G00263740

Hype Cycle for Infrastructure Protection, 2014

Published: 30 July 2014

Analyst(s): Greg Young

The numbers and volumes of threat-facing technologies that defend our IT grow at a relentless pace. Driven by persistent threat and technology change, there has never been so much hype in enterprise security; however, there are more than enough technologies for enterprises to consider.

Table of Contents

List of Tables

List of Figures

Analysis

What You Need to Know

In 2014, the threat level to enterprise IT (that is, networks, systems, data and applications) is very high. Enterprises are likely unable to deploy all possible technology and service defenses on this Hype Cycle, and must make difficult choices. 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 infrastructure.

Infrastructure protection technologies are segmented according to the infrastructure component that is protected: the network, host systems 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.

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, the increasing opportunity is for intelligence exchange between products and services to assist in correlation, and to provide context, rather than a single solution that protects all infrastructure components. No megaconvergence is coming. The 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). 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, thereby putting pressure on security budgets. The idea of all-cloud, all-virtual or single-vendor security remains mythical.

The Hype Cycle

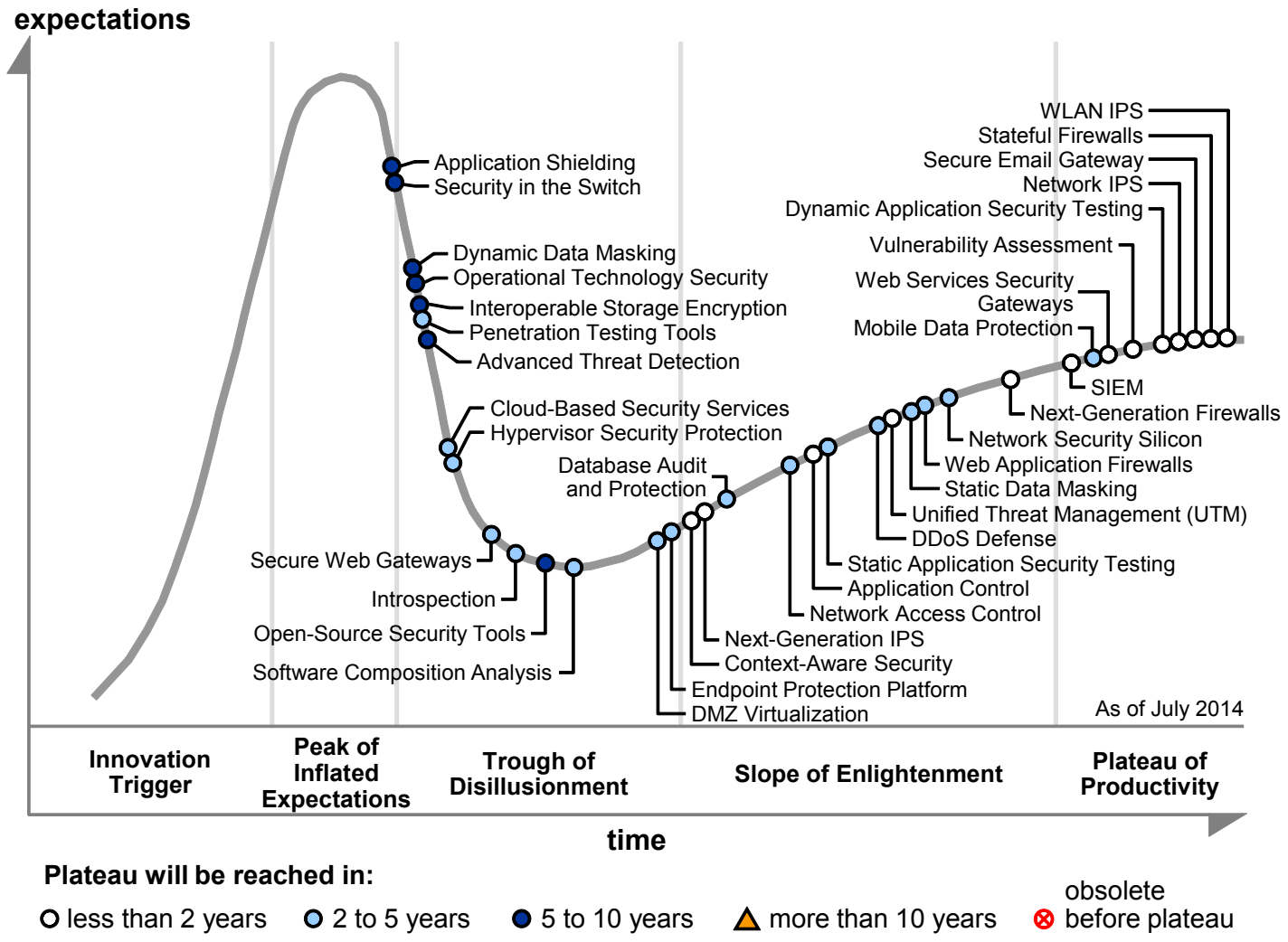
In this Hype Cycle, infrastructure protection refers to all protective measures in IT. In order to "keep the bad guys out," Gartner subdivides IT security into three macrodomains: identity and access management (IAM), business continuity and governance, and infrastructure protection. Infrastructure protection is threat-facing and reactive to new types and vectors of attack.

This Hype Cycle once again shows considerable clustering of technologies at the slope and plateau. The absence of technologies at the trigger and peak areas is also noteworthy. There are almost too many tools that enterprises could adopt, exceeding their ability to develop supporting processes and ongoing staff operations. The overhyping of existing infrastructure protection technologies has "removed the oxygen from the room," thereby stifling real innovations. Most of

what is labeled a "new approach" to infrastructure protection is just a trivial variant on current mainstream technologies.

The clustering at the slope and plateau has been evident for the past four years. The continued reliance on plateau technologies is a consequence of the fact that older threats haven't gone away and must still be defended against. Most of the attacks today are based on known threats, and they are being countered with technologies that are already in place (for example, antivirus and IPSs). However, the labeling of threats as "advanced" (for example, advanced persistent threats) means that very few attackers have figured out how to bypass traditional defense mechanisms. Enterprises need to adopt signatureless and behavior-based advanced threat defense technologies if they desire to combat these threats. Advanced Threat Detection is sliding toward the Trough of Disillusionment, but the adoption of this technology is now in the early mainstream phase (see Figure 1).

Figure 1. Hype Cycle for Infrastructure Protection, 2014



Source: Gartner (July 2014)

The Priority Matrix

Infrastructure protection is driven by the need to protect against existing "legacy" threats while reacting against new and emerging threats. Infrastructure protection technologies and services that enable the consolidation of legacy approaches, and that 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, but point solutions are no longer required because capabilities are provided as features of existing mainstream offerings (see Figure 2).

Figure 2. Priority Matrix for Infrastructure Protection, 2014

benefit	years to mainstream adoption			
	less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational	**Context-Aware Security**	**Introspection**		
high	**Dynamic Application Security Testing** **Next-Generation Firewalls** **Next-Generation IPS** **Secure Email Gateway** **WLAN IPS**	DDoS Defense Endpoint Protection Platform Mobile Data Protection Network Access Control Secure Web Gateways Static Application Security Testing Static Data Masking	Advanced Threat Detection Operational Technology Security	
moderate	Application Control SIEM Stateful Firewalls Unified Threat Management (UTM) Vulnerability Assessment Web Services Security Gateways	Cloud-Based Security Services Database Audit and Protection DMZ Virtualization Network Security Silicon Penetration Testing Tools Software Composition Analysis Web Application Firewalls	Application Shielding Dynamic Data Masking Interoperable Storage Encryption	
low	Network IPS	Hypervisor Security Protection	Open-Source Security Tools Security in the Switch	

As of July 2014

Source: Gartner (July 2014)

At the Peak

Application Shielding

Analysis By: Neil MacDonald; Joseph Feiman

Definition: Application shielding refers to a set of technologies that is employed to add security functionality directly to applications for the prevention and detection of application-level intrusions.

Position and Adoption Speed Justification: Ideally, security capabilities are injected directly into an application without requiring developers to modify the source code. Java and .NET applications are easier to inject in this way; however, for other types of applications, "wrappering" the application code with supplemental security code is an alternative. In some cases, the application may have to be recompiled, but this is not the preferred approach.

This category has received significant attention recently because of the need to protect mobile applications. With the rise in the number of mobile applications, interest has increased in wrapping applications as a way to add encryption and authentication capabilities to protect application information. Adoption rates in specific scenarios — for example, the protection of military assets, gaming systems and licensing mechanisms — are higher because of the value of the intellectual property (IP) being protected and the awareness of determined hackers targeting these systems. However, in general, adoption rates and awareness of application-shielding technologies are low because most organizations are unaware of the benefits until they directly experience the theft of IP or an attack that compromises an application.

Application-shielding techniques can be applied proactively (for example, protecting against and alerting for tampering, or implementing the type of input filtering that developers should have written to protect against exploits) or reactively (injecting protection as a result of a vulnerability that is discovered in production, or performing some predetermined action based on exploitation attempts). Nonetheless, for application protection techniques that rely on the insertion of code, development organizations may be reluctant to allow the injection of new code into an application from a source other than a developer.

As an alternative to application shielding by modifying the application, Web and database applications may be shielded by external-network-based Web and database application firewalls that provide alternative, application-level protection mechanisms. In addition, as an alternative to shielding by directly modifying the application, runtime application self-protection (RASP) may offer a simpler solution by instrumenting the application's runtime platform (specifically, the Java or .NET runtime platform) versus the application itself.

User Advice: Consider application shielding as a way of proactively inserting security protection into applications. If vulnerabilities are present in production applications, then application-level shielding offers a way to protect an application by inserting security protection to guard vulnerable applications while waiting for the vulnerabilities' remediation to be addressed in development. For mobile applications and embedded systems, the wrapping of applications provides an alternative method to protect an application and the information that the application manages. Favor solutions that can shield applications without requiring changes to source code and that, ideally, do not

require recompilation. For network-based Web and database applications that remain on-premises, Web and database firewalls offer alternatives that require no changes to the application.

Business Impact: Application shielding provides protection for an organization's software-based assets (especially those placed on mobile devices, machines, sites and locations that the organization doesn't control — including mobile devices) from tampering, reverse engineering, and attacks on the application and the information that it manages. Application shielding also provides several types of application-level security without requiring developers to natively modify source code.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Arxan Technologies; HP (Fortify); Inside Secure; Irdeto; PreEmptive Solutions; Symantec (Nukona); V.i. Labs

Recommended Reading: "Emerging Technology Analysis: Mobile Application Shielding"

"Cool Vendors in Security: Infrastructure Protection, 2013"

"Avoiding Mobile App Development Security Pitfalls"

"Runtime Application Self-Protection: A Must-Have, Emerging Security Technology"

"Runtime Application Self-Protection: Technical Capabilities"

"Toolkit: Best-Practice Checklist for Intellectual Property Protection"

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, and integrating security built into the data center switching fabric provides much more separation of control and higher performance than relying on security functions built into VMware and other virtualization solutions. 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 fabric. As SDN is being moved forward without any material security, it introduces more security issues. The benefit rating of low recognizes the absence of practical enterprise switch-based security in vendor offerings.

User Advice: Depending on security, controls built into switches, routers, WLAN access points, 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.

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: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Cisco; Extreme Networks (Enterasys Networks); HP; Juniper Networks; VMware

Recommended Reading: "Magic Quadrant for Enterprise Network Firewalls"

Sliding Into the Trough

Dynamic Data Masking

Analysis By: Joseph Feiman

Definition: Dynamic data masking (DDM) is a technology that aims at real-time data masking of production or nonproduction data. Typically, DDM changes the data stream so that the data requester does not get access to the sensitive data, while no physical changes to the original data take place.

Position and Adoption Speed Justification: Sensitive data (such as credit card numbers, personally identifiable information and medical diagnoses) and even nonpersonal sensitive data

(such as corporate financial information and intellectual property) are exposed to abuse or negligence from enterprise employees and outsiders. Data masking aims to prevent the abuse of sensitive data by hiding it from users. Data masking comes in two forms: static data masking (SDM) and DDM.

An example of a business case where DDM is necessary is when a customer representative of a firm (such as a bank) invokes an application that accesses a client's profile (for example, to change a credit card limit per a client's request), and the application displays all the related information retrieved from the database, including sensitive data. A possible solution to the problem is a re-engineering, rewrite or modification of the applications to make them hide sensitive data according to the entitlements of the users. This approach is very expensive and lengthy, and it would not solve the problem in the case of ad hoc queries. DDM is a solution that can help.

Typical DDM works in the following ways:

- A DDM monitor intercepts each request to a database (either an ad hoc query or an application's query) that retrieves data and passes or displays it to a user (for example, to a client service agent).
- A DDM monitor gets real-time access to the information about the data that should be masked due to its sensitivity, and also to the definitions of the data-masking rules. It can be stored on a prepopulated repository, along with masking rules, and can be accessed in real time.
- A DDM monitor gets real-time access to users' entitlements by dynamically, in real time, querying respective identity and access management systems or a prepopulated repository for the entitlements of particular application or database users. This up-to-date information is essential for enabling selective masking based on these entitlements.
- A DDM monitor modifies the database response by masking sensitive data according to the masking rules and user entitlements.

Gartner has long predicted that the data-masking market would eventually split into these two (static and dynamic) segments, and this prediction is now being realized. Since this market began to develop, most data-masking providers have offered — and prospective buyers have asked for — only SDM technologies. Recently, however, Gartner has identified a shift in the market. Some vendors have begun offering DDM solutions, and Gartner's client interactions make it clear that security professionals and other stakeholders are recognizing that certain problems of sensitive data abuse cannot be solved by SDM or by other currently available data security technologies. The result is that a differentiated DDM market is beginning to emerge to address business cases whose requirements cannot be met by SDM.

Recently, we have even witnessed new business cases when DDM was used to mask nonproduction data in real time. It was when SDM was too slow to meet the challenge of several-times-a-day refreshments and masking of test data. In that case, DDM provided real-time masking of test data, so that testers could see only masked data.

We also expect that synergy between DDM and database auditing and protection (DAP) will take place, resulting in more comprehensive and intelligent security detection and protection capabilities,

and, potentially, DAP and DDM capabilities merging in a single tool. In order to mature, DDM technology should address concerns that modifying sessions in real time might impact applications' logic and performance — factors that slow technology evolution.

User Advice: Enterprises should start evaluating DDM. They also should:

- Pressure SDM and other data security vendors (for example, DAP vendors) to deliver DDM technology. Use the same vendor for SDM and DDM, if possible.
- Make DDM enablement a criterion in the SDM vendor selection process.
- Watch the evolution of DDM, and use it once it reaches the maturity acceptable for the enterprise's needs.

SDM and DDM will typically target two different adoption centers within IT. SDM will be used mainly by application development teams, while DDM will be mainly used by operations. At the same time, the buying center — the one that makes the decision to implement data masking — will be an enterprise's compliance, risk management and auditing team (see "Securing Production Data With Dynamic Data Masking").

The application of data-masking technologies and best practices should be a strategic enterprise objective, but provider and product selection still remain tactical. The DDM market is just emerging. DDM vendors are few, although some large vendors have started offering their newly developed DDM technologies or acquired DDM startups. SDM and DDM are not necessarily a pair, and a DDM vendor is not necessarily an SDM vendor also.

Business Impact: Adopting data masking will help enterprises raise the level of security and privacy assurance against insider and outsider abuses. At the same time, data masking will make enterprises compliant with the security and privacy standards recommended by regulating and auditing organizations.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Camouflage Software; GreenSQL; IBM; Informatica; Mentis; Oracle

Recommended Reading: "Securing Production Data With Dynamic Data Masking"

"Key Trends in Securing Sensitive Data With Data-Masking Technologies"

Operational Technology Security

Analysis By: Earl Perkins

Definition: Operational technology (OT) security is the governance, development, management and operations of digital and physical security for industrial automation and control systems, processes, and organizations.

Position and Adoption Speed Justification: OT security products and services provide security for and protection of OT hardware and software. OT detects and/or causes changes through the direct monitoring and/or control of physical devices, processes and events. OT goes by names such as supervisory control and data acquisition systems, distributed control systems, process control systems and process control networks, and makes extensive use of machine-to-machine communications, sensors, actuators, programmable logic controllers and other types of collection, aggregation and embedded systems. OT overlaps a broader product and service category known as the "Internet of Things" (IoT). OT and the IoT share many architectural building blocks, with OT addressing primarily industrial environments, and the IoT addressing commercial and consumer environments.

The worldwide network of billions of sensors and other intelligent and semi-intelligent devices in all industries (such as oil and gas, utilities, manufacturing, healthcare, and transportation) require secure environments to be effective. Many IT security technologies and practices are applicable to OT security, but some OT security requirements are unique, particularly in specialized control networks and endpoint devices not found in IT environments. OT security infrastructure uses many IT security components, often employed in a different manner. OT security infrastructure must support real-time, event-driven processes and, as such, have high-availability, high-reliability requirements, higher even than fault-tolerant IT systems. While IT security staff is common in most enterprises of sufficient size, most OT engineering and administration organizations do not have full-time security equivalents. This is changing in progressive organizations, with IT/OT convergence and alignment occurring in increasing numbers.

OT security implementation faces significant obstacles due to:

- The impact (and uncertainty) of mandated security regulations in some OT industries
- A lack of coordination between OT and IT security personnel and practices in many industries
- A lack of OT security technology maturity (and IT security product abilities to address OT security requirements)
- Modernization of OT systems via repurposed IT systems and the associated security impact

The market for OT security technologies and services is growing, with numerous product and service vendors from IT, as well as new OT security players. Governance and organizational challenges related to OT security represent a significant opportunity for consulting and system integration providers. Some industries have established IT/OT security integration programs from an organizational, planning or governance perspective, but this is still not as common a practice as it needs to be.

OT security has advanced slightly in Hype Cycle maturity as more security products and services targeting OT industries appear, and as IT/OT security convergence and alignment within enterprises

increases. Progress remains slow, but will accelerate as communication and awareness of the issue grow.

User Advice:

- Establish integrated IT/OT security governance for major decisions regarding security, allocating specific organizational assets to support it.
- Engage reputable consultants and system integrators when needed to assess existing OT security and develop an effective OT security management strategy.
- Integrate IT/OT security management to establish a top-down program for managing regulation. Do not allow regulatory requirements to define your security program.
- Monitor security product and service markets for solutions that specifically address OT security requirements for network segmentation, privileged access control and threat intelligence, to name a few.

Business Impact: OT security implementations are found everywhere. OT security implementations can be managed; for example, in system control centers of specific industries — centers chartered with observing, reporting and controlling networks of control points and data collection points. Implementing effective OT security practices will determine success or failure of an OT-enabled organization modernizing amid regulatory and business change. As networks and systems are upgraded or replaced, their potential complexity grows exponentially (in terms of the points of control available, the granularity of control, and the availability of much more information regarding activities and performance). As IT and OT networks are integrated, and access to worldwide networks grows, the degree and scale of threats increase. Most OT-centric enterprises today are unprepared for the expanded networking of their OT infrastructure and the potential exposure it brings. Advances in OT and IT security program maturity are required urgently to address this shift in these industries.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: AlertEnterprise; Applied Intelligence; Bayshore Networks; Belden (Byres Security); Boeing; Cisco; Cyberoam; Digital Bond; Echelon; Emerson Process Management; GE; Honeywell; IBM; IOActive; Lockheed Martin (Industrial Defender); McAfee; Microsoft; Mocana; OSIsoft; Owl Computing Technologies; Positive Technologies; Quantum Secure; Schneider Electric; Siemens; Waterfall Security Solutions

Recommended Reading: "NIST Framework Establishes Risk Basics for Critical Infrastructure"

"How to Organize IT/OT Security for Success"

"Competitive Landscape: Critical Infrastructure Protection, Worldwide, 2014"

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 storage devices. The showcase technology for standardized self-encrypting drives (SEDs), commonly referred to as Opal, was released in open source in 2009 by the Trusted Computing Group (TCG) and covers individual drives, arrays and storage interfaces. All major mass-storage manufacturers support Opal-based SEDs as a type of solid state drive; some also support Opal on magnetic hard-disk drives.

Position and Adoption Speed Justification: SEDs are plug-and-play alternatives for conventional mass storage drives. When activated, they provide high bit rate encryption processing within the drive controller so there is little or no impact on the OS, and the risk of keys being exposed in OS memory is reduced. Separately encrypted OS and user partitions can be isolated within the drive. While the mobile data protection (MDP) market is dominated by software-based encryption systems, SEDs can certainly play an important role. But progress toward the plateau is slow for several reasons:

- Gartner clients still complain that SEDs may be difficult to obtain. If SEDs are desired, companies should negotiate supplier inventory guarantees in their purchase contracts.
- Upgrading to SEDs is too expensive to promote standardization among deployed systems, which may have several years of investment life.
- The fact that SED technology is implemented only in mass storage drives forces companies to continue to rely on various implementations of software encryption for areas such as cloud storage, removable media, flash-based mobile devices, and mobile device security wrappers and containers.
- SEDs must be policy-managed in order to scale key handling, data recovery and compliance audits by a separate process. This responsibility falls logically to vendors in the "Magic Quadrant for Mobile Data Protection" and "Magic Quadrant for Endpoint Protection Platforms," but not all of these vendors will support Opal drives.
- OS support is not consistent across different mainstream OS. For example, Microsoft supports Opal drives in Windows 8, but not Windows 7; Apple does not support them in OS X. With the exception of Windows Surface Pro devices, it has not yet appeared in the mobile phone and tablet markets.
- The failure of Opal to spread beyond mass storage devices limits its usefulness. Flash drive vendors, for example, did not adopt it. There are also competing initiatives (see white paper: "Introducing Next Generation Secure Memory Technology").
- Increasing size, speed and reliability of CPUs and memory make software-based encryption sufficient for most basic use cases. And OS-embedded encryption systems such as Microsoft BitLocker and Apple Filevault can be put under policy management, making a "good-enough" solution for many users and reducing the need to purchase premium hardware.

In the context of individual user system encryption, the issues raised above mean that SEDs are nice to have, but fall short of making SEDs a critical requirement. Based on these prevailing market indicators, SEDs may find more use in servers, where software-based encryption can create measurable input/output (I/O) bottlenecks.

Client feedback suggests that fewer than 20% of companies have succeeded in efforts to adopt interoperable encryption based on TCG specifications. The time scale will be maintained at five to 10 years, taking a cue from five years of sluggish activity.

User Advice: SEDs are increasingly significant as a component of an enterprise encryption program, but they are not ready to replace other methods. Enterprise security decision makers should continue to rely on established encryption software vendors that can run on a variety of platform configurations, and can meet Federal Information Processing Standard (FIPS) Publication 140-2 standards in software when making procurement decisions. IT planners and procurement managers must demand road maps for support for hardware-based encryption, including TCG-compliant drives from all hardware and platform providers in the PC, PDA, smartphone, tablet, embedded device and other storage device markets. Purchasing decisions for mobile data encryption should consider that vendors with a road map for SEDs are pursuing an important product vision.

The choice to use embedded drive encryption in SEDs will not eliminate the need for a management platform. Companies still need a key manager to store, protect and authorize enrollment, locking/unlocking, help desk diagnostics and postretirement disk wipes. Vendors in the "Magic Quadrant for Endpoint Protection Platforms" and the "Magic Quadrant for Mobile Data Protection" will continue to fill the management role, and their costs must continue to be factored into security decisions.

Business Impact: Hardware-based encryption offers the promise of better performance and less system interference than software tools. However, companies must remember that all methods of encryption — SEDs are no exception — need to be centrally managed for the application of security policies, compliance audits and key management:

- Business data vulnerabilities are reduced because encryption keys can be stored in the hardware during operation, rather than exposed to attacks through system memory.
- 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, particularly in I/O-intensive applications.
- Disposal of data on SEDs is more reliable because the key can be revoked in hardware, and no local remnant would remain to allow access to be restored by a hacker.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Dell; Hitachi; Intel; McAfee; Micron; Samsung; Seagate; Sophos; Symantec; Toshiba; Trend Micro; Wave Systems; WinMagic

Recommended Reading: "Protecting Sensitive Data on Decommissioned SSDs and HDDs"

"Magic Quadrant for Mobile Data Protection"

"Encryption Options for Centralized Data Storage and Document Management Environments"

Wikipedia Entry for Opal Storage Specification

TCG Self-Encrypting Drive Overview

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.

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. However, penetration testing products are getting easier to use and becoming better at minimizing the impact on business resources, so enterprises that have the required skills should evaluate commercial and open-source products. 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. Social engineering testing as part of a penetration testing engagement is typically of limited value because the tests always succeed.

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; Rapid7; Saint

Recommended Reading: "How to Evaluate a Security Consulting Firm"

"MarketScope for Vulnerability Assessment"

"Tips and Guidelines for Sizing Your Information Security Organization"

Advanced Threat Detection

Analysis By: Lawrence Orans; Jeremy D'Hoinne

Definition: Advanced threat detection (ATD) devices are used as an extra security approach to examine all communications that standard layers of security controls have allowed to pass. These solutions look at combinations of source reputation, sandboxing and behavioral analysis of payloads (Web objects, email file attachments and executables), and network traffic analysis to detect advanced targeted attacks (ATAs).

Position and Adoption Speed Justification: Advanced threats have earned the name "advanced" because they bypass traditional security defense mechanisms. Firewalls, intrusion prevention systems (IPSs), secure Web gateways (SWGs), secure email gateways and endpoint protection platforms (EPPs) are still necessary, but they are no longer sufficient to defend against advanced attacks. Enterprises that are highly security-conscious have already deployed ATD solutions, whereas many organizations with "average" security requirements still have not budgeted for ATD solutions. Special-purpose ATD appliances face increased pressure from next-generation firewall vendors and SWG vendors that have been adding sandboxing, traffic analysis and other ATD capabilities as a cloud-assist service to complement their hardware appliances. However, highly security-conscious enterprises typically avoid cloud-based services in favor of on-premises appliances.

User Advice: High-security enterprises with budgets and staffs that support a "lean forward" approach to network security should investigate the use of ATD devices to detect malware and to determine whether they have already been compromised by advanced targeted threats. Enterprises that don't have the budget to do so should first perform a network security audit or penetration test

to gather data to get budget approval. Enterprises with smaller or lower-skilled staffs and limited budgets should adopt ATD enhancements when their firewall, intrusion prevention system and SWG vendors make them available.

Business Impact: Advanced targeted threats can cause severe business impact and disclosure of sensitive business and customer information.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: AhnLab; Arbor Networks; Blue Coat; Check Point Software Technologies; Cisco; Cyphort; Damballa; FireEye; Fortinet; General Dynamics; General Dynamics Fidelis Cybersecurity Solutions; Lancope; Lastline; LightCyber; McAfee; Palo Alto Networks; Proofpoint; Trend Micro; Vectra Networks; Websense; Zscaler

Recommended Reading: "Five Styles of Advanced Threat Defense"

"Strategies for Dealing With Advanced Targeted Attacks"

Cloud-Based Security Services

Analysis By: Kelly M. Kavanagh

Definition: Cloud-based security services enable the delivery of security controls, without on-premises technology deployment and management. Security controls differ in their appropriateness for cloud-style delivery.

Position and Adoption Speed Justification: Service providers must meet customer expectations for the availability, effectiveness, scalability, deployment, management ease and cost savings of cloud-based security controls. Customers must assess service capabilities for policy enforcement, for management and monitoring controls across hybrid cloud and on-premises deployments, for maintaining availability of critical controls, and for customization and configuration of cloud-based controls. Threat-facing services can more easily meet these expectations, while internal or business-facing services encounter obstacles to adoption, such as an established internal capability with sunk costs or data location concerns. Initial adoption of business-facing cloud-based security controls is typically focused on and limited to specific domains, vertical markets or use cases (such as securing other cloud-based IT services, meeting compliance requirements or securing remote office locations.) Controls such as network-based firewalls, intrusion detection and prevention systems, vulnerability scanning, antivirus protection, distributed denial of service protection, messaging security and Web gateway security services are often selected for early deployments. Recently, Gartner has noted the increasing adoption of identity and access management as a service (IDaaS), especially among small or midsize businesses (SMBs) and those providing employee access to SaaS applications. Cloud-based controls' deployment ease and lower price points make them attractive to SMBs or to Type B and Type C companies. Enterprises can extend

security controls provided by on-premises technology with cloud-based services to address employee-owned devices, remote office locations and cloud-based IT infrastructure. Cloud-based security offerings can be embedded into other service offerings by providers of bandwidth, cloud services and security as a service, thus giving buyers an additional option in product or service decisions. The cloud-based security approach is also well-suited to deliver security controls for other cloud-based IT services.

User Advice: Consider service continuity, response time, customization and switching requirements — in addition to functional requirements — for security controls. Look at leveraging cloud-based security providers, as well as bandwidth and remote connectivity service providers, for opportunities to consolidate on-premises-based security technologies into cloud-based delivery options — especially for mobile technology and remote office or branch office environments that would otherwise require on-site deployment and hardware maintenance. Where service deployment requires a blend of on-premises-based equipment and cloud-based delivery, look for uniform policy enforcement, administration, configuration and reporting capabilities across the service components.

Business Impact: Cloud-based security has the potential to deliver cost savings, fast deployment and broader coverage — compared with equivalent-capacity, on-premises-based equipment — and may result in better security for users that cannot effectively manage on-premises security technology.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Akamai; Alert Logic; AT&T; Blue Coat; CipherCloud; Cisco; CloudFlare; McAfee; Neustar; Okta; Panda Security; Qualys; Symantec; Verisign; Verizon; Websense; WhiteHat Security; Zscaler

Recommended Reading: "Forecast Analysis: Public Cloud Services, Worldwide, 1Q14 Update"

Hypervisor Security Protection

Analysis By: Neil MacDonald

Definition: Hypervisor security protection is the set of technologies and processes used to secure and protect virtualization platforms from attacks.

Position and Adoption Speed Justification: Hypervisor security and protection from a potential compromise of the hypervisor remain top virtualization security concerns of Gartner clients. A worst-case scenario from a security perspective is an attack and successful compromise of the virtualization platform, because the integrity of all hosted workloads running above the virtualization platform relies on the integrity of the hypervisor. However, running antivirus or similar types of protection software in the hypervisor isn't the right approach, because it increases the surface area for attack, and this layer shouldn't be running arbitrary code.

User Advice: As an alternative to the deployment of a specific high-assurance hypervisor point solution, hypervisor security protection should be treated as a defense-in-depth problem, using multiple strategies to ensure the overall integrity of this critical layer:

- Ensure this critical layer is hardened to defined configuration standards, using publicly available best-practice hardening guidelines.
- Ensure that the hypervisor is part of an established vulnerability management process, and that this layer is periodically scanned for vulnerabilities, to ensure patches have been applied and that the expected configuration state hasn't drifted.
- Ensure that external network-based intrusion prevention vendors actively research hypervisor-level vulnerabilities and provide signature sets and filters to prevent network-based attacks where possible.
- Use the embedded version of the hypervisor from your vendor, if available, to reduce the surface area for attack, and ideally, place this in firmware to protect it from tampering.
- Use a hardware-based root-of-trust measurement at bootup to ensure the hypervisor hasn't been modified.
- For security-critical deployments, consider the use of a high-assurance hypervisor as an alternative to commercial hypervisors.
- Check with the audit team regarding the use of hypervisors for the separation of different trust zones (for example, for Payment Card Industry Data Security Standard [PCI DSS] segmentation), because not all security auditors consider hypervisor-level security adequate for zone isolation.

Business Impact: Investments in hypervisor security protection reduce risk, but provide no direct return on investment. These investments reduce overall risk, because the breach of a hypervisor places the integrity of all hosted workloads and information at risk of compromise.

Benefit Rating: Low

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Check Point Software Technologies; Cisco; Citrix; Juniper Networks; Microsoft; Palo Alto Networks; Sourcefire; VMware

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

"Security Considerations and Best Practices for Securing Virtual Machines"

"Building Blocks for Trusted, Secure Hypervisors"

Secure Web Gateways

Analysis By: Lawrence Orans; Peter Firstbrook

Definition: Secure Web gateways (SWGs) utilize URL filtering, malware detection, and application control technology to protect organizations and enforce Internet policy compliance. SWGs are delivered as on-premises appliances (hardware and virtual) or as cloud-based services.

Position and Adoption Speed Justification: SWGs continue to progress down the slide toward the Trough of Disillusionment. They need improvement in three key areas: cloud-based services, advanced threat defense and legacy malware protection, and they also need broader support for mobile devices. Cloud-based services vary greatly in their maturity, global data center footprint, and support for advanced features like DLP. Advanced threat defense (ATD) capabilities are still in the early stages in the SWG market, as most vendors have only begun to include ATD functionality in 2013 and 2014. Legacy malware protection also must improve if SWGs are to progress along the Hype Cycle curve. Many solutions still lack detailed threat information and fail to prioritize threat severity, therefore providing limited value in the battle against malware. Mobility and the bring your own device (BYOD) phenomenon present difficult challenges for cloud-based SWGs that must protect heterogeneous mobile endpoints. Many vendors lack support for the full range of mobile devices, or they require third-party mobile device management to enforce policies on devices. SWG cloud vendors must make it easier to support mobile workers.

User Advice: Enterprises should go beyond basic URL filtering and implement SWG solutions that offer strong protection against advanced threats and legacy malware. They should also consider using cloud-based services to protect mobile devices when they are off-network, or as an alternative to on-premises appliances. Branch offices are also good candidates for cloud-based SWG services, so that traffic does not have to be backhauled to a centralized Internet egress point.

Business Impact: SWGs protect end users from Internet-borne malware, and higher-end SWGs can help to protect enterprises against targeted attacks. Other benefits include the ability to apply policies that govern the use of social media. For example, policies can be established to allow users to access Facebook, but not to upload photos or post comments. Some SWGs can also be used to monitor Web posts for acceptable language, and to monitor traffic for data loss.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Barracuda Networks; Blue Coat; Cisco; ContentKeeper Technologies; iboss Network Security; McAfee; Sangfor; Sophos; Symantec; Trend Micro; Trustwave; Websense; Zscaler

Recommended Reading: "Magic Quadrant for Secure Web Gateways"

"Decision Framework for Implementing Cloud-Based Secure Web Gateway Services"

"Secure Web Gateway Malware Detection Techniques"

"Analyze Secure Web Gateway Pricing Models to Negotiate a Favorable Contract"

Introspection

Analysis By: Neil MacDonald

Definition: Introspection is the use of hypervisor- and virtual machine monitor (VMM)-level APIs to expose low-level system information from all virtual machines (VMs) hosted by the VMM. The APIs can enable security and management capabilities that span multiple VMs without requiring the installation of an agent on each, without requiring virtual network reconfiguration and with potentially better performance than agents running in a separate VM. Introspection also provides separation of security policy enforcement from the container it is protecting.

Position and Adoption Speed Justification: VMware first introduced its VMsafe set of APIs with the vSphere 4.0 release of its virtualization platform in 2009, advancing their capabilities in subsequent versions, which added agentless file integrity and data loss prevention monitoring. Similar capabilities are available with LibVMI on Xen-based and kernel-based VM (KVM)-based platforms. However, Citrix XenServer does not yet directly provide this capability, and Microsoft recently added only network introspection capabilities with its virtual switch platform in Windows Server 2012 Hyper-V.

Security issues are associated with the use of these APIs, and vendors have yet to apply suitable restrictions on the types of code that may access them. There are no standards for these APIs across virtualization platform vendors, creating lock-in when they are used. Also, due to the lack of context from the introspected VM, some functionality may be lost as compared with an agent running in the VM. Because of the relative newness of introspection capabilities and APIs, as well as the complexity in their use by developers, few software packages are available at this time, with the most common being anti-malware scanning and network security appliances. Another challenge is that this low level of access will not typically be provided in public cloud infrastructure as a service, further inhibiting widespread use of introspection.

User Advice:

- Introspection benefits will not be limited to security scenarios. Investigate the use of introspective agents as a way to protect and manage VM containers that were built without security and management capabilities — for example, virtual appliances.
- Introspection solutions for VMware and Hyper-V are available today. Evaluate these vendors based on the performance and reduced complexity of their solutions.
- Introspection use involves trade-offs. Weigh the additional code at the hypervisor level, and lock into a specific vendor's architecture against the security and operational benefits.
- Require vendors using software with introspection capabilities to provide documented proof of security, quality testing of their codes and suitable reference accounts.

- Require virtualization platform vendors that provide introspection capabilities to enable administrators to disable this capability and enforce mandatory access controls on the APIs. Demand that software vendors provide proof of security testing in development.

Business Impact: As shown in multiple vendors' "agentless" antivirus scanning for VMware, introspection capabilities are potentially transformational, offering the ability to deliver security and management capabilities without requiring the use of agents running in each VM. However, this approach has its own set of pros and cons. Still, we expect that the approach will be adopted by more than half of all enterprises during the next five years. As a result, exploit disruptions in pricing to lower the cost of security and management functionalities for virtualized server and desktop workloads.

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: 5nine Software; Bitdefender; Check Point Software Technologies; Cisco; Citrix; Juniper Networks; Kaspersky Lab; McAfee; Reflex Systems; Sophos; Symantec; Trend Micro; VMware

Recommended Reading: "Make Optimizing Security Protection in Virtualized Environments a Priority"

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

Open-Source Security Tools

Analysis By: Greg Young

Definition: Open-source security (OSS) tools and products are distinct security products and add-on tools with open-source licenses.

Position and Adoption Speed Justification: Previous Gartner Hype Cycles plotted OSS tools on the Plateau of Productivity for OpenSSL, OpenSSH, Snort, Nessus and some others. That assessment remains for the few success cases. However, there is even less talk about open-source security than before, and still few options. The market for OSS tools has continued to be pressured negatively by:

- A flood of immature new entrants — some of which are introductory versions of proprietary products.
- Successful OSS products being taken commercial, or being overseen by a commercial player.
- The "OSS" moniker being misapplied by vendors to free versions or non-OSS products made up of some OSS components, or commercial vendors forking the OSS with a commercial or proprietary version.

- Almost all new OSS products remaining niche or absent from entire security product markets — and being used only tactically in enterprises.
- The changing threat environment, currently at a very high level of activity and success, not being countered in any noteworthy manner by OSS solutions over non-OSS ones; the current threat level has been driving fast adoption of new solutions, and the open-source marketplace has not stepped up.
- The Heartbleed vulnerability in 2014 highlighted the absence of an ecosystem to support more-utilized OSS security projects, emphasizing the need to track new versions of already adopted products, and showing that open source does not automatically equate to being secure.

Tactical or siloed use of OSS tools is on the increase, especially in response to budget and expense control pressures or for use with open-source software, such as OSs.

User Advice: The mature tools, such as Snort, OpenSSL and OpenSSH, present a considerable opportunity. In addition, tactical or operator tools, such as Metasploit and Wireshark, are in wide use. Small and midsize businesses have a wider selection, such as the ModSecurity Web application firewall, but enterprises will be challenged to find products and tools that can meet their requirements across the security product spectrum.

Even so, enterprises should consider using OSS tools as a means of determining the value of a type of safeguard before committing to non-OSS tools in the same class that incur considerable commitment, even though they will meet all requirements. The best advances have been made in identity and access management (IAM) OSS tools and frameworks. OSS frameworks, such as those in IAM, are the best path for future OSS success.

Business Impact: OSS tools provide a means for enterprises to drive down pricing on commercial tools. They also serve as mechanisms for enterprises with technical expertise to develop business-specific security solutions that mainstream vendors may never sell. Enterprises that rely on Snort should consider the Sourcefire Vulnerability Research Team (VRT)-certified rules. The tactical use of OSS tools remains a good use case. OSS for IAM has the best opportunities; however, commercial software dominates in enterprise security.

Benefit Rating: Low

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Cisco; Open Information Security Foundation; OSSIM; Trustwave

Software Composition Analysis

Analysis By: Joseph Feiman

Definition: Software composition analysis (SCA) is a technology that analyzes application composition to detect components known to have security and/or functionality vulnerabilities or that require proper licensing.

Position and Adoption Speed Justification: SCA does not typically inspect components internally (that is, it does not conduct components' code analysis — although, Gartner believes that it should be done), but instead tags them with information collected from sources such as open-source software communities. That information typically includes intellectual property (IP) ownership, known security and functionality vulnerabilities, known remedies for those vulnerabilities, and references to outdated and most recent versions of components, along with their locations on the Web.

An increasing number of developers have grown up assuming that anything located on the Internet is free for the taking. The ease with which developers can search the Web and download component, and open-source and (unfortunately) proprietary code, combined with a culture that treats others' IP without due respect, has meant that they are increasingly creating software that contains code that they have not developed, and yet have not formally acknowledged its use (for example, through proper license agreements).

SCA technology can ensure that developers are meeting compliance requirements and ethical standards for code use, and can improve code quality by increasing the level of rigor and documentation, thereby reducing the likelihood of unwanted or unapproved code. Unfortunately, today's culture does not acknowledge urgency in adopting SCA and the rigor that it will bring. Recently, SCA has been evolving to support secure component assembly in the software supply chain processes, to verify the security of components used in software or application development processes.

Adopting SCA requires establishing an auditing process that goes beyond application development departments. We expect SCA to reach the Plateau of Productivity in two to five years.

User Advice: SCA technologies should be used along with static application security testing (SAST) and dynamic application security testing (DAST). SAST and DAST inspect applications internally, while SCA only classifies known components according to the security, version or IP status. We have also started witnessing some AST vendors that combine AST with SCA: conducting AST of the components that they inventory. The use of composition analysis requires legal experts to review the results of the analysis and to address legal issues stemming from components' IP ownership.

Enterprises should use SCA tools on a regular basis to audit repositories containing software assets (such as version control and configuration management systems) to ensure that software developed and/or used by the enterprise meets security and legal standards, rules and regulations. Application developers should have access to SCA tools to inspect components that they plan to use. SCA tools should ideally be used in conjunction with a formal corporate IP strategy — one in which clear responsibility has been delineated across the company, including the IT organization.

Business Impact: SCA increases assurance that the software components used in applications are up-to-date, properly licensed and secure.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Black Duck Software; Codenomicon; OpenLogic; Palamida; Protecode; Sonatype; Veracode

DMZ Virtualization

Analysis By: Neil MacDonald

Definition: Demilitarized zone (DMZ) virtualization is the use of virtualization in the enterprise DMZ, typically for cost savings, through the consolidation of physical servers, networks and storage.

Position and Adoption Speed Justification: Because organizations have now virtualized the majority of workloads in their data centers, they are turning their attention to higher-risk scenarios, such as virtualizing servers and storage in the enterprise DMZ. However, these workloads represent some of the riskiest workloads in the enterprise, and virtualization of the workloads should be carefully considered. Tools and processes are maturing, so we expect that virtualization in the DMZ will be considered a mainstream practice within the next several years. However, adoption will vary, depending on an organization's tolerance for risk balanced against the additional cost when dedicated hardware is used.

User Advice:

- As a foundation, ensure that vulnerability, configuration and patch management processes at the hypervisor level are top-notch, that the responsible group for each of these processes has been identified, and that monitoring and periodic scanning for drift and misconfiguration are put in place.
- Reduce the surface area for attack in the DMZ by favoring the use of embedded, reduced-footprint hypervisor platforms with root-of-trust measurements during bootup to detect tampering.
- As a first phase, consolidate the workloads of similar trust levels within the DMZ onto physical platforms.
- As a second phase, workloads of different trust levels within the DMZ may be combined onto the same physical server platform, but use existing physical network separation and network security policy enforcement points to maintain the separation (that is, physical firewalls and network-based intrusion prevention systems [IPSs]). This is where most organizations are in 2014.
- As a third phase, consider the use of virtualized firewalls and IPSs; however:

  - Favor virtualized solutions from the same vendor as your physical network to maintain consistency in policy administration and management, and to reduce the chance of misconfigurations or mistakes.
  - Favor virtualized solutions that are "virtualization aware" so they understand virtualization-specific events, such as live migrations and virtual machine (VM) identities, and so they are able to apply policies to logical groupings of VMs.
  - Insist that these solutions be evaluated and certified against accepted industry standards and testing groups, such as Common Criteria, ICSA Labs and NSS Labs.
  - Ensure that the performance limitations inherent in a software-based security policy enforcement point meet your throughput and latency requirements.
- Do not span DMZ and internal networks with a single piece of server hardware.
- Spanning DMZ and internal networks with a storage area network incurs more risk, but the risk can be reduced by compensating with change control processes, change monitoring and separation of the storage network from the operational network.

Business Impact: Cost savings can be achieved through the consolidation of server and storage hardware in the organization's DMZ.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Brocade; Check Point Software Technologies; Fortinet; IBM; Juniper Networks; McAfee; Palo Alto Networks; Sourcefire; Trend Micro; VMware

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

"From Secure Virtualization to Secure Private Clouds"

"Hype Cycle for Virtualization, 2013"

Endpoint Protection Platform

Analysis By: Peter Firstbrook

Definition: An EPP is a solution that provides comprehensive personal device security. Most of these solutions include antivirus, anti-spyware, personal firewall, device control and other styles of host intrusion prevention capabilities. More advanced EPP solutions are starting to integrate application management functions (such as vulnerability, endpoint application patch and application control capabilities), mobile device management (MDM) capabilities and data protection functions (such as encryption, data loss prevention and device control).

Position and Adoption Speed Justification: The endpoint protection platform (EPP) remains in the trough this year, due to the continued failure of even leading solutions to ensure the security of endpoints. The primary purpose of an EPP is to protect endpoints from infection. However, a continued focus on reactionary security and an abject failure to deal with the root cause of infections are aptly illustrated by persistently high infection rates, which are now resulting in more financial damage. Proactive anti-malware capabilities such as application control and application management (vulnerability, endpoint application patching and configuration management capabilities) are found in only a few solutions and vary widely in terms of capability. Patch management remains primarily an enterprise desktop operations function, but it is a critical task for proactive security of endpoints. More than 90% of threats are neutralized if the current patch is installed on targeted software.

A new crop of endpoint protection solutions — endpoint detection and remediation (EDR) tools — which focus on detection of suspect events, rapid investigation and remediation, are emerging to fill in gaps in current EPP solutions. None of the EDR vendors currently replace EPP solutions; however, several have aspirations to do so in the near future. We anticipate that existing EPP solution providers will gradually adopt more detection and response capabilities over the next several years.

Dominance of the Windows PC as the primary or only business computing platform is at its peak. Leading EPP vendors have adjusted to this new reality by integrating MDM functions in their primary EPP solutions. Mobile devices do not need the same style of security as traditional PCs, but most existing mobile anti-malware solutions are stubbornly repeating the mistake of relying on reactionary malware signatures. A number of EPP vendors will miss this transition and become isolated to Windows-only niche status.

User Advice:

- Look for EPP approaches to malware detection that categorize and enumerate the attributes of good applications and can manage vulnerabilities and limit application execution. Restricting application execution to the "known good" is considerably more accurate, and good application metadata is useful for a broader range of business goals.
- EPP buyers should look for fully integrated basic MDM capabilities and a solid development road map of MDM functionality in addition to anti-malware.
- EPP buyers should look for solutions that can detect suspect events and provide detailed data for malware investigation and remediation capabilities.

Business Impact: The failure of EPP vendors to stop malware with any reliability will increase operational and security costs as IT organizations attempt to layer on additional security technology and react to incidents.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Check Point Software Technologies; IBM; Intel; Kaspersky Lab; Landesk; Panda Security; Sophos; Symantec; Trend Micro

Recommended Reading: "Market Guide for Endpoint Detection and Response Solutions"

"Malware Is Already Inside Your Organization; Deal With It"

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

"Magic Quadrant for Endpoint Protection Platforms"

"Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence"

Climbing the Slope

Context-Aware Security

Analysis By: Neil MacDonald

Definition: Context-aware security is the use of supplemental information to improve security decisions at the time they are made, resulting in more accurate security decisions capable of supporting dynamic business and IT environments. The most commonly cited context information types are environmental (such as location and time). However, context information valuable to information security exists throughout the IT stack, including IP, device, URL and application reputation; business value context; and the threat context in which the decision is made.

Position and Adoption Speed Justification: Rapidly changing business and threat environments, as well as user demands for alternative devices and cloud-based services, are stressing static security policy enforcement models. Information security infrastructure must become adaptive by incorporating additional context at the point when a security decision is made. We are already seeing direct evidence of this transformation in next-generation endpoint, network, application and data protection platforms, as well as the incorporation of context into next-generation security information and event management platforms available today. Specific examples include adaptive access control, context-aware fraud detection, reputation-aware endpoint protection platforms, as well as application and identity-aware next-generation firewalls. Application, identity and content awareness are all part of the same underlying shift to incorporate more context at the point when a security policy enforcement decision is made, and major vendors, such as Cisco, Trend Micro, Check Point Software Technologies, Sourcefire, HP, IBM and others, are marketing various forms of context awareness in their next-generation security offerings.

User Advice:

- Begin the transformation to context-aware and adaptive security infrastructure as you replace legacy, static security infrastructure, such as access control systems, next-generation firewalls, and secure Web gateways and endpoint protection platforms.

- Question security vendors on their specific road maps for application, identity and content awareness, as well as their ability to incorporate other types of context information into their policy enforcement decisions in real time.
- Use the attributes of Gartner's next-generation, context-aware security platforms as a guide to evaluating next-generation security platforms for network, endpoint, identity, application and content security.

Business Impact: Context awareness helps make security an enabler, not an inhibitor, of dynamic business requirements. To enable faster and more-accurate assessments of whether a given action should be allowed or denied, we must incorporate more real-time context information at the point when a security decision is made.

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Blue Coat; Check Point Software Technologies; Cisco; EMC; HP; IBM; Juniper Networks; Lancope; McAfee; Palo Alto Networks; Sophos; Sourcefire; Trend Micro

Recommended Reading: "Adaptive Access Control Brings Together Identity, Risk and Context"

"Emerging Technology Analysis: Cloud-Based Reputation Services"

"The Future of Information Security Is Context Aware and Adaptive"

"Effective Security Monitoring Requires Context"

Next-Generation IPS

Analysis By: Adam Hils

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, upgrade paths to integrate new information sources, and new techniques to enable mitigation of future threats.

Position and Adoption Speed Justification: Leading IPS vendors have found rising market acceptance as they've introduced NGIPS features on top of their existing IPS product lines. Vendors with mature NGIPS offerings are gaining market share from IPS vendors that don't have robust NGIPS features. NGIPSs will remain viable in lean-forward customers as first-generation IPSs sunset. Through 2015, penetration will grow at the expense of old-line IPSs, but will eventually stabilize as next-generation firewall (NGFW) and NGIPS adoption grows.

User Advice: Network security administrators: Consider replacing your Internet-facing intrusion detection system/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 network firewall, then consider an NGFW that includes an NGIPS.

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 in the future.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Cisco; HP; IBM; McAfee; Radware

Recommended Reading: "Magic Quadrant for Intrusion Prevention Systems"

"Defining Next-Generation Network Intrusion Prevention"

Database Audit and Protection

Analysis By: Brian Lowans

Definition: Database audit and protection (DAP) tools provide a centralized security for different relational database management systems (RDBMSs). The core capabilities of DAP tools have developed beyond basic activity monitoring to include data discovery and classification, threat and vulnerability management, application user analysis, intrusion prevention, and activity blocking. Most tools also offer data protection options through encryption, tokenization or data masking.

Position and Adoption Speed Justification: Databases are typically the main repository for regulated data, such as healthcare, financial, personal and credit card, as well as intellectual property. DAP provides a real-time forensic and preventive control. It mitigates risks that are not addressed solely by preventive controls, such as identity and access management and encryption.

There are four primary use cases for DAP:

1. **Privileged user monitoring:** This identifies and assesses the who, what, why, where, when and how of database administrators, system administrators and other users with highly privileged access. This use case covers access to data, as well as anything that goes on "under the covers," including configuration changes, schema changes and account management activity.

2. **Application user monitoring:** Users with legitimate access may use this access, either accidentally or maliciously, to violate policy and cause exposures. Accessing too much data too fast, or mistakenly leaking data to which they have access, may result in a significant security incident.
3. **Attack prevention:** The ability to identify and mitigate open vulnerabilities or exposures within the RDBMS and then map them to malicious activity is growing in importance with Gartner clients and has become more common as DAP tools continue to mature the extended capabilities.
4. **Data privacy/residency:** The ability of DAP to manage the segregation of duties of privileged and application users has shown increased interest by Gartner clients to protect the privacy of data within geographic jurisdictions. This has led to increased interest in adding data protection through encryption, tokenization or data masking.

DAP's move through the Hype Cycle has slowed because of the enhancement of functionality. The core monitoring capabilities are quite mature, but the extended capabilities are still continuing to develop to include big data platforms such as Hadoop.

The DAP market continued to experience moderate growth through 2013/2014, due to organic growth of existing customer deployments, strong growth to cater for data residency issues and adding new clients in EMEA and Asia/Pacific. While the preventive controls continue to mature, vendors need to continue developing the capabilities for protection at rest and also in use. Use of encryption, tokenization and data masking can offer enhanced segregation of duties for particular use cases.

User Advice: DAP provides a comprehensive security suite compared with alternatives. Moreover, DAP provides comprehensive, cross-platform support in heterogeneous database environments. Clients should implement DAP functionality to mitigate the high levels of risk resulting from database vulnerabilities, to address audit findings or to enforce segregation of duties. However, alternative technologies can be used in limited use cases:

- Consider security information and event management (SIEM) tools as an alternative option in cases where native logging is available, overheads fall within acceptable limits and there is minimal need for granular monitoring.
- Consider content-aware data loss prevention (DLP) tools as an option only in cases where the focus is skewed toward the data accessed from the database, with the understanding that DLP can't tell you anything about what goes on within the RDBMS structures "under" the data.

Business Impact: DAP is an important addition to risk management programs and to implement enterprise data security governance strategies. It is a worthwhile investment for clients with RDBMSs or Hadoop deployments containing regulated or business-critical data. It is also showing increasing value to simplify audits, and it is enforcing the segregation of duties.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Fortinet; GreenSQL; IBM; Imperva; McAfee; Oracle; Trustwave; WareValley

Recommended Reading: "Apply the Nine Critical Capabilities of Database Audit and Protection"

"Big Data Needs a Data-Centric Security Focus"

"Five Cloud Data Residency Issues That Must Not Be Ignored"

Network Access Control

Analysis By: Lawrence Orans

Definition: A network access control (NAC) process adds policies to the network for controlling access by devices and users. Policies may be based on device and/or user authentication and the status of endpoint configuration.

Position and Adoption Speed Justification: The bring your own device (BYOD) phenomenon continues to be the primary driver for NAC adoption. Enterprises are implementing NAC to establish policies for controlling network access by personally owned devices. NAC solutions are used to profile and identify mobile devices, and to assess their configuration. For example, organizations may choose to grant wireless LAN access to tablets and smartphones, but only if they are able to control the device using a mobile device management (MDM) solution. In this scenario, NAC could be used to check for the presence of an MDM agent before granting network access for the device. Most NAC vendors have integrated with one or more MDM solutions to address this use case. Some NAC vendors have built (or plan to build) their own MDM-lite functionality, so they can enforce basic policies on mobile devices without a separate MDM product. NAC policies are also used to enforce the configuration of laptops by controlling network access.

NAC solutions have become "stickier" as enterprises 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 and advanced threat defense solutions. Sharing contextual information (for example, user identity, operating system type and level) with these other components helps security operations teams respond more effectively to security alerts. NAC can also be used to respond to alerts from these other security components. For example, if an advanced threat defense product flags an endpoint as being compromised, NAC can automatically remove that device from the network. These integrations highlight the maturation of NAC, and are a key reason for our positioning NAC further along the Slope of Enlightenment in 2014.

User Advice: If an organization's goal is to integrate NAC and MDM, then choosing an NAC vendor first will limit MDM options. Conversely, choosing an MDM vendor first will limit NAC options. All NAC and MDM integrations are driven by vendors that have partnered to integrate their solutions. An interoperability framework needs to be established to facilitate more widespread NAC and MDM integration. MDM is the larger and faster-growing market, so most enterprises will deploy an MDM solution before implementing NAC. Network managers responsible for NAC projects should influence MDM product selection to ensure NAC interoperability.

Business Impact: NAC helps enterprises provide a flexible approach to securely supporting BYOD. Technologies like MDM and virtualized desktop infrastructure (VDI) will be key components in enabling enterprises to safely allow personally owned devices in the workplace. NAC will enable enterprises to ensure that these technologies are in use on mobile devices, and provide the appropriate level of network devices for compliant and noncompliant endpoints. NAC also improves an enterprise's overall security by providing visibility into the devices that are on their network.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Aruba Networks; Auconet; Bradford Networks; Cisco; Extreme Networks; ForeScout Technologies; Impulse Point; InfoExpress; Juniper Networks; McAfee; Portnox; StillSecure; Trustwave

Recommended Reading: "Magic Quadrant for Network Access Control"

"Network Access for Guests or Contractors Requires More Than an Open-Network, Coffee Shop Strategy"

"Securing BYOD With Network Access Control, a Case Study"

"Using NAC to Reduce Risk Related to BYOD and Unmanaged Devices"

Application Control

Analysis By: Neil MacDonald

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

Position and Adoption Speed Justification: 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, which can't keep up with the explosion in malware variants and the increases in targeted attacks. In addition, for users who retain administrative rights on their systems, these tools can help to restrict applications that administrators can execute. Recent highly publicized attacks, such as on The New York Times and Target, have raised awareness of the increasing ineffectiveness of traditional, signature-based approaches to endpoint security.

Although there are many smaller point solution vendors providing application control, the large antivirus vendors are making progress with their own offerings — for example McAfee, Trend Micro and Kaspersky. Microsoft has also raised awareness of application control with the inclusion of AppLocker in Windows 7 and Windows 8. However, widespread adoption of application control with desktops has been slow. Disillusionment comes from cultural changes, as well as the ongoing care and feeding to make a whitelisting-based solution scale to support highly dynamic endpoint environments. However, on servers and embedded devices, application control should be the foundational approach and can replace the need for signature-based anti-malware scanning. Network-based application control solutions, such as those from next-generation firewalls and Web security gateways, complement endpoint-based approaches.

User Advice:

- 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.
- Use approaches rooted in application control and whitelisting as the cornerstone of your server and embedded device protection strategy, not signature-based anti-malware.
- 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.

Business Impact: Application control provides operational and security benefits. 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: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: AppSense; Bit9; Blue Ridge Networks; Check Point Software Technologies; Cryptzone; Faronics; IBM; Kaspersky Lab; Lumension Security; McAfee; Microsoft; Savant Protection; Sophos; Symantec; Trend Micro

Recommended Reading: "Designing an Adaptive Security Architecture for Protection From Advanced Attacks"

"Malware Is Already Inside Your Organization; Deal With It"

"How to Successfully Deploy Application Control"

"How to Devise a Server Protection Strategy"

"Best Practices for Removing End-User Administrator Rights on Windows"

"Magic Quadrant for Endpoint Protection Platforms"

"Toolkit: Application Control Evaluation and Selection Tool"

Static Application Security Testing

Analysis By: Joseph Feiman; Neil MacDonald

Definition: Static application security testing (SAST) is a set of technologies designed to analyze application source code, bytecode and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions analyze an application from the "inside out" in a nonrunning state.

Position and Adoption Speed Justification: Proactively detecting security vulnerabilities earlier in the application development process is less expensive than fixing the vulnerability later when the application is in production and reduces the overall security exposure of the application and its data. Because of the development process changes and cultural changes necessary to incorporate SAST tools or services in the software development life cycle, SAST has not been as widely adopted as its sister technology, dynamic application security testing (DAST). It will take several more years before SAST technologies and their adoption reach the Plateau of Productivity. An alternative approach, interactive application security testing (IAST) offers an alternative to SAST (and also DAST) with higher assurance results and lower barriers to adoption.

User Advice: SAST for security vulnerabilities should be a mandatory requirement for all IT organizations that develop or procure applications. Ideally, application vulnerability detection would be conducted continuously during the entire software life cycle (SLC). Enterprises that lack application security skills and resources should consider application security testing as a service.

False positives are a concern. Therefore, enterprises should fine-tune the tools, so that detection and remediation efforts can be focused first on high-confidence, high-severity vulnerabilities starting at the unit test, build or quality assurance phase of the SLC.

At a minimum, SAST should be performed on all critical applications. For outsourced application development, as a part of the contract, organizations should require external service providers to perform SAST and provide evidence that testing has been performed. The contract should also make it clear that the remediation of security defects is covered under the standard agreement. In addition, organizations should perform their own testing as part of the acceptance process of any outsourced applications whose contractual agreements did not cover this.

Enterprises, cloud computing adopters and cloud service providers should conduct SAST on the applications being uploaded to the cloud and on the applications/software that provide cloud services. Enterprises should require that packaged systems should be tested by third-party SAST providers. Enterprises should start pressing vendors for more-intelligent solutions, specifically for solutions that offer different security technology interaction, integration and correlation. In particular, enterprises should look for solutions with SAST and DAST technology features' interaction (referred to as interactive application security testing, or IAST), because they typically enable higher accuracy and breadth of vulnerability detection. Enterprises should also look for solutions that enable the integration of SAST, DAST and other security information in persistent storage, which enables information querying and analytics — solutions that might be offered by security information and event management vendors in collaboration with SAST and DAST vendors. Enterprises should expect that point solutions will eventually be replaced by platforms.

Business Impact: The most critical impact of using SAST is minimizing the risk of possible exploitation of application vulnerabilities. Adopting SAST will enable organizations to detect the vulnerabilities embedded in applications before hackers detect them. As with any security investment, a cost-benefit risk analysis should be performed. Making a definitive ROI calculation will be difficult, because the primary purpose of SAST is risk reduction, not cost savings. Catching vulnerabilities earlier saves money, but this must be balanced against the process and cultural changes necessary for implementing SAST adoption. Discovery and removal of vulnerability in the development phase is less expensive compared with its discovery and removal in the operation phase. Later discovery increases the probability that the rectifying action will have to touch on more modules and classes. In the longer term, another source of cost savings will come from the automation of security testing and procuring security testing as a service.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Checkmarx; Denim Group; HP (Fortify Software); IBM; Positive Technologies; Veracode; Virtual Forge; WhiteHat Security

Recommended Reading: "Evolution of Application Security Testing: From Silos to Correlation and Interaction"

"Cost-Saving Tips for Acquisition and Implementation of Application Security Technologies"

"Application Security Detection and Protection Must Interact and Share Knowledge"

"Cost-Saving Tips for Acquisition and Implementation of Application Security Technologies"

"Application Security Road Map Beyond 2012: Breaking Silos, Increasing Intelligence, Enabling Mass Adoption"

DDoS Defense

Analysis By: Lawrence Orans

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 products and services detect and mitigate such attacks. Attackers continue to increase the complexity and sheer volume of the attacks.

Position and Adoption Speed Justification: For the second straight year, DDoS defense slips further back on the Hype Cycle, due to changes in the attack landscape that have resulted in tougher DDoS challenges for enterprises. Last year, DDoS defense was also positioned on the Slope of Enlightenment, but it was closer to the Plateau of Productivity.

There are several reasons that the positioning of DDoS defense has regressed in the Hype Cycle. Attackers have launched record-setting attacks in 2013 and 2014, there is a wide range of efficacy among some DDoS mitigation providers, and many enterprises lack an overall understanding of DDoS mitigation best practices. For example, in 2013, the most damaging attacks were based on DNS amplification, whereas in 2014, the most damaging attacks have been based on Network Time Protocol (NTP) amplification. The efficacy of DDoS mitigation services varies greatly, and will continue to do so as more vendors enter the market to respond to customer demand. Finally, enterprises that are experiencing DDoS attacks for the first time typically don't have the experience to mitigate the attacks quickly and effectively.

User Advice: DDoS mitigation services should be a standard part of business continuity/disaster recovery planning, and 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 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 non-Web targets (for example, corporate firewalls, VPN servers and email servers).

Business Impact: Any business-critical Internet-enabled application or service can be disrupted by DDoS attacks.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Akamai; Arbor Networks; AT&T; CenturyLink; CloudFlare; Corero Network Security; Defense.Net; F5; Neustar; NSFOCUS Information Technology; Prolexic Technologies; Radware; RioRey; Verisign; Verizon

Recommended Reading: "Master These Eight Steps to Control the Damage From DDoS Attacks"

"Leverage Your Network Design to Mitigate DDoS Attacks"

"Enterprise Strategies for Mitigating Denial-of-Service Attacks"

"Denial of Service: A Comparison of Defense Approaches"

Unified Threat Management (UTM)

Analysis By: Jeremy D'Hoinne

Definition: Unified threat management (UTM) platforms are network appliances that implement a variety of point security controls and network infrastructure capabilities particularly suited to SMBs. Feature availability continues to grow, copying new features from other network security technologies; but performance degrades as they 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: As small or midsize businesses (SMBs) continue to expand business-critical use of the Internet, more use UTM platforms. However, UTM budget more often competes with Internet-hosted services (cloud based) and mobile security solutions. The adoption of UTM technologies continues to grow with some distributed enterprises adopting it, in addition to its traditional base of small and midsize organizations. Features such as wireless management, cloud-based centralized management consoles and high-level reporting dashboards also get higher adoption rates. The market is consolidating, with a number of small players acquired, while the others fight for a global presence.

Enterprise security buyers often consider that the consolidation of '"good-enough" features on UTM platforms provides limited benefits and impacts performance. To continue to grow adoption, UTM technology must continue to improve to provide cost-effective network and security solutions to a fast-changing SMB environment.

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 UTM 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, a retail enterprise or hotel chain with many locations, where there is a limited local IT staff in each location) may find UTM products appealing. Larger enterprises should first look at branch-office firewalls from the same vendor as their central firewalls, and should not underestimate the costs that could come from potential misconfiguration, inconsistent security and duplicated processes when using more than one brand of firewall.

When evaluating UTM, organizations should pay attention to the effectiveness of the different security modules, the reality of the cost-saving 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.

Recurring costs can be considerably higher for a UTM 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, and that includes 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: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Aker Security Solutions; Barracuda Networks; Check Point Software Technologies; Cisco; Clavister; Cyberoam; Dell SonicWALL; Fortinet; gateprotect; Hillstone Networks; Huawei; Juniper Networks; Kerio; Netasq; Netgear; Sophos; WatchGuard; ZyXEL

Recommended Reading: "What You Should Expect from Unified Threat Management Solutions"

"Magic Quadrant for Unified Threat Management"

"Bring Branch Office Network Security Up to the Enterprise Standard"

"Next-Generation Firewalls and Secure Web Gateways Will Not Converge Before 2015"

Static Data Masking

Analysis By: Joseph Feiman

Definition: Static data masking aims to deter the misuse of data by users of nonproduction (mostly testing, and also training and analytics) databases (typically programmers and testers) through transformation of data items in advance of its use in the database.

Position and Adoption Speed Justification: Three factors affect the speed of static data-masking maturity and adoption:

- Static data masking is a variation of a well-known and long-known data transformation, when a dataset is transformed into a set with a somewhat different content (that is, some fields are changed). Therefore, when the need for data masking became acute, it did not take vendors long to develop solutions that were relatively mature. Not surprisingly, within the past few years, more than a dozen vendors came to this market to evolve their technologies and practices.
- Static data masking is a reasonable security precaution that an enterprise may take on its own initiative. These days, it is also recommended by rule bodies and regulators — for example, by the PCI Security Standards Council group and the U.S. Health Insurance Portability and Accountability Act — to protect clients of the credit card and healthcare industries, respectively. Another adoption factor is application development outsourcing, which raises concerns about the security of the data that becomes accessible to external service providers and developers domestically or offshore.
- However, implementation of data masking in more complex security/privacy protections can require a more complex transformation, which in turn affects data utility; some organizations find this to be an obstacle to adoption.

For these reasons, we expect a relatively high speed of technology maturity for data masking, and that it will reach the Plateau of Productivity within five years.

User Advice: Enterprises should use static data masking to limit users' access to sensitive data. Potential abusers, whom static data masking aims to deter, are often enterprise employees — users of test databases (programmers, testers and database administrators) who seek to abuse their access privileges to sensitive data. Data-masking technologies should satisfy a simple, yet strict, rule: Masked data should be quasi-real — that is, it should satisfy the same business rules as real data. This is to ensure application integrity — to ensure that the application running against masked data performs as if the masked data is real. Data masking must not limit users' ability to adequately use applications.

Recently, we have witnessed the emergence and evolution of dynamic data masking aimed at real-time data masking, typically in production databases. Also, we have witnessed emerging clients' interest in "data redaction," a variation of data masking applied to nonstructured data, such as Microsoft Word, Excel and PDF. We will keep evaluating clients' interest and vendors' offerings in this space.

Business Impact: Sensitive data (such as credit card numbers), personally identifiable information (such as U.S. Social Security numbers), medical diagnoses and even nonpersonal sensitive data (such as corporate financial information and intellectual property) are exposed to abuse or negligence from enterprise employees and outsiders. Adopting data masking will help enterprises raise the level of security and privacy assurance against insider and outsider abuses. At the same

time, data masking will make enterprises compliant with the security and privacy standards recommended by regulating or auditing organizations.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Axis Technology Software; Camouflage Software; Compuware; Dataguise; Epi-Use; GreenSQL; Grid-Tools; IBM; Informatica; Mentis; Net 2000; Oracle; Privacy Analytics; Solix Technologies; Voltage Security

Recommended Reading: "Magic Quadrant for Data Masking Technology"

"How Data Masking Evolves to Protect Data From Insiders and Outsiders"

"Toolkit: Static Data-Masking Vendor Evaluation Criteria"

"Toolkit: Checklist for Implementing Static Data-Masking Best Practices in Nonproduction Environments"

"Selection Criteria for Data-Masking Technologies"

Web Application Firewalls

Analysis By: Jeremy D'Hoinne

Definition: A Web application firewall (WAF) is a shielding safeguard positioned in front of Web servers and intended to protect Web applications. WAFs focus primarily on Web server protection at Layer 7 — 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 for more accurate protection.

Position and Adoption Speed Justification: WAF capabilities are available as stand-alone appliances, as a software module in most application delivery controllers (ADCs), and often bundled with protection against distributed denial of service (DDoS) in cloud services. The PCI standard continues to be one of the drivers for WAF use, but many enterprises without WAF obligation now understand that their need for Web application security should not be limited to compliance issues. The position in the Hype Cycle has moved due to growing adoption of SaaS and ADC WAFs. The individual products have matured, and innovation from incumbent WAF vendors might slow down while new alternate, more focused, solutions emerge.

As the responsibility for Web application security is shared across several teams within organizations, the continued challenge of a fragmented buying center slows down adoption of WAF technology.

User Advice: The best way to secure Web applications is to ensure that they have no vulnerabilities before enabling them to be run in production. Enterprises should assess their tolerance for a fully in-line security engine with blocking capabilities, then evaluate how the different teams would collaborate if WAF is deployed in established ADC/load balancers versus a stand-alone WAF. Stand-alone WAF vendors are usually the first to market with new security features and are typically better at custom support than ADC WAF vendors, but WAF in ADC might provide a better incremental price, solid performance and SSL decryption capabilities, and it could ensure a single pass for traffic inspection. Organizations looking to protect public Web applications without customer configuration, and that are also exposed to DDoS, should consider new cloud WAFs, or "WAF as a service."

Reality often dictates that a WAF should be used due to weak change control, no ability to scan third-party code or highly dynamic applications. Enterprises should carefully review how WAF integrates with their Web access management (WAM), dynamic application security testing (DAST) technologies, database security solutions, and the other components of the data center infrastructure.

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

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: AdNovum Informatik; Akamai; Barracuda Networks; Bee Ware; Citrix; CloudFlare; DenyAll; Ergon Informatik; F5; Fortinet; Imperva; NSFOCUS Information Technology; Penta Security Systems; Radware; Trustwave; United Security Providers

Recommended Reading: "Magic Quadrant for Web Application Firewalls"

"Web Application Firewalls Are Worth the Investment for Enterprises"

"Application Security Detection and Protection Must Interact and Share Knowledge"

"Magic Quadrant for Application Delivery Controllers"

Network Security Silicon

Analysis By: Greg Young

Definition: Network security silicon refers to the use of specific network security processors to perform very high-speed security processing, such as deep packet inspection and stream processing. This is different from application-specific integrated circuits and field-programmable gate arrays that are already in use, and different from cryptographic accelerators. However, combinations of all of these devices are increasingly needed to deal with complex networks and advanced targeted threats.

Position and Adoption Speed Justification: The continually increasing data rates on business networks, combined with the growing complexity of advanced targeted threats, have increased the demand for high-speed network security processing. While multicore x86-based platforms can be used at higher and higher rates, the evasion techniques used by advanced threats consume processor power, making dedicated processors win price/performance trade-offs. Network processors typically use many smaller processors in a high-bandwidth framework, favoring throughput over complexity.

However, cloud computing services will also make inexpensive computer power available for security as a service, negating the need for security silicon in security applications where the latencies involved in cloud-based processing are acceptable. Cloud-based security service providers will consume network security processors as their business bases increase.

User Advice: Where flexibility is the primary requirements, software-based approaches within custom-built appliances are likely to be better choices for network security devices. Where multigigabit data rates with small packets or low-latency requirements are in use, and targeted threats are likely, hardware acceleration should be evaluated, since it could provide better price/performance compromise. However, no matter the hardware optimization, network security silicon is inefficient at antivirus or similar Layer 7 content inspection.

Business Impact: Network security silicon is relevant to firewalls/intrusion prevention, advanced threat appliances, intrusion detection, malware detection, content inspection and any applications in which encrypted data streams must be inspected.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Broadcom; Cavium; Exar; Freescale; Napatech; Netronome; SafeNet; Xilinx

Next-Generation Firewalls

Analysis By: Greg Young

Definition: Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall. An NGFW should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or nonenterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated.

Position and Adoption Speed Justification: Commercially available NGFWs are achieving good market share, and capabilities continue to advance. First-generation firewall vendors have road maps and initial offerings of NGFW.

User Advice: Consider NGFWs for your shortlist if you're replacing or upgrading a 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 road map), 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.

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

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Check Point Software Technologies; Cisco; Dell; Fortinet; Hillstone Networks; Juniper Networks; McAfee; Palo Alto Networks

Recommended Reading: "Magic Quadrant for Enterprise Network Firewalls"

Entering the Plateau

SIEM

Analysis By: Kelly M. Kavanagh

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

Position and Adoption Speed Justification: The increase in targeted attacks has caused a growing number of organizations to use SIEM for threat management to improve security monitoring and early breach detection, in addition to meeting regulatory compliance reporting requirements. Large and midsize companies continue to deploy SIEM for monitoring perimeter security controls, with growing adoption of other use cases that include monitoring of servers, database management system applications and users. There is growing interest in outsourced or co-managed SIEM with a range of support options from external service providers.

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 effective 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

predefined security monitoring and compliance reporting functions. Data access and user activity monitoring for early detection of targeted attacks and data breaches has emerged as the high-priority use case for SIEM technology. Several vendors are developing big data security analytics platforms and integrations that increase scale of and types of security analytics available from SIEM technologies.

User Advice: Security managers considering SIEM deployments should first define the requirements for log management, user and resource access monitoring, threat monitoring, security incident response and workflow, and compliance reporting. This may require the inclusion of other groups in the requirements definition effort, such as audit/compliance, network operations, server administration, database administration and application support areas. Organizations should also estimate event rates, document their network and system deployment topology, and anticipate deployment growth and analytic requirements. SIEM vendors can use this data to propose a company-specific solution. Technology and service selection decisions should be driven by organization-specific requirements 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.

Business Impact: SIEM improves the IT security organization's ability to quickly detect targeted attacks and data breaches, and improves incident investigation and response. SIEM also supports the privileged-user- and resource-access-monitoring activities of the IT security organization and the reporting needs of the internal audit and compliance organizations.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: AccelOps; AlienVault; BlackStratus; EMC (RSA); EventTracker; HP (ArcSight); IBM; LogRhythm; McAfee; NetIQ; SolarWinds; Splunk; Tenable Network Security; Tibco Software; Trustwave

Recommended Reading: "Magic Quadrant for Security Information and Event Management"

"Critical Capabilities for Security Information and Event Management Technology"

"Planning for an SIEM Technology Deployment"

"How to Deploy SIEM Technology"

"Using SIEM for Targeted Attack Detection"

Mobile Data Protection

Analysis By: John Girard; Eric Ouellet

Definition: Mobile data protection (MDP) tools encrypt and implement access controls for enterprise data stored on mobile devices. The main use case continues to be company-owned workstations, typically mobile notebooks running a full OS, such as Windows 7 or Mac OS X, and removable media. The same products may be used for desktops and servers. Data protection for cloud storage, smartphones and tablets is more aggressively pursued in adjacent technologies and markets, with some vendors overlapping.

Position and Adoption Speed Justification: MDP tools encrypt information on fixed and removable storage systems used in mobile contexts, ranging from hard drives to solid-state and flash drives. Products and services for encrypting end-user data continue to sell well enough to support more than a dozen discernible vendors. Public outcry over the loss of data on notebook computers, as well as civil and government actions against companies over high-profile data leakage debacles, ensures that this product category continues to demand attention. Products range from suites that can protect a wide range of platforms to single-purpose solutions, with the bulk of revenue deriving from notebook (laptop) computers running Windows 7. The management of MDP can be delivered as an in-house solution or a managed service. MDP products are mature and generally perform well as fresh installations on new systems with up-to-date hardware and current OS versions. However, it is also important to realize that, when major new OS platforms are released (for example, Windows 8), even mature MDP products may suffer from new or renewed problems and must adapt to new capabilities such as UEFI. Thorough testing is always advised.

The MDP problem has been recognized since the 1990s, it is widely known among Gartner clients, and it should be fully mature and embedded; however, several factors continue to freeze our assessment at "mature mainstream." These include:

1. For most companies, MDP has been an expensive add-on, compared with the cost of other endpoint protection tools. Even when embedded encryption features are chosen, there is a need for a management system and, therefore, a significant incremental cost per device.
2. Performance-improving technologies, such as self-encrypting drives based on Trusted Computing Group (TCG) specifications, are still in limited use (see related technology profile: Interoperable Storage Encryption).
3. All enterprise-feasible products are proprietary and labor-intensive to change if buyers want to change vendors.
4. The current MDP tools are not designed to support "bring your own device (BYOD) use cases" and are not yet borrowing from the containment design concepts that are working on consumer smartphones and tablets.
5. Microsoft continues to promote BitLocker, which has a disruptive influence in product selection, but which needs to be managed in order to qualify for the MDP definition. The cost associated with Microsoft's Management solution, Microsoft BitLocker Administration and Monitoring (MBAM), lack of interoperability with non-Windows workstation platforms and other limitations are providing an opportunity for other MDP vendors to manage BitLocker as one encryption engine among many. The effort needed for companies to understand this situation further impedes progress toward the plateau.

Mind share for managing policies, including encryption for smaller devices, has been held in a separate enterprise mobility management (EMM) market, formerly tracked as mobile device management (MDM). Vendor overlap between MDP and EMM as well as endpoint protection platforms (EPPs) is increasing as large vendors make acquisitions, but the administration of policies for workstations versus smaller devices, and variants, such as iOS and Android, is typically segregated.

User Advice: The loss or theft of data on mobile devices is among the largest and most publicly damaging data exposure risks that companies face, and is frequently reported for workstations (particularly laptops). Therefore, data protection is one of the first investments that should be made on a mobile platform. 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. A good MDP investment 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.

The steady stream of inquiries about MDP and data loss, particularly for BYOD and international travel situations, shows that protection is a recognized need. However, Gartner clients reveal a trend of patchy and incomplete support for encryption that must still be addressed. We recommend the following:

- Do not waste effort picking and choosing which devices to encrypt based on the belief that only some users work with sensitive data; it is an impossible task. In practice, sensitive data can move across many systems, and the exploit value of data may be unknown in advance of a breach.
- Do not postpone MDP implementations while waiting for something better to come along.
- Do recognize that MDP solutions must protect information that moves onto removable media, noncompany systems and into the cloud.
- Do negotiate in advance with hardware suppliers to ensure access to new technologies, such as self-encrypting drives.
- Do incorporate a reliable and documented key destruction process into your device redeployment and retirement processes.

Business Impact: The business value for data protection can seem low because encryption doesn't contribute directly to productivity and, like most security topics, it isn't real to a stakeholder until a problem has already occurred. However, the number of laws coming 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, which 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, and businesses should get on with it.

IT planners must pay attention to adjacent technologies and markets that ultimately share responsibility for data access policies and controls. Examples include enterprise file synchronization and sharing (EFSS), content-aware data loss prevention (DLP) and enterprise mobility management (EMM).

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Beachhead Solutions; CenterTools; Check Point Software Technologies; Dell; McAfee; Microsoft; Novell; SafeNet; Secude; Sophos; Symantec; Trend Micro; Verdasys; Wave Systems; WinMagic

Recommended Reading: "Magic Quadrant for Mobile Data Protection"

"A Buyer's Guide to Secure USB Flash Drives"

"Magic Quadrant for Mobile Device Management Software"

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

"Protecting Sensitive Data on Decommissioned SSDs and HDDs"

Web Services Security Gateways

Analysis By: Ross Altman; Ray Wagner

Definition: Web services security gateways secure access to WS-* and REST Web services. Often deployed in a demilitarized zone (DMZ), these gateways provide content threat protection, XML parsing, schema validation, data transformation and load balancing. They support authentication based on an included security token service or third-party identity management products, and provide tooling to manage the development and enforcement of policies for security and traffic management.

Position and Adoption Speed Justification: Interest in Web services security gateways has developed in concert with interest in service-oriented architecture (SOA) and mobile applications. Web services security gateways are often deployed at the edge of the internal network to provide security for Web services requests and API access that crosses enterprise or other security boundaries. However, Web services security gateways are also used internally where security concerns are high. In many cases, security-related functions are packaged with other SOA support functions similar to those found in enterprise service buses (ESBs); some refer to these gateways as "an ESB in a box." This packaging often causes confusion because of the highly variable feature

content in different devices. Purpose-built XML security devices provide a level of security not attained by multipurpose products at present. After several recent acquisitions (IBM acquired DataPower, CA Technologies acquired Layer 7, Intel acquired Mashery and Axway acquired Vordel), major vendors are taking a more prominent position in this market. Interest in the acquisition of this technology as hardware appliances is tapering off, because these vendors also now make their functionality available as software that can be loaded into on-premises servers or as cloud offerings that are generally presented as "API management" services.

User Advice: Organizations deploying low- to moderate-value services across an enterprise boundary or internally may find a measure of Web services security gateway functionality in other product types, such as access management and identity federation tools, policy management technologies, SOA governance products, cloud-based API management services, and some Web application firewalls. Use purpose-built Web services security gateways when high-value services (that is, those having significant financial or regulatory components) and/or high-volume/high-velocity services are deployed internally and externally. These products are available as both hardware and software appliances. When delivered as hardened hardware appliances, they are appropriate for deployment in DMZs, something that would be less appropriate for some software-based access control and policy enforcement products.

Business Impact: Web services security gateways offer significant security value when processing transactions that have high financial value, intellectual property considerations and/or privacy restrictions. For applications that have only moderate security requirements, Web services security gateways enable high throughput for XML processing and message load balancing. For some applications, some enterprises may not believe that the heavy-duty access control and policy management provided by hardware appliances are necessary, but these enterprises may find that they benefit from the Web services security gateway's ability to, in effect, provide an ESB in a box.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Alcatel-Lucent; Apigee; Axway; Bee Ware; CA Technologies; Crosscheck Networks; DenyAll; F5; IBM; Intel; Layer 7; Vordel

Recommended Reading: "Application Integration and SOA Gateway Appliances Losing Market Share to Cloud Alternatives"

"Using SOA Gateways for Secure SOA Communications"

"Web Application Firewalls: Where Do We Go From Here?"

"Intel's Acquisition of Mashery Bridges SOA Governance and API Management"

"Sensing a Growing API Management Market, CA Technologies to Buy Layer 7"

Vulnerability Assessment

Analysis By: Kelly M. Kavanagh

Definition: Vulnerability assessment (VA) products and services scan enterprise networks and:

- Establish a baseline and trending of vulnerability conditions for devices, applications and databases.
- Identify and report on the security configuration of IT assets.
- Discover unmanaged assets.
- Support specific compliance reporting and control frameworks.
- Support risk assessment and remediation prioritization.
- Support remediation by IT operations groups.

Position and Adoption Speed Justification: VA is an essential 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 PCI Data Security Standard (DSS), the U.S. Federal Information Security Management Act (FISMA) and United States Government Configuration Baseline (USGCB) configuration requirements. The widespread recognition of vulnerability management as a best practice for risk reduction, these compliance requirements and others — as well as pressure from business partners, customers and auditors — have been the primary drivers of VA projects in recent years.

The VA market is mature. It is characterized by a number of VA-specific and other vendors competing for scanning business, and by the existence 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 continue to evolve, driven by changing threats, compliance requirements, use of new technologies and enterprise efforts to reduce the cost of vulnerability management processes.

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 uncredentialed or credentialed (via login to an account on the scan target). Credentialed scanning provides a more-detailed assessment of the scan targets, resulting in improved accuracy and the ability to determine security configurations. For large deployments, credential 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. Passive observation can provide information about devices that cannot be actively scanned, but this technique alone generally does not provide sufficient data to support remediation activity.

- **Agents** reside on the scan targets, either as persistent software or as dissolvable temporary elements, collecting state information in real time. Agents provide information about the target that 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.

Most VA deployments rely on active network scanning. There are typically areas in larger IT environments that benefit from passive observation and agent-based assessment. Gartner recommends that security-conscious enterprises use a combination of two of the three described techniques for comprehensive coverage.

Buyers should assess VA tools' capability to scan for vulnerabilities in virtual environments and mobile devices, to assess security configuration settings related to formal or corporate standards, to manage multiple scanners in large deployments, and to provide targeted remediation support with flexible reporting, threat analysis and asset identification. VA vendors increasingly compete on these extended features — and on price, rather than on claims about the speed or accuracy of network vulnerability scans. Deployment options for VA typically include software, appliance, virtual appliance and remote hosted or cloud-based services, and often support mixed deployments that incorporate several modes.

Business Impact: VA is an important component of the vulnerability management process to support enterprise 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 exploit 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: Beyond Security; BeyondTrust; Critical Watch; Digital Defense; McAfee; Positive Technologies; Qualys; Rapid7; Saint; Tenable Network Security; Tripwire; Trustwave

Recommended Reading: "Four Ways to Close the Gap Between Enterprise Mobility and Vulnerability Management"

Dynamic Application Security Testing

Analysis By: Neil MacDonald; Joseph Feiman

Definition: Dynamic application security testing (DAST) technologies are designed to detect conditions indicative of a security vulnerability in an application in its running state. Most DAST solutions test only the exposed HTTP and HTML interfaces of Web-enabled applications. However, some solutions are designed specifically for non-Web protocol and data malformation (for example, remote procedure call, Session Initiation Protocol [SIP] and so on).

Position and Adoption Speed Justification: Enterprises understand the importance of application security vulnerability testing — both static application security testing (SAST), a separate technology, and DAST. The adoption of DAST solutions, primarily in the form of Web application testing tools, has been rapid, and is more mature than SAST for several reasons:

- DAST doesn't require access to source code.
- DAST can be performed by security, audit or compliance teams outside of development.
- DAST tools can help automate penetration testing, which many organizations already perform.
- Most organizations have vulnerable, external-facing, Web-enabled applications deployed, and there is an immediate need (often driven by the regulatory environment) to reduce risk.

The need for DAST tools continues to grow due to:

- The growing number of applications and APIs that are Web-enabled and externally accessible
- The growing number of targeted and financially motivated attacks at the application level
- Emerging mobile applications that require HTML5 testing and testing of Web interfaces to back-end systems

The market for application security testing tools is maturing, as demonstrated by:

- Vendor mergers and acquisitions as software life cycle (SLC) vendors provide capabilities for security vulnerability testing as an integral part of the entire SLC platform.
- Static analysis and dynamic testing capabilities are being integrated into a single product or SaaS. IBM, HP and WhiteHat Security SAST acquisitions and Veracode internal development of both SAST and DAST SaaS are evidence of this trend.

DAST delivery as a cloud service is growing:

- Enterprises that lack application security skills and resources increasingly consider DAST as a service.

- Multiple vendors provide DAST as a service, lowering barriers to adoption, including several vendors that do not offer DAST as a tool, but only DAST as a service.

User Advice:

- All Web applications should be tested for security vulnerabilities. If an application is found to be vulnerable and cannot be fixed, a Web application firewall is a protection alternative. Use code coverage mechanisms to ensure that all accessible parts of the applications are tested.
- Ideally, application vulnerability detection would be conducted throughout the entire SLC, and for DAST — as one of the components of that overall testing — we recommend starting in the quality assurance and testing phase.
- As DAST testing shifts into the development organization, don't overlook the associated cultural and process-change issues.
- Enterprises that lack application security skills and resources should consider application security testing as a service.
- Focus first on externally facing, business-critical applications, but don't overlook the threat from internal hackers on business-critical applications and legacy applications that have been modernized with Web interfaces.
- Favor next-generation DAST tools that will move beyond scans to providing more application-level intelligence, specifically for solutions that offer DAST and SAST interaction, integration and correlation that enable higher accuracy and greater breadth of vulnerability detection.
- Ensure your vendors can handle complex Web navigation scenarios and complex JavaScript, and include support for testing emerging HTML5 and mobile applications.

Business Impact: The most significant benefit of using DAST is minimizing the risk of possible exploitation of application vulnerabilities. In some cases, DAST testing is a regulatory requirement. For example, the Payment Card Industry (PCI) specification requires the security testing of applications or the adoption of a Web application firewall. Adopting DAST tools will enable organizations to better detect vulnerabilities that are embedded in applications before hackers detect them. Although most purchases today are for users outside the development organization, security testing capabilities should be embedded in SLC platforms, thus enabling vulnerability detection during the earlier stages of the development life cycle. DAST as a service has the potential to reduce capital expenses and time of adoption for resource-constrained organizations.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Acunetix; Denim Group; HP; iViZ Security; IBM; N-Stalker; Nikto; NT OBJECTives; PortSwigger; Qualys; Trend Micro; Trustwave; Veracode; WebScarab; WhiteHat Security

Recommended Reading: "Magic Quadrant for Dynamic Application Security Testing"

"Toolkit: Checklist for 360-Degree Application Security Assessment"

"Toolkit: Best Practices Checklist for Secure Application Development"

"Toolkit: Application Security Testing Checklist for Outsourced Application Development and Maintenance"

"Toolkit: Sample RFP for DAST Tool Selection"

"Cost-Saving Tips for Acquisition and Implementation of Application Security Technologies"

"Magic Quadrant for Application Security Testing"

Network IPS

Analysis By: Adam Hils

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 is driving this market. The market is mature 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 vendors continue to introduce NGIPS features for stand-alone competitiveness, and as IPSs are increasingly subsumed within next-generation firewall (NGFW) deployments, IPSs without next-generation features are approaching obsolescence.

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. Use an IPS as a prepatch shield to allow for more time to test and deploy system patches. Follow a process approach. An IPS can be deployed on switches and routers as an alternative to stand-alone appliances, but beware of overloading infrastructure devices. If you are replacing or installing a network firewall at the perimeter, then consider an NGFW that includes an IPS.

Buyers need to drive vendors for advances in dealing with "gray list" events and targeted malware by adopting NGIPS capabilities. NGFWs incorporate IPSs, 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 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: Legacy

Sample Vendors: Cisco; HP; IBM; Juniper Networks; McAfee; NSFOCUS Information Technology; Radware

Recommended Reading: "Magic Quadrant for Intrusion Prevention Systems"

"Defining Next-Generation Network Intrusion Prevention"

Secure Email Gateway

Analysis By: Peter Firstbrook

Definition: The secure email gateway protects an email service from external threats, filters unwanted inbound email and monitors outbound email for corporate and regulatory compliance. Key functions include message transfer agent capabilities, anti-spam, antivirus, outbound content filtering and encryption.

Position and Adoption Speed Justification: A secure email gateway (SEG) is an essential element in any email system. The SEG market is highly saturated and very mature. Basic spam and virus detection effectiveness is currently over 99% for almost all vendors and is within acceptable limits for most organizations. The ability to detect highly targeted phishing attacks is improving in leading solutions, providing time-of-click protection for malicious URLs, attachment behavioral analysis (sandboxing) and active content stripping. We anticipate that targeted attack protection will be a major differentiator and an area of continued investment for vendors. Enabling personal settings for filtering bulk marketing email is another area of future investment. Many solutions today are capable of identifying bulk email messages, but almost all lack methods for end users to set up their own preferences.

Outbound email security features such as content-aware data loss prevention (DLP) and encryption are critical for intellectual property protection and regulatory compliance (for example, HIPAA, PCI and GLBA). These features should be weighed heavily in buyer analyses. DLP and encryption are less mature than inbound filtering. Over 40% of organizations used advanced encryption and email DLP in 2013. We expect both DLP and encryption usage to surpass 50% penetration by the end of 2015.

Security software as a service (SaaS) and hosted virtual appliance offerings that put all filtering in the cloud, along with ancillary services such as archiving, mailboxes and Web filtering, are increasingly popular among larger enterprise buyers and should be the default deployment option for organizations with fewer than 5,000 seats. Over the next decade, integration of these functions into the mail solution stack from vendors like Microsoft and Google and mailbox hosting providers will decrease the need for point solutions.

User Advice: Organizations must consider targeted spear phishing, DLP and encryption the leading differentiators of SEG solutions and the most important selection criteria. Email administrators should make an effort to understand business requirements for DLP and encryption over the next three years and evaluate vendors and solutions accordingly. Although it is not optimal, SEG DLP capability can be implemented independently of enterprise DLP to satisfy email-specific aspects of regulatory compliance, enforce acceptable usage or enable automatic email encryption. For IP protection, however, buyers of SEG DLP must understand how SEG DLP will integrate into a more holistic enterprise data management strategy. Organizations should attempt to consolidate infrastructure that has accumulated over the years and look for leading solutions that can satisfy future business needs. SaaS and hosted solutions can significantly reduce cost and complexity, and should be considered by all buyers. Longer term, organizations should consider opportunities to converge the entire email stack, from mailboxes to archiving, into a single vendor's service or a combination of on-premises and service solutions.

Business Impact: Organizations must protect their email traffic from security risks and institute controls on outbound email to meet compliance requirements.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Barracuda Networks; Cisco; Clearswift; McAfee; Microsoft; Mimecast; Proofpoint; Sophos; Symantec; Trend Micro; Websense

Recommended Reading: "Magic Quadrant for Secure Email Gateways"

Stateful Firewalls

Analysis By: Greg Young

Definition: The earliest firewalls used only the IP address source, destination and ports, whereas using "state" imparts better security knowledge about how the connection is being used. Stateful firewalls incorporate packet filtering and controls based on the source IP, destination IP, ports used and the past interactions between source and destination.

Position and Adoption Speed Justification: This is a well-established technology. Although most stateful firewalls will be mostly subsumed eventually by next-generation firewalls (NGFWs), there will continue to be placements for which a firewall alone is required. Almost every enterprise uses state-based network firewalls at the Internet and/or in the data center and branch offices. Stateful firewalls are incorporated within NGFWs. Software versions are now available to be deployed within virtual machines. However, appliance-based firewalls will continue to be the dominant platform for some time. Although there have been claims that exclusive use of application control can make stateful firewalls obsolete, Gartner still sees almost every firewall deployment based primarily upon IP address and port.

User Advice: Continue to deploy edge-of-network safeguards, because the perimeter is more important than ever. Consider an NGFW if you are looking to replace or upgrade your stateful-only firewall. Monitor for improvements in NGFWs, and beware of traditional stateful firewalls being labeled as NGFW without substantive improvements.

Business Impact: Stateful firewalls affect all Internet-enabled businesses and, essentially, all enterprises use them.

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Barracuda Networks; Check Point Software Technologies; Cisco; Dell; F5 Networks; Fortinet; Hillstone Networks; HP; Huawei; Juniper Networks; McAfee; Netasq; Palo Alto Networks; Sophos; WatchGuard

Recommended Reading: "Magic Quadrant for Enterprise Network Firewalls"

"Magic Quadrant for Unified Threat Management"

WLAN IPS

Analysis By: John Girard

Definition: Wireless LAN (WLAN) intrusion prevention is the capability to perform continual monitoring, vulnerability assessments and active blocking of wireless attacks. WLAN monitoring also helps to improve network performance and capacity, as well as streamlining diagnostic efforts when users report operational problems with their wireless connections.

Position and Adoption Speed Justification: Rogue, unexpected and unexplained wireless events are not just triggered by hackers. They may also be caused by new or changed wireless technologies, interference from neighboring systems and vulnerabilities created by undefended or misconfigured access points and wirelessly-enabled equipment. Legal scrutiny under rules (such as PCI protection) and ongoing evidence of hacking mean that wireless intrusion prevention capabilities will remain important in the original scope of Wi-Fi and for other technologies that share company airspace, such as 4G/LTE and Near Field Communication (NFC).

WLAN IPS has transitioned from a stand-alone market to become an integral feature of the major WLAN infrastructure vendors. Basic WLAN IPS features are good enough for most typical buyer needs, and buyers typically select the WLAN IPS that comes from their primary infrastructure provider. As of 2014, WLAN IPS has reached the Plateau of Productivity, representing a feature in a mature WLAN infrastructure market.

User Advice: All companies must determine acceptable levels of risk against wireless privacy challenges to their business operations, and conduct interference and performance tuning on all

wireless bands and protocols. IT security planners must keep in mind that compromises of WLANs are still happening and represent serious risks. Operations teams should prepare for new network access control policies and guest networks for bring your own device (BYOD) scenarios, while also continuing to monitor and phase out legacy equipment, weak security protocol choices (such as MAC address inventories), unencrypted guest networks and unsupervised public hot spots. Gartner recommends Wi-Fi Protected Access 2 (WPA2) Enterprise with Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) as the enterprise device access standard. Further advances in other wireless technologies and general concerns about the use of smartphones have carried the scope of WLAN IPS beyond Wi-Fi, with vendors in this market expanding into Bluetooth, mobile phones, wireless cameras, cordless phones and other non-Wi-Fi services. These additional wireless signals can cause interference, expose information, violate usage policies and create an opportunity for WLAN IPS vendors to consider them as a direction for expanding business opportunities.

Business Impact: Wireless networks are essential to IT-enabled businesses, and usage will continue to expand, creating new vulnerabilities and extending old ones. Enterprises must ensure that vulnerability management and intrusion prevention processes are extended to cover wireless and wired networks. WLAN IPS provides the means to manage acceptable risks. Support and compliance demands have increased the importance of WLAN system management capabilities, such as richer audit trails, and the identification and location of interference sources.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

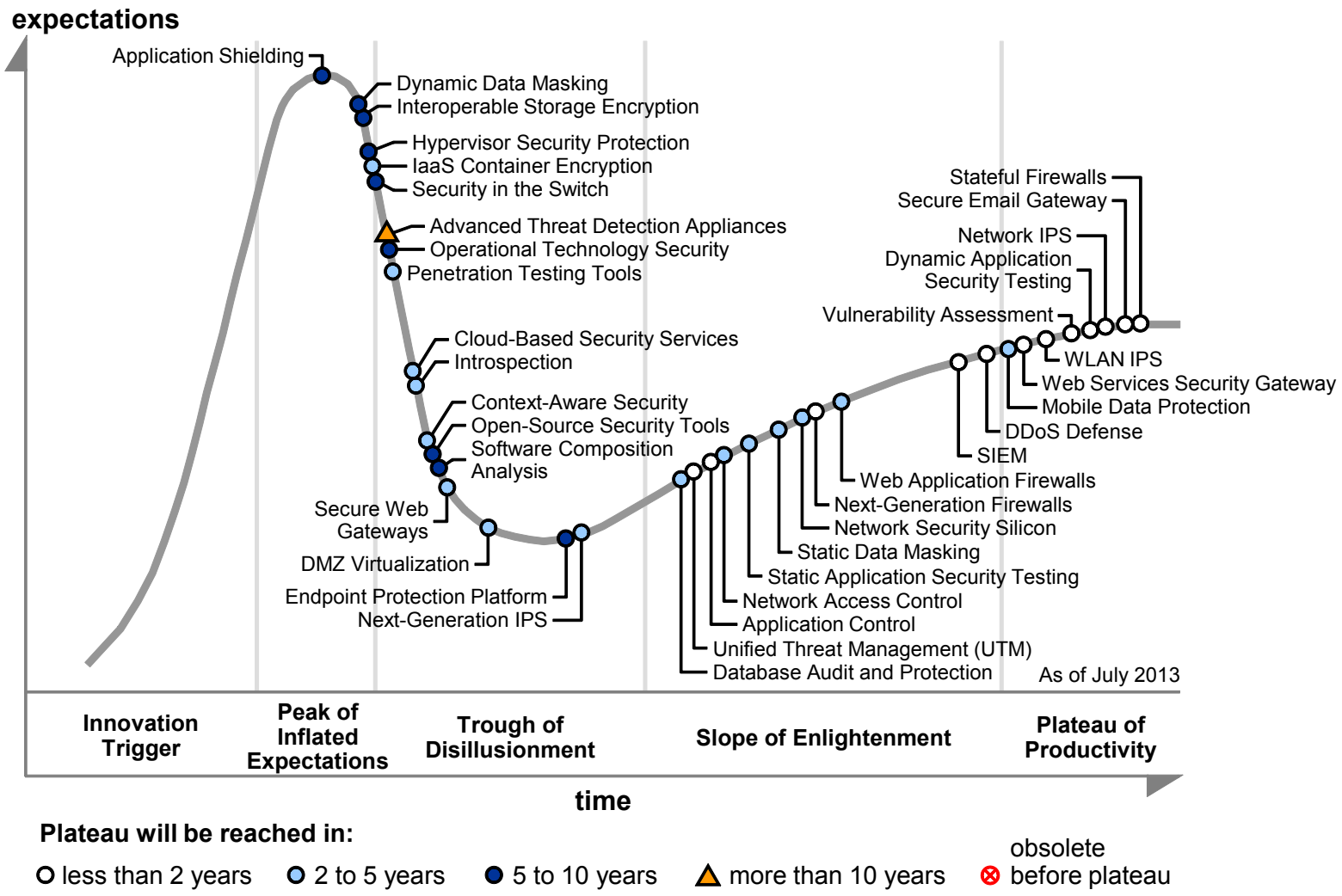
Sample Vendors: AirTight Networks; Aruba Networks; Cisco; Enterasys Networks; Fluke Networks (AirMagnet); Motorola (AirDefense); Xirrus

Recommended Reading: "Magic Quadrant for the Wired and Wireless LAN Access Infrastructure"

"Decision Criteria for Selecting a Wireless Intrusion Prevention System"

Appendixes

Figure 3. Hype Cycle for Infrastructure Protection, 2013



Source: Gartner (July 2013)

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 2014)

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 2014)

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 2014)

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"

"Use Peak Threat Analysis to Balance Security Sustainability"

More on This Topic

This is part of an in-depth collection of research. See the collection:

- Gartner's Hype Cycle Special Report for 2014

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