Gartner

Research

Publication Date: 30 September 2008 **ID Number: G00160731**

Hype Cycle for Data and Application Security, 2008

Jay Heiser, Avivah Litan, L. Frank Kenney, Jeffrey Wheatman, John Girard, Ray Wagner, Eric Ouellet, Joseph Feiman, French Caldwell, Paul E. Proctor, David Furlonger, Greg Young, Neil MacDonald, Ruggero Contu, Mark Nicolett, Gregg Kreizman, Carsten Casper, Kristen Noakes-Fry, Peter Firstbrook

Enterprise boundaries continue to blur as data is shared across the Internet into partner organizations and unmanaged endpoints, increasing concerns about data leakage and manipulation. This is forcing greater attention to security controls within and around applications and data objects.

TABLE OF CONTENTS

LIST OF TABLES

Gartner

LIST OF FIGURES

What You Need to Know

Larger organizations are increasingly pressured to protect their data and applications. Organizations with a mission-critical or highly complex Web presence usually benefit from state-of-the-art security mechanisms to protect their data and Web-enabled applications against increasingly sophisticated attacks. However, targeted malicious software (malware) means that applications within the enterprise are also more at risk of attack, requiring growing levels of attention to reduce vulnerabilities and monitor activities. Regulations, especially those related to fraud control, breach notification and privacy, have increased the expectations that transactions and communications content will be monitored for inappropriate and illegal activity. Customers of software as a service (SaaS) also need to be cognizant of the risks associated with an externally hosted service, and demand that their providers secure and monitor their infrastructure appropriately.

Inexpensive new hardware and a proliferation of Web-based applications are providing a productivity boom for the end user. The flexibility of plug-and-play computing also provides significant opportunities for accidental data leakage and deliberate theft. Although debate continues on the question of whether the staff of partner organizations and outsourcers should be considered less honest than direct employees, it is clearly the case that the greater the separation between the data owner and the data user, the greater the concern about security. Larger amounts of critical information are being accessed on endpoints that are not under the direct control of the organization, leading to growing interest for control technologies that accompany the data to the remote desktop, or provide limits on the amount of information that can move across the organizational perimeter.

The Hype Cycle

This Hype Cycle highlights technologies that are primarily meant to enhance control over information by enhancing access control, application reliability and activity tracking. This ensures that confidentiality requirements are met and reduces the potential for deliberate manipulation of data. The technologies on this Hype Cycle do not directly address availability or continuity requirements, although they reduce the potential for and impact of sabotage.

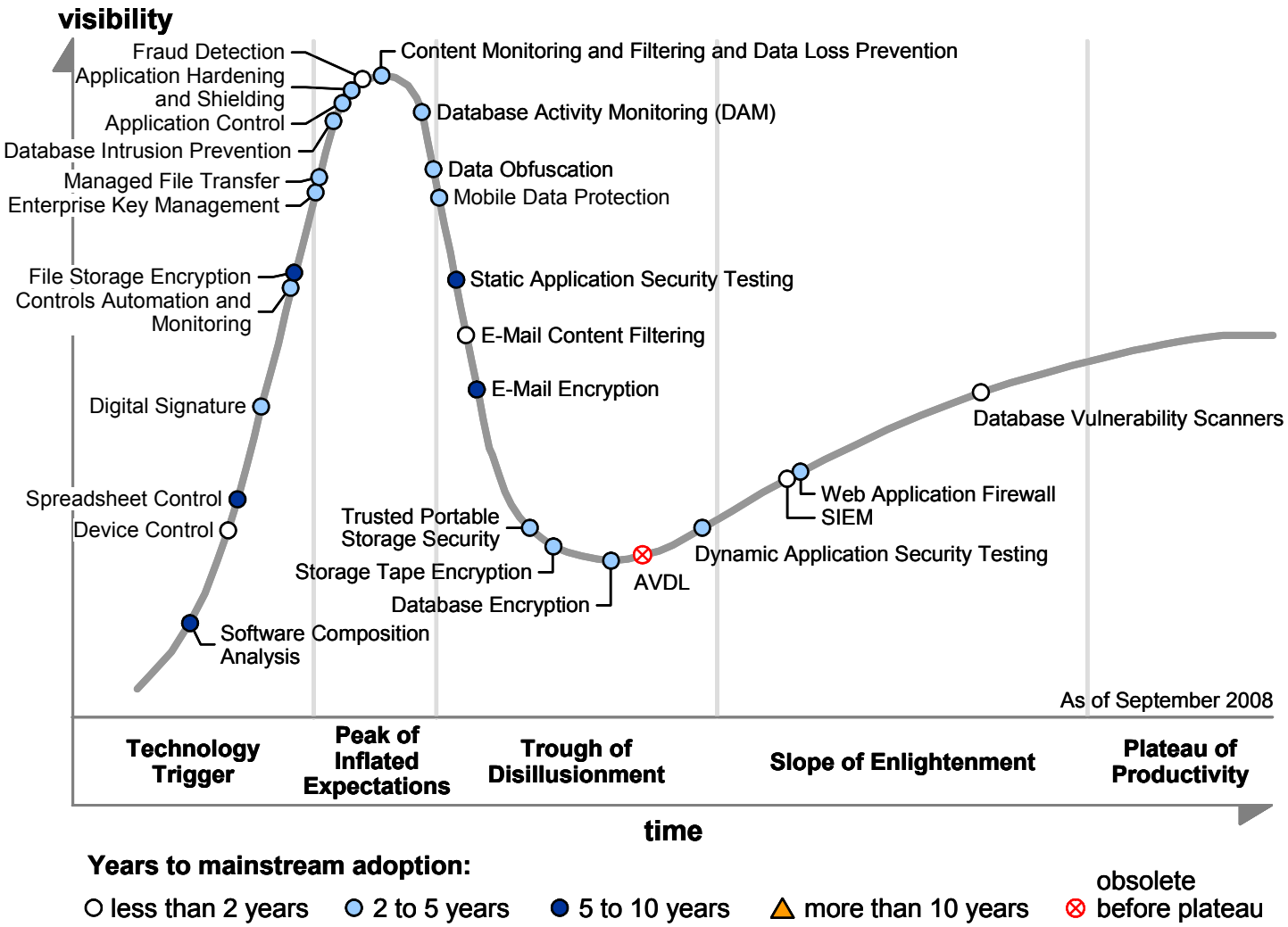
Grouping technology controls into a designation such as "data and application security" distinguishes these products from controls that are based in operating system and content management platforms. Perimeter technologies are included in this Hype Cycle if they have visibility of the data contents.

Most, but not all, the new technology categories in this revision of the Hype Cycle represent the current evolutionary point of technologies that appeared in previous Hype Cycles. In alphabetical order, the following category names are new for this revision:

- Application Control
- Controls Automation and Monitoring
- Dynamic Application Security Testing
- Enterprise Key Management
- File Storage Encryption

- Software Composition Analysis
- Static Application Security Testing
- Storage Tape Encryption

Figure 1. Hype Cycle for Data and Application Security, 2008



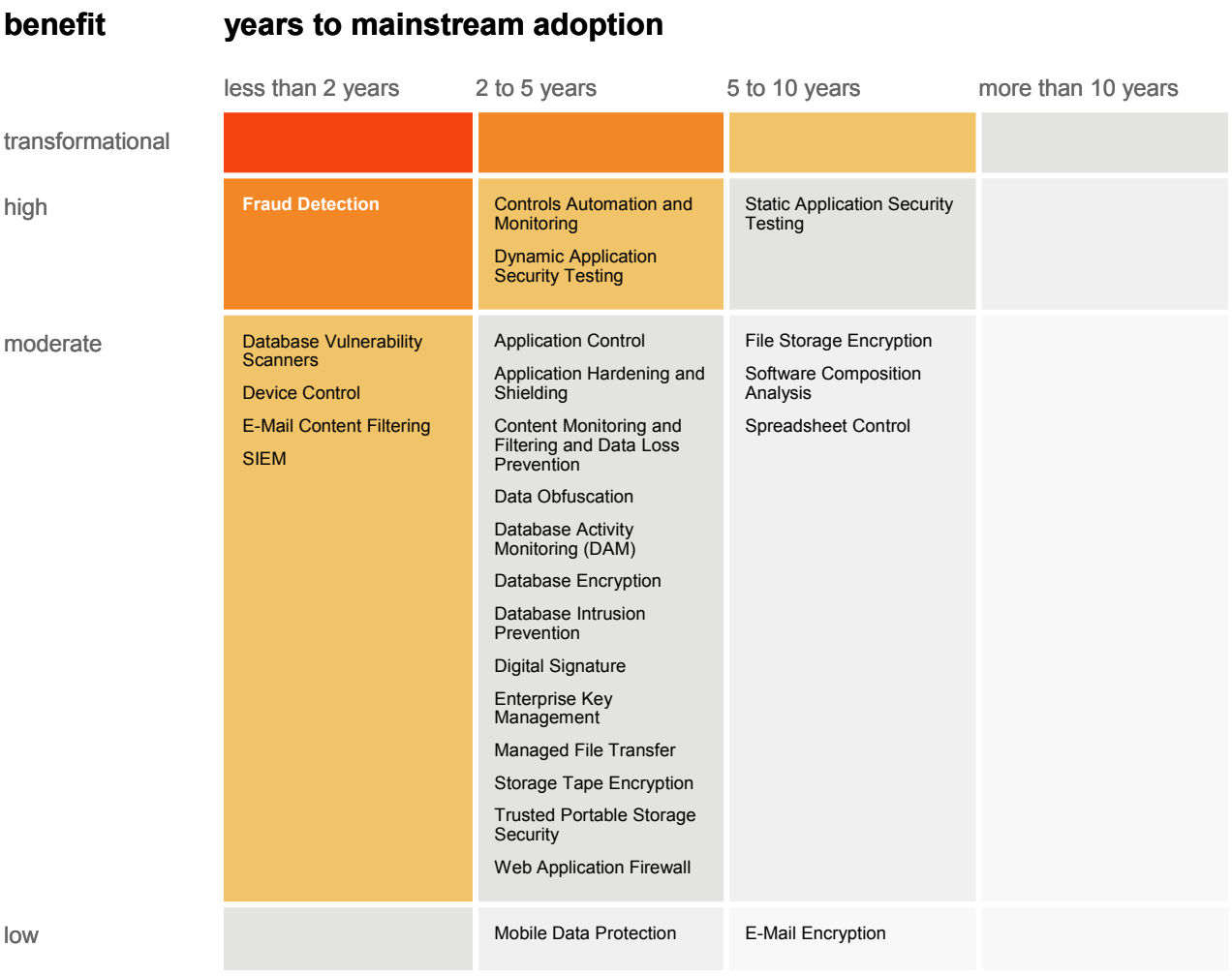
Source: Gartner (September 2008)

Gartner

The Priority Matrix

Although the implementation of these products may help an organization undertake an activity that it would otherwise avoid, the products are not generally considered to provide significant improvements in productivity. Consequently, most are categorized as having only moderate benefit. The products considered highly beneficial are those such as Fraud Detection and Controls Automation and Monitoring, which enable employees to do their jobs without unnecessary limitations, while tracking their activities in the background and alerting or blocking when anomalous or unwanted circumstances occur. Database Activity Monitoring and Data Loss Prevention technologies also provide this sort of functionality, but are a bit less mature. The use of Application Security Testing tools is expected to become relatively common during the next few years.

Figure 2. Priority Matrix for Data and Application Security, 2008



As of September 2008

Source: Gartner (September 2008)

Off The Hype Cycle

None of the categories discussed in previous revisions of this Hype Cycle have completely fallen off of this year's Hype Cycle. However, multiple categories have been renamed, and other categories have been consolidated into broader designations:

- Application Activity Monitoring and Prevention is renamed as Controls Automation and Monitoring.
- Application Scanning is broken out separately into two major subcategories, Dynamic Application Security Testing and Static Application Security Testing.
- Endpoint Activity Monitoring is consolidated into Content Monitoring and Filtering and Data Loss Prevention.
- Data at Rest Key Management is renamed as Enterprise Key Management.
- Data Masking is renamed as Data Obfuscation.
- Distributed Encryption is consolidated into File Storage Encryption.
- Mainframe Tape Encryption is consolidated into Storage Tape Encryption.
- SAN/NAS Encryption (Appliance) is consolidated into File Storage Encryption.
- Storage Tape Encryption (Hardware) is consolidated into Storage Tape Encryption.
- Storage Tape Encryption (Software) is consolidated into Storage Tape Encryption.
- Transaction Anomaly Detection is renamed as Fraud Detection.

This level of change is typical in a rapidly evolving security product market, and we expect to see continued change as existing and new product categories compete to establish their usefulness in a rapidly changing environment.

On the Rise

Software Composition Analysis

Analysis By: Joseph Feiman

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

Software composition analysis does not inspect components internally (that is, it does not conduct components' code analysis), but 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 the outdated and most-recent versions of components, along with their locations on the Web.

Position and Adoption Speed Justification: The simplicity with which developers download software from various Web sites and the ease of searching the Web for pieces of code and components that rapidly solve developers' problems, combined with a widespread negligence in the age of Web 2.0 for software IP rights, have created a culture that does not acknowledge urgency in adopting software composition analysis and the rigor that it will bring. Adopting

software composition analysis also requires establishing an auditing process that goes beyond application development (AD) departments. For these reasons, we expect a relatively slow speed of technology maturity, with software composition analysis reaching the Plateau of Productivity in five to 10 years.

User Advice: Software composition analysis technologies should be used along with static application security testing (SAST) and dynamic application security testing (DAST), since SAST and DAST inspect applications internally, while software composition analysis only classifies known components according to their security, version or IP status.

The use of composition analysis requires the involvement of legal experts in the AD process to review the results of the analysis and to address legal issues stemming from components' IP ownership.

Repositories containing enterprises' software assets (such as version control and configuration/management systems) should be regularly audited by software composition analysis tools 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 software composition analysis tools to inspect components that they plan to use.

Business Impact: Software composition analysis ensures that software components used in applications are up to date, properly licensed and secure.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Black Duck Software; Palamida

Device Control

Analysis By: Ruggero Contu; Jay Heiser

Definition: Device control tools are primarily delivered as software products.They are designed to support a more secure use of portable storage devices (such as Universal Serial Bus [USB] flash drives, portable media players, mobile phones, and flash cards, including the SD card and memory stick and other memory media) by enabling granular control use of these devices.

Granular management allows device use policies to be applied at the individual level or by roles, based on device type, make or interface. Logging and reporting capabilities, through a management console, are also included. Portable device control tools also can enable the enforced encryption of the data being downloaded to a device, and several vendors support data shadowing (keeping an additional copy on the enterprise for backup and investigation support).

Position and Adoption Speed Justification: Portable device control products received a considerable amount of attention at a time when issues of leaking data through USB or FireWire ports were first highlighted. However, similar capabilities are now being incorporated into other types of security products, clouding the future for a stand-alone market in device control. Endpoint security platforms and mobile data protection products typically include device control functionality, and the continued improvement in functionality and practicality of data loss prevention (DLP) products, which use sophisticated content-aware technology to control data in transit, has ensured that the market for portable device control products remains small. The increasing integration of device control functionalities within broader suites may well result in portable device control disappearing as a stand-alone market.

User Advice: Organizations that allow employees or outsiders to access large amounts of regulated or sensitive information need to explicitly assess the risks associated with the leakage of data through the Internet and portable storage devices. A decision should be made as to whether the existing risk of data leakage is acceptable, and if not, an information control plan should be developed that encompasses all channels, both Internet and physical media.

Adoption of stand-alone device control tools is advisable for those organizations with an immediate need to secure use of portable storage devices and/or access to interfaces such as USB or FireWire (Institute of Electrical and Electronics Engineers [IEEE] 1394) ports; however, from this point on, the integration of device control within broader and centrally managed endpoint security platforms will be the ideal approach.

Business Impact: The availability and popularity of inexpensive high-capacity personal devices, and the growing significance of regulation, along with the numerous incidents involving use of storage devices, have encouraged organizations to look for a solution to minimize data leaking through the endpoint.

This technology offers an answer to help control the flow of data between corporate computers and plug-and-play storage devices.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: BeCrypt; CenterTools; Check Point Software Technologies (Reflex Magnetics); ControlGuard; DeviceLock; FrontRange Solutions (Centennial); GFI; GuardianEdge Technologies; Lumension Security; RedCannon; Safend; SanDisk; SkyRecon; Sophos (Centennial)

Recommended Reading: "Market Overview: Portable Storage Device Control Products, Worldwide, 2006"

"Trusted Portable Personality Devices Promote Secure Access"

Spreadsheet Control

Analysis By: David Furlonger; Jay Heiser

Definition: Spreadsheet control is stand-alone software that provides additional controls over the use of spreadsheets without breaking backward compatibility with Excel. All products in this category improve process documentation by providing more-robust change tracking than native Excel. Most products also provide some unique mix of additional functionality, such as workflow, multiuser access to server-based spreadsheets, user roles and granular permissions, or output validation. Increasingly, products in this space also include functionality to locate spreadsheets and even analyze their content, providing reports that can help identify which ones are most important. Vendors are also improving their level of support for other user-developed application (UDA) platforms, such as Microsoft Access.

Position and Adoption Speed Justification: Numerous high-impact losses, both accidental and fraud-related, have occurred because spreadsheets lack the control mechanisms that are taken for granted in enterprise applications. Despite the wide use of business intelligence applications as a reporting front end to enterprise resource planning systems, their tremendous flexibility means that spreadsheets are virtually always on the critical path toward financial reporting. A growing number of companies, currently at least a dozen, offer products intended to reduce the

risks associated with the use of spreadsheets. However, the sense of urgency associated with the control of spreadsheets is still relatively low, and neither IT nor spreadsheet users are widely aware of the potential benefits of these control products. Their use is most prevalent in the pharmaceutical and financial services industries, where U.S. Food and Drug Administration requirements for document validation have forced virtually all laboratories to implement additional Excel controls and where financial services providers are facing increased scrutiny over operational risk and compliance requirements — for example, for the Sarbanes-Oxley Act (SOX). Most publicly held companies are managing user-developed application risk through simple policies on manual workflow and approval. However, auditors are becoming more aggressive in identifying financially material spreadsheets as being highly relevant to SOX. In the U.K., the Financial Services Authority, along with the tax authorities, is putting more pressure on corporations to better manage the risks associated with UDAs. As a result, the expectation that companies should implement more-stringent controls over UDAs is growing slowly but steadily.

User Advice: To ensure that risk is kept within acceptable limits, all midsize and large organizations should develop a written strategy for the use of UDAs. In today's regulatory environment, undocumented ad hoc applications are no longer acceptable, so at a minimum, controls should include processes to identify, track and audit the use of spreadsheets supporting high-risk and regulated activities. If the analysis indicates that uncontrolled spreadsheets represent an unacceptably high level of risk, then some use of third-party compliance products should be part of the overall strategy. Organizations that have not yet started tracking their use of UDAs should also evaluate products that locate them, and analyze links and content. Because these products maintain backward compatibility with Excel, vendor lock-in and product obsolescence are not concerns. Financial institutions and enterprises should note that, while these spreadsheet control products help in "activity tracking" (for example, who changed a spreadsheet and when), most of these products lack the functionality to analyze quality of input data within the spreadsheet. It must be recognized that governance of spreadsheets (or any data) isn't just about what it is, where it is and who touches it. Good governance also requires understanding the need for specifying and maintaining the necessary level of data quality.

Business Impact: Spreadsheet control products are commonly used to aid in tracking, auditing and reporting data that directly impacts the financial statements of the firm. In many cases, this includes the ancillary benefit of improving the efficiency of process in managing large, user-defined sets of information that would otherwise be isolated to individual employee environments. In the U.S. and, increasingly, in other countries, products to supplement Excel have become virtually mandatory in the pharmaceutical and financial services industries. Several years of lessons learned in adding rigor to the reporting of laboratory results can now be productively applied to the creation of controls over financial reporting. Spreadsheet controls are also highly desirable for operational uses of spreadsheets that involve high-value transactions, such as derivative trading, which typically relies heavily on Excel. In all cases, change tracking can be performed with virtually no negative impact on the spreadsheet user, although it may also be necessary to apply workflow or access controls that would reduce user flexibility. However, supplemental technical controls for UDAs have significant potential to prevent multimillion-dollar losses, providing a high level of protection at a relatively low cost.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Cimcon Software; ClusterSeven; Compassoft; Finsbury Solutions; Prodiance

Recommended Reading: "MarketScope for Spreadsheet Control Products, 2008"

"Bank Controls Runaway Use of Microsoft Excel, Improves Risk Management"

"Developing a Strategy to Control Spreadsheets"

"Recognize the Risks of Uncontrolled Spreadsheets"

Digital Signature

Analysis By: Gregg Kreizman; Carsten Casper; Kristen Noakes-Fry

Definition: Digital signature is a specific type of electronic signature (e-signature) that relies on public-key cryptography to support identity authentication and provide record integrity through a pair of mathematically related keys — the public key and the private key. It is used toward a goal of providing irrefutable evidence that a specific digital object originated with a specific individual and has not been altered.

Position and Adoption Speed Justification: Digital signature has been widely anticipated for more than 10 years, but the level of effort to implement a digital signature infrastructure has usually exceeded the benefit. Early projects with e-signature made use of public-key infrastructure (PKI), and involved the private-key (the signing key) generation and placement on users' workstations or on smart tokens. Adding smart tokens improved protection for the private keys but also drove up costs. Many simple commercial e-signature processes avoid the use of digital signature technology. A number of U.S. regulations theoretically indicate a need, or at least an option, for some form of digital signature. Only a few of these regulations, such as the Food and Drug Administration (FDA) 21 Code of Federal Regulations (21 CFR Part 11), have led to a change in corporate practices, and those involve only small numbers of people.

The European Union (EU) Directive 1999/93/EC on e-signature has been in force since 2000, but has not brought the intended uptake due to diverging interpretations of the directive and inconsistent guidance on technical standards from the EU. This has caused differences in national legislation and implementations, such as leading to rather strong technical solutions in Germany and a comparatively pragmatic approach in Italy. This confines investments to national markets, making them even less profitable. In parallel to smart cards issued by banks but not being used for digital signatures, some EU countries such as Belgium and Estonia have started to issue electronic identity cards that also contain keys for use in digital signature applications, but application demand remains low. High-value transactions of citizens occur rarely (buying a house, renewing a passport) and usually justify the effort of a physical presence for a signature, whereas low-value transactions (buying books, filing taxes), which citizens prefer to conduct online, do not justify the cost of a digital signature infrastructure. Auditable business records such as invoices are used by commercial organizations to substantiate their tax returns. EU tax authorities are increasingly concerned that some commercial organizations using electronic invoices will commit tax fraud by manipulating those business records after the fact. Because of these concerns and because business-to-business (B2B) and government-to-business (G2B) invoice applications don't require widespread distribution and management of certificates and private keys on consumer end-point machines, digital signatures will likely and increasingly be used for e-invoice applications to provide record integrity and support transaction non-repudiation.

Overall, the number of pilot projects continues to increase slowly, yet the feasibility of supporting personal signature keys on a widespread consumer use-case basis remains to be proved. Internal enterprise use cases for digital signatures are growing when smart cards or common access cards are being deployed. See Smart Token and Common Access Card profiles/sections in the Identity and Access Management Hype Cycle.

User Advice: Because the signature is based on a protected private key known only to the user, the primary risk to a digital signature is the compromise of the private key. Thus, maintaining the

security of the key should be an essential concern for companies considering this signature solution. Enterprises interested in experimenting with digital signature should look to the EU countries that are providing citizen smart cards and promulgating the use of compliant applications. Tax authorities and e-invoicing applications will also provide proving grounds for digital signatures.

Most benefits attributed to any form of e-signature are really a result of automating a business process, and the signature is a small but important step in the process. When the signature is automated as part of the process, it's important to consider whether you need the same degree of security as you had with "wet" signatures or if you need a much-higher level of security. Many organizations — when the primary motivation is to reduce the expense and delay of obtaining wet signatures for a transaction — may conclude that a cryptographic-based digital signature is not necessary.

Other less-expensive methods of e-signature, such as using a user ID and password, as well as acknowledging a text prompt, may suffice — particularly in applications that require a signature but have low-impact consequences of fraud or repudiation.

Business Impact: E-signatures, including digital signatures, add efficiencies to formerly paper-based processes, enabling them to be put online for business-to-business and business-to-consumer, as well as e-government applications. Cryptographic-based digital signatures add the assurance of making the signature and the document in which it is embedded virtually tamper-proof — enabling organizations to comply with a higher level of security requirements.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Adobe; Algorithmic Research; CIC; Entrust; Gemalto; Giesecke & Devrient; Oberthur Card Systems; OpenTrust; Silanis Technology; VeriSign; Verizon; XYZMO

Recommended Reading: "Electronic Signature Suites and Services Mature"

"A Quick Look at E-Signature Vendors and Products"

"Tutorial: Understanding Electronic and Digital Signatures"

"Case Study: Loan Company Uses E-Signatures to Cut Costs and Save Time"

"IBM-Led Team to Create E-Forms Solution for U.S. Army"

"Time's Running Out to Prove the Value of Government PKI"

"No 'Big Bang': HSPD 12 Smart-Card Implementations Will Be Evolutionary"

Controls Automation and Monitoring

Analysis By: French Caldwell; Paul Proctor

Definition: Controls automation and monitoring tools act proactively to implement controls through business rules or reactively to monitor controls through analysis of processes, transactions and events. Controls automation and monitoring can take many forms and operate at several levels of the enterprise architecture. At the infrastructure level, controls automation and monitoring focuses on configuration management and network access. At the system level, it focuses on identification and access. At the application level, it focuses on segregation of duties and, most recently, on rules governing transactions and behavior.

Position and Adoption Speed Justification: There is a high demand to reduce the amount of labor associated with compliance. These tools automate process controls and their monitoring, particularly as related to financial processes, and as related to automation of the analysis of the proper functioning of IT general computer controls.

Enterprises that have implemented Sarbanes-Oxley (SOX) or SOX-like requirements, whether in response to regulations or as a self-directed initiative, will adopt controls automation and monitoring as a means to improve the reliability of controls and to lower audit costs. For enterprises that must report to the U.S. Securities and Exchange Commission, changes made by the Public Company Accounting Oversight Board in mid-2007 in the SOX internal controls audit standard AS5 strongly encourage controls automation and will accelerate investment to reduce audit costs.

User Advice: One of the more-common solutions for controls automation and monitoring that enterprises acquire is ERP transaction monitoring for segregation of duties violations. Additionally, there are tools called "continuous controls monitoring" that perform analysis of financial transactions and monitor for patterns of behavior. Business rule engines are also used to automate controls, especially when business process management is implemented to standardize and automate critical regulated processes. Other controls automation and monitoring tools analyze changes to configurations, and still others analyze content on the network or on the client as it is created. Consider any of these various categories of tools when there can be considerable savings in labor from automation or improved reliability from continuous monitoring. While many of these tools are represented by other points on this Hype Cycle (for example, separation of duties, content monitoring and filtering, and security information and event management), many are best represented by the description of the business rule engine on the business process management Hype Cycle.

Business Impact: Controls automation and monitoring improve the reliability of controls and potentially reduce the cost of compliance by reducing the labor component of compliance activities. As enterprises automate and standardize more regulated processes, the application of controls automation and monitoring will increase.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: 170 Systems; ACL Services; Approva; Oracle; Oversight Systems; Reliant Solutions; SAP

Recommended Reading: "Best Practices for Role-Based Separation of Duties in ERP"

"Sarbanes-Oxley Update: How to Best Support the CFO"

File Storage Encryption

Analysis By: Eric Ouellet; Jeffrey Wheatman

Definition: File storage encryption is a new technology profile for this Hype Cycle. It is an aggregation of distributed encryption and storage area networks (SANs)/network-attached storage (NAS) encryption technologies. Storage encryption tools are used to encrypt files and folders on server storage and on other shared storage mechanisms, such as SANs, NAS and direct-attached storage (DAS). Implementations enable local encryption, while the centralized management console manages the overall encryption infrastructure. Some of the vendor offerings include solutions that are resident in the network, supporting encryption and decryption

of data "on the fly," transparently, as is it written to and from storage. Typical solutions broadly provide centralized tools for supporting key management, policy definition, distribution and enforcement, and access controls.

Vendors use two different approaches: hardware- and software-based encryption engines. Hardware is more expensive, although faster, sometimes using application-specific integrated circuits (ASICs) as the core of the product. Many of the products have Federal Information Processing Standard certification, which is a good stamp of approval — encryption products need to provide a high degree of certainty that keys won't be compromised.

Position and Adoption Speed Justification: Although these tools have existed for several years, adoption is still limited and slow. There are a small number of vendors in the space, and we've seen some acquisitions over the past 12 to 18 months. However, as the focus on data security increases, we believe that these products will see increased interest and adoption. There is a crossover between these products and the category covered in the Technology Profile of enterprise encryption management. Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and privacy disclosure laws have also resulted in increased interest in encryption and other data protection technologies, which has stoked further interest in this space.

User Advice: Leverage file storage encryption, as needed, as part of your overall encryption strategy. For organizations that are already using point solutions at a variety of endpoints, this is a good capstone to help centralize management and policy development and deployment. This is also a good solution for organizations that are geographically dispersed because it enables a centralized management approach to encryption. For organizations that are using only a small number of encryption products, it might be more beneficial to look at an enterprise encryption management solution.

Business Impact: File storage encryption provides a good, solid, centralized way to protect enterprise data spread across myriad storage platforms and implementations. Additionally, the centralized management of spot encryption solutions, coupled with fairly robust key management, will allow organizations to get a better handle on risk management issues.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Microsoft; NetApp; Protegrity; SafeNet; Voltage Security; Vormetric

At the Peak

Enterprise Key Management

Analysis By: Jeffrey Wheatman; Eric Ouellet

Definition: Enterprise encryption key management solutions are centralized software or network appliances that provide a single point of management for encryption keys in a deployment environment. These tools provide the capability to develop policies for all your encryption products, facilitate key distribution, secure key storage and facilitate key life cycle management. These processes support multiple deployment approaches, but essentially provide a single console to develop a policy set and deploy it across your encryption infrastructure. These tools can handle encryption keys from myriad encryption solutions, including (but not limited to) storage area networks (SANs), network-attached storage (NAS), direct-attached storage (DAS), backup

infrastructure, databases, endpoints and, in some cases, keys for transmission encryption solutions.

Position and Adoption Speed Justification: There has been a lot of movement in this market, and many of the solutions are just beginning to come into their own. The number of supported platforms continues to grow, and integration with other systems continues to get better. We see a fairly significant increase in interest in these products as organizational focus on data security begins to shift away from the historical siloed approach to the more holistic strategy of protecting enterprise data throughout its life cycle.

There will continue to be increased focus on and demand for enterprise key management solutions during the next two to three years. The focus on standard approaches to key generation, key management and overall encryption management solutions will also lead to more-rapid uptake of these products.

Additionally, increased focus on data protection, as a result of legal and regulatory requirements, will continue to remain high on the requirements list for most security departments.

User Advice: Organizations that are currently focused on siloed approaches to encryption would be well served by evaluating enterprise key management solutions. In the midterm to long term, it will be critical to centralize the management of your data protection mechanisms, and key management solutions are critical to the success of that effort.

If you currently have encryption in a variety of areas, then it is important to start evaluating enterprise key management solutions as part of your road map of data protection.

Although these products are definitely improving, we still see some issues with compatibility, centralization and manageability. Therefore, if you don't have a pressing need, then it is advisable to wait until the market settles during the next 12 to 18 months.

Business Impact: Encryption is a critical component of organizations' efforts to protect data from malicious and inadvertent disclosure. The lack of centralized key management has been a hurdle to full implementations. As enterprise key management products continue to mature and improve, clients will be better able to implement an enterprise encryption strategy; thereby protecting data, achieving legal and regulatory compliance, and limiting risk in a significant way, while decreasing costs.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: NetApp; Protegrity; RSA; SafeNet; Vormetric

Managed File Transfer

Analysis By: Frank Kenney

Definition: Managed file transfer (MFT) suites usually are comprised of four discrete functionalities that can be deployed separately but usually are deployed as a suite. The functionalities are:

- Server: Technologies that include the ability to manage all aspects of the file transfer support multiple communication and security protocols and mechanisms, workflow, provisioning, some transformation, application programming interfaces and adapters, and streaming input/output.

- Client: This is a subset of server technologies but mainly is used for tight integration with a server product. Clients are used by applications (via programmatic means) and humans for collaboration, such as large file transfers using e-mail systems.
- Proxy: Technologies used to abstract other elements of the infrastructure, such as a proxy deployed in a demilitarized zone used to conceal the true IP addresses and ports of senders and recipients.
- Plug-in: Technologies that interoperate or integrate with applications, enabling them to communicate natively with MFT servers or enabling ad hoc file transfers.

Position and Adoption Speed Justification: The market for MFT continues to mature but not as fast as vendors' solutions. Although a few vendors strategically have decided to remain niche players, others have decided to continue to benefit solely from established license and maintenance revenue. As the overall market for MFT solutions is growing at a healthy rate, the overall pool of enterprises that need MFT solutions is growing even faster.

For the most part, the largest and most-common competitors are homegrown FTP solutions, which technically are free of charge, however, as many Gartner clients realize, are neither well-managed nor secured without maintenance headaches. The best business-to-business (B2B) gateway technologies have MFT functionality to ensure that they can manage the movement and security of any file or message of any size, regardless of the file or message's need to be transformed, for example, electronic data interchange or XML-based transactions. The adoption of MFT technology is growing as the combination of compliance requirements, partner mandates, modernization initiatives and security concerns increases.

User Advice: Managing file transfers will become a necessity driven by internal and external mandates, increasing requirements for high-performance data integration, compliance initiatives and intellectual-asset protection. Users should look for this functionality to be offered by service-oriented architecture infrastructures, middleware vendors and service providers. When the needs are mostly external, users should consider obtaining MFT technologies from their B2B gateway provider as a unified and centralized gateway; MFT suites are preferable to separate solutions.

Business Impact: Organizations with high-volume data centers will continue to be affected by these technologies but will benefit from added functionality from these technologies. Companies doing multienterprise collaboration will find that MFT becomes more important and will be included in B2B gateway technologies, further consolidating companies' external communications. Companies with even the simplest MFT functionality will find it easier to manage nonrepudiation and audit issues and can start to gain insights into their and their partners' file transfers.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Early mainstream

Sample Vendors: Accellion; Axway; Biscom; Cyber-Ark Software; GlobalSCAPE; Inovis; Ipswitch; Metastorm; nuBridges; Primeur; Proginet; Radiance Technologies; Sterling Commerce; Tumbleweed Communications

Database Intrusion Prevention

Analysis By: Jeffrey Wheatman

Definition: Database (DB) intrusion prevention (IP) tools provide a complementary technology to traditional network and application IP. DB IP tools have visibility into relational database management system (RDBMS) databases and have a deeper understanding of the complex behaviors that take place in them. These tools can be leveraged to block privileged user access, as well as identify and block the abuse of excessive use of privileges, such as a user downloading the entire CRM database.

The tools are implemented as in-line devices or as agents that reside on the DB server host that block malicious activity using a variety of techniques, such as session termination, proactive blocking, command substitution and network resets. In some limited cases, network appliances in passive listening mode can use basic techniques, such as TCP resets, to close down malicious connections; however, this approach is limited in effectiveness.

Blocking is configured based on policies and includes, but is not limited to, blocking SQL injection, the abuse of legitimate privileges and unapproved configuration changes.

Position and Adoption Speed Justification: The move from monitoring to prevention has been slow. Similar to what happened in the network intrusion detection system space, organizations are justifiably concerned about dropping legitimate traffic. Other concerns are related to the performance issues and implications for application architecture. Despite these concerns, and as we also saw on the network side, more organizations are beginning to include blocking or prevention as a "need to have" requirement. Coupled with the maturing intelligence of the tools, we expect an increase in client adoption of prevention technologies.

DB IP tools are often an extension of database activity monitoring (DAM) (see "DAM Technology Provides Monitoring and Analytics With Less Overhead"), although some products have been developed by application firewall vendors as extensions of application layer protection. As a result of increased interest and the various pedigrees of the vendors, long-term DB IP will become a feature rather than remain a stand-alone offering.

User Advice: The implementation of blocking activity that is obviously "bad," such as privileged users accessing confidential data, is advisable; however, implementing prevention across all activity and behavior should be placed on a medium- to long-term road map for data protection. Begin by assessing the access profiles of your data; there will be some activity that is clearly undesirable, such as a DB administrator accessing U.S. Social Security Numbers or credit card numbers, or a customer support representative who suddenly accessed 5,000 records per day when peers access only 100 per day. Organizations with smaller implementations and databases that don't contain significant amounts of highly confidential or proprietary data can and should wait until the prevention tools have matured if prevention is even required or desired.

Care should be taken when implementing blocking for fraud-prevention use cases — applications are getting more complicated, and it is critical to avoid false positives, that is, incorrectly identifying and blocking of traffic that is *not* malicious.

Business Impact: DB IP is a reasonable component of an organization's data protection program. It can also provide some additional protection from the leakage of personally identifiable information (PII), personal healthcare information (PHI) and financial information as part of compliance programs.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Blue Lane Technologies; Guardium; Imperva; Secerno

Recommended Reading: "DAM Technology Provides Monitoring and Analytics With Less Overhead"

Application Control

Analysis By: Neil MacDonald

Definition: Application control solutions are a style of endpoint (desktop and server) protection under the category of host-based intrusion prevention systems. Application control solutions offer varying degrees of control over what an application can do as it interacts with system resources (at its most basic level, whether an application can execute or not), which is sometimes referred to as application whitelisting and blacklisting.

Position and Adoption Speed Justification: In most cases, application control software doesn't replace traditional antivirus and personal firewall offerings. 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. Application control solutions are of interest to information security and operations managers, typically for reducing the chances of image corruption, system damage or data loss by end users, rogue applications or malicious software (malware).

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 configuration vendors, in addition to point solutions. Reducing agents and consoles (as well as cost and complexity) should be weighted in the evaluation.
- When antivirus agents and patching aren't possible, consider application control and system hardening as alternative security controls for point-of-sale terminals, supervisory control and data acquisition systems, and other devices that fall under regulatory requirements.

Business Impact: Operational and security benefits: Application control solutions help to augment deficiencies in the signature-based antivirus model, providing protection against malware variants and targeted attacks. Operationally, application control 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 work spaces in ways that comply with policy. Application control with managed, trusted change provides potentially transformational benefits if antivirus is replaced.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: AppSense; Bit9; Check Point Software Technologies; CoreTrace; Internet Security Systems; Lumension Security; McAfee; Symantec

Recommended Reading: "Application Control Market Update"

"Magic Quadrant for Endpoint Protection Platforms, 2007"

"Application Control Market Update"

Application Hardening and Shielding

Analysis By: Neil MacDonald; Joseph Feiman

Definition: Application hardening and shielding refers to a set of technologies used to add security functionality within applications specifically for the detection and prevention of application-level intrusions. At their most basic level, the technologies include obfuscation technologies to protect the application code as the increasing use of intermediate language representations (such as Java and .NET) enables hackers to easily reverse-engineer intellectual property (IP) embedded in software. More-advanced capabilities include the ability to inject security protection directly into the application without requiring developers to modify the source code. This can be applied proactively (for example, obfuscating the application to protect against and alert for tampering, or implementing the type of input filtering that the developers should have written to protect against exploits) or reactively (injecting protection as a result of a vulnerability discovered in production or performing some predetermined action based on exploitation attempts).

Position and Adoption Speed Justification: Of the various approaches to protecting applications, code obfuscation is more widely adopted and more mature, but estimated adoption rates are still in the single digits because most organizations are unaware of its benefits until they directly experience the theft of intellectual property or an attack from an application compromise. Furthermore, 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. Basic code obfuscation is built into Microsoft's Visual Studio, but the capability is missing from other large software development life cycle platforms. For proactive shielding, no widely accepted standard for converting vulnerability knowledge into application shields exists, although some vendors have developed proprietary links.

User Advice: Consider application hardening as a way of proactively inserting security protection into externally facing applications, especially more-mature obfuscation approaches for the protection of IP in an organization's software-based assets. If vulnerabilities are present in production applications, then application-level shielding may provide an alternative for proactively inserting security protection to protect vulnerable applications while waiting for the vulnerabilities to be addressed in development.

Business Impact: Application hardening and shielding provide protection for an organization's software-based assets (especially those placed on machines, sites and locations that the organization doesn't control) from tampering, reverse engineering and attack. They also provide several types of application-level security without requiring developers to natively modify source code.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Arxan; Cloakware; Fortify Software; PreEmptive Solutions; V.i. Laboratories

Recommended Reading: "Cool Vendors in Infrastructure Protection, 2007"

Fraud Detection

Analysis By: Avivah Litan

Definition: Fraud detection (formally called "transaction anomaly detection") refers to an application security tool that compares the behavior of an incoming user transaction with what's expected from a continuously updated user profile and/or from rules on "acceptable" behavior. The analysis typically gathers information and characteristics from a user session, and analyzes the device and its location, user navigation and/or user transactions. Suspect transactions are flagged for follow-up — for example, reauthentication of a user, electronic signing of a transaction, manual investigation or transaction blocking. The most-effective fraud detection systems examine user behavior and transactions across channels (such as stores, PCs and phones) and accounts.

Position and Adoption Speed Justification: Tools have matured, and the industry has consolidated — several large, disparate technology providers have acquired small fraud detection firms that specialize in online fraud prevention. However, the market still has to mature, so that enterprises trying to defend themselves against fraud can deploy cross-channel, cross-account fraud detection systems, rather than just focus on single-channel solutions that are isolated from one another.

Financial institutions are interested in these tools, but many of them are reluctant to spend a lot of money on the tools, because their fraud-related losses don't always justify the expenditures. However, as the rate of cross-channel and cross-account attacks escalates, so does interest and willingness to spend money on fraud detection.

User Advice:

- Implement a comprehensive enterprise strategy to manage fraud across channels and accounts.
- Put a high priority on easy-to-use cross-channel and cross-account data analytics, and enterprise case management. If you can't see the fraud, you can't stop it.
- The use of multiple vendors and best-of-breed point solutions is often necessary, but integrate, through weighting and blending, their scores and results in an umbrella fraud management system that feeds into an enterprise case management tool.
- Once actions have been taken as a result of casework and analysis, automatically feed the results and the lessons learned back to the legacy systems from which the fraud originated.

Business Impact: Most organizations that suffer from fraud don't even know the extent of their losses. Fraudulent activity is often "stuffed under the covers" and/or misrepresented as accounts that "went bad" due to unforeseen circumstances, such as borrower default, that are really fraud in disguise. The crooks are moving across enterprises, accounts, channels and consumer desktops, and are socially engineering their way through processes used by customer service representatives. Merely implementing point solutions to combat fraud won't work anymore; stopping fraud in one area will simply move it to the next. That's been most recently proved in Europe, with the rollout of Chip-and-PIN payment (credit/debit) cards at the point of sale, after which more fraud quickly migrated to the e-commerce channel.

Fraud detection and customer authentication must work across multiple channels, functions and other customer touchpoints, and that often means integrating multiple best-of-breed products. Priority should be given to analytics and enterprise case management, so fraud analysts can effectively manage and stop fraudulent activities. Lessons learned from past fraud should be applied to legacy systems that touch customers and sensitive data.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Actimize; Entrust; Memento; Norkom Technologies; RSA Security; Senactive

Recommended Reading: "Critical Capabilities for Enterprise Fraud Management Tools"

"Fraud Detection and Customer Authentication Market Overview"

Content Monitoring and Filtering and Data Loss Prevention

Analysis By: Eric Ouellet; Jay Heiser

Definition: Gartner defines content monitoring and filtering (CMF)/data loss prevention (DLP) solutions as the set of content-aware tools used to prevent inadvertent or accidental leaks or exposure of sensitive enterprise information outside authorized channels using monitoring, filtering, blocking and remediation features. DLP technologies include hardware and software solutions that are deployed at the endpoint (desktop and servers), at the network boundary and within the enterprise for data discovery purposes, and they perform deep content inspection using sophisticated detection techniques that extend beyond simple keyword matching (for example, advanced regular expressions, partial document matching, Bayesian analysis and machine learning). DLP products maintain detailed logs that can be used to support investigations.

Position and Adoption Speed Justification: This market continues to experience rapid growth, but Gartner still considers it to be in its "adolescent" phase. The market's total value was an estimated $50 million in 2006 and $120 million in 2007. Gartner believes it will reach $200 million to $250 million in 2008. A key factor in the ongoing maturation of solution and technology offerings has continued to be the infusion of significant amounts of venture capital into relatively small vendors in 2006 and 2007. Many of these vendors have fewer than 100 employees and received funding in the $30 million to $40 million range. During 2006 through 2007, several of these vendors were acquired by incumbent security players (including Symantec, McAfee, Trend Micro, Websense, RSA and Raytheon) with solid positions in the larger security market. We expect further consolidation through 2008 with the remaining independents.

A key driver of this market continues to be the need to address regulatory requirements, including those of the Payment Card Industry (PCI) Initiative and the U.S. Health Insurance Portability and Accountability Act (HIPAA), among other compliance requirements. Another form of market maturation is the increasing appearance of DLP functionality within products such as e-mail security boundary, endpoint monitoring solutions and planned offerings around enterprise digital rights management (EDRM).

User Advice: This technology is commonly perceived as being an effective way of preventing theft of intellectual property and for preventing accidental disclosure of regulated information. In practice, it has proved much more useful in helping identify and correct faulty business processes and accidental disclosures. The inadvertent data leakage actually represents the lion's share of the problem, so these automated controls are proving useful. However, motivated insiders will always find ways to steal data, and no technology will ever be able to fully control this. As the technology matures, network-only mechanisms will evolve to a more comprehensive model that also addresses host protection. However, only the network components are mature enough for enterprise use today.

Business Impact: This technology is not foolproof, and it is relatively easy for a smart attacker to circumvent, but it effectively addresses the 80% of leakage that is due to accidents and ignorance. Organizations with realistic expectations are finding that this technology does indeed meet their expectations and significantly reduces nondeliberate outflows of sensitive data.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Fidelis Security Systems; Orchestria; Reconnex; Tablus; Vericept; Vontu; Websense

Recommended Reading: "Content Monitoring and Filtering Helps Find Faulty Business Process, Accidental Disclosures"

"Market Trends: Content Monitoring and Filtering and Data Loss Prevention, Worldwide, 2008"

"Develop an Enterprise Strategy for Content Monitoring and Filtering/Data Loss Prevention"

"Tips for Midsize Businesses Considering Data Leakage Prevention"

Database Activity Monitoring (DAM)

Analysis By: Jeffrey Wheatman

Definition: Database activity monitoring (DAM) is a type of governance, risk and compliance control that transparently monitors database activity to identify fraudulent, illegal or other undesirable behavior. DAM monitors and analyzes database activity. It operates independently of the database management system (DBMS) audit functionality, or as an extension of it. DAM contains embedded knowledge about database structures and provides analytics and reporting. There are two primary use-cases for DAM: monitoring of privileged users (for example, database administrators [DBAs] and root or system administrators), who, by nature of their permissions, have the ability to read and update all data in the DBMS. DBAs also can modify database structures using data definition language, and can manage access controls using data control language. DAM is used to identify and, in some cases, prevent privileged users from accessing data, making modifications to schema or table structure, or creating or modifying user accounts or permissions. Application user monitoring focuses primarily on database access that results from transaction activity from the end users and applications that connect to the database. The primary purpose of this monitoring is to detect fraud and other abuses of legitimate access privileges. Some auditors and security teams are evaluating or implementing DAM technologies to fulfill legal and regulatory requirements, enhance overall risk management, and achieve data governance goals.

Position and Adoption Speed Justification: Auditors are increasingly requiring tighter controls around data stores to preserve the confidentiality and integrity of data, while limiting access by privileged users and identifying fraudulent activities. Preventative controls, such as encryption, are not effective against authorized user threats. DAM, as a real-time detective control, provides a "last stop" that can be helpful in closing the gaps arising despite the use of preventative controls, such as identity and access management and encryption. DAM is still a young market, with much opportunity for growth. Gartner saw close to 100% growth, year over year, in 2007, and we expect similar growth through 2008. There has been some consolidation in the market, with Symantec dropping its DAM product and the acquisition of IPLocks by Fortinet. Although some DAM products come from vendors with a wide variety of offerings, most of the vendors are focused on database and application security. The relatively young age of the market has resulted in rapid change, and the addition of product functions and high levels of responsiveness to customer requests and requirements. Increased interest has been spurred by increased focus on legal and regulatory compliance needs. DAM products are improving and adding new functionality at a rapid pace; on average, we are seeing incremental upgrades quarterly and full upgrades every nine months. Some of the extended functions are dynamic and static discovery of

data types (for example, credit card numbers or Social Security numbers), tight integration with security information and event management (SIEM), and vulnerability scanning, as well as future data-loss-prevention-type functions.

Several SIEM vendors, including NitroSecurity and netForensics, have added DAM capabilities to their offerings.

User Advice: Although some clients use native DBMS auditing, there are limitations and constraints to its efficiency and effectiveness:

- Native logging can add significant overhead to the database server CPU.
- A lack of granularity in capturing and reporting makes it more difficult to extract relevant data.
- Clients with heterogeneous environments need to manage multiple logging and reporting platforms.

Clients should:

- Implement DAM functionality to mitigate the high levels of risk resulting from database vulnerabilities and to address audit findings in areas such as database segregation of duties and change management.
- Use DAM technology when there is a need for granular monitoring, or when the overhead of database audit functions is unacceptable.
- Consider SIEM as a valid option in cases where native logging overhead falls within acceptable limits

As with any technology, there are always caveats. Although there have been a few large implementations, enterprises with large installed bases should take a cautious approach and focus on a pilot group of servers to iron out any issues. Pay careful attention to using the "blocking" or prevention functions; application-database interaction can be complicated, and great care must be taken to avoid blocking of what may prove to be false positives. Support for certain database and operating system platforms is sometimes incomplete or partial; assemble a full requirements list before talking to vendors, and recognize that your enterprise might need to wait on certain platform support.

Business Impact: Although DAM has not reached its full potential, it is a worthwhile investment for clients with databases containing confidential data, intellectual property, or any data that must be protected according to legal and regulatory requirements. DAM will continue to grow in maturity, function and usability.

In addition to helping clients with compliance, DAM is a beneficial addition to risk management programs. Many installations start small and grow rapidly over time as enterprises see increased value and benefit from their investments.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Application Security; Fortinet; Guardium; Imperva; Lumigent; MENTISoftware; Oracle; Secerno; Sentrigo; Tizor

Recommended Reading: "DAM Technology Provides Monitoring and Analytics With Less Overhead"

Data Obfuscation

Analysis By: Joseph Feiman

Definition: Data obfuscation is a set of techniques to prevent the abuse of sensitive data by hiding it from users. Technology vendors offer multiple data obfuscation techniques, such as replacing some fields with similar-looking characters, replacing characters with masking characters (for example, with "X"), replacing real last names with fictional last names and reshuffling data in the columns. Data obfuscation is also known as data masking, data privacy, data sanitization, data scrambling and data de-identification.

Position and Adoption Speed Justification: Data obfuscation is a variation of an old technique: data integration or data transformation, when a dataset is transformed into a set with a different format (that is, some fields are dropped, merged or inserted). Therefore, when the need for data obfuscation became acute, it did not take vendors long to come up with solutions that were relatively mature.

Data obfuscation is a reasonable security precaution that an enterprise might take on its own initiative. These days, it is also recommended by rule bodies and regulators — for example, by the Payment Card Industry group and the Health Insurance Portability and Accountability Act (HIPAA) to protect clients of the credit card and healthcare industries, respectively.

For all these reasons, we expect a relatively high speed of technology maturity for data obfuscation, reaching the Plateau of Productivity within a five-year time frame.

User Advice: Enterprises should use data obfuscation for limiting users' access to sensitive data.

Data obfuscation can be static or dynamic. Potential abusers, whom static data obfuscation aims to deter, are mainly users of test databases (programmers, testers and database administrators). Static obfuscation hides a test database with sensitive data obfuscated in advance from these users. Dynamic (or real-time) data obfuscation hides data in, typically, production databases from users such as client service personnel of credit card call centers. Currently, static obfuscation is more mature, more broadly adopted and offered by more vendors.

Data obfuscation 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 that the application that runs against obfuscated data performs as if this obfuscated data is real (for example, data obfuscation must not limit developers' capability to adequately test applications).

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 not only exposed to abuse or negligence from (mainly) enterprise employees, but also from outsiders. Adopting data obfuscation will help enterprises raise the level of security and privacy assurance against insiders' and outsiders' abuses. At the same time, data obfuscation will make enterprises compliant with the security and privacy standards recommended by regulating/auditing organizations.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Applimation; Camouflage; Compuware; Direct Computer Resources; IBM; MENTISoftware; Oracle

Recommended Reading: "Data Obfuscation (Masking, Privacy, Scrambling): Many Names for the Same Technique"

"Testing Times for HR Systems and EU Data Protection Law"

Sliding Into the Trough

Mobile Data Protection

Analysis By: John Girard; Ray Wagner

Definition: Mobile data protection employs software- and/or hardware-based encryption of stored enterprise data in files, folders, partitions and drives on mobile systems, including laptops, PDAs and smartphones. Systems may be company-owned or supplied by an employee or contractor. Note that workstation versions of these products may also be used on nonmobile systems, such as desktops and servers.

Position and Adoption Speed Justification: Sales of mobile data protection tools grow strongly year over year. Disillusionment over product complexity and usability can't pull this topic into the Trough of Disillusionment because public paranoia caused by continuing stories of high-profile data leakage keep this topic fresh in terms of hype and drive a steady stream of Gartner inquiries. Privacy laws are raising corporate alarms and causing more implementations to move forward, primarily on notebook computers. However, even though the baseline technologies are mainstream, and the market contains many long-term players, a large percentage of companies still have not implemented encryption at all or have only implemented it partially, believing that they can identify a few systems containing sensitive data. Anticipation over embedded "free" protections, such as BitLocker, have actually halted installations when migrations stall or are incomplete. Large numbers of smartphones and PDAs go unprotected because of the reduced concern for "small" devices and the higher proportional cost to add security to devices that have acquisition costs far below PCs. The growing influx of noncompany devices brought by employees and contractors constantly adds new gaps, increases risks for data leakage and erodes the percentage of protected systems used in business, even as sales march forward.

Factors that will help move this topic to productivity in five years have been set in place through hardware innovations as well as acquisitions. Encryption engines in processors and other hardware subsystems will become standard issue in a few years, complemented by secure key repositories, such as the Trusted Platform Module. Acquisitions by larger endpoint protection (EPP) vendors (Check Point Software Technologies acquired Pointsec, McAfee acquired SafeBoot, and Sophos is bidding to acquire Utimaco Safeware) will reduce the barriers to widespread deployment. EPP vendors have larger support organizations, a "single console" view for all endpoint security policies and will be forced to reduce seat prices to keep data protection costs in line with the discounts offered for endpoint antivirus, anti-spyware, firewalling and intrusion prevention systems.

User Advice: The loss or theft of mobile devices is the largest data exposure risk that companies face; 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 — mobile or not, large or small. Products should be thoroughly trialed before adoption — look for lean products with good performance and the ability to take advantage of embedded hardware (if present).

Business Impact: The business value for data protection can seem low because encryption doesn't contribute directly to productivity. However, the value of data protection in terms of avoiding the costs of embarrassment, lost business deals and reputation, as well as legal and civil penalties, is significant and can be appraised in the many stories of companies that have been forced to disclose and recover from data-leakage events.

Benefit Rating: Low

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

Sample Vendors: Check Point Software Technologies; Credant Technologies; GuardianEdge Technologies; McAfee; PGP; Utimaco Safeware; WinMagic

Recommended Reading: "How to Avoid Mobile Data Protection Failures"

"Implementation Advice for Mobile Data Protection"

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, byte code 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. Enterprises are beginning to understand the importance of application security vulnerability detection, which is creating market demand for static and dynamic testing tools. Balancing false positives and false negatives within static analysis is an issue — too many false positives will consume development resources and will frustrate developers. Because of the development process and cultural changes required to incorporate these tools, it will take more than five years before SAST technologies plateau.

User Advice: Ideally, application vulnerability detection would be conducted continuously during the entire software development life cycle. As happened with dynamic application security testing (DAST) tools, enterprises acquiring SAST technologies should expect substantial market and product consolidation within the next 18 months; therefore, vendor selection should be tactical. Enterprises that lack application security skills and resources should be considering an emerging opportunity to purchase application security scanning as a service. For initial deployments, enterprises should fine-tune the tools so that development resources can be focused first on high-confidence, high-severity vulnerabilities. For outsourced code development, organizations should require vendors to perform similar testing as part of the contract negotiation process. In addition, organizations should perform their own testing as part of the acceptance process of any outsourced application.

Business Impact: The most critical impact of using SAST is minimizing the risk of possible exploitation of application vulnerabilities. Adopting this technology 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. Catching vulnerabilities earlier saves money, but this must be balanced against the process and cultural changes

necessary in development, and must balance false positives and false negatives. In the longer term, another source of cost savings will come from the automation of security testing.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Coverity; Fortify Software; HP; Klocwork; Ounce Labs; Veracode

Recommended Reading: "Market Definition and Vendor Selection Criteria for Source Code Security Testing Tools"

"Static Application Security Testing: Vendors and Products, Part 1"

"Static Application Security Testing: Vendors and Products, Part 2"

"Static Application Security Testing: Vendors and Products, Part 3"

E-Mail Content Filtering

Analysis By: Peter Firstbrook; Eric Ouellet

Definition: E-mail content filtering or data leak prevention (DLP) involves inspecting outbound corporate e-mail for corporate and regulatory compliance and leak prevention. Effective solutions will include contextual keyword analysis, intellectual property fingerprinting, Boolean operators and formatted wildcard detection. They will also include general and industry-specific lexicons and preformulated policies for common regulations and corporate compliance. Flagged message actions (in other words, encrypt, block, delete, archive and forward) and delegated workflow for flagged messages are also critical requirements.

Position and Adoption Speed Justification: Corporations are only gradually identifying the need and experimenting with available solutions. Initial experiments with immature software are likely to lead to the Trough of Disillusionment. Not until organizations have clear business goals in mind will this technology reach the Plateau of Productivity. Also, confusion and conflict between leak prevention and broader compliance tools will hamper implementation. E-mail tools will have to expand to Web communications media — such as instant messaging, chat, Web mail and blog posting — or risk becoming silos of policy. Longer-term integration with enterprise DLP tools will be necessary for more-advanced DLP requirements.

User Advice: Users should develop a plan for managing compliance and leak prevention across all networks and communications media. Start small with the high-impact and probable business risks first and gradually expand as you gain confidence in using tools and procedures. The use of enterprise DLP tools should be considered for complex data definitions, workflows and policies.

Business Impact: Businesses seeking to reduce the risk of unfettered dissemination of intellectual property, or corporate and government compliance must invest in e-mail content filtering and encryption.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: BorderWare Technologies; Clearswift; IronPort Systems; Marshal; Proofpoint; Secure Computing

Recommended Reading: "Magic Quadrant for E-Mail Security Boundaries"

"How to Select Secure E-Mail Gateway Functionality"

E-Mail Encryption

Analysis By: Eric Ouellet; Jay Heiser

Definition: E-mail encryption solutions protect the confidentiality and/or the selected integrity of e-mail message traffic by using one of three models: desktop-to-desktop, gateway-to-gateway and gateway-to-desktop protection. Several different standards and proprietary solutions are commonly used, including Secure Multipurpose Internet Messaging Extensions (S/MIME), Pretty Good Privacy (PGP), Identity-Based Encryption (IBE) and Secure Sockets Layer/Transport Layer Security (SSL/TLS).

Position and Adoption Speed Justification: Despite the proliferation of standards and solutions, the stand-alone market remains small in terms of revenue and the number of enterprise installations. Although inclusion of e-mail encryption as a feature of secure e-mail boundary products increases the number of organizations that can apply it, even when the capability is available, fewer than 5% of end users in an enterprise apply encryption to person-to-person e-mails. Companies continue to struggle with the business justification and the impact on the end users involved, even with growing concerns about the protection of personally identifiable information and Payment Card Industry requirements. Solutions continue to be perceived as difficult and expensive to deploy, and are used only when absolutely required. Although the benefits are well understood, the impact on business processes remains unacceptably high. The anticipated complexity of managing groups, policies and keys, and the basic challenge of actually knowing which e-mail needs encryption, discourage widespread use of this technology. Although an approach that automatically applies encryption when needed, based on the content, seems to offer the best compromise between security and convenience, today's enterprise data loss prevention (DLP) tools can only awkwardly be integrated with e-mail, and single-channel E-mail content filtering/DLP is not yet widely deployed or used. Desktop-to-desktop encrypted e-mail cannot be searched, which can interfere with e-discovery requests, and can also complicate restoration.

Market demand is mainly for gateway-based solutions, in which no client-side software is required. On a volume basis, the dominant method is to use SSL/TLS for sensitive information, such as banking and brokerage statements, and health-related messages for consumer application. The adoption of TLS for gateway encryption with business partners is also increasing, and TLS is typically simple to administer.

User Advice: Before selecting a vendor or product, determine the specific business reason for e-mail encryption deployment, the specific groups of users expected to use it and its likely impact on them. Remember that desktop-to-desktop encrypted e-mail can create compliance and e-discovery issues that require key escrow techniques to recover encrypted messages.

Vendors in this market do not target different types of recipients (for example, internal users, consumers or business partners) equally well, and you'll need to ensure that your company's requirements align with the vendor's feature set and architecture.

There are multiple ways to protect messaging traffic, and alternatives should be considered. For occasional use, tools to encrypt data separately and manually attach it to e-mail messages are undeniably inexpensive, and skilled users can also take advantage of PGP or S/MIME capabilities integrated into their local e-mail clients. For organizations seeking a more comprehensive solution to multiple security problems, encryption as a feature in a secure e-mail boundary solution that also includes e-mail content filtering is an appealing option. Finally,

gateway- based TLS is low cost, and completely transparent to the end user, although it is only applicable between partner organizations that regularly exchange sensitive information.

Business Impact: Failure to provide e-mail encryption will increase the risk of information disclosure, and will potentially increase the risk of noncompliance with government and industry regulations. In a few cases, the implementation of e-mail encryption can provide a productivity increase by enabling the use of e-mail to support sensitive communication that otherwise wouldn't take place, or would use a more cumbersome mechanism.

Benefit Rating: Low

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Entrust; IronPort Systems; PGP; Secure Computing; Tumbleweed Communications; Voltage Security; ZixCorp

Recommended Reading: "Magic Quadrant for E-Mail Encryption, 2007"

"Enhanced Vendor Commentary on the 2007 E-Mail Encryption Magic Quadrant"

"Standard Feature Requirements for E-Mail Encryption Deployments"

"Enhanced Feature Requirements for E-Mail Encryption Deployments"

"Differentiators of Leading Secure E-Mail Architectures"

Trusted Portable Storage Security

Analysis By: John Girard; Ray Wagner

Definition: Trusted portable storage security is a self-contained, portable, removable data storage system with built-in access controls and encryption intended to enforce security policies and standards for data access, typically offered with a Universal Serial Bus (USB) interface.

Position and Adoption Speed Justification: Trusted portable storage security solutions have been implemented as stand-alone products by several visible flash drive vendors and as software extensions to generic media by most vendors in the mobile data protection Magic Quadrant. Buyers are concerned with extra cost and complexity to use, how to limit access to only approved work scenarios, how to enforce policy and data expiration, how to recover access logs, and about ability to "plug in." (For example, is a USB port available to accept a trusted portable security solution built into a flash drive? Will the workstation and operating system allow it to launch?)

User Advice: Consider this technology if users will have predictable access to workstations, and those workstations will be able to support flash drives with executable security utilities. Addition of a synchronization and/or backup process is advisable because USB drives are easily lost.

Business Impact: This technology reduces data leakage on offline portable storage, and it promotes secure, auditable sharing of data between two parties. Public concern and legal penalties for data leakage are still on the increase, so prevention of private data loss and avoidance of negative publicity are strong drivers for market adoption.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: BeCrypt; Credant Technologies; Giritech; GuardianEdge Technologies; PGP; RedCannon Security; Route1

Storage Tape Encryption

Analysis By: Jeffrey Wheatman; Eric Ouellet

Definition: Storage tape encryption refers to technologies that reduce the risk of data leakage through backup media. There are four basic approaches to encrypting your backup data:

- **Native tape drive encryption.** Some storage vendors offer encryption and basic key management in their latest offerings, such as the encryption offered with LTO4, IBM TS1120, Sun StorageTek T10 and T9840D drives.
- **Encryption bundled with backup software.** Many backup software vendors offer the option of native data encryption.
- **Third-party encryption appliances.** These are available in configurations supporting in-line devices designed for backup tape encryption.
- **Switch-fabric-based encryption.** These have begun to be incorporated into offerings by network and storage vendors.

Position and Adoption Speed Justification: Although the actual risk associated with losing data resulting from loss of backup tapes is somewhat overstated, there are significant risks associated with the requirement to report potential losses of personally identifiable information (PII), protected health information (PHI) and financial information. Gartner's experience has indicated a trend toward the adoption of enterprise encryption infrastructures, rather than the historical siloed approach (that is, discrete products were implemented to encrypt data on different platforms and in different formats). However, there is still often a need, largely as a result of compliance, for short-term solutions to the problems associated with data leaving client environments on unprotected backup tapes. Over time, backup encryption products will be integrated in an overall encryption framework. Although the technologies have improved and matured, we still see issues with key management and the inability to manage cross-platform encryption tools.

User Advice: If your organization is currently found deficient by auditors regarding the protection of data in your backup infrastructure, then it is advisable to look at solutions in this space. If you do make investments in this area, then it is important to focus on future requirements and benefits of an overall data protection program that will include enterprise encryption and key management. Look at products that are Federal Information Processing Standard (FIPS)-compliant, provide strong crypto, and enable future integration with other encryption and key management products. For organizations that are not being hit with audit findings in this area, that are already using encryption in other areas in their environment (such as databases and file systems) or that don't see an immediate need to implement backup encryption, it will be beneficial to wait for the enterprise encryption market to mature and stabilize further during the next 12 to 18 months.

Business Impact: Backup encryption provides significant benefit from a regulatory perspective; if you lose your tapes and they are encrypted, then there is no need to report them as a loss. There is also some inherent benefit in protecting all data that leaves your site. That said, Gartner recommends protecting data closer to its source, wherever possible; this makes it easier to manage your access controls, protect the data that puts your organization most at risk and map controls to business requirements. Overall, protecting backup data should be part of an overall data protection strategy, as a stand-alone solution or, ideally, as part of an overall data encryption framework.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Brocade; Cisco; IBM; NetApp; SafeNet; Sun StorageTek; Symantec; Vormetric

Database Encryption

Analysis By: Eric Ouellet

Definition: Database encryption software is used to protect data within relational database management systems (RDBMSs) at the table or column levels.

Position and Adoption Speed Justification: This technology has been available for some years, but has been plagued with performance and technical problems. Current products work well on databases designed initially with provisions for the support of encryption functionality integration, but can be difficult to implement on legacy systems. Use of encryption on certain fields results in a fundamental level of impact, altering the behavior and usability of the RDBMS when indexing or performing wild-card searches. Existing offerings require significant schema changes to support encryption. Portability of encrypted fields from one application to another remains difficult under most scenarios, as does centralized key management. Export of large encrypted datasets to third-party partners for external processing remains problematic. RDBMS vendors are improving native encryption capabilities, but most continue to fail in protecting data from database administrators. Third-party vendors will be seriously challenged if RDBMS vendors resolve this problem.

User Advice: Despite the difficulty involved, enterprises should plan to encrypt all credit card numbers, Social Security numbers, bank account numbers and other information that is deemed sensitive in databases within two to three years. Begin planning, testing and integrating cryptographic functions in projects today, even though they may take two to three years to complete due to internal political sensitivity, application testing, and workflow or database use modifications.

Business Impact: Arguably, encryption offers the most certain form of control against unauthorized access to data. Consequently, concerns about privacy, and especially payment card industry standards, are putting pressure on enterprises to make greater use of cryptographic mechanisms to protect person-related information. Although it remains difficult to implement and use, database encryption is increasingly perceived as desirable and even mandatory. Enterprises with a business need to demonstrate the highest level of practice in the protection of personal data will have no alternative to the use of database encryption software.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Application Security; IBM; Ingrian; Microsoft; NetLib; Oracle; Protegrity; Valyd; Yantra

Recommended Reading: "When and How to Use Database Encryption"

AVDL

Analysis By: Neil MacDonald

Definition: Application Vulnerability Description Language (AVDL) is a largely defunct, XML-based standard for the exchange of application vulnerabilities between vulnerability assessment tools and other products, typically shielding tools, such as application firewalls, that could proactively shield the application from the vulnerability. Although AVDL has stalled, the concept of application vulnerability shielding is quite useful and is increasingly being provided using proprietary links between Web application scanning and Web application firewall vendors.

Position and Adoption Speed Justification: Although AVDL was adopted as a standard in 2004 by the Organization for the Advancement of Structured Information Standards (OASIS) and has been implemented in a small number of products, the move to AVDL 2.0 has stalled and is stuck in the Trough of Disillusionment. The AVDL committee was officially closed by OASIS in January 2006. The need for the proactive shielding of application-level vulnerabilities is increasing, and a successor to AVDL (or continued proprietary links) will likely move forward and become mainstream during the next five to 10 years. Recently, several vendors have linked their security testing tools to application firewalls using proprietary links, but with the same end result as AVDL — linking the knowledge of application vulnerabilities gained from security testing to proactively shield vulnerable applications until their source code can be fixed or patches applied.

User Advice: AVDL has stalled because enterprises aren't demanding it and because vendors would rather remain proprietary. As enterprises evaluate products that scan applications for vulnerabilities, they should request specific information on how these vulnerabilities can be proactively shielded from attack using technologies such as Web application firewalls, and whether AVDL is supported for the communication of this vulnerability information. In any static or dynamic application security testing evaluation, ask the vendor if it has any links to use the vulnerability knowledge to create real-time shields until the vulnerability can be addressed. This is especially true of binary analysis tools where one of the drivers is the lack of availability of source code. The risk of false positives is a concern, so organizations must press vendors on how "high-fidelity" real-time shields are created and tested.

Business Impact: Ideally, the vulnerabilities in the application would be removed from the application itself by fixing the source code. However, this isn't always possible. Going back and fixing applications in development takes time and isn't possible if the organization doesn't have access to the original source code. AVDL would enable the exchange of vulnerability knowledge among systems for the purpose of proactively shielding vulnerable applications.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Barracuda Networks; F5; HP; WhiteHat Security

Recommended Reading: "MarketScope for Web Application Security Vulnerability Scanners, 2006"

"An Introduction to Web Application Firewalls"

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 Web-enabled applications; however, some solutions are designed specifically for protocol and data malformation.

Position and Adoption Speed Justification: Enterprises are beginning to understand the importance of static and dynamic application security vulnerability detection, which is creating market demand in both categories. Adoption of DAST solutions, primarily in the form of Web application testing tools, has been rapid for a few reasons:

- Testing doesn't require access to source code and can be performed by security, audit or compliance teams.
- DAST tools can help automate penetration testing, which many organizations already perform.
- An immediate risk must be addressed regarding already-deployed, external-facing, Web-enabled applications.

The speed of adoption will accelerate because of a pressing need to resolve the collision of two trends:

- The growing exposure of e-business applications on the Web
- The relentless attacks on those applications

The plateau of technology productivity will be reached in two to five years.

This market is undergoing significant changes:

- Integration of static analysis and application scanning features into a single product
- Vendor mergers and acquisitions, as software life cycle (SLC) vendors provide capabilities for security vulnerability testing as an integral part of the entire SLC

User Advice: Continuous attacks on Web applications have demonstrated not only the strength and relentlessness of attackers, but also the security vulnerability of Web applications. Therefore, DAST technologies should be in the toolboxes of every enterprise's IT and security departments. Application vulnerability detection should be conducted continuously throughout the entire SLC, but for DAST testing we recommend starting in the quality assurance (QA) and testing phase. Enterprises that lack application security skills and resources should be considering an emerging opportunity to purchase application security scanning as a service. They should focus first on externally facing, business-critical applications, but shouldn't overlook the threat from internal hackers on business-critical applications. Enterprises that modernize their legacy applications should implement DAST to raise security assurance of their newly Web-enabled legacies.

Business Impact: The latest payment card industry (PCI) specification requires the security testing of applications or adoption of a Web application firewall, so adoption of DAST solutions fulfills this requirement. Adopting these scanning 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, significant cost reduction will be realized when scanners are embedded in software life cycle platforms, thus enabling vulnerability detection during the earlier stages of the life cycle. In the longer term, another source of cost savings will come from the automation of security testing. The most critical effect of using DAST is minimizing risk of possible exploitation of application vulnerabilities.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Acunetix; Cenzic; Codenomicon; HP; IBM; Mu Security; NT Objectives; WhiteHat Security

Recommended Reading: "MarketScope for Web Application Security Vulnerability Scanners, 2006"

Climbing the Slope

SIEM

Analysis By: Mark Nicolett

Definition: Security information and event management (SIEM) technology provides two main capabilities. Security event management (SEM) analyzes security event data in real time (for threat management, primarily in network events). Security information management (SIM) analyzes and reports on log data (for privileged user and resource access monitoring and compliance reporting, primarily in host and application events).

Position and Adoption Speed Justification: Early adoption of the technology was limited to very large companies, and the focus was SEM. Many smaller companies are now adopting this technology. Application of the technology is trending more toward the SIM use case, driven by regulatory compliance reporting requirements and the rise in targeted attacks.

User Advice: Product selection decisions should be driven by organization-specific requirements in areas such as the relative importance of SIM versus SEM capabilities, speed of deployment requirements, acquisition cost and the IT organization's support capabilities, and integration with established system and application infrastructures.

Business Impact: SEM helps IT security operations personnel be more effective in responding to external and internal threats. SIM provides reporting and analysis of data to support regulatory compliance initiatives, internal threat management and security policy compliance management.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: ArcSight; CA; Cisco; eIQnetworks; ExaProtect; High Tower; IBM; Intellitactics; LogLogic; LogRhythm; netForensics; NetIQ; NitroSecurity; Novell; OpenService; Prism Microsystems; Q1 Labs; Quest Software; RSA (EMC); SenSage; Symantec; Tenable Network Security; TriGeo

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

"Critical Capabilities for Security Information and Event Management Technology, 2008"

"Select the Right Monitoring and Fraud Detection Technology"

Web Application Firewall

Analysis By: Greg Young

Definition: A Web application firewall (WAF) is a shielding safeguard intended to protect applications accessed via HTTP and HTTPS against attack. WAFs focus primarily on Web server protection at Layer 7 — the application layer — but they may include safeguards against other known forms of attack. These tools do not typically protect against unpatched vulnerabilities in commercial products, which is the domain of network- and host-based intrusion prevention systems (IPSs). Instead, they focus on classes of "self-inflicted" vulnerabilities in configured commercial applications or in custom-developed code that make Web applications subject to attacks, such as cross-site scripting, directory traversal and forced URL browsing. A WAF operates as a shield, and does not "fix" the underlying vulnerability, although developers can use WAF reporting as a guide to what requires remediation. WAFs are most often deployed in front of Web servers, usually in the data center.

Position and Adoption Speed Justification: WAF capabilities are available as a feature in most leading application delivery controllers (ADCs). The market will remain small for the pure-play WAFs, because ADC use is growing rapidly; however, some increase is due to compliance with the Payment Card Industry (PCI) standard for companies handling credit card information. Pure-play placements are suitable where an ADC is not deployed.

User Advice: The best way to secure Web applications is to ensure that they have no vulnerabilities before enabling them to be run on production. Look first to deploy WAFs in established ADCs; however, 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.

Business Impact: WAFs provide specific protection for data center servers.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Barracuda Networks; Breach Security; Check Point Software Technologies; Cisco Systems; Citrix; Deny All; F5 Networks; Fortify Software; Imperva; Microsoft; Protegrity; Radware

Recommended Reading: "An Introduction to Web Application Firewalls"

Database Vulnerability Scanners

Analysis By: Jeffrey Wheatman

Definition: Database vulnerability scanners are software-based tools that probe relational database management systems (RDBMSs) to identify known vulnerabilities, common misconfigurations and other technical vulnerabilities. They function in a manner similar to network vulnerability scanners; however, they have a much deeper understanding of the inner workings of databases and, therefore, are capable of finding many vulnerabilities that a traditional network scanner will not.

Some of these tools will also integrate with database activity monitoring (DAM), change and configuration management systems, or security event and information management (SEIM) as part of a comprehensive threat and vulnerability management program.

Position and Adoption Speed Justification: The scanning tools are relatively mature and leverage common techniques for scalability, flexibility and manageability. As a result of legal and regulatory compliance requirements, we have seen an increase in the use of these tools. Several vendors in the DAM space have indicated an increased focus on vulnerability scanning as an

easier-to-implement solution and as an enhancement to their monitoring solutions. We also expect that some network-vulnerability scanners will begin to add functionality to their tools that will enable them to go deeper into the RDBMS.

User Advice: Implement a database-specific vulnerability scanner if your organization's database management systems (DBMSs) are used as repositories for data that has significant value, such as confidential/proprietary information, intellectual property, personally identifiable information (PII), personal healthcare information (PHI) or financial data. Implementing database scanners can also have a positive impact on compliance programs as a result of the increase in the size and use of DBMSs for highly confidential privacy and financial data. Organizations should also consider using database vulnerability scanners to supplement change and configuration management programs — these scanners can enhance operational controls for maintaining system integrity and minimizing configuration drift in production systems. Some organizations will be satisfied with the typical results from a traditional network vulnerability-scanning tool.

Business Impact: Database vulnerability scanners can help augment organizations' vulnerability management programs. Additionally, organizations with legal and regulatory compliance requirements to protect the contents of database stores should also leverage database vulnerability scanners as part of their compliance programs. All these benefits can reduce the costs associated with manual efforts.

Benefit Rating: Moderate

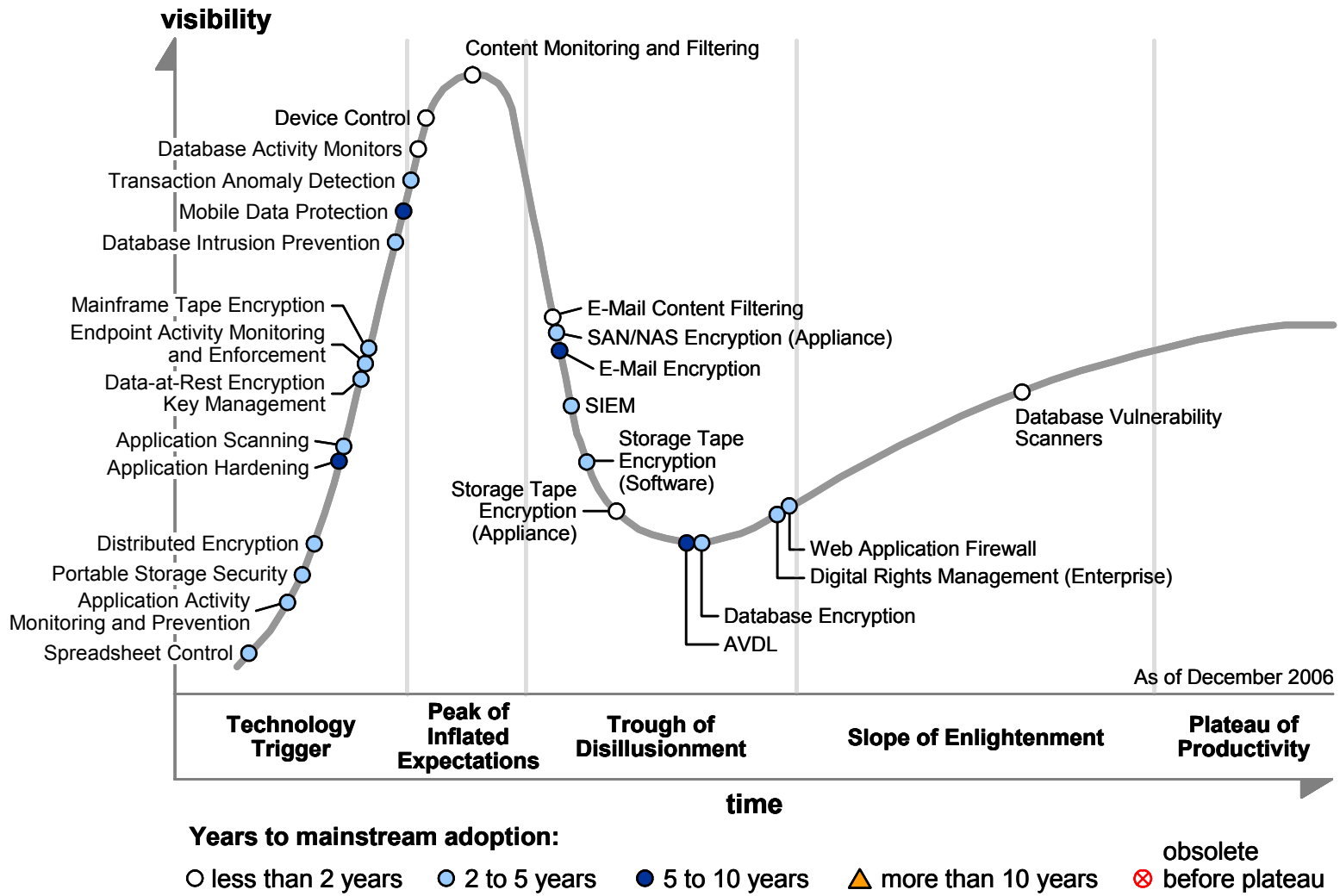
Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Application Security; Fortinet; Imperva; Lumigent; NextGen

Appendixes

Figure 3. Hype Cycle for Data Security, 2006



Source: Gartner (December 2006)

Gartner

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

Phase	Definition
Technology 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 (September 2008)

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

Benefit Rating	Definition
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (September 2008)

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 (September 2008)

RECOMMENDED READING

"Understanding Gartner's Hype Cycles, 2008"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner