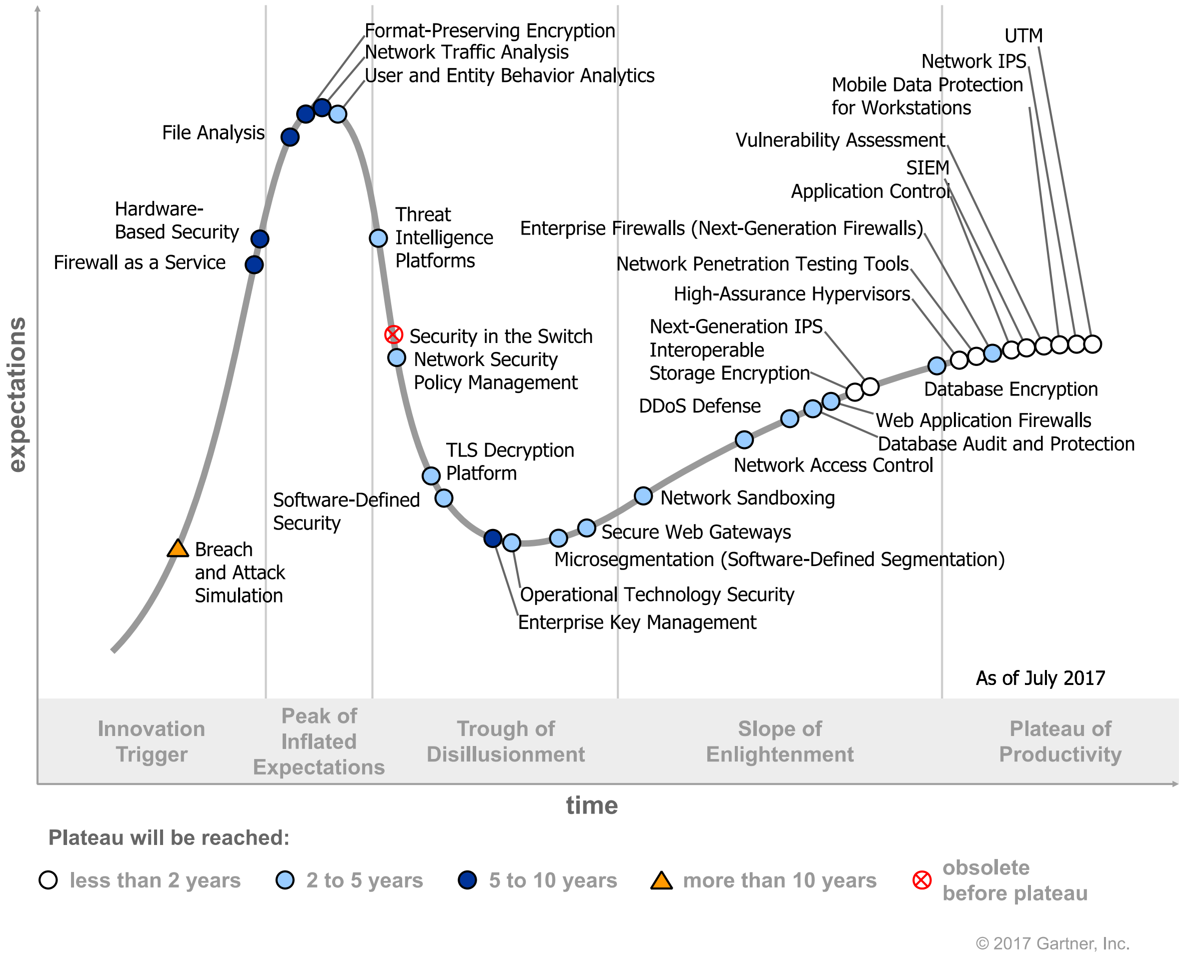
Being solely concerned with threats, these technologies are constantly changing, because they need to be reactive to new types and vectors of attack.

This Hype Cycle shows a change in trend, with the last four years having a clustering of technologies at the slope and plateau. In 2017, technologies are more evenly distributed across the Hype Cycle. The Trough of Disillusionment is quite full, highlighting that newer technologies for virtual security and threat detection have been highly hyped and these markets have been overmarketed and underdeveloped. Overall, there are almost too many tools that enterprises could adopt, exceeding their ability to develop supporting processes and ongoing staff operations. The overhyping of products that should, in many cases, only be features within other products has "removed the oxygen from the room," thereby stifling real innovation. Most of what is labeled a "new approach" to stopping threats is just a minor step in the "move and countermove" of today's security.

Plateau technologies must not be ignored, as older threats that haven't gone away still require defense. The efficiency of more-advanced, yet not fully mature, protection technologies is negatively affected in environments where the foundational technologies are not good enough. Gartner research shows that almost all successful attacks exploit vulnerabilities known for more than a year. These known threats are countered with plateau technologies that are already in place (for example, antivirus and IPSs). The Hype Cycle can be viewed as, from right to left, shifting from coarse to finer filters. If they want to combat these threats, then enterprises need to adopt signatureless and behavior-based advanced threat defense technologies.

Highlighting the fast changes in this market are six new technologies. Threats change, and so do the technologies they attack.

Figure 1. Hype Cycle for Threat-Facing Technologies, 2017

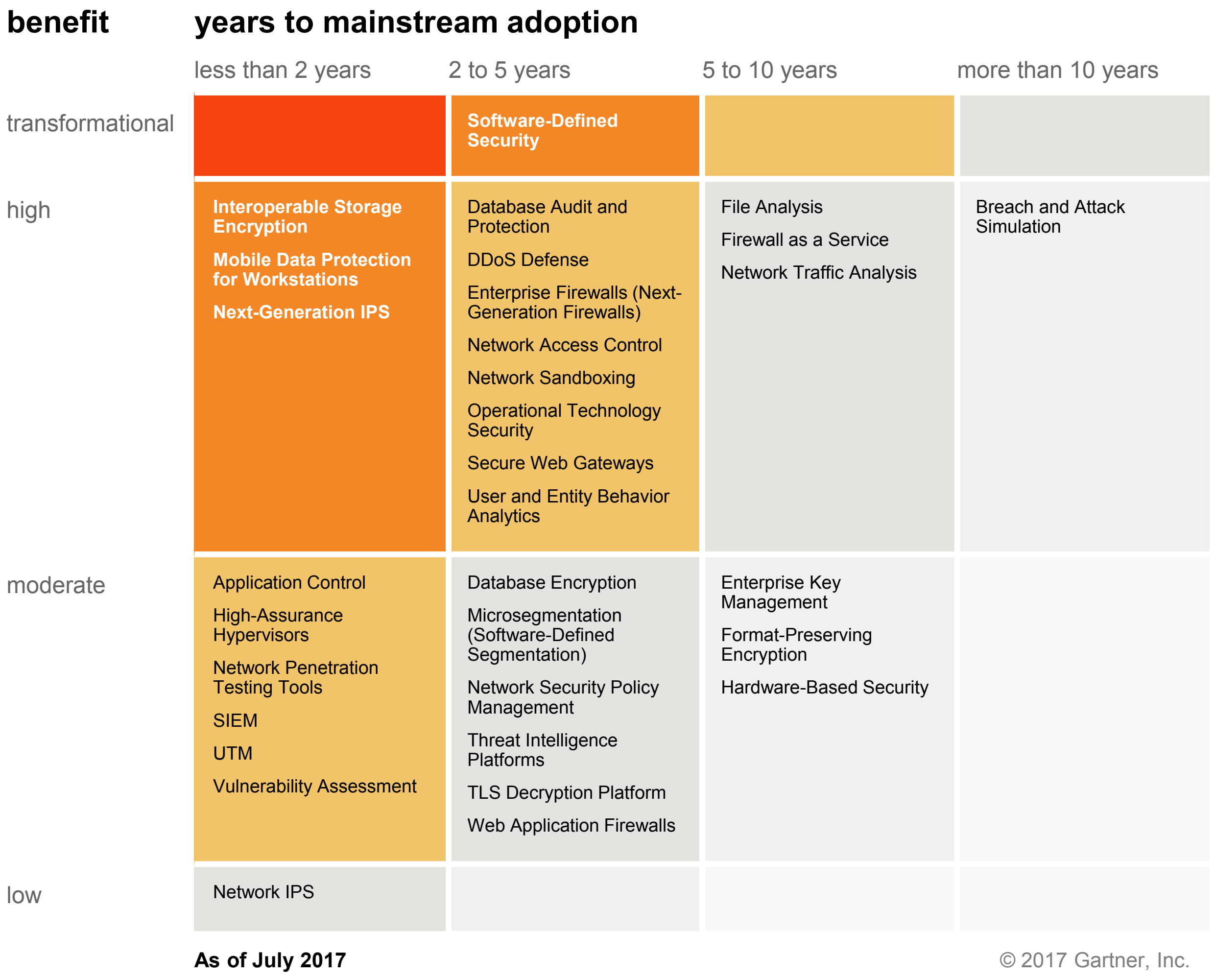


Source: Gartner (July 2017)

The Priority Matrix

Infrastructure protection is driven by the need to protect against "legacy" threats, while reacting to new and emerging threats. Infrastructure protection technologies and services that enable the consolidation of legacy approaches, as well as reduce operational burden, will experience greater adoption during the short-term and the midterm. Many organizations still need to improve detection and protection strategies for targeted attacks. This drives the adoption of technologies that counter advanced threats or focus on targeted malware filtering. Early adopters of these technologies have been organizations with higher-than-average security requirements; however, point solutions are no longer required, because capabilities are provided as features of mainstream offerings (see Figure 2).

Figure 2. Priority Matrix for Threat-Facing Technologies, 2017



benefit	years to mainstream adoption less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational		**Software-Defined Security**		
high	**Interoperable Storage Encryption** **Mobile Data Protection for Workstations** **Next-Generation IPS**	Database Audit and Protection DDoS Defense Enterprise Firewalls (Next-Generation Firewalls) Network Access Control Network Sandboxing Operational Technology Security Secure Web Gateways User and Entity Behavior Analytics	File Analysis Firewall as a Service Network Traffic Analysis	Breach and Attack Simulation
moderate	Application Control High-Assurance Hypervisors Network Penetration Testing Tools SIEM UTM Vulnerability Assessment	Database Encryption Microsegmentation (Software-Defined Segmentation) Network Security Policy Management Threat Intelligence Platforms TLS Decryption Platform Web Application Firewalls	Enterprise Key Management Format-Preserving Encryption Hardware-Based Security	
low	Network IPS			

As of July 2017

© 2017 Gartner, Inc.

Source: Gartner (July 2017)

Off the Hype Cycle

Stateful Firewalls has been removed, reflecting that most deployed firewalls are Enterprise or Next-Generation Firewalls. Hardware-Based Security has been removed, because it has become less relevant in this software-defined world.

On the Rise

Breach and Attack Simulation

Analysis By: Jeremy D'Hoinne; Matthew T. Stamper

Definition: Breach and attack simulation (BAS) technologies use agents and other means to simulate attacks against enterprise infrastructure. BAS can effectively emulate insider threats, lateral move or data exfiltration techniques without the risks to production environments inherent with other testing approaches. Breach and attack simulation cannot replace sophisticated red team penetration testing, including social engineering, but provides automated, continuous security assessment for the parts of the infrastructure than can be emulated.

Position and Adoption Speed Justification: The breach and attack simulation market is in its infancy, with only a few vendors having real customer deployments. The ability to provide continuous testing at limited risk is the key advantage of BAS technologies, which are used to alert IT and business stakeholders about existing gaps in the security posture, or validate that security infrastructure, configuration settings and prevention technologies are operating as intended.

To grow quickly, the BAS market will need to prove the value and accuracy of the security assessment resulting from simulated attacks, overcome deployment and maintenance challenges, and beat competition from adjacent markets with overlapping objectives, features or functionality, such as penetration testing, application security testing, vulnerability management or security operation center (SOC) training tools.

User Advice: Because breach and attack simulation relies on simulated attacks, the first thing to evaluate is the ability for a BAS technology to accurately emulate the risks faced by the organizations, and test their current security infrastructure. BAS deployment options influence what can be emulated or not. The size and frequency of updates for the portfolio of simulated attacks determines the value of repeating the audit, versus a point-in-time approach.

Prospective buyers should evaluate whether BAS would improve their existing risk assessment, threat monitoring and vulnerability management practices. They should not expect to replace targeted penetration testing with BAS. Organizations in regulated environments should discuss with their auditors to determine whether BAS technology can be used as a means to validate the efficacy of existing security controls.

Business Impact: Security and risk management leaders looking to build a proactive and safer risk assessment program can use BAS tools to automate a security evaluation process that otherwise has sporadic assessment frequency because it requires solid preparation and contractual agreement when operated on real production assets.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: AttackIQ; Core Security; Cymulate; SafeBreach; Verodin

Recommended Reading:

"Cool Vendors in Monitoring and Management of Threats to Applications and Data, 2017"

Firewall as a Service

Analysis By: Jeremy D'Hoinne

Definition: Firewall as a service (FWaaS) is a multifunction firewall delivered as a cloud-based service or hybrid solution (that is, cloud plus on-premises appliances). FWaaS is primarily delivered as a multitenancy infrastructure that is shared among multiple enterprises. The promise of FWaaS is to provide simpler and 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 is still emerging, with only a few vendor solutions, focusing on the branch security use case. FWaaS vendors are at the early stages of piloting or implementing their solutions with enterprise clients. FWaaS progresses closer to 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 and web application firewalls delivered as cloud services are growing more quickly than their appliance-based equivalents. FWaaS has fast growth potential. However, 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 points of presence. Failure to properly integrate with other cloud services and software-defined WAN (SD-WAN) could be another obstacle for FWaaS development.

User Advice: There is limited vendor choice for FWaaS, and products are still maturing. 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, and work better in environments where there is no DMZ with public-facing applications in branches. Another key aspect to evaluate is where the FWaaS provider has located its closest points of presence. Ensure that the FWaaS provider has presence close to all branch offices, i.e., latency should be no more than 20ms. If needed, verify the ability of the FWaaS provider to offer dedicated virtual instances dedicated to your enterprise, or other means used to ensure separations between the FWaaS's customers.

Multifunction security platforms often 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 potentially reduced cost by using a fully or partially hosted security workload.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Cato Networks; My Digital Shield; Opaq Networks; Secucloud; Versa Networks; Zscaler

Recommended Reading:

"What You Should Expect From Unified Threat Management Solutions"

"Next-Generation Firewalls and Unified Threat Management Are Distinct Products and Markets"

"Market Guide for WAN Edge Infrastructure"

"Technology Insight for Software-Defined WAN (SD-WAN)"

Hardware-Based Security

Analysis By: Neil MacDonald; Martin Reynolds

Definition: Hardware-based security uses hardware-based isolation techniques for security control isolation in host systems independent of OS integrity. Typical control isolation includes encryption key handling, secure I/O, authentication credentials and process monitoring. A key feature is isolated local memory not accessible to the OS, protecting against attackers and malicious DMA access, even if the OS or hypervisor is compromised.

Position and Adoption Speed Justification: As workloads are increasingly virtualized and cloud-based, there has been a shift to the use of security controls that are included with the workload they are protecting. However, if the workload is compromised, the security controls may be disabled or tampered with. Hardware-based security control isolation approaches isolate the workload security controls from a breach of the application or OS. These new protected spaces could also be integrated in containers deployed on the latest Intel servers based on the Skylake processor family, providing a trusted core to the container. This core can authenticate the container and its transactions. It is possible, in the future, that the entire function could run in an encrypted partition, improving security and perhaps supporting new business models based on renting algorithms.

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 Software Guard Extensions (Intel SGX) provide 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. Once set up and sealed, these processes can authenticate their code and gain access to credentials and encryption keys. The processes also run in encrypted memory, a feature intended for content protection and an indicator that development funding will remain strong. Content protection remains an unsolved problem in general-purpose computing.
- Microsoft is using hardware-based virtualization features in Windows 10 to create a protected code space for monitoring the operating system and providing security features with Device Guard and Credential Guard. Microsoft has also announced (but not yet shipped) Application Guard to isolate potentially compromised applications from the rest of the Windows OS.

User Advice:

- Hardware-based security is strong, but may still be broken by software flaws. Patch and remain vigilant for unexpected breaches.
- Although the SGX approach does not appear to break compatibility with the hypervisor, there may be unanticipated interactions. For example, it may not be possible to snapshot, suspend and restore a partition with a protected process. Test for full hypervisor functionality before implementing SGX.
- Open a discussion with your container development managers to get their perspectives on container security and potential linkages to hardware isolation.
- Ask your suppliers about the use and positioning of SGX in their product as a way of better understanding their future security approaches. Windows 10 uses existing virtualization hardware to create its isolated processes, but may create compatibility issues with approaches that also use virtualization techniques.
- Hypervisor-based approaches using introspection are another way to achieve similar levels of strong isolation. For example, Bracket Computing uses a hypervisor to "wrap" server workloads and Barkly uses a similar approach for endpoints to protect from security control tampering.
- Evaluate container-based approaches using privileged containers as an alternative way to achieve isolation of security controls (albeit software-based). We are already seeing similar architectures using privileged containers without agents that appeared in 2016 with more expected in 2017.

Business Impact: The use of security controls that run within the workload in cloud computing environments is desirable as these can scale automatically as the workloads they are protecting spin up and down. Further, the protection can move with the workload across on-premises and public cloud IaaS in hybrid data center configurations. However, these can be attacked or disabled unless these controls are protected or provided by the hardware underneath. Although nothing can materially change the balance in securing against system attacks, strong security control isolation is a worthwhile step forward.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Aqua Security; Barkly; Bracket Computing; Bromium; Intel; Microsoft; Samsung; Tripwire; Twistlock; VMware

Recommended Reading:

"Market Guide for Cloud Workload Protection Platforms"

At the Peak

File Analysis

Analysis By: Alan Dayley; Julian Tirsu

Definition: File analysis (FA) tools analyze, index, search, track and report on file metadata and, in most cases (such as in unstructured data environments), on file content. FA tools are usually offered as software options. FA tools report on file attributes and provide detailed metadata and contextual information to enable better information governance and data management actions.

Position and Adoption Speed Justification: FA is a growing technology that assists organizations in understanding the ever-growing repository of unstructured "dark" data, including file shares, email databases, SharePoint, enterprise file sync and share (EFSS), and cloud platforms, especially the rapid adoption of Microsoft Office 365. Metadata reports include data owner, location, duplicate copies, size, last accessed or modified, security attribute changes, file types and custom metadata. The primary use cases for FA for unstructured data environments include:

- Organizational efficiency and cost optimization
- Information governance and analytics
- Risk mitigation

The desire to mitigate business risks (including security and privacy risks), identify sensitive data, optimize storage cost and implement information governance is a key factor driving the adoption of FA. The identification, classification, migration, protection, remediation and disposition of data are key features of FA tools.

User Advice: Organizations should use FA to better understand their unstructured data, including where it resides and who has access to it. Data visualization maps created by FA can be presented to other parts of the organization and be used to better identify the value and risk of the data, enabling IT, line-of-business and compliance organizations to make better-informed decisions regarding classification, information governance, storage management and content migration. Once known, redundant, outdated and trivial data can be defensibly deleted, data can be migrated or quarantined, and retention policies can be applied to other data.

Business Impact: FA tools reduce risk by identifying which files reside where and who has access to them. They support remediation in areas such as the elimination or quarantining of sensitive data, identifying and protecting intellectual property, and finding and eliminating redundant and outdated data that may lead to unnecessary business risk. FA shrinks costs by reducing the amount of data stored. It also classifies valuable business data so that it can be more easily leveraged and analyzed, and it supports e-discovery efforts for legal and regulatory investigations. In addition, FA products feed data into corporate retention initiatives by using file attributes.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Active Navigation; Bloomberg; Capax Discovery; Hewlett Packard Enterprise; IBM (StoredIQ); Kazoup; Komprise; STEALTHbits; Varonis; Veritas

Recommended Reading:

"Market Guide for File Analysis Software"

"Organizations Will Need to Tackle Three Challenges to Curb Unstructured Data Glut and Neglect"

"How to Move From Data Negligence to Effective Storage Management"

"Information Governance Gets Real: Four Case Studies Show the Way Out of Information Chaos"

"Overcome Data Gravity and the 'Heavy' Bits That Keep Data From Moving"

"Market Guide for Data-Centric Audit and Protection"

Format-Preserving Encryption

Analysis By: Brian Lowans; Joerg Fritsch

Definition: Format-preserving encryption (FPE) is used to protect data at rest, in use and when accessed through applications while maintaining the original data length and structure. It is used to protect fields within an increasing variety of relational database management systems (RDBMSs), data warehouses and NoSQL databases. FPE is growing in importance to minimize the risks of hacking or insider abuse, and to meet compliance requirements by controlling access by administrators and users.

Position and Adoption Speed Justification: The early adoption has been rapid, due to the National Institute of Standards and Technology (NIST) accepting the two vendor-proposed standards/algorithms FF1 and FF3 in NIST Special Publication 800-38G in 2016. The new standard is accelerating adoption to protect sensitive medical and personal information, and other sensitive data.

User Advice: FPE is typically used across a variety of RDBMS, data warehouses and NoSQL platforms, such as Hadoop, Cassandra and MongoDB. It can be used to protect data strings at the point of capture, stored in a database or accessed through applications. However, it is still basically a blunt-force access control. Authorized users with application or database access privileges will have access to the data in clear-text, and other tools are required to understand what those users do with the data. Hence, when implementing FPE, organizations must also consider tools to monitor and audit all user and administrator access to sensitive data, with database audit and protection (DAP) tools, and use data loss prevention to monitor data movement across endpoints.

FF2 (VAES) is not approved under the standard and is not considered secure. The 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, and enterprise key management (EKM) should be implemented. DBAs should not have EKM responsibility for FPE. Although FPE can be used to protect personally identifiable information (PII) and protected health information (PHI), it has not yet been approved for use for credit card numbers by the payment card industry data security standard (PCI DSS).

When considering FPE, conduct a careful assessment to identify the following:

- What is the data security governance strategy, and what data fields need to be protected in accordance with perceived risks, threats and compliance requirements?
- What is the overall data security policy? Should FPE be combined with DAP?
- What will be the impact of encryption on application functionality?
- Are tokenization and dynamic data masking (DDM) appropriate alternatives to FPE?
- How will EKM work?

The most common successful deployments focus on specific types of regulated data — such as credit card numbers, PII, PHI and financial 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. Ensure that any interfaces to applications are able to establish all user identities, even if a connection pool is used between the application and database. Evaluate any impact on performance and functionality of applications accessing the RDBMS, and be aware that other security and database functionality, such as data discovery, can be affected.

Business Impact: FPE will help organizations address evolving compliance and threat landscapes without having to extensively modify existing databases or applications. It can provide an agile and cost-effective way to provide a strong level of control against unauthorized data access. Consequently, this will help meet data residency requirements for PII and PHI, and for data breach disclosure regulations. The new NIST standard has allowed acceptance of FPE to be used for PCI

Data Security Standard applications. FPE should be deployed as part of a broader data security governance approach that balances business needs against appropriate security controls.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Dataguise; Gemalto; HPE; Mentis; Penta Security Systems; PKWARE; Protegrity; Thales e-Security

Recommended Reading:

"Develop Encryption Strategies for the Server, Data Center and Cloud"

"Develop an Encryption Key Management Strategy or Lose the Data"

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

"Market Guide for Data-Centric Audit and Protection"

"Market Trends: Database Security, Worldwide, 2017"

Network Traffic Analysis

Analysis By: Jeremy D'Hoinne; Lawrence Orans

Definition: Network traffic analysis (NTA) technology uses a combination of rule-based detection, machine learning and other advanced analytics to detect suspicious activities on the enterprise network, typically postbreach events. NTA gathers data (including NetFlow records and selective full-packet capture) by listening to traffic and extracting interesting artifacts. Most NTA vendors specialize in monitoring critical LAN segments (north-south and east-west traffic), and are less frequently deployed to monitor the entire network.

Position and Adoption Speed Justification: Network traffic analysis moves to the Peak of Inflated Expectations on the basis of a growing number of pilots and implementations for NTA to complement, and sometimes replace, existing security monitoring solutions. Both midsize organizations and enterprises expect the simplified dashboard to alert them on "incidents that matter" only, and avoid an overwhelming amount of low-priority alerts or false positives. These expectations are unrealistic, as NTA technology is focused on detecting deviations from legitimate network activity, but do not promise to fully replace other security monitoring technologies.

A few NTA vendors gain high market visibility, and the first acquisitions have already happened. Yet the technology is still immature. Gartner clients report that security teams often detect as many network anomalies as "true" security incidents. Its long-term value will depend on its ability to continuously add new detection techniques to keep pace with attackers, and optimize its use of advanced analytics techniques. Mainstream security vendors will also add more traffic analysis features in next-generation firewalls, intrusion prevention systems, and security information and event management, so market competition will become stronger for NTA players.

User Advice: NTA solutions, because they analyze internal traffic consisting of either lateral traffic (east-west), inbound/outbound traffic (north-south) or both, may be able to detect malware and other malicious activities as they spread through the network. However, the network traffic the attacker generates will be analyzed by NTA solutions, providing contextualized information to differentiate legitimate and abnormal activities. NTA vendors are heavily focused on workstation behavior analysis.

As the technology is still emerging, prospective customers should perform a competitive evaluation of NTA engines and detection capabilities, of no fewer than 30 days. Many organizations give positive feedback on their NTA projects. However, Gartner has observed a few frequent reasons as to why a NTA deployment might fail:

- A wrong scope or expectation (attempt to replace IPS or SIEM)
- A poor implementation (the technology cannot access to the relevant traffic, or is not integrated in the incident response workflow)
- An insufficient fit (technology does not deliver on its promise, the detection rate is too low to justify the additional investment, or the split between business anomaly and attacks is not favorable)

Organizations will require highly skilled security analysts to fully benefit from most NTA solutions. Because these tools highlight anomalies, gaining maximum value from NTA tools requires a strong understanding of the overall traffic patterns and specific protocol patterns in your enterprise network. Enterprises that are considering NTA tools should ensure that their security teams have the skills to gain maximum value from these solutions, and the personnel to triage the alerts and other signals from the NTA.

When evaluating NTA solutions, security teams should ensure that they are comparing "apples to apples." They should prioritize the use case that is most appropriate for their organization before undertaking a complete product evaluation. Even if NTA vendors overemphasize the value of their management console, the long-term benefit for enterprises will heavily depend on the depth and breadth of what the analysis engines can detect. The evaluation period should demonstrate that selected NTA technology can regularly detect new events, not just clean up historic issues.

Business Impact: Malware and other threats that have gone inside the network without being detected and have managed to infect the organization's assets is a use case where enterprises experience long dwell times before noticing an intrusion and acting on it. This gives attackers time to exfiltrate data, including the enterprise's intellectual property. Network traffic analysis improves the ability of security analysts to spot these attacks with a higher degree of certainty, facilitating a triage of events and prioritization of actions to be taken. NTA also provides additional visibility to the security team on unusual network activities with legitimate business reasons.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Cisco (StealthWatch); Darktrace; Fidelis; Flowmon Networks; Palo Alto Networks (LightCyber); SS8; Trend Micro; Vectra Networks; Webroot

Recommended Reading:

"Five Styles of Advanced Threat Defense"

"Designing an Adaptive Security Architecture for Protection From Advanced Attacks"

User and Entity Behavior Analytics

Analysis By: Avivah Litan

Definition: User and entity behavior analytics (UEBA) include packaged advanced analytics and machine-learning models that evaluate and correlate the activity and behavior of users and other entities (for example, applications, IP addresses, devices and networks) to discover anomalies that could indicate insider or external security infractions. User activities are evaluated beyond an initial login, and include user movement and interactions with organizational assets and the context in which those movements and interactions occur.

Position and Adoption Speed Justification: UEBA brings profiling and anomaly detection based on machine learning and advanced analytics to security. Discussions with enterprises that have implemented UEBA indicate that the technology is effective in early breach detection and the other use cases it supports. According to customers, it often achieves a better signal-to-noise ratio than security information and event management (SIEM) or data loss prevention (DLP) for detecting breaches or insider threats. UEBA focuses on specific use cases — such as an intruder's lateral movements, insider threats, data exfiltration and privileged-user monitoring — and reduces and prioritizes alerts through effective profiling and machine-learning techniques.

Additionally, because UEBA applications typically analyze and retain a longer time window of data and activity than SIEM or DLP tools, it has a distinct advantage in detecting advanced "low and slow" attacks that shorter analyses would miss.

To be successful, UEBA applications need to coexist with existing enterprise security systems and other relevant applications where substantial investments have been made, such as SIEM, DLP and big data warehouses. This has in fact happened in many instances. User expectations regarding UEBA's effectiveness have peaked, in part because past project results have been mixed. Many have returned solid results in short time frames, while others have failed to yield timely results because of both vendor shortcomings and enterprise readiness.

The market is characterized mostly by startup companies, but it is quickly morphing so the UEBA market will no longer be a stand-alone market by 2022 (see "Forecast Snapshot: User and Entity Behavior Analytics, Worldwide, 2017"). Some leading UEBA vendors are already becoming SIEM vendors by adding SIEM features such as log management, workflow, orchestration and automation. Other UEBA vendors are finding their way into other market domains, such as identity and access management (IAM).

User Advice: Security and risk management leaders should:

- Choose UEBA vendors aligned with the threats you want to detect, such as malicious insiders and external hackers. Choose vendors with packaged solutions that align with your use cases and fill gaps in existing security tools, for example, security event monitoring.
- Clearly define use cases and be prepared to confirm those use cases through extensive proofs of concept (POCs) before choosing a vendor.
- Identify required data sources and understand how that data must be provided to UEBA solutions, which is critical for a successful implementation and use in production. Some essential information, such as HR data, may be difficult to obtain because of organizational processes.
- Identify organizational staff who can maintain and manage the UEBA solution, including the training of machine-learning models, in terms of data inputs and supervising model outputs.
- Favor UEBA vendors who profile multiple entities including users and their peer groups, devices, network traffic, data, and applications; and who use machine learning to detect anomalies. These features enable better detection of malicious or abusive users that might otherwise go unnoticed.
- Do not expect UEBA to replace people with domain and organizational knowledge. Resources are still required to configure and tune the UEBA tools, and validate potential incidents detected by the tools.
- Consider replacing your SIEM platform with a UEBA vendor who can deliver SIEM-like functionality in addition to UEBA advanced analytics if your SIEM vendor is failing to meet your organizational requirements. But carefully evaluate the UEBA vendor's foundational platform features, such as log collection and management, before replacing your incumbent SIEM. Conversely, ask your incumbent SIEM vendor for their roadmap for including UEBA functionality.

Business Impact: UEBA implementations have been successful at detecting insider threats, bad actors and hackers that penetrate organizational defenses and/or circumvent existing access and data protection controls. Often, these egregious acts and security incidents will show up as alerts in existing monitoring systems, but because of heavy alert volume, they will likely be buried in the mix and not prioritized. UEBA has also proven to be successful at detecting notable security infractions, and in improving alert management by reducing alert volume and prioritizing those that remain. Most UEBA applications also reduce the time and resources it takes to investigate alerts by bringing together most of the underlying supporting data that generates alerts.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: E8 Security; Exabeam; Fortscale; Gurucul; Interset; Niara; Rapid7; Securonix; Splunk

Recommended Reading:

"Forecast Snapshot: User and Entity Behavior Analytics, Worldwide, 2017"

"Market Trends: User and Entity Behavior Analytics Expand Their Market Reach"

"Market Guide for User and Entity Behavior Analytics"

"The Fast-Evolving State of Security Analytics, 2016"

"Best Practices and Success Stories for User Behavior Analytics"

Sliding Into the Trough

Threat Intelligence Platforms

Analysis By: Craig Lawson

Definition: Threat intelligence platforms (TIPs) are used to collect, correlate, categorize, share and integrate security threat data in real time to support the prioritization of actions and aid in attack prevention, detection and response. They also integrate with and complement existing security technologies and processes like SIEM, IPSs and firewalls. TIPs facilitate the sharing of machine-readable threat intelligence (MRTI) among multiple stakeholders and disparate groups at wire speed and support the extensive use of open standards like STIX/TAXII.

Position and Adoption Speed Justification: There are a small number of TIP providers today that are targeted at their problem statement. The majority are startups, and they drive this market in terms of features while delivering on aggressive product roadmaps. Recently, large high-profile and small security providers have shipped various threat intelligence (TI) capabilities or are signaling improvements in how native and third-party TI are handled for tactical and strategic benefit to customer security programs. Examples of this are from some SIEMs and orchestration/automation vendors.

User Advice: Security organizations should consider the use of TIPs in the following use cases:

- Multiple TI sources and formats are already in use, or there is a desire to increase usage to help improve and automate the use of threat intelligence.
- There is a want or need to participate in TI sharing and in leveraging the use of TI-sharing initiatives.
- They are looking for ways to improve the operational efficiency of using TI in their security programs to have more of an "intelligence led" security program.

- Generally, larger security teams with well-funded security programs will today be the best candidates for a TIP.
- Some TIPs can also be delivered as SaaS, increasingly allowing smaller organizations to consider a TIP; but, they often lack the funding, security maturity level or knowledge of the solution to take full advantage of it.

A TIP supports a large number of TI sources and enterprise use cases "out of the box," thereby increasing value in existing security investments and improving efficiency by automating traditionally manual processes that can improve an organization's security posture by bringing better intelligence into its security program. They also integrate with a number of existing "downstream" security processes and technologies (security information and event management [SIEM], intrusion prevention and detection systems [IPSs/IDSs], secure web gateways [SWGs], security operations, analytics and reporting [SOAR] tools, and endpoint detection and response [EDR]) to make these tools and processes more efficient and to increase the ROI and utility of these existing investments.

Business Impact: At this stage of the evolutionary process, a TIP will be used by larger security teams and industry sharing initiatives, and also service providers (managed security service providers [MSSPs], for example), to help deliver on intelligence-driven security initiatives within IT security programs. This technology accelerates the breadth and depth of TI in an organization by significantly improving the ability to action TI. It can assist with a number of existing IT security use cases, like threat detection and prevention, anti-phishing, incident response, and fraud and threat analytics, as well as new use cases like TI sharing.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Anomali; Blueliv; EclecticIQ; LookingGlass; Perch Security; Soltra; ThreatConnect; ThreatQuotient

Recommended Reading:

"Technology Overview for Threat Intelligence Platforms"

"Innovation Insight for Machine-Readable Threat Intelligence"

"How to Collect, Refine, Utilize and Create Threat Intelligence"

Security in the Switch

Analysis By: Greg Young

Definition: Security in the switch involves incorporating network security controls into network and other infrastructure products. This enables cost reduction by implementing network security segmentation and internal network security functions as part of the network fabric, rather than in discrete appliances. This technology has evolved due to virtualization, network function virtualization (NFV) and software-defined networking (SDN).

Position and Adoption Speed Justification: Trusting the infrastructure to protect the infrastructure has always proven to be a bad idea. For a variety of reasons, separation of security controls from infrastructure will always be a requirement in all but the smallest of businesses. However, the rapid rise of data center virtualization has made "sprinkling" security boxes throughout the data center a difficult proposition. SDN has so far failed to be a "fully self-defending network." There are, however, other technologies (such as microsegmentation) where NFV designed with security in mind is successful today in the data center. However, as next-generation firewalls (NGFWs) have evolved to have deep inspection (IPS), application control and malware inspection, it leaves the concept of embedding all security in switches even less likely to evolve.

As Cisco and Juniper Networks expand and extend their data center switching and security offerings, cloud-based service providers will increasingly offer tighter integration between data center switching fabrics and the cloud offering's fabric. As SDN is being moved forward without any material security, it introduces more security issues. The bottom line is that even in the virtual switches, advanced security has not been added and access control list (ACL)-like features are mostly what have been added: virtual switches are switch replacements rather than firewall ones. The low benefit rating recognizes the absence of practical enterprise switch-based security in vendor offerings. This technology is assessed as being obsolete before the plateau, as enterprises will not rely on high-security services from switches — switches are the target, not the shield.

User Advice: Depending on security, controls built into switches, routers, WLAN access points and application delivery controllers, WAN optimization controllers or virtualization infrastructure can be appropriate approaches for internal zoning/segmentation; however, they don't replace a separate perimeter network security control plane. Where security functions built into the network infrastructure are evaluated, determine the true performance effects to ensure that network operations are not degraded.

Service providers can also use security in the switch to provide in-the-cloud security functions, where name brand security products are not required. Security in the switch can be accomplished by the use of security blades in the switch, or with dedicated network security silicon integrated natively into the switch. The former raises performance issues, but provides more flexibility. The latter will minimize throughput degradation, but may require hardware upgrades, because security threats change faster than switch replacement life cycles. Switch-based ACLs continue to represent a basic isolation mechanism, but this is not a full security replacement of alternatives.

Be skeptical of any claims of "secure SDN."

Business Impact: This technology affects network segmentation, malware prevention, traffic enforcement and identity-aware networking.

Benefit Rating: Low

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Arista Networks; Cisco; Extreme Networks; Huawei; Juniper Networks

Recommended Reading:

"Magic Quadrant for Enterprise Network Firewalls"

"Innovation Insight for Ethernet Switching Fabric"

Network Security Policy Management

Analysis By: Adam Hils; Rajpreet Kaur

Definition: Network security policy management (NSPM) tools go beyond user policy administration interfaces that firewall vendors provide. 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. NSPM tools are often in suites, containing adjacent functions such as application connectivity management, policy optimization and risk-oriented threat path analysis

Position and Adoption Speed Justification: Third-party network security policy management is a small, but fast-growing market. Basic firewall rule management is mature within these tools. The main suite providers are broadening their capabilities, but users report occasional difficulties with scalability of adjacent functions. Organizations that purchase NSPM solutions for firewall rule cleanup or firewalls rule conversions or migrations often do not move beyond these tactical use cases. However, some clients buy these tools to achieve enhanced application visibility, asset control and automated change management, which also drive this market. Some vendors focus their NSPM solutions on addressing operations-focused buying audiences, while others try and appeal to security and risk-driven buyers. As tools mature to provide good operational and security visibility across hybrid infrastructures, Gartner expects these tools to gain broader demand and adoption.

User Advice: Network security administrators who wish to optimize, visualize and reduce firewall rule policies, or who are migrating rules, especially to a first-time NGFW implementation, should evaluate NSPM tools for this purpose. If an organization has multiple firewall brands in place because of acquisitions or geographical diversity, NSPM tools are useful for providing a consolidated view, analysis of the various firewall rules, security policies, potential policy overlaps, interactions and conflicts. In addition, a large organization conducting a multistage rollout needs an overarching security policy and firewall management view. Once these initial use cases are satisfied, network security administrators should investigate whether the functions purchased are useful for ongoing rule management, or whether they wish to add adjacent functions from the NSPM vendor's suite.

NSPM tools are not just for rule reduction, but are also useful for managing thousands of rules and security policies across many distributed intertwined enforcement points. Some NSPM vendors have added capabilities for policy-within-the cloud, and for migrating security to the cloud and across hybrid environments. Users with cloud deployments or considering cloud deployments should prefer NSPM solutions with these capabilities. Most NSPM tools are usually implemented as on-premises software and hardware, although some managed security service providers use NSPM tools to optimize managed firewall services for their customers. Managed security service provider (MSSP) customers should inquire as to whether NSPM-based services are available and useful for their customer goals. Once the main firewall management component is fully configured and deployment is mature, users should consider other features, such as application connectivity management, risk analysis and threat analytics, to have improved visibility into their security architecture. NSPM tools can be integrated with many other security solutions such as proxies, web application firewalls and network switch technologies to expand beyond firewall-only use cases.

Business Impact: To the degree that an enterprise struggles with firewall diversity, complexity and large tangled rule sets, along with strict regulatory requirements that mandate visibility into firewall policy change management, these NSPM tools are relevant. For that reason, these tools are most present within large enterprise environments and regulated industries. They are increasingly delivered as services by MSS providers and security professional services firms, which will broaden the reach and relevance of network policy management projects.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: AlgoSec; FireMon; IBM-Q1 Labs; RedSeal; Skybox; SolarWinds; Tufin

TLS Decryption Platform

Analysis By: Adam Hils; Jeremy D'Hoinne

Definition: The Transport Layer Security (TLS) decryption platform is an in-line dedicated appliance used to decrypt, forward to other technologies and re-encrypt TLS (SSL) traffic. The TLS decryption platform makes the decrypted traffic available to multiple stand-alone security inspection solutions for traffic inspection, then re-encrypts 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 the TLS decryption platform heading toward the Trough of Disillusionment. Security and risk leaders have become increasingly aware of the issues raised by the growing amount of HTTPS traffic traversing their networks. In fact, for enterprises that are too slow to adopt web traffic decryption best practices, the main risk is 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 limited adoption.

Deploying a TLS decryption placement is the right choice when the benefits of decrypting TLS traffic once exceeds the challenges of managing a duplicate access policy. This is generally achieved when the objective of TLS decryption includes not only malware detection, but also other security services. The ability to create a chain of services that receive decrypted traffic from the TLS decryption platform is one of the key benefits of the TLS Platform solutions. Several alternatives to adoption of this technology exist, including efforts to perform inbound decryption on an organization's ADC or WAF, and to perform outbound decryption on the firewall, or on a cloud or on-premises web proxy. Compared to alternative approaches to inbound and outbound TLS inspection, the TLS decryption platform improves the overall performance and simplifies the encryption key management, but could create an environment that is more complex to manage, maintain and audit.

It also adds another potential point of failure to the infrastructure. Unfortunately, there are only a few vendors in this space, which limits the available choices. As encrypted traffic comprises a greater percentage of the total traffic stream, more IT security and risk leaders will turn to these purpose-built appliances in order to achieve greater security without overburdening other infrastructure and network security platforms with compute-intensive decryption tasks.

An organization launching a web traffic decryption project will face many challenges that will impact speed to adoption:

- **Organizational:** Decrypting HTTPS creates privacy challenges for monitored employees. Local regulations or enterprise culture might hinder the decryption project or create internal tensions.
- **Technical:** The use of decryption architecture might degrade user experience, introducing poor performance and unexpected blocking of legitimate business applications.
- **Budgetary:** The average cost per user of network security controls will increase dramatically because of the decryption costs, but the overall organizational perception of value might be low.

In addition, the use of certificate pinning in many mobile applications prevents traffic decryption based on a man-in-the-middle approach. If security and risk leaders are not able to drop traffic destined for these applications, they are forced to allow the traffic through uninspected, limiting the efficacy of decryption

User Advice: Security and risk 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 respect of employee's rights to privacy
- Ensure that network traffic will be decrypted only once.
- Decide whether to decrypt with existing network security appliances or with dedicated decryption appliances

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 cleartext traffic.
- Test, extensively, the integration between the platforms and the security solutions that access, and possibly modify, the decrypted traffic.
- Review log policy for each of the equipment part of the decryption infrastructure to avoid unwanted logging of confidential data.

Business Impact: To solve security visibility problems, this technology can be applied in organizations outside of certain highly-regulated nations. Security and risk leaders implementing a dedicated TLS decryption platform will get massively improved visibility necessary to protect organizational data and to let other security protections inspect and process the traffic. This technology is mostly applicable to large enterprises, as they are more 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 those solutions to achieve necessary performance with TLS decryption offload happening.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: A10 Networks; ARA Networks; Blue Coat; F5; Gigamon; Ixia

Software-Defined Security

Analysis By: Neil MacDonald; Mike J. Walker

Definition: Software-defined security (SDSec) is an umbrella term covering a number of security processes and controls that benefit when the security policy management is abstracted from the underlying security policy enforcement points.

Position and Adoption Speed Justification: Information security infrastructure is too rigid and static to support the rapidly changing needs of digital business and to provide effective protection in a rapidly changing threat environment. Increasingly, security vendors are shifting more of the policy management out of individual hardware elements and into a software-based management plane for flexibility in specifying security policy, regardless of location. There are several areas within SDSec that are emerging — software-defined perimeters, software-defined segmentation (microsegmentation), software-defined data protection and cloud workload protection platforms.

User Advice:

- Look beyond the hype. There are several areas where organizations are finding value in SDSec use cases today.
- Don't make the mistake of assuming "software-defined" means software only. Security hardware will still be needed for deep inspection at demarcation points.
- Require all security platform vendors to open up via APIs for full programmability of their infrastructure.
- Pressure security platform vendors for their roadmaps to support OpenStack and other cloud management platforms.

Business Impact: Information security cannot be an inhibitor to the needs of digital business. SDSec will bring speed and agility to the enforcement of security policy regardless of the location of the user, the information or the workload.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Catbird; Certes Networks; CloudPassage; Fortinet; Illumio; Security First Corp.; Trend Micro; Unisys; vArmour; Vidder

Recommended Reading:

"It's Time to Isolate Your Services From the Internet Cesspool"

"Market Guide for Cloud Workload Protection Platforms"

"What Is the Value of a Software-Defined Data Center?"

Enterprise Key Management

Analysis By: Brian Lowans; David Anthony Mahdi

Definition: Enterprise key management (EKM) provides a single, centralized software or network appliance for multiple symmetric encryption or tokenization cryptographic solutions. Critically, it enforces consistent data access policies through encryption and tokenization management. It also facilitates key distribution and secure key storage, and maintains consistent key life cycle management.

Position and Adoption Speed Justification: EKM solutions are improving, but we still see some issues with compatibility, centralization and manageability. Cryptographic solutions that implement encryption or tokenization are a critical component of a data-centric security strategy to meet growing data residency and compliance requirements, and to prevent data breaches or theft due to hacking, malicious insiders and inadvertent disclosure.

User Advice: EKM products adopt the Key Management Interoperability Protocol (KMIP) standard, sponsored by the Organization for the Advancement of Structured Information Standards (OASIS). EKM solutions can manage any cryptographic solutions that are compliant with KMIP, but legacy solutions that do not comply will need separate management. Many storage, backup and emerging cloud cryptographic solutions support KMIP. Gartner finds that vendors offering both EKM and cryptographic solutions still prefer to rely on proprietary protocols and have not yet converted their cryptographic solutions to support KMIP. This is a protectionist strategy that retains control of cryptographic infrastructures and, despite strong interest from clients, it remains a barrier to the adoption of EKM. Cryptography is an important access control that should be combined with other data security tools, 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 solutions and managing EKM through separate business-focused security teams must be addressed. Focus on reducing the number of cryptographic solutions deployed by different vendors while the market continues to evolve.

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

1. Deploy solutions from more than one vendor across different silos: Clients will gain the benefit of best-of-breed, but it results in uncoordinated EKM and data access policies.
2. Deploy a single vendor's solution across multiple silos: Operational or functional compromises will be required, but this provides consistent EKM and data access policies.

EKM is becoming critical to addressing 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-centric security strategy that will lead to the appropriate selection of either multiple siloed KM solutions 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: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Gemalto (SafeNet); Hewlett Packard Enterprise; IBM; PKWARE; Protegrity; QuintessenceLabs; Thales e-Security; Townsend Security

Recommended Reading:

"Develop Encryption Strategies for the Server, Data Center and Cloud"

"Develop an Encryption Key Management Strategy or Lose the Data"

"Choosing Between Cloud SaaS and CASB Encryption Is Problematic"

"Market Guide for Data-Centric Audit and Protection"

Operational Technology Security

Analysis By: Earl Perkins

Definition: Operational technology (OT) security is the governance, development, management and operations of digital security for industrial automation and control systems, processes and organizations. OT is an early form of the Internet of Things (IoT), and many concepts of OT security can be found today in IoT security. A large segment of OT security associated with industrial-oriented digital transformation uses industrial IoT (IIoT).

Position and Adoption Speed Justification: OT security technologies provide controls to secure OT environments, with the aim to preserve reliability and safety of production and operations environments. Established international standards such as IEC 62443 and several NIST 800 Series guidance frameworks provide product and service providers with direction related to function, and verticals have specific requirements regarding performance and usability that the OT security market is starting to address. The market itself consists of IT security companies that have extended capabilities of existing solutions to address specific OT functional differences and requirements, OT system providers adding security controls to their OT platform offerings and OT security companies that have evolved more recently to do the same thing. The most recent offerings now attempt to address IIoT requirements as well.

Obstacles will remain in (1) coverage across all verticals and all major OT company systems, (2) addressing the issues of age of many OT systems, (3) keeping pace with regulatory requirements and changes to those requirements, (4) cultural and organizational challenges in IT/OT integration, and (4) providing scalability and support globally. OT security providers are making progress has 2017's rating implies, and many products are entering a phase of significant adoption. IIoT security technologies are leading future evolution with less expensive offerings, more extensive data collection and flexible command functionality.

User Advice: Security and risk managers should:

- Pursue an IT/OT alignment and integration strategy for security that underscores governance, strategy and planning as a more centralized process reporting to the same executive.

- Accelerate OT assessments with reputable consulting firms to determine risks and gaps to be addressed by OT security controls and infrastructure, and create skills training and transfer between IT and OT where possible.
- Map OT key performance indicators against IT/OT risk indicators to write security policies consistent with maintaining and improving performance. Apply OT security controls based on those policies across OT infrastructure where needed.
- Build repeatable processes for service portfolio management to manage the growing security service portfolio supplementing in-house OT security systems. Develop coordination in the OT supply chain to assess partner security controls affecting your organization.
- Focus early infrastructure purchasing on asset discovery, tracking and visualization, anomaly and incident detection and response, vulnerability management, access control, and network segmentation.
- Focus on organizational and cultural challenges by restructuring as required and establishing complete communications and awareness programs between IT and OT.

Business Impact: OT security is particularly useful in asset-intensive and asset-centric organizations, such as critical infrastructure (for example, energy and utilities, transportation, oil and gas, manufacturing, and natural resources) and other general industrial verticals. It is also found in commercial markets in areas such as building automation and facilities management, healthcare, and retail. OT security is particularly useful in addressing specific engineering needs for protecting real-time, event-driven systems that have high impact on safety of people and environments. As such, adoption rates for OT security solutions have risen year over year as understanding and market availability have provided options for organizations.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Belden (Tofino Security); Claroty; CyberX; Dragos; Leidos (Industrial Defender); Owl Cyber Defense Solutions; PAS; Radiflow; Sentryo; Waterfall Security

Recommended Reading:

"Market Guide for Operational Technology Security"

"Predicts 2017: IT and OT Convergence Will Create New Challenges and Opportunities"

"Take an Integrated Approach to Improve Digital Security for the Supply Chain"

"Don't Let Your IoT Projects Fail: Use the Right IoT Security Pattern to Protect Them"

Microsegmentation (Software-Defined Segmentation)

Analysis By: Greg Young; Neil MacDonald

Definition: Microsegmentation (referred to as software-defined segmentation in previous Hype Cycles) uses policy-driven firewalling (typically software-based) or network cryptography to isolate workloads in data centers and public cloud infrastructure as a service, and into containers, including workloads in hybrid and multicloud scenarios spanning all of these.

Position and Adoption Speed Justification: With advanced threats bypassing traditional firewalling and intrusion prevention, antivirus, and anti-evasion mechanisms, enterprises now see payload-free attacks like spear phishing gaining a foothold and then moving laterally within, and there has been an increased interest in visibility and further segmentation of "east-west" data center traffic. The increasingly dynamic nature of data center workloads makes traditional segmentation strategies complex, if not impossible, to apply. Further, the shift to microservice architectures for applications has also increased the amount of east-west traffic and further complicated the ability of traditional fixed firewalls to provide this segmentation. The extension of data centers into public cloud also has placed a focus on software-based approaches for segmentation. VMware is heavily marketing microsegmentation as a use case for NSX, and infrastructure as a service vendors such as Amazon and Microsoft are promoting the mechanisms they offer as segmentation without requiring third-party controls. The rapid adoption of Linux containers has increased the need to extend segmentation policies into container networking environments to apply segmentation policies between containers.

User Advice: Don't oversegment. Oversegmentation is the foremost cause of failure and an unnecessary expense for segmentation projects:

- Consider products with established security expertise, such as those from security vendors targeting this market. Isolation alone isn't segmentation: If communication is required between zones, this requires different functionality than merely keeping them apart.
- Consider a host-based approach for scenarios where this makes sense; alternatively, several vendors use virtual-appliance approaches to provide this capability.
- Ensure that your segmentation strategy extends into containers and container networking environments.
- Pressure your existing network security vendors to extend their capabilities into virtualized and cloud-based environments with native integration for the cloud environments' tagging infrastructure.
- Look beyond technical considerations when segmenting. Consider the business processes and the information being protected.
- Reduce the threat and breadth of duties aperture through network function virtualization (NFV), which limits security interaction to the network and not the entire virtualized stack. NFV can be further enhanced with third-party products that are NFV-enabled and offer additional services, such as firewalls and intrusion prevention systems.

Business Impact: Microsegmentation is an approach that reduces the risk of a lateral spread of advanced attacks in enterprise data centers and enables enterprises to enforce consistent segmentation policies across on-premises and cloud-based workloads, including workloads that host containers. In addition, several solutions provide extensive visibility 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: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Amazon Web Services; Bracket Computing; Cisco; CloudPassage; GuardiCore; Illumio; Microsoft; ShieldX; Tempered Networks; vArmour

Recommended Reading:

"Market Guide for Cloud Workload Protection Platforms"

"Best Practices in Network Segmentation for Security"

"Technology Insight for Microsegmentation"

Secure Web Gateways

Analysis By: Lawrence Orans; Peter Firstbrook

Definition: Secure web gateways (SWGs) use URL filtering, advanced threat defense (ATD) and malware detection, and application control technology 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 are still positioned in the Trough of Disillusionment, because most providers are resisting the inevitable movement to cloud-delivered services, and have displayed a lack of innovation. While numerous providers offer some level of cloud delivery, solutions vary greatly in their maturity and global data center footprint. Very few of the on-premises providers have the commitment to cloud that will be necessary to survive the transition to a predominantly cloud data center and mobile device age. Pure-play on-premises solutions will struggle to differentiate from enterprise firewall solutions. Presently, support for advanced threat defense is still inconsistent throughout the market. For example, some vendors offer network sandboxing appliances, but they lack sandboxing support in their cloud services. At this stage in the market, any vendor that is offering a cloud-based SWG also needs to offer cloud-based advanced threat defense. Support for mobile and portable (laptop) devices has improved, with several vendors offering a broader set of options (for example, endpoint clients and mobile apps) to enable user authentication and traffic redirection to the SWG cloud.

User Advice: Enterprises must go beyond basic URL filtering and implement SWG solutions that offer strong protection against advanced threats and legacy malware. Many SWGs are capable of automatically depositing suspicious objects (for example, files and executables) into the sandbox for analysis. Implementations vary widely, as some vendors only offer on-premises sandboxes and others only offer cloud sandboxes. Other techniques for advanced threat protection include browser code emulation (static analysis) and threat intelligence integration. Enterprises will need to match their threat defense strategies to their long-term SWG direction (for example, on-premises, cloud or hybrid).

Enterprises considering cloud services should recognize that there are two categories of vendor offerings. Some vendors have optimized their cloud services to protect customers' remote offices (for example, these vendors are experienced in supporting tunnel-based traffic redirection from routers or firewalls). And, some vendors have optimized their cloud services to protect mobile workers when they are off the corporate network (for example, these vendors rely heavily on endpoint-based traffic redirection, and are inexperienced in supporting tunnel-based redirection). All vendors support multiple forms of traffic redirection to their cloud services, but most have a definite bias toward supporting either tunnel-based redirection or endpoint-based redirection. Enterprises should prioritize which use case is the most important (protecting remote offices or protecting mobile users), and evaluate vendors that target that use case.

Longer term, the SWG survivors will be the vendors that have made the difficult transition to cloud delivery, and those that have adopted CASB-like functionality to manage access to legacy corporate applications, cloud infrastructure as a service and software as a service across all ports and protocols.

Business Impact: SWGs protect end users from internet-borne malware, and higher-end SWG product suites can help to protect enterprises against targeted attacks and advanced threats. Cloud-based services can protect mobile workers, who are otherwise vulnerable to attack when they are off the corporate network, and safely and easily connect branch offices with commodity telecom services. Monitoring employees' web-surfing habits, enforcing internet access policies and generating reports for management remain important functions of SWGs.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Barracuda Networks; Cisco; ContentKeeper; Forcepoint; iboss; McAfee; Sophos; Symantec; Trend Micro; Zscaler

Recommended Reading:

"Magic Quadrant for Secure Web Gateways"

"Market Guide for Network Sandboxing"

"Designing an Adaptive Security Architecture for Protection From Advanced Attacks"

Climbing the Slope

Network Sandboxing

Analysis By: Lawrence Orans; Jeremy D'Hoinne

Definition: Network sandboxes rely on sensors to monitor network traffic for suspicious objects (for example, executables, Microsoft Office files, PDF files and JavaScript code) and automatically submit them to a sandbox environment, where they are analyzed and assigned malware probability scores and severity ratings.

Position and Adoption Speed Justification: Over 25 vendors offer network sandboxing solutions, either as a stand-alone product or as a feature of a mainstream security solution. For example, many firewall, intrusion prevention system (IPS) and unified threat management (UTM) vendors offer sandboxing as an optional feature, and so do several secure email gateway (SEG) and secure web gateway (SWG) vendors. The broad availability of sandboxing as a feature has resulted in lower prices and accelerated adoption in enterprises that don't have large security budgets.

Network sandboxing is maturing, which is why we positioned it on the Slope of Enlightenment this year. When it emerged as an early mainstream solution, around 2010, enterprises mainly implemented sandboxing as on-premises appliances. Now, nearly all vendors are leading with their cloud-based sandboxing services, primarily because the cloud approach offers a more cost-effective solution. The acceptance of cloud-based sandboxing services means that it can more easily be integrated as a feature of a mainstream security solution (for example, firewall, secure web gateway and other products), thereby becoming even more widely implemented. In order for network sandboxing technology to progress further along the Hype Cycle, solutions need tighter integration with forensics tools and improved workflow, so that security teams can respond more effectively to malware incidents.

User Advice: Consider sandboxing technology if you need to improve perimeter-based inbound malware detection. Once enterprises have determined to implement sandboxing, the most common decision is whether to purchase it as a feature from one of the enterprise's current security vendors or as a best-of-breed solution that can be implemented independently of other security products. If your organization is budget-constrained or looking for a quick path to add sandboxing, first evaluate sandboxing as a feature from one of your current security vendors. Assess the sandboxing capabilities of your firewall, IPS or UTM solutions, and do the same for your SWG, SEG and endpoint security vendors. It's likely that adding sandboxing as a feature will be the most cost-effective option, because it utilizes existing infrastructure to feed suspicious objects to the sandbox. Another benefit of using sandboxing as a feature is that the vendor may have integrated workflow that makes it more efficient to respond to alerts.

If budget permits, or when targeted malware is identified as high-risk, evaluate independent best-of-breed sandboxing solutions. This is likely to be a more expensive option, because it requires adding additional components to the network. Best-of-breed sandboxes typically include more advanced functionality and stronger anti-evasion technology than sandboxing-as-a-feature capabilities that have been added to firewalls, UTM devices and SWGs, although this is not always the case. The increased cost should come with additional benefits, such as higher detection rates and a lower number of false positives.

Business Impact: Network sandboxing has had a strong impact, because its behavioral-based technology has proved to be effective in detecting malware and advanced threats that have bypassed traditional security solutions — for example, firewalls, IPS, SWG, SEG and endpoint protection platforms (EPPs). Sandboxes are typically easy to implement and have been adopted by a broad spectrum of companies across many industry verticals.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Check Point Software Technologies; Cisco; Cyphort; FireEye; Lastline; McAfee; Palo Alto Networks; Symantec; Trend Micro; Zscaler

Recommended Reading:

"Market Guide for Network Sandboxing"

"Five Styles of Advanced Threat Defense"

Network Access Control

Analysis By: Claudio Neiva; Lawrence Orans

Definition: Gartner defines network access control (NAC) as technologies that enable organizations to implement policies for controlling access to corporate networks by both user-oriented devices and Internet of Things (IoT) 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. For example, organizations may choose to grant wireless LAN access to tablets and smartphones, but use different context variables — such as location, time/date, day of the week or even type of device — to determine whether the permission will be only for internet access or for access to the enterprise network. In many cases, enterprises can take advantage of NAC integrations with other security components. For example, many NAC vendors have integrated with security information and event management (SIEM), next-generation firewalls (NGFWs) and advanced threat defense (ATD) solutions.

In 2017, Gartner client inquiries show a high demand for a response to auditors' comments about the lack of visibility and the need to control devices connecting to the corporate network. Other NAC use cases include management of access from an external contractor or guest, and management of IoT devices. NAC solutions should include the following capabilities:

- Policy life cycle management: Through a policy server, NAC solutions should define security configuration requirements and role-based access in order to apply access controls for compliant and noncompliant devices.
- Security posture check: NAC solutions should determine and optionally implement the proper level of access, based on the security state of the endpoint. Today this is mostly used in monitoring mode only.
- Guest management: NAC solutions should include the ability to manage guests through captive portals.
- Profiling and visibility: With IoT and traditional devices connecting to corporate infrastructure, NAC solutions should be able to automate policy enforcement through detection of device type (profiling), providing visibility of all connected devices.

User Advice: Although NAC solutions can stand alone, we often find that the organization's goal is to integrate NAC and enterprise mobility management (EMM). It is important to understand that choosing an NAC vendor first will limit EMM options. Conversely, choosing an EMM vendor first will limit NAC options. All NAC and EMM integrations are driven by vendors that have partnered to integrate their solutions. There is no standards-based interoperability framework for integrating NAC and EMM solutions, but many NAC vendors have published APIs or use other approaches for facilitating integration. EMM is the larger and faster-growing market, so most enterprises will deploy an EMM solution before implementing NAC. Network managers responsible for NAC projects should influence EMM product selection to ensure NAC interoperability.

When evaluating NAC solutions, select vendors that integrate well with existing security solutions, such as NGFWs, SIEM and ATD tools. The most valuable integrations are bidirectional. For example, NAC policy servers can send contextual information, such as user ID and device type, to an ATD system. When the ATD tool flags an IP address as suspicious, the NAC policy server provides relevant context, such as "This is the CEO's tablet." In the reverse direction, an ATD tool can send malicious IP addresses to the NAC system to enforce the appropriate policy (for example, to block or quarantine the IP address). However, this automatic policy enforcement should only occur when there is a high degree of certainty that the IP address is malicious.

Business Impact: NAC helps enterprises provide a flexible approach to securely supporting "bring your own device" (BYOD) policies, often with the help of integrating with EMM solutions. NAC will enable enterprises to ensure that EMM 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 overall security by providing visibility into the devices that are on its network. With a new category of ransomware that combines behavior of malware and worms (self-propagation), security posture may come back as a requirement to allow an endpoint to connect to corporate infrastructure. WannaCry ransomware would reflect 2006 requirements (Sasser and Blaster worms as drivers to implement NAC to minimize the impact of an infection through all internal infrastructure).

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Bradford Networks; Cisco; Extreme Networks; ForeScout Technologies; HP (Aruba Networks); IntelliGO; OpenCloud Factory; Pulse Secure

Recommended Reading:

"Market Guide for Network Access Control"

"Market Guide for IoT Security"

"Use Proofs of Concept to Guarantee Successful Network Security Purchases"

DDoS Defense

Analysis By: Lawrence Orans; Claudio Neiva

Definition: Distributed denial of service (DDoS) attacks use multiple techniques to disrupt business use of the internet or to extort payment from businesses to stop the attacks. Hacktivism, linked to politically or socially motivated purposes, is another driver for DDoS attackers. DDoS defense products and services detect and mitigate such attacks.

Position and Adoption Speed Justification: This year, the positioning of DDoS Defense moved slightly to the left, to the same position that it occupied in 2015. 2016 was a challenging year for DDoS mitigation providers, as volumetric attacks soared to record levels. The highest-profile attack was the one against DNS provider Dyn, where the attackers used the Mirai botnet (consisting of IoT devices, such as CCTV video cameras and digital video recorders) to generate a 1.2 Tbps attack. The attack had a broad impact, limiting the availability of many popular websites including Twitter, Amazon, Tumblr, Reddit, Netflix and others.

Now that we have seen attacks evolve to a new scale, it's clear that DDoS mitigation providers need to increase the capacity and sophistication of their infrastructure. Gartner believes that we will continue to see a tiered market of DDoS mitigation providers. The "A-list" providers will have the capacity and the expertise to mitigate the largest attacks. Other providers will be unable to compete at the highest level, but many will be good choices for enterprises seeking protection from more typical attacks (about 20 to 30 Gbps).

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 ISPs or DDoS security-as-a-service specialists. To defend against complex, application-based attacks, a mix 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 valid 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).

Because of the increased awareness of DDoS attacks, more ISPs 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 ISP providers and make sure that the price of their services reflects their level of experience. Also, we still hear that some ISPs are "black-holing" traffic, when they have been unable to mitigate an attack against a customer. This technique protects the ISP's other customers from collateral damage, but it completely removes the targeted customer from the internet. Enterprises considering ISP-based DDoS mitigation services should request clauses that their traffic will not be dropped.

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.

Business Impact: Any business-critical internet-enabled application or service can be disrupted by DDoS attacks. DDoS mitigation technology and services are highly beneficial, when combined with incident response best practices, in combating DDoS attacks.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

Sample Vendors: Akamai; Amazon Web Services; AT&T; F5; Imperva; Level 3 Communications; Netscout (Arbor Networks); Neustar; Radware; Verisign

Recommended Reading:

"Best Practices to Defend Your Organization Against DDoS Attacks in India"

"Leverage Your Network Design to Mitigate DDoS Attacks"

"DDoS: A Comparison of Defense Approaches"

Database Audit and Protection

Analysis By: Brian Lowans

Definition: Database audit and protection (DAP) tools provide centralized management of data security policies, user activity monitoring, data protection and vulnerability management for relational database management systems (RDBMSs), and big data or NoSQL databases such as Hadoop, MongoDB and Cassandra. DAP is a critical data security control to meet data residency, sovereignty and compliance requirements, such as audit in large-scale heterogeneous environments, and to prevent data breaches.

Position and Adoption Speed Justification: DAP provides forensic and real-time breach detection and data protection by mitigating risks that are not addressed by tools such as identity and access management, security information event management (SIEM), or user and entity behavior analysis (UEBA).

The core DAP monitoring capabilities are quite mature, but the extended capabilities are still continuing to innovate support for big data platforms such as Hadoop and cloud-based databases.

The DAP market experienced strong double-digit growth through 2016 and into 2017, due to organic growth of existing customer deployments, strong growth to cater for data residency and regulatory issues, and new client growth in EMEA and Asia/Pacific. While the preventive controls continue to mature, vendors will continue developing capabilities for modern NoSQL databases and algorithmic detection of malicious activity due to hacking or insider misuse.

User Advice: DAP provides a comprehensive and uniform database-level security suite, and offers cross-platform support in heterogeneous database environments. Clients should implement DAP functionality to mitigate the risks of data breaches resulting from user and administrator activities, database vulnerabilities, and poor segregation of duties. DAP provides unique security functionality because it intercepts all communication paths to the database to then analyze and/or modify SQL commands and/or responses.

Use DAP for four common use cases:

- **Unification of data security policies:** Application and monitoring of a unified database security policy across large-scale heterogeneous database environments including the segregation of duties of privileged and application users to maintain data privacy across geographic jurisdictions.
- **User monitoring and audit:** The identification and assessment of the who, what, why, where, when and how of all users, including administrators and highly privileged application users. Activity monitoring with data context detects any privilege changes, unusual data access and security policy violations, either accidental or malicious, that might lead to data breaches. The audit report provides a full record of activity for compliance reporting.
- **Policy enforcement:** If access to sensitive data is not permitted, then particular fields can, for example, be blocked or redacted. Some vendors may even be able to anonymize the field (using masking, tokenization and encryption, for example). If privileges change, access can also be blocked until verified.
- **Attack prevention:** Identifies and mitigates open vulnerabilities within the RDBMS, and configuration or schema changes to prevent malicious activity. Applies virtual patches to block SQL attacks.

If not provided by the vendor, data protection tools such as format preserving encryption (FPE), tokenization and dynamic data masking should be used in parallel with DAP to restrict access and protect data at rest and/or in use. This allows a greater focus on and monitoring of the privileged users.

Business Impact: DAP is an important addition to enterprise data security governance programs because it provides data context against user privileges and activity; other tools, such as identity and access management, SIEM or UEBA, do not. It is a critical investment for clients with large and/or heterogeneous database infrastructures or Hadoop deployments containing regulated or business-critical data. It is important to address typical audit recommendations, such as enforcement of segregation of duties, vulnerability management, user activity monitoring and providing an audit record of all activities. With increasing risks of hacking and insider abuse, DAP is becoming a critical detective and preventive technology.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Beijing DBSec Technology Co.; Datiphy; IBM; Imperva; McAfee; Mentis; Oracle; Trustwave; WareValley

Recommended Reading:

"Market Guide for Data-Centric Audit and Protection"

"Securing the Big Data and Advanced Analytics Pipeline"

"Rethink and Extend Data Security Policies to Include Hadoop"

"When to Use Database Audit and Protection to Enhance Database Security and Compliance"

"Big Data Needs a Data-Centric Security Focus"

Web Application Firewalls

Analysis By: Jeremy D'Hoinne; Adam Hils; Claudio Neiva

Definition: A web application firewall (WAF) is a detection and prevention technology positioned primarily in-line of web servers to protect web applications and web APIs. WAFs focus primarily on web server protection at the application layer, which includes classes of "self-inflicted" vulnerabilities in configured commercial applications or in custom-developed code, and may also include safeguards against some attacks at other layers. Many WAFs include a combination of negative ("signatures") and positive ("whitelist") security models.

Position and Adoption Speed Justification: WAF is moving backward slightly, as the rise of cloud-based-as-a-service WAF is disrupting the appliance market, but not delivering yet on the promise of technological breakthrough for application security. Historically, WAF capabilities have been available as stand-alone appliances and as a software module in most application delivery controllers (ADCs). Unlike appliances, cloud-as-a-service WAFs 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. Vendors often offer managed services for their cloud-as-a-service

WAF, and sometimes make it mandatory. Cloud-as-a-service WAFs are often bundled with content delivery networks (CDNs) or bot mitigation, or with protection against distributed denial of service (DDoS). Many enterprises use WAFs to protect their public-facing applications, with a minority of the projects being driven by compliance only. Mobile applications and the Internet of Things (IoT) create new development opportunities for WAFs, but Gartner observes that innovation continues to happen outside of the traditional WAF vendor landscape. Cloud-as-a-service WAFs focus on adding more features and offer managed services while maintaining ease of use, but innovative techniques are slow to prove value.

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 cloud-as-a-service WAF, such as simplicity and bundled protection with DDoS and bot mitigation, against deployment challenges, such as certificate management, 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 protect features against what API gateways can offer, 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.

Reality often dictates that a WAF is used in the context of weak change control, with no ability to scan third-party code or highly dynamic applications, all situations reducing its efficacy Enterprises should carefully review how WAFs integrate with security monitoring tools, web access management (WAM), application security testing (AST) technologies, 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; Barracuda Networks; Citrix; DenyAll; F5; Fortinet; Imperva; Radware; Rohde & Schwarz

Recommended Reading:

"Magic Quadrant for Web Application Firewalls"

"Web Application Firewalls Are Worth the Investment for Enterprises"

"Magic Quadrant for Application Delivery Controllers"

Interoperable Storage Encryption

Analysis By: John Girard

Definition: Interoperable storage encryption built on industry standards and embedded into drive controllers can dramatically improve performance of secure mass storage drives. The showcase technology for standardized self-encrypting drives (SEDs) is Opal Security Subclass System (SSC). Opal was released in open source in 2009 by the Trusted Computing Group (TCG) and covers individual drives, arrays and storage interfaces. Microsoft Windows 7, 8.1 and 10 natively support SEDs.

Position and Adoption Speed Justification: SEDs provide high bit rate encryption processing within the controllers of mass storage drives, so there is little or no impact on the OS, and the risk of keys being exposed in OS memory is reduced. SEDs are relatively easy to obtain, are in the early mainstream and are progressing toward the Plateau of Productivity. Several factors keep them from legacy status:

- Many buyers are unaware of SEDs as drive choices. Upgrading to SEDs after the fact is labor-intensive.
- SEDs are not supported for OS X.
- Native OS-embedded encryption systems, such as Microsoft BitLocker and Apple File Vault 2, provide a "good enough" solution with reduced chance of failure after patches and updates.
- SED technologies have not appeared in popular smartphone or tablet platforms, flash drives, etc., limiting their ability to trigger innovative new solutions.
- SEDs do not compartmentalize information in ways that would solve BYO security problems.

User Advice: SEDs can play a valuable role as a mass storage component of an enterprise workstation and server encryption plan to prevent data breaches on lost, stolen or misused equipment. Purchasing decisions for new computing platforms should give consideration to vendors that offer SEDs as part of their standard configurations. SEDs may be purchased even if there is no immediate plan to activate the encryption feature, since they otherwise function as normal drives. Buyers must specify that they want SEDs in hardware purchase contracts because suppliers default to conventional drive types. IT must ensure that the procurement group is instructed to specify SEDs, as these will not normally be the default drive type.

The choice to use SEDs will not eliminate the need for a management platform. Companies still need to store, protect and authorize keys for enrollment and locking/unlocking, and will need a central support method for audits, help desk diagnostics and postretirement disk wipes. Vendors with SED support are mentioned in "Market Guide for Information-Centric Endpoint and Mobile Protection."

Business Impact: Interoperable, hardware-based encryption offers better performance and less system interference than software tools. Companies must remember that all methods of encryption — including SEDs — must be centrally managed for the application of security policies, compliance audits and key management. Factors that favor SEDs:

- Business data vulnerabilities are reduced because encryption keys can be stored in the hardware during operation, rather than exposed to attacks through system memory.
- FIPS 140-2 certified Opal SEDs are available.
- Activation startup time is minimized because the contents of a drive do not need to be encrypted in a separate step from system imaging. Furthermore, the drive encryption is fully active if a host system is put in sleep mode.
- System performance and stability will not be impacted by the use of encryption, even at large key sizes beyond 256 bits, and particularly with input/output (I/O)-intensive applications.
- Disposal of data on SEDs is more reliable because the keys can be revoked in hardware, and no local remnant would remain to allow access to be restored by a hacker.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Broadcom; Hitachi; Intel; Kingston Technology; Marvell Technology Group; Micron Technology; Samsung; Seagate; Toshiba; Western Digital

Recommended Reading:

"Market Guide for Information-Centric Endpoint and Mobile Protection"

"Protecting Sensitive Data on Decommissioned SSDs and HDDs"

Next-Generation IPS

Analysis By: Adam Hils; Craig Lawson

Definition: In addition to first-generation intrusion prevention system (IPS) capabilities (providing threat-facing and vulnerability-facing signatures, and detecting and blocking at line speed), next-generation IPSs (NGIPSs) provide application awareness and full-stack visibility, context and content awareness, and upgrade paths to integrate new information sources (including threat intelligence, new techniques to enable mitigation of future threats, network sandboxing and payload analysis).

Position and Adoption Speed Justification: IPS vendors have found rising market acceptance as they've introduced NGIPS features on top of their existing IPS product lines. Most stand-alone vendors have NGIPS offerings, and are fighting with each other for market share based on the robustness of NGIPS features. NGIPSs will remain viable in lean-forward customers as first-generation IPSs continue to sunset. Through 2018, penetration will grow within a flat stand-alone IPS market, but will stabilize as enterprise firewall with IPS adoption grows at the expense of stand-alone perimeter IPS.

User Advice: Network security administrators should consider replacing their internet-facing IPS with a stand-alone NGIPS appliance. 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 NGIPS features. If you are replacing or installing a perimeter network firewall, then consider an NGFW that includes an NGIPS. NGIPS should also be considered for internal deployment use cases, like detecting lateral movement and workstation compromise.

Business Impact: Like first-generation IPSs, NGIPSs support vulnerability management, and 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.

Using these techniques, NGIPSs can help protect organizations against potentially costly advanced threats.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Bricata; Cisco; Huawei; IBM; McAfee; NSFOCUS; Trend Micro

Recommended Reading:

"Magic Quadrant for Intrusion Detection and Prevention Systems"

"Network and Gateway Security Primer for 2017"

Database Encryption

Analysis By: Brian Lowans

Definition: Database encryption solutions are used to protect the column, table or database instance of relational database management systems (RDBMSs) on-premises.

Position and Adoption Speed Justification: There is increasing regulatory focus on encryption as a risk-based access control by data privacy laws and data residency issues, but regulations lack guidance on the implementation of segregation of duties and access controls. Encryption is growing in importance to help minimize the risks of hacking or malicious insiders, and to meet data residency and compliance issues by preventing access to administrators and unauthorized users.

User Advice: Encryption is basically a blunt-force data access control. Any authorized users with database access privileges have access to *all* the data. Hence, when implementing encryption, organizations must also consider tools to monitor and audit all user and administrator access to sensitive data with database audit and protection (DAP) tools. Although several RDBMS vendors are offering native encryption capabilities, these are siloed, and they may not protect data from database administrators (DBA). Security policies must be coordinated across all data silos, and enterprise key management (EKM) should be implemented. DBAs should not have management responsibility for encryption, but EKM will provide consistent security policies across the different RDBMS platforms. When considering database encryption, conduct a careful assessment to identify:

- What is the data security governance strategy, and what data needs to be protected, based upon perceived risks, threats and compliance requirements?
- What is the overall data security policy? Should encryption be combined with DAP?
- How will segregation of duties and access control be handled?
- Are format-preserving encryption (FPE), tokenization and dynamic data masking (DDM) needed where field- or column-level protection is required?
- How will EKM work?

The vast majority of deployments focus on specific types of regulated data — such as credit card numbers, personally identifiable information (PII), protected health information (PHI) and financial data. Mature users then branch out using risk-based approaches to include critical but nonregulated data. Evaluate any impact on performance and functionality of applications accessing the RDBMS, and be aware that other security and database functionality, such as data discovery, can be affected.

Business Impact: Database encryption, when implemented correctly and aligned with the correct risks, can offer a strong level of control against unauthorized access to data. Consequently, concerns about the privacy of PII and PHI, data breach disclosure regulations, and the PCI Data Security Standard are putting pressure on organizations to make greater use of encryption. Data residency across borders is also driving need for FPE, tokenization or DDM to enforce stronger segregation of duties. RDBMS encryption is increasingly recommended by auditors (who misunderstand that encryption is a blunt-force tool that has very limited access control, unless combined with other tools such as DAP). Organizations need to consider how compensating controls (such as DAP, identity and access management, and other technologies) can be implemented within their environments to reduce risks and unauthorized access, instead of simply applying encryption in isolation. Encryption should be deployed as part of a broader, data-centric security strategy.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: eperi; Gemalto; HPE; IBM; Oracle; Penta Security Systems; PKWARE; Protegrity; Thales e-Security; Townsend Security

Recommended Reading:

"Develop Encryption Strategies for the Server, Data Center and Cloud"

"Develop an Encryption Key Management Strategy or Lose the Data"

"Market Guide for Data-Centric Audit and Protection"

"Big Data Needs a Data-Centric Security Focus"

Entering the Plateau

High-Assurance Hypervisors

Analysis By: Philip Dawson; Neil MacDonald

Definition: A high-assurance hypervisor is a hypervisor that establishes a high level of trust that it is hardened, has not been tampered with or compromised. Once high assurance of trust is established, mission-critical workloads and sensitive data are provided a high level of confidence from the platform underneath.

Position and Adoption Speed Justification: Most organizations deploy commercial hypervisor-based virtualization platforms without adequate insight as to the trustworthiness of the platforms. On the positive side, the current releases of Microsoft Windows' Hyper-V and VMware's vSphere all support root-of-trust measurements at bootup. Trusted platform module capabilities are built into most server platforms, and the latest generation of Intel processors supports trust measurements and extensions as well.

Delivering a high-assurance hypervisor shouldn't require a significant amount of code running in the hypervisor, because this defeats the purpose of keeping the hypervisor/VMM thin to reduce the surface area for attack. Techniques such as root-of-trust measurements, configuration standards, small footprint hypervisors and hardware-enforced memory protection are straightforward, low-impact ways to better secure the hypervisor. Publicly disclosed breaches of hypervisors are rare, but several high-profile vulnerabilities in Xen have raised awareness of the issue.

User Advice: Implement mechanisms to establish trust in the virtualization platform being used, and to minimize the chance that the hypervisor has been compromised through bootup measurement techniques:

- Favor implementations in which the hypervisor is as small as possible to reduce the surface area for attack.

- Favor implementations in which the hypervisor is capable of being stored in firmware, making it less susceptible to being compromised.
- Require all hypervisor vendors to demonstrate proof-of-assurance security testing.
- Implement strong configuration and patch management processes for the hypervisor.

Business Impact: A compromise of the virtualization platform is a worst-case security scenario that places all virtual machines hosted on the virtualization platform at risk. While there is no panacea, high-assurance hypervisors placed in nonvolatile storage should be considered a mandatory least common denominator of protection for virtualization platforms hosting critical applications.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Armor; Citrix; Cloud Raxak; Green Hills Software; HyTrust; Integrity Global Security; Lynx Software Technologies; Microsoft; VMware

Recommended Reading:

"Use Trustable Application Overlay Principles for Secure Services Delivery"

"How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center"

"Addressing the Most Common Security Risks in Data Center Virtualization Projects"

Network Penetration Testing Tools

Analysis By: Adam Hils

Definition: Penetration testing uses multistep attack scenarios to find vulnerabilities and exploit them to map device roles, trust relationships, accessible network services and potential vulnerabilities, and to access target systems. Penetration testing also provides visibility into misconfigurations or vulnerabilities that could allow compromise, thereby causing serious impact. Penetration testing tools provide a means for prioritizing high-risk vulnerabilities, and for launching complex attacks to demonstrate the vulnerability of existing defenses.

Position and Adoption Speed Justification: Whether financially or ideologically motivated, sophisticated targeted attacks have driven the need to extend vulnerability assessment beyond simple vulnerability discovery. A penetration testing suite takes the next step and offers strong evidence that a vulnerability is exploitable, providing valuable input into a vulnerability management strategy. The PCI Data Security Standard has mandated yearly penetration testing, as have other compliance regimes, such as the U.S. Federal Information Security Management Act (FISMA) and North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection. Many organization would rather bring in third party pen testers to perform periodic compliance-focused testing rather than maintain a security-focused internal program. However, for those that choose to operate an in-house capability, selecting a COTS toolkit for performing penetration test is a common approach

User Advice: Penetration testing can provide benefits for most businesses, but its use is especially valuable for organizations with complex and frequently changing IT environments. Penetration testing comes with a cost, whether through engaging an outside firm to conduct the tests or in personnel time and training — plus tool acquisition costs for organizations that do it themselves. Penetration testing done badly can also impact operational systems and inaccurately report breaches (that is, false positives).

The effectiveness of network penetration tools largely depends on the skill of the practitioner. Enterprises that need to regularly perform penetration testing, but do not have the necessary technical skills, should focus on using services rather than buying products. Penetration test service providers are numerous, and often serve specific cities or regions. However, penetration testing products are getting easier to use and are becoming better at minimizing the impact on business resources, so enterprises that have the required skills should evaluate commercial and open-source products. Some network vulnerability assessment tools also offer "light" network penetration testing. Some best practices are to create a standard toolset to ensure that penetration testing is structured and repeatable, and to perform penetration testing quarterly, as well as after any major IT change. Penetration testing should also include "inside out" testing, wherein an internal PC is used to access a simulated malicious website.

Users should differentiate between network penetration tools and application testing. While pen testers use both toolsets, application testing is an effort to find vulnerabilities in internet-facing and internal applications, not to find exploitable network vulnerabilities.

Business Impact: Well-executed penetration testing increases the likelihood that vulnerabilities enabling highly damaging attacks will be detected and remediated before exploitation occurs.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Core Security; Immunity; Kali; Metasploit; Rapid7; Saint; Wireshark

Recommended Reading:

"Understand the Types, Scope and Objectives of Penetration Testing"

"How to Select a Penetration-Testing Provider"

"Threat and Vulnerability Management Primer for 2016"

Enterprise Firewalls (Next-Generation Firewalls)

Analysis By: Greg Young; Adam Hils

Definition: Enterprise, or next-generation firewalls (NGFWs), are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection and intrusion prevention, as well as bring intelligence from outside the firewall. These extra firewall intelligence services include cloud-based advanced threat detection (ATD) and threat intelligence (TI). An NGFW should not be confused with a stand-alone network intrusion prevention system (IPS) or SMB multifunction firewalls (unified threat management [UTM]).

Position and Adoption Speed Justification: Commercially available enterprise firewalls (NGFW) are achieving a very large market size, and capabilities continue to advance. This technology has advanced greatly and has supplanted the preceding technology of stateful firewall in most enterprises. The time to plateau has been adjusted to a longer time in reflection of the increased number of services being added to the firewall, and the disruptive effects on public cloud-based versions by the public cloud infrastructure vendors' limited adoption of a third-party network security ecosystem.

User Advice: Consider enterprise firewalls (NGFW) for your shortlist if you're replacing or upgrading a legacy stateful firewall network firewall at the network edge, and you don't have a significant investment in a stand-alone IPS. However, if you have such an IPS investment, ensure that any selected firewall has an NGFW as a current option (or on the near-term roadmap), so that, when the IPS needs to be replaced, you'll have the option to move to an NGFW with the least amount of disruption. NGFW rarely includes slower inspection mechanisms, such as antivirus or local anti-malware sandboxes, as these can introduce unacceptable latency. Although not housed in the same appliance, better firewall vendors now have "good enough or better" cloud-based sandboxes, or connections to local sandboxes from the same or a partnered vendor providing a single console view. A difficulty for any cloud-based sandbox is the limited adoption and efficiency of TLS decryption on firewalls, which reduces the coverage for the sandboxing feature; encrypted traffic cannot be inspected for redirection to a sandbox.

Business Impact: An NGFW closely integrates the capabilities of enterprise firewalls with network intrusion prevention and other services.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

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

Recommended Reading:

"Magic Quadrant for Enterprise Network Firewalls"

Application Control

Analysis By: Neil MacDonald

Definition: Application control solutions for endpoints, sometimes referred to as "application whitelisting," are a type of endpoint protection (server workloads and desktops) typically included with endpoint and cloud workload protection platforms. Basic solutions control whether a given piece of executable code is allowed to execute. More advanced solutions offer more granular control over what an application can do once it is running and interacting with system resources.

Position and Adoption Speed Justification: Application control is difficult to fully implement on end-user-facing systems, but is a powerful protection strategy for server workloads.

On end-user facing systems, in most cases, application control software doesn't replace traditional antivirus and personal firewall offerings or the traditional PC configuration tools used to manage user applications. Instead, it acts as an additional layer of protection for endpoints to supplement the increasing ineffectiveness of signature-based antivirus solutions. In addition, for users who retain administrative rights on their systems, these tools can help restrict applications that administrators can execute.

In contrast, most workloads in on-premises VMs and in public cloud IaaS run a single application. This is almost always the case with containers hosting microservice-based applications. The use of whitelisting to control what executables are run on a server provides an extremely powerful security protection strategy. All malware that manifests itself as a file to be executed are blocked by default. Many cloud workload protection platform (CWPP) solutions provide built-in application control capabilities or dedicated point solutions offer them. Alternatively, the built-in application control capabilities of the OS might be used, such as software restriction policies, AppLocker and Device Guard with Windows, or SELinux or AppArmor with Linux. Some of the application control vendors can further constrain the runtime behavior of whitelisted applications, using more-granular policy enforcement.

User Advice:

- Disable antivirus on most servers, and use application control and whitelisting as the primary protection strategy for server workloads unless the server hosts a file-sharing repository.
- For end-user facing systems, don't overlook the political and cultural challenges of exerting more control over desktop computing, especially in environments where users run as administrators and install whatever they want.
- When evaluating application control solutions, consider incumbent endpoint protection platform and PC life cycle management vendors in addition to security point solutions. Reducing agents and consoles as well as cost and complexity should be weighed in the evaluation.
- Pressure incumbent EPP and CWPP vendors to include application control capabilities at no extra cost. Several already do this.

- Use approaches rooted in application control and whitelisting as the cornerstone of your server and embedded device protection strategy, not signature-based anti-malware. This should extend to containers with newer vendors supporting this.
- As an alternative to antivirus — or where antivirus and patching aren't possible — consider application control as an alternative security control for point-of-sale terminals, supervisory control and data acquisition systems, and other devices that fall under regulatory requirements.
- For end-user machines, simply removing administrative rights from end users and running them as standard users may provide a better cost-benefit or risk trade-off than deploying and managing an application control solution.
- Don't use a one-size-fits-all approach. Classify and segregate users by their work styles and phase in application control solutions to end users with less dynamic work-style environments first.
- Favor application control solutions that enable the detailed monitoring of endpoints, even if blocking is not enabled for use in advanced threat detection and forensics.
- Investigate network-based application control solutions as a possible alternative to endpoint/server-based solutions, depending on the use case.

Business Impact: Properly implemented application control is the most significant solution to reduce the attack surface of endpoints and should be mandatory on servers. Application control solutions help augment deficiencies in the signature-based antivirus model, providing protection against malware variants and targeted attacks. Operationally, these solutions can restrict the applications that users run, providing protection from unlicensed applications, increasing compliance and prohibiting unwanted software, while also enabling end users to extend their workspaces in ways that comply with policy, even for applications installed outside the IT organization's purview or control. Application control helps to balance users' demand for freedom in their computing environments with the IT organization's need for some operational and security controls.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Aqua Security; Blue Ridge Networks; Carbon Black; Check Point; Ivanti; Kaspersky Lab; McAfee; Microsoft; Trend Micro; Twistlock

Recommended Reading:

"Market Guide for Cloud Workload Protection Platforms"

"How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center"

"Magic Quadrant for Endpoint Protection Platforms"

"Best Practices for Securing Workloads in Amazon Web Services"

"Market Guide for Application Control Solutions"

SIEM

Analysis By: Toby Bussa

Definition: Security information and event management (SIEM) technology supports threat detection and security incident management through the collection and real-time analysis of security events, as well as a wide variety of other event and contextual data sources. It delivers compliance reporting and incident investigation through historical data analysis. The core capabilities are a broad scope of event collection and normalization, the ability to correlate and analyze events across disparate sources, and workflow and reporting features.

Position and Adoption Speed Justification: Targeted attacks and broad-based malware infections, resulting in breaches and data loss events, have resulted in threat management as the primary use case for SIEM. New buyers, and those with existing SIEM deployments, seek earlier, and more effective, incident and breach detection through active security monitoring. Regulatory compliance reporting is also a driver; however, it is generally secondary to threat management. Enterprise organizations continue to deploy SIEM tools for monitoring perimeter and internal security controls, endpoints and servers, and, increasingly, database management systems (DBMSs), applications and users. As upper midmarket and small enterprise organizations adopt SIEM solutions, and enterprise organizations compete for limited SIEM tool expertise, there is growing interest in remotely managed and co-managed SIEM from external service providers. Organizations looking to shorten the deployment cycle and to transfer responsibility for managing SIEM tools, are opting to leverage SIEM as a service delivered from the cloud and hosted SIEM tool options.

Capabilities that support the threat monitoring use cases and aid in targeted attack detection include user activity monitoring, application activity monitoring, profiling and anomaly detection, use of threat intelligence feeds, and advanced analytics. Adoption of SIEM technology by a broad set of companies has fostered demand for products that are easy to deploy and support, and provide out-of-the-box security event monitoring and compliance-reporting functions. User behavior activity monitoring, and data access and usage for early detection of targeted attacks and data breaches have emerged as high-priority use cases for SIEM technology.

SIEM vendors continue to develop and refine big data capabilities and analytic functions in their own products, and provide integration with third-party technologies for these functions (e.g., user and entity behavior analytics [UEBA]). The result is improved security analytics capabilities, ranging from basic capabilities being included as part of core product functionality to advanced, machine-learning-oriented detections provided by third-party solutions. Threat intelligence feeds are commonly supported, with several going beyond basic threat feed capabilities to support industry standards, such as STIX and TAXII. SIEM tools are adopting more-advanced incident response workflow capabilities through the addition of core capabilities that add basic automation and orchestration, as well as integration and support for more-advanced solutions offered by third parties.

User Advice: Security and risk leaders considering SIEM solution deployments should first define their use cases and then requirements for log management, threat monitoring, user and resource access monitoring, security incident response management, and compliance reporting. This may require the inclusion of other groups in the requirements definition effort, such as audit and compliance, network operations, server administration, database administration, and application support areas. It may also require SIEM tool integration with data sources that provide context for security monitoring, such as user directories, configuration management databases (CMDBs) and vulnerability scanning products. Organizations should document their network and system topologies, and where security controls are deployed in the organization, along with future use cases that will affect SIEM tool deployment growth and analytic requirements. Estimates of log volume sizes and event rate velocities should be documented for initial use cases and future use cases that may be implemented during the next 12 months.

SIEM vendors can use this data to propose a company-specific solution. Technology and service selection decisions should be driven by organization-specific requirements (i.e., SIEM use cases) in areas such as the relative importance of real-time monitoring and analytics, integration with established system and application infrastructures, and the IT security organization's technology deployment and operations capabilities. Considerations should also be made for how the SIEM will be administered, run and used, and whether third-party support will be required.

Business Impact: SIEM solutions improve an organization's ability to quickly detect attacks and data breaches, and improve incident investigation and response capabilities. SIEM tools also support other use cases, such as the reporting needs for organizations with regulatory compliance obligations, as well as those subject to internal and external audits.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: AlienVault; Dell Technologies (RSA); Fortinet; HPE; IBM; LogRhythm; McAfee; SolarWinds; Splunk; Trustwave

Recommended Reading:

"Magic Quadrant for Security Information and Event Management"

"Critical Capabilities for Security Information and Event Management"

"Planning for an SIEM Technology Deployment"

"How to Deploy SIEM Technology"

"Using SIEM for Targeted Attack Detection"

Vulnerability Assessment

Analysis By: Kelly M. Kavanagh

Definition: Vulnerability assessment (VA) products and services assess IT environments and:

- Discover, identify and report on device, operating system and software vulnerabilities
- Establish a baseline and trending of vulnerabilities
- Identify and report on the security configuration of IT assets
- Discover and report on network-attached IT and OT assets
- Support specific compliance reporting and control frameworks
- Support risk assessment and remediation prioritization
- Support remediation by IT operational teams

Position and Adoption Speed Justification: The VA market is mature. It is characterized by a number of pure-play and other related vendors competing for vulnerability scanning and complementary capabilities, and by the growth of multiple alternative forms of delivery, including products, SaaS and managed services. Gartner expects stable, long-term demand for security VA capabilities. This will continue to increase pressure on pricing and margins. Nonetheless, VA capabilities will have to continue to evolve, driven by changing threats, compliance requirements, use of new technologies and organizational efforts to reduce the cost, while simultaneously driving improvements, of vulnerability management processes.

VA is a foundational component of the vulnerability management process. The use of VA products or services as a best practice has been incorporated into a number of prescriptive compliance regimes, including the Payment Card Industry Data Security Standard (PCI DSS), the U.S. Federal Information Security Management Act (FISMA) and ISO 27001. These regimes, the widespread recognition of vulnerability management as a best practice for threat management and risk reduction, as well as pressure from business partners, supply chain customers and auditors, have been the primary drivers of VA projects in recent years.

User Advice: There are three approaches to VA:

- **Active network scanning** is the most widely used technique. It involves remote scans of network-attached devices. Active scanning can be unauthenticated or authenticated (via credentials for the scan target). Authenticated scanning provides a more in-depth and reliable assessment of the scan targets, resulting in improved accuracy, reduced false negatives and false positives, as well as the ability to determine security configurations. For large deployments, authenticated management capabilities may be an important criterion for ease of management.
- **Passive observation** is based on the assessment of the content and the pattern of captured network traffic or data import via third-party technology integrations (e.g., asset inventory systems). Passive observation can provide information about devices that cannot be actively

scanned (e.g., in OT environments), but this technique alone generally does not provide sufficient data to support remediation activity.

- **Agents** reside on the scan targets, either as persistent or as temporary software, collecting state and configuration information in real time. Agents provide information about the target that often cannot be determined remotely, such as applications or services that are installed but not running, or about changes in files or configurations. Persistent agents can be used only on devices that are known and managed and run a supported OS.

Most VA deployments rely on active network scanning. There are typically areas in larger IT environments, for example unmanaged or mobile devices, which benefit from passive observation or agent-based assessment. Gartner recommends that organizations combine active scanning with one of the other two described techniques for comprehensive coverage.

Buyers should assess VA tools' capability to scan virtual environments and mobile devices, to assess security configuration settings, to manage multiple scanners in large deployments, and to provide targeted remediation support with flexible reporting, threat analysis and asset identification. VA vendors compete on these features — and on price — rather than on claims about scan speed or accuracy. Deployment options include software, appliance, virtual appliance and remote-hosted or cloud-based services, and mixed deployments that incorporate several modes. VA vendors are also adding dynamic application security testing (DAST) capabilities for web application security (WAS). Organizations lacking WAS should consider adding these capabilities through a VA vendor, even though they may not be as feature rich as stand-alone application security tools (AST) or services.

Business Impact: VA is an important component of the vulnerability management process to support an organization's security management and conformity with regulatory requirements or compliance regimes. Vulnerability and configuration data can provide additive value when available to other elements in the vulnerability management process:

- VA data can be used to improve the granularity and accuracy of network security technologies, such as intrusion prevention systems and web application firewalls, by matching blocking rules with vulnerabilities.
- VA results can be used to identify targets for exploiting validation with penetration testing tools.
- Assets discovered during scanning can be compared with asset databases and user directories to identify unmanaged assets, and to provide business and risk context to VA reporting.
- Asset configuration and vulnerability data enriches security event monitoring related to those assets.
- Vulnerability data, asset data and risk context support patch management or system management activities by identifying high-value assets and high-risk vulnerabilities for priority attention.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: BeyondTrust; Digital Defense; F-Secure; Outpost24; Positive Technologies; Qualys; Rapid7; Tenable Network Security; Tripwire; Trustwave

Recommended Reading:

"Market Guide for Vulnerability Assessment"

"It's Time to Align Your Vulnerability Management Priorities With the Biggest Threats"

"Threat-Centric Vulnerability Remediation Prioritization"

Mobile Data Protection for Workstations

Analysis By: John Girard

Definition: Mobile data protection (MDP) tools encrypt mass storage (e.g., magnetic and solid-state drives) and implement boot access controls. The main use case is company-owned notebooks/laptops running Microsoft Windows or Mac OS X, and associated removable media. MDP products may be used for desktops and servers. Broader solutions for information-centric data protection for shared files, cloud storage, smartphones and tablets are blending with MDP through the appearance of extended product features and bundles involving EMM, DLP and EDRM.

Position and Adoption Speed Justification: MDP tools have existed since the 1990s and are used primarily to protect hard drives on company-owned Wintel notebook/laptop computers. Products range from suites that link to larger endpoint protection (EPP) frameworks and protect multiple OS platforms to single-purpose solutions. The management of MDP can be delivered as an in-house solution or a managed service. The majority of vendors support self-encrypting drives (SEDs), native Windows BitLocker and Mac FileVault 2. MDP vendors compete on other factors, particularly breadth of policy management and reporting features.

Several MDP companies have investments in EMM, but product lines have not merged in ways that add value for MDP buyers. Others have investments in DLP, EDRM and data classification that become strategically valuable as the typical mobile use case is refocusing to protect individual files and online sharing. In 2017, MDP is still a critical protection feature for all devices with mass-storage drives.

User Advice: The loss or theft of data on mobile devices is among the most frequent data exposure risks that companies face, and is frequently reported for workstations (particularly notebooks/laptops). However, nonmobile desktop systems and servers are also major sources of breaches, and should also be given due attention. Data protection is one of the first investments that should be made on *any* endpoint workstation platform, mobile or not. It is wise to include data protection in the plan for the standard image, administration and maintenance for all devices — whether fixed or mobile, large or small. Data avoidance is not a viable approach: Many organizations have tried to implement a policy forbidding the use of sensitive data on laptops, but all of them have failed to motivate users to comply, and often do not account for intrinsic application data storage.

A good MDP investment makes its *first* payback when a new workstation is provisioned. Unencrypted data on drives is difficult and costly to erase, so no business data should be stored before encryption is in place. MDP is also the *last* payback companies will realize on a platform, in the sense that revoking the access key is an effective step for data disposal at the retirement of an encrypted system. For practical purposes, deletion of the key is the logical equivalent of a full drive wipe, so device encryption provides an extremely valuable data protection role when devices are being retired or redeployed.

Business Impact: The business value for data protection is clear, and the consequences of failing to implement even basic data protection are severe. The number of laws that come into play and the increasingly severe penalties help to raise business awareness of the value of data protection in terms of avoiding the costs of embarrassment; mitigation of exposed records, such as customer accounts, lost intellectual property and other critical corporate data; lost business deals and reputation; and legal and civil penalties. In "Pay for Mobile Data Encryption Upfront, or Pay More Later," Gartner quantified a cost scenario that demonstrates that even simple breaches can cost many times more than the investment to protect data properly. The bottom line is that there is no downside to implementing MDP for mobile and fixed workstations.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: CenterTools Software; Check Point; Dell; Digital Guardian; EgoSecure; McAfee; Microsoft; Sophos; Symantec; WinMagic

Recommended Reading:

"Data Can Move Without Leaking — Eliminate Four Flaws in Your Mobile Information Protection Strategy"

"Market Guide for Information-Centric Endpoint and Mobile Protection"

"Pay for Mobile Data Encryption Upfront, or Pay More Later"

Network IPS

Analysis By: Adam Hils; Craig Lawson

Definition: A network intrusion prevention system (IPS) uses in-line, deep packet inspection appliances with a combination of technologies to detect, block and shield against attacks and unwanted traffic. Network IPSs do not leverage user and application contexts like next-generation IPS (NGIPS) technologies do.

Position and Adoption Speed Justification: Enterprise demand for prepatch vulnerability shielding and worm defenses has kept this market alive. The market is mature and consolidated, and shortlists are less varied. IPS technology as a market has matured since most enterprises routinely block, rather than just detect, attacks — especially at the network edge. As most vendors have introduced NGIPS features for stand-alone competitiveness, and as IPSs are increasingly subsumed within next-generation firewall (NGFW) deployments, IPSs without next-generation features are obsolete.

User Advice: Network security administrators: Consider replacing your internet-facing intrusion detection system/IPS with a stand-alone IPS appliance that has discernible NGIPS features. Look for network-edge placements first, and then expand the deployment inward, but only in tactical locations. Follow a process approach. If you are replacing or installing a network firewall at the perimeter, then consider an NGFW that includes NGIPS. Enterprises looking for strong intrusion detection/prevention should first investigate next-generation IPS. Specific deployment constraints can force adoption of basic network IPS as a stand-alone solution, but most enterprises should take one of the approaches mentioned above.

Buyers need to drive vendors for further advances in dealing with "gray list" events and targeted malware by adopting NGIPS capabilities. NGFWs increasingly incorporate NGIPSs, so enterprises should consider consolidating IPSs during firewall refreshes.

Business Impact: Network IPSs support vulnerability management, and improve network security by blocking attacks that are focused on exploiting known vulnerabilities in the network and at endpoints, or by causing a denial of service.

Benefit Rating: Low

Market Penetration: More than 50% of target audience

Maturity: Obsolete

Sample Vendors: Alert Logic; Cisco; FireEye; Huawei; IBM; NSFOCUS; Radware; Trend Micro; Trustwave

Recommended Reading:

"Magic Quadrant for Intrusion Detection and Prevention Systems"

"Network and Gateway Security Primer for 2017"

UTM

Analysis By: Jeremy D'Hoinne; Rajpreet Kaur

Definition: Unified threat management (UTM) platforms are multifunction network security appliances particularly suited to small or midsize businesses (SMBs). Feature availability continues to grow, copying new features from other network security technologies; however, performance degrades as more features are enabled. That's why the primary UTM use cases are employee productivity and internet security. While none of the functions may be best-of-breed, UTM products meet the need for low-cost, due-diligence levels of security.

Position and Adoption Speed Justification: This year, UTM reached the Plateau of Productivity. The technology is mature, and the addition of new features aim to place the technology as a component of a broader platform approach, or to reduce its scope to slow down refresh cycle. UTM integrates with third-party solutions to maintain their role of multifunction security gateway, but have reached capacity for what can be done on a single appliance. Integration with endpoint protection agents are more easily accepted in SMBs than in larger organizations, and the next step could be to integrate with SaaS solutions, or with cloud access security brokers to gain visibility and control on SaaS. UTM also needs to fight against the risks of becoming a commodity, as the rise of encrypted traffic drives distributed organizations to increasingly use cloud-based secure web gateways to replace UTM's embedded URL filtering capabilities.

Use of multifunction firewalls in SMBs is mainstream, but the number of features in use might vary greatly. Enterprise security buyers often consider that the consolidation of "good enough" features on UTM platforms provides limited benefits and impacts performance. UTM budgets often compete with internet-hosted, secure web gateway services (cloud-based) or basic stateful firewalls. Fully cloud-based firewall-as-a-service vendors are trying to emerge as new competitors, moving the entire workload to the cloud. Features such as VPNs, URL filtering, wireless management, cloud-based centralized management consoles and high-level reporting dashboards also get higher adoption rates. Network sandboxing is available with most vendors, and SMBs are adopting it because of channel partner active campaign, and an increased awareness of ransomware risks.

User Advice: UTM products can efficiently meet the security needs of SMBs that do not have complex business dependencies or industry-specific risk appetites. However, enabling too many features — especially file inspection (antivirus, cloud-based sandboxing and data loss prevention) — can severely harm the overall performance in many ways, including throughput, latency and the maximum number of concurrent connections.

Generally, Gartner sees multifunction firewalls products being used in midsize organizations with constrained budgets to meet firewall, intrusion prevention system and web security gateway functions, and also for remote connectivity for mobile employees. Multilocation SMBs or distributed enterprises that have branch-office security needs similar to SMBs (for example, multilocation retail enterprises or hotel chains with limited local IT staff) may find UTM products appealing. Distributed organizations considering UTMs for branch offices alone should not underestimate the costs that could come from potential misconfiguration, inconsistent security and duplicated processes when using more than one brand of firewall. Larger enterprises should first look at branch-office firewalls from the same vendor as their central firewalls.

When evaluating UTM, pay attention to the effectiveness of the different security modules, the reality of the cost savings coming from feature consolidation once the performance impact is estimated, and the long-term ease of use of stand-alone and centralized management beyond the initial deployment of the UTM platform. Compare UTM with alternate and emerging choices, including hybrid approaches with cloud-based centralized management, cloud-based web and email traffic inspection, or even firewall as a service.

Subscription costs can be considerably higher for a UTM solution compared with other network security solutions. Bundled features and aggressive first-year discounts coupled with higher yearly maintenance rates and ancillary services for SMBs with no dedicated security staffs all contribute to increased lifetime costs. SMBs should evaluate the total cost of ownership for a five-year period before making a purchase decision, including management and maintenance costs when delegated to a managed security service provider.

Business Impact: This technology mostly affects SMBs, remote-office applications and branch-office applications with needs similar to SMBs.

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Sample Vendors: Barracuda Networks; Check Point Software Technologies; Cisco; Cisco Meraki; Fortinet; SonicWall; Sophos; Stormshield; Venustech; WatchGuard

Recommended Reading:

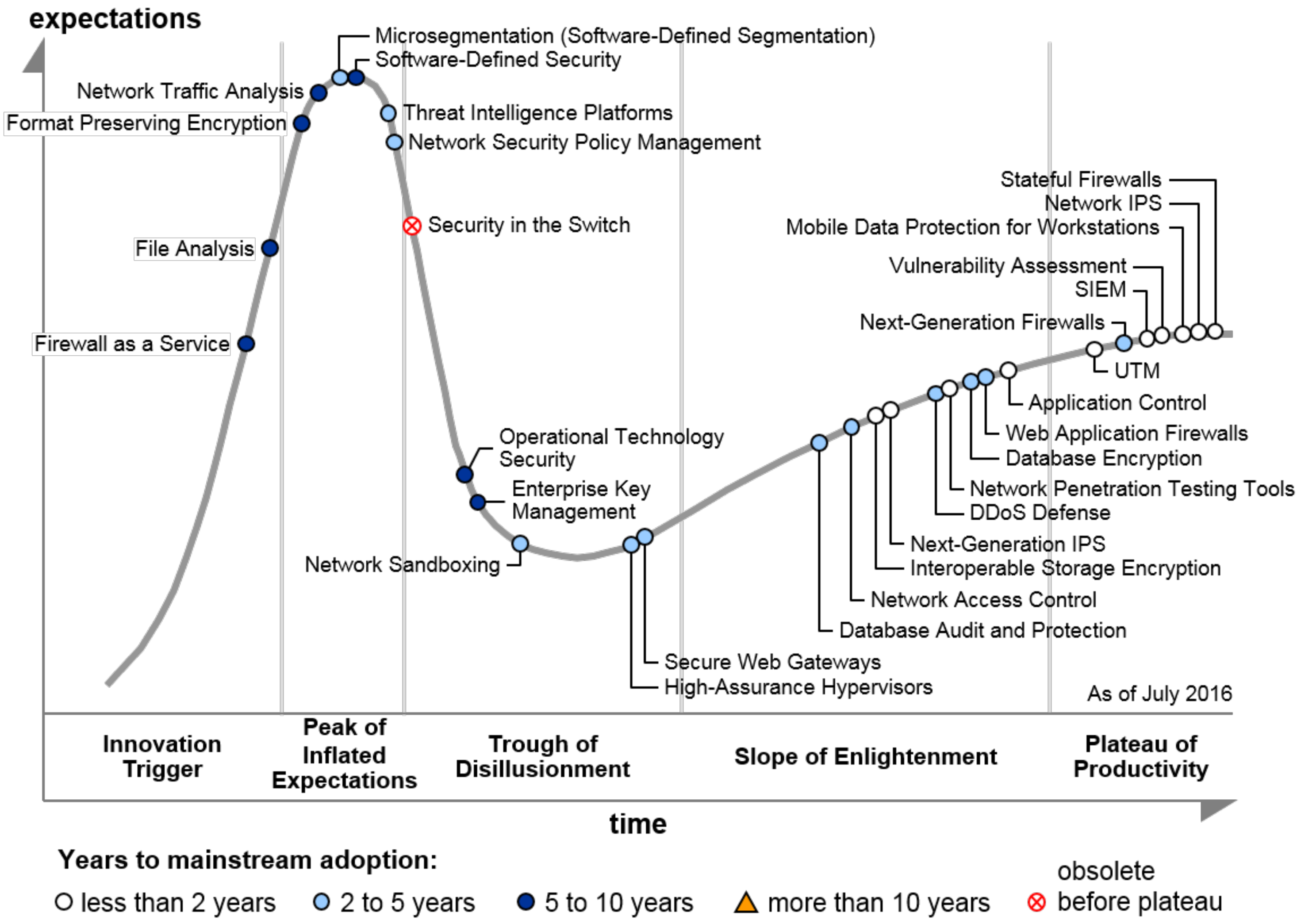
"What You Should Expect From Unified Threat Management Solutions"

"Magic Quadrant for Unified Threat Management"

"Next-Generation Firewalls and Unified Threat Management Are Distinct Products and Markets"

Appendixes

Figure 3. Hype Cycle for Infrastructure Protection, 2016



Source: Gartner (July 2016)

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

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 (July 2017)

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

Source: Gartner (July 2017)

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
Legacy	■ Not appropriate for new developments ■ Cost of migration constrains replacement	■ Maintenance revenue focus
Obsolete	■ Rarely used	■ Used/resale market only

Source: Gartner (July 2017)

Gartner Recommended Reading

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

"Understanding Gartner's Hype Cycles"

"Magic Quadrant for Network Intrusion Prevention Systems"

"Magic Quadrant for Unified Threat Management"

"Magic Quadrant for Enterprise Network Firewalls"

"Magic Quadrant for Secure Web Gateways"

"Magic Quadrant for Endpoint Protection Platforms"

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."