

Magic Quadrant for Security Information and Event Management, 1Q07

Mark Nicolett, Kelly M. Kavanagh

Security information and event management functional requirements are rapidly changing as the technology is adopted broadly to solve compliance and security gaps. Ease of deployment and support and the ability to analyze more detail over a longer period have become key.

WHAT YOU NEED TO KNOW

The security information and event management (SIEM) market is now driven by a broader set of buyers who need the technology to quickly address audit issues but who also want to improve security monitoring capabilities. A solution that is optimal for the current market will support real-time collection and analysis of log data from host systems, security devices and network devices; will support long-term storage and reporting; will not require extensive customization; and will be easy to support and maintain. This year's SIEM Magic Quadrant evaluation model has changed from last year in response to these market changes. Ease of deployment and support and log management functions are now weighted more heavily than in previous years.

Gartner has defined evaluation criteria for a broad set of SIEM functions, but the SIEM market is composed of vendors with products that either are optimized for specific use cases or are relatively broad and complex. A product that can address many use cases is likely to be more expensive to deploy and maintain than a product that is optimized for a specific set of functions. Therefore, organizations may need to evaluate offerings from vendors in all quadrants, depending on their requirements. Product selection decisions should be driven by organization-specific requirements in areas such as the relative importance of security information management (SIM) and security event management (SEM) capabilities, ease and speed of deployment, the IT organization's support capabilities, and integration with existing network, security and infrastructure management applications. Vendor viability is also an important consideration. The SIEM market consolidation will continue. Although strong demand exists for less-expensive, targeted capabilities, point solution vendors will face growing competition from the offerings of large vendors as they mature their SEM solutions for compliance-driven use cases. During 2007, we also expect some large vendors that have expensive and complex offerings to announce or introduce simpler and less-expensive deployment options.

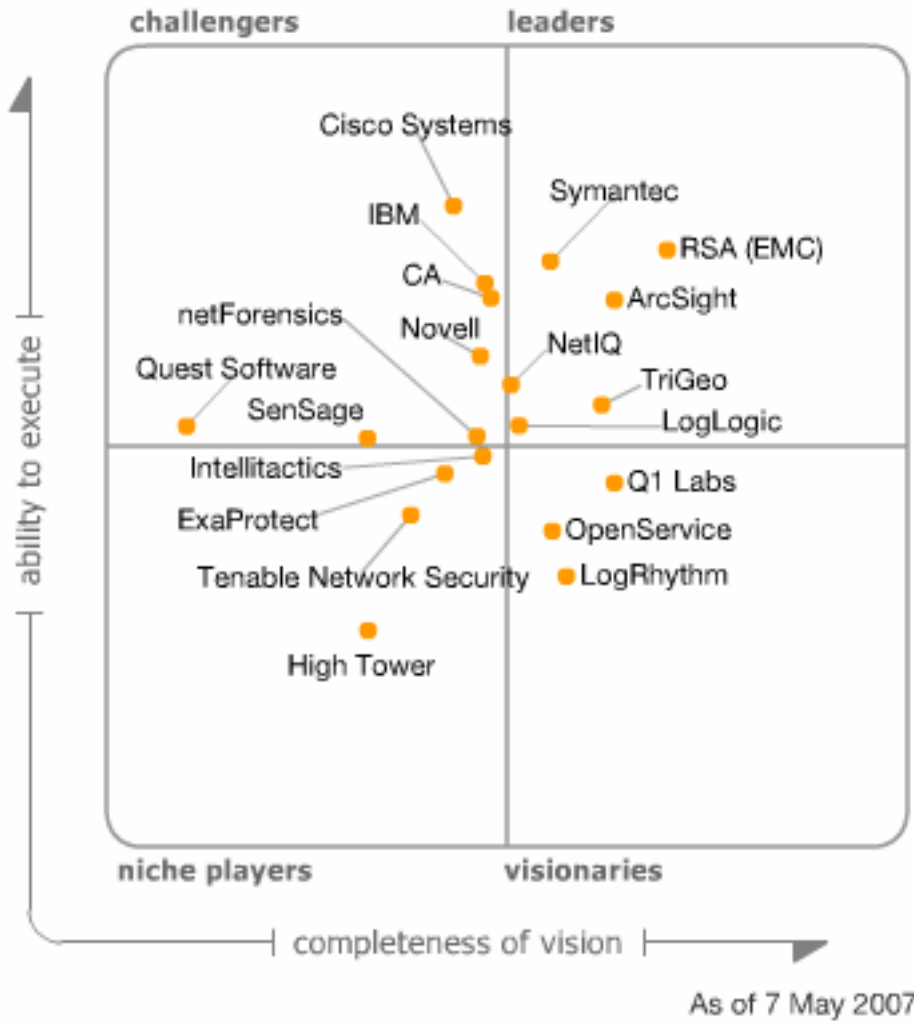
A few common use cases have surfaced in our analysis, which can help organizations pick the best product for their needs. These use cases are intended to highlight groups of vendors that are typically evaluated by a client with a specific deployment focus. Some vendors appear under multiple use cases:

- Use Case 1 — Collect and analyze all log data and basic event management: LogLogic, LogRhythm and SenSage. (Note: ArcSight, netForensics and Intellitactics also have recently introduced log management offerings.)
- Use Case 2 — Collect and analyze all log data with full-function event management: RSA (the security division of EMC), Symantec and Q1 Labs.
- Use Case 3 — Simple deployment and support: LogLogic, TriGeo, OpenService, LogRhythm and High Tower.
- Use Case 4 — Full-featured SIEM products designed to deliver a broad set of capabilities, including security operations center console functions for large, complex environments: ArcSight, ExaProtect, Novell, Intellitactics, netForensics, CA Security Command Center (SCC) and IBM Tivoli Security Operations Manager (TSOM).
- Use Case 5 — SIEM integrated with network behavior analysis (NBA): Cisco Systems and Q1 Labs. Tenable Network Security also offers some NBA functionality.
- Use Case 6 — User- and access-oriented analysis: CA, IBM (Insight), NetIQ, SenSage, Quest Software and Novell.

- Use Case 7 — SIEM products that are integrated with an incumbent vendor's vulnerability management and systems management products: CA, IBM, NetIQ, Symantec, Tenable and OpenService.

MAGIC QUADRANT

Figure 1. Magic Quadrant for Security Information and Event Management, 1Q07



Source: Gartner (May 2007)

Market Overview

The SIEM market is undergoing a rapid transformation that is caused by three factors: the emergence of user and access monitoring as the primary customer problem to be solved; demand for the technology from a broader set of customers; and the availability of the technology from large vendors that also sell related products or services.

Changing Customer Requirements — The Rise of SIM and Log Management and New Buyers

The primary driver of the SIEM market is now regulatory compliance. Security organizations typically have funding for the technology because there is an audit gap, but there is also the realization that the technology should be deployed to improve responsiveness to an external attack and to improve the ability to sense an internal breach. Initial deployment of SIEM technology is now focused primarily on user activity and resource access monitoring for host systems, but real-time event management for network security remains a common requirement. Log management functions are becoming a more important customer requirement because of the following factors:

- A lack of guidance on what needs to be captured for the regulatory compliance use case (creating a need to collect, store and index more log data)
- A mandated (or perceived) need to store the detail for a long period
- The usefulness of detailed and historical log data analysis for breach investigation and general forensics

Vendors that provide log management (for example, LogLogic and LogRhythm) are growing rapidly; others (such as ArcSight and Symantec) have recently introduced enhancements to existing function in this area. Intellitactics and netForensics announced log management extensions to their products in April. Many vendors have development initiatives under way and are expected to announce log management extensions during 2007. The compliance driver also has changed the buyer profile, which is now extended to organizations that have smaller security staffs and more-limited system support capabilities. For these buyers, pre-defined function and ease of deployment and support is valued over advanced function and extensive customization.

Changing Vendor Landscape — The Rise of Large and Broad Vendors

The way that SIEM products are sold is also changing because of the continuing acquisition of SIEM point solution technology by large vendors with broad product portfolios and because of the integration of SIEM technology with other portions of a large vendor's portfolio. An increasing percentage of SIEM technology purchase decisions are noncompetitive because the technology is sold by a large vendor as an adjunct to related security or network technology. IBM (acquired Consul), Novell (acquired e-Security), and EMC (acquired RSA Security and Network Intelligence) are integrating their acquisitions with related identity and access management (IAM) offerings and will sell their SIEM solution as part of an IAM-related deal. CA has been executing on a similar strategy for the past two years (see "Security and Identity Management Auditing Converge"). CA, IBM and NetIQ are also integrating their SIEM technology with related systems management functions, such as configuration management and configuration management database (CMDB). Symantec sells SIEM to large enterprises that use its endpoint security products. Cisco positions its Monitoring, Analysis and Response System (MARS) as a centralized monitoring and automation platform for its self-defending network, and the majority of Cisco MARS sales is a part of an equipment acquisition.

In addition to the 20 vendors evaluated, a number of other companies' solutions have SIEM capabilities but do not fully meet inclusion criteria. AdventNet provides software solutions that are simple, easy to deploy and primarily oriented to small and midsize businesses. However, the software products are limited in areas such as correlation and report customization. NitroSecurity is just entering the SIEM space with a product that utilizes its core data storage and analysis

technologies. Splunk provides event collection and search technology, and some customers use it to solve problem sets that are also addressed by SIEM vendors. Prism Microsystems provides host-oriented log management and event monitoring software to midsize businesses for IT operations and security use. The vendor sometimes competes with CA Audit, Quest InTrust or NetIQ Security Manager.

Market Definition/Description

The SIEM market is driven by customer needs to analyze security event data in real time (for threat management, primarily focused on network events) and to analyze and report on log data (for security policy compliance monitoring, primarily focused on host and application events). SIM provides reporting and analysis of data primarily from host systems and applications, and secondarily from security devices — to support security policy compliance management, internal threat management and regulatory compliance initiatives. SIM supports the monitoring and incident management activities of the IT security organization, and supports the reporting needs of the internal audit and compliance organizations. SEM improves security incident response capabilities. SEM processes near-real-time data from security devices, network devices and systems to provide real-time event management for security operations. SEM helps IT security operations personnel be more effective in responding to external and internal threats.

Inclusion and Exclusion Criteria

The following criteria must be met for vendors to be included in the SIEM Magic Quadrant:

- The product must provide both SIM and SEM capabilities.
- The product must support data capture from heterogeneous data sources.
- The vendor must appear on the SIEM product evaluation lists of end-user organizations.
- The vendor must have production reference accounts relevant to Gartner end-user clients.
- The solution must be delivered to the customer environment as a product.

Vendors are excluded if:

- The vendor provides SIEM functions that are oriented exclusively to data from its own products.
- The vendor positions its product as a SIEM offering, but the product does not appear in competitive shortlists of end-user organizations.
- The solution is delivered exclusively as a managed service.

Added

The current Magic Quadrant adds evaluations for the following vendors:

- LogRhythm
- ExaProtect
- High Tower
- RSA (EMC)

Dropped

The current Magic Quadrant removes evaluations for the following vendors:

- Consul — Acquired by IBM.
- eIQnetworks — Gartner could not validate production reference accounts relevant to Gartner end-user clients.
- Network Intelligence — Acquired by EMC.

Evaluation Criteria

Ability to Execute

Product/Service evaluates current product function in areas such as SIM, SEM, log management, incident management, workflow and remediation support, and reporting capabilities.

Viability includes an assessment of the overall organization's financial health, the financial and practical success of the overall company and the likelihood of the business unit to continue to invest in the product. The competitive environment is changing as more SIEM point solution vendors are acquired by larger vendors.

Sales Execution/Pricing evaluates the technology providers' success in the SIEM market and its capabilities in pre-sales activities. This includes SIEM revenue and the installed base, pricing, pre-sales support and the overall effectiveness of the sales channel. The level of interest from Gartner clients is also considered.

Market Responsiveness and Track Record evaluates the match of the SIEM offering to the functional requirements stated by buyers at acquisition time and the vendor's track record in delivering new function when it is needed by the market. Also considered is how the vendor differentiates its offerings from those of its major competitors.

Customer Experience is an evaluation of product function or service within production environments. The evaluation includes ease of deployment, operation, administration, stability, scalability and vendor support capabilities. This criterion is assessed by conducting qualitative interviews of vendor-provided reference customers and also uses feedback from Gartner clients that are currently using or have completed competitive evaluations of the SIEM offering.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	high
Sales Execution/Pricing	high
Market Responsiveness and Track Record	high
Marketing Execution	no rating
Customer Experience	high
Operations	no rating

Source: Gartner

Completeness of Vision

Market Understanding evaluates the ability of the technology provider to understand buyers' needs and translate these needs into products and services. SIEM vendors that show the highest degree of market understanding are adapting to customer requirements in areas such as log management, simplified implementation and support, and compliance reporting, while also meeting SEM requirements.

Sales Strategy evaluates the vendors' use of direct and indirect sales, marketing, service, and communications affiliates to extend the scope and depth of market reach.

An **Offering (Product) Strategy** is the vendors' approach to product development and delivery that emphasizes functionality and feature set as they map to current requirements for both SIM and SEM. Development plans during the next 12 to 18 months are also evaluated.

Innovation evaluates the vendors' development and delivery of SIEM technology that is differentiated from the competition in a way that uniquely solves critical customer requirements.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	high
Marketing Strategy	high
Sales Strategy	high
Offering (Product) Strategy	high
Business Model	no rating
Vertical/Industry Strategy	no rating
Innovation	high
Geographic Strategy	no rating

Source: Gartner

Leaders

EMC folded Network Intelligence into its RSA security division when it acquired the company in September 2006. The enVision appliance provides a combination of SEM, SIM and log management function that is easy to deploy. RSA (EMC) is also developing the technology as the common audit platform across EMC storage and RSA security products, and there is existing integration with EMC storage technologies.

Symantec's Security Information Manager appliance provides SIM and SEM capabilities, and the recent release of version 4.5 implements a design change that enables log management functions. During 2006, Symantec delivered the pre-defined reporting and correlation rules that the initial offering lacked, and it has rapidly achieved a large installed base by transitioning its SIEM software customers. The technology supports large-scale production deployments that collect all data from network security and host sources for real-time event management and compliance reporting.

ArcSight continues to be the most visible SIEM point solution vendor. ArcSight's function-rich Enterprise Security Management (ESM) software is oriented to large-scale SEM-focused deployments, but the vendor is developing sales channels and implementing product simplifications to address the broader market. ArcSight has recently augmented its complex ESM

technology with ArcSight Logger, a log management appliance that can be deployed "stand alone" or in combination with ESM.

LogLogic has established itself as the primary provider of log management functions to the SIEM market, and its presence has affected many other SIEM vendors. The company positions its appliance technology as a log management solution that provides data analysis and real-time alerting to both IT security and IT operations. During the past year, an increasing percentage of organizations have placed log management requirements ahead of SEM, and LogLogic sales have accelerated. The appliance is sometimes installed as a data collection and analysis tier in conjunction with another SIEM product because of its limited SEM capabilities.

NetIQ's Security Manager has a large installed base that is primarily oriented to SIM, user activity monitoring and compliance reporting. The software is easy to deploy for host log monitoring, and NetIQ also provides an optional log management and archive component. The technology can be used for network and security device sources but is not optimized for this use case.

TriGeo's Security Information Manager has been designed for ease of deployment, provides a combination of SEM and SIM function, and is oriented to midsize companies that need both SEM and compliance reporting. Sales accelerated during 2006 because of the match of the offering to organizations that needed SEM and SIM but have limited project and support capabilities. TriGeo has also developed much-needed sales channels.

Challengers

Cisco Systems has successfully positioned its MARS appliance as a component of its self-defending network strategy, and it has achieved the largest installed base in the SIEM market by selling MARS to network-focused buyers. Cisco MARS is not optimized for SIM or compliance reporting, and there are limitations in heterogeneous support when compared with most other SIEM vendors. There is also a lack of data source integration incentive from vendors that also compete with Cisco in this and other markets. However, Cisco has a large impact on all other SIEM vendors because of its SIEM technology presence in such a large number of customer sites.

Three of the other large challengers — CA, IBM and Novell — provide broad-function SIEM software that is also complementary to the IAM products within each vendor's portfolio. CA and IBM also provide integration between their SIEM offering and their operations event management, workflow and vulnerability management products. All three vendors have not yet addressed recent customer requirements in areas such as ease of deployment for SEM, and log management.

IBM has two SIEM technologies — TSOM — from the Micromuse acquisition and primarily oriented to SEM — and Insight — from the Consul acquisition and primarily oriented to user activity monitoring and compliance reporting. IBM has a road map to integrate Insight with TSOM and intends to provide integration with TSOM in a way that enables real-time event management for Insight.

CA has two products in the SIEM space. CA Audit provides basic log data collection and analysis for host systems, and SCC, which provides broad SIEM functions. CA has achieved a large installed base by selling its SIEM products to its IAM customers. There are also some SEM-focused deployments of SCC in large environments. To meet requirements for the majority of current SIEM buyers, CA needs to improve the user interface and provide simplified deployment options for use cases that require SEM and log management in addition to host log auditing functions.

Novell's SIEM technology — from the recent eSecurity acquisition — is designed for large-scale deployments that require broad and flexible SIEM capabilities. The technology is well-suited for this use case. Novell needs to adapt the technology so that it is simpler to deploy for SIM and log-management-oriented use cases that require less SEM capability. Integration with some related Novell IAM solutions is complete, and integration with additional Novell products is in the process.

netForensics' nFX provides full-function SIEM software that has traditionally competed with SIEM point solutions from ArcSight, Intellitactics and Novell. The technology is suitable for large-scale deployments that require full-function SEM, and it can also be deployed by organizations that have limited support capabilities but that can expend some effort in areas such as customization and tuning. On 24 April, netForensics announced nFX Log One — log management (appliance or software) that can be deployed either stand-alone or loosely coupled with nFX, but this new function was not evaluated as part of this Magic Quadrant.

The SenSage solution is optimized for analytics and compliance reporting against a very large log event data store. SenSage provides explicit audit support for multiple packaged applications, and the company has OEM arrangements with Cerner (healthcare applications), Symantec (e-mail archive) and HP (the HP Trusted Compliance Solution appliance). The software is limited in real-time collection and event management capabilities, and SenSage needs to continue efforts to make the product easier to deploy and support through improvements in the user interface and report generation capability.

Quest Software's InTrust offering is primarily oriented to the periodic collection of host log data and the analysis of a subset of the data collected. InTrust also provides basic event alerting. Quest has a large installed base for InTrust, but the narrow function limits its applicability to a small subset of current SIEM technology buyers.

Visionaries

Q1 Labs entered the SIEM market late in 2005, through an expansion of QRadar's NBA capabilities, to include log data analysis for host and network security devices. The data analysis provides a network-oriented view of the threat environment using NetFlow and direct network traffic monitoring, in combination with host activity monitoring and reporting. During 2006, Q1 improved support for compliance reporting and has recently implemented changes that carry known identity information across all related events. The vendor has recently resolved deployment complexity issues through the introduction of an additional appliance that eliminates the need for management tier software. Log management functions are provided via collector appliances.

LogRhythm is rapidly growing its small installed base by providing appliances that deliver a mix of log management and SEM functions. The appliances provide a mix of log management and basic SEM functions to midsize organizations that require both capabilities.

OpenService's Security Management Center software solution is composed of two components: Security Threat Manager, which provides SIEM, and Security Log Manager, which provides log management functions. Security Management Center is scalable, easy to deploy, easy to maintain, and low in server resource requirements.

Niche Players

ExaProtect's SIEM appliance offering was initially developed from the SIEM software infrastructure of a European managed security service provider (MSSP). The company has built an SIEM customer base in Europe and is expanding into the U.S. market. ExaProtect acquired Solsoft (a North American network configuration management vendor) and now maintains major

offices in the United States and Paris. The technology is primarily oriented to SEM, but ExaProtect has developed compliance reporting capabilities.

Intellitactics provides broad-scope SIEM software that is highly customizable and optimal for large-scale deployments. The vendor has improved the user interface and has implemented changes to simplify deployment, but these changes have not brought the product to the point at which it meets the requirements of the most-common use cases in the current market. On 27 April, Intellitactics announced a log management appliance that is tightly coupled with Security Manager, but the new function was not evaluated as part of this Magic Quadrant.

Tenable's SIEM software solution is composed of the Security Center console environment and the Log Correlation Engine, which gather host and network device logs and correlate events with data from their active and passive vulnerability scanning technologies. The SIEM technology is oriented to customers that have deployed Tenable's vulnerability scanning technologies. Tenable has recently improved the reporting interface and has introduced an event management console.

High Tower provides SIEM appliances that are oriented to midsize businesses that require basic SEM and basic reporting. The appliance is designed to collect all log data from every source. High Tower needs to continue its development work to enhance reporting capabilities.

Vendor Strengths and Cautions

ArcSight

Strengths

- ArcSight continues to be the most-visible point solution vendor and provides the broadest SIEM function set.
- The recently introduced log management appliance provides functions that address a broader set of compliance use cases and also provides simpler, lighter-weight deployment options that complement ESM.

Cautions

- ArcSight ESM requires substantial end-user expertise in areas such as database tuning, and customers typically comment on the investment in server-side resources needed to support the deployment.
- Because the direct sales force remains focused on large-enterprise deals and ArcSight's midmarket channel focus is relatively new, smaller organizations do not always get attention.

CA

Strengths

- CA's SIEM solutions provide SIM and SEM capabilities for network and security devices, but they are most commonly deployed for user activity monitoring on host systems.
- CA's SIEM solutions complement the audit functions provided by CA and other IAM vendors.
- CA's SIEM solutions are especially well-suited for organizations that have already implemented other CA host security or systems management products that integrate

with SCC or are willing to implement the CA suite to address requirements beyond SIEM.

Cautions

- Deployments for the network security use case are not widespread.
- CA must continue to reduce the amount of initial customization required and make other changes to simplify deployment.

Cisco Systems

Strengths

- The MARS SIEM appliance provides "out of the box" network SEM capabilities, and it is one of only three SIEM products that provide some NBA function.
- The integration of network flow information and log data enables management functions that can be used by IT security and network operations. MARS also provides automated threat response through interaction with routers, firewalls and other network devices.
- MARS is most appropriate for organizations that have a Cisco-centric network, have SIEM requirements that are focused primarily on network SEM, and do not need to customize event management or reporting beyond what is provided by MARS.
- MARS should also be considered by organizations that wish to gain some NBA capability from an SIEM investment.

Cautions

- MARS is not well-suited for user- and access-oriented compliance monitoring — the use case that drives many competitive SIEM decisions.
- While MARS does provide pre-defined functions for network SEM, it is not optimal for SIM deployments that require customized audit/reporting functions.
- Larger enterprises with heterogeneous network device data source requirements and those that require flexible analysis of host-based event logs and user activity analysis for compliance will find MARS insufficient for those specific needs.

ExaProtect

Strengths

- ExaProtect's appliance-based offering is oriented primarily to large deployments that require a mix of SEM and SIM functions.
- Integration between ExaProtect's SIEM and network device management technology provides automated response and network device change discovery/reconciliation capabilities.

Cautions

- While ExaProtect has a major presence in Europe, the company is just beginning to expand its presence within the North American SIEM market.

High Tower

Strengths

- High Tower provides a low-cost appliance that is easy to deploy and oriented primarily to SEM.

Cautions

- Although the most-recent release provides improvements in correlation support, SEM capabilities remain basic when compared with competing solutions.
- Support for report customization is limited.

IBM

Strengths

- Recent acquisitions provide Tivoli with complementary SEM and SIM technologies.
- The Insight technology (Consul acquisition) provides strong reporting capabilities for compliance, identity and user activity.
- TSOM (Micromuse acquisition) provides SEM functions.

Cautions

- Tivoli now has two SIEM solutions that are complementary but require at least loose integration (scheduled for July 2007).
- Insight support for real-time monitoring of log events is limited, and organizations that need real-time event monitoring of host log events would need to deploy two IBM products that are in the process of being integrated by the vendor.
- Customers that are considering IBM's offerings will need to evaluate IBM's integration road map.

Intellitactics

Strengths

- Intellitactics Security Manager is best-suited for organizations that value deployment flexibility, customization and well-developed functions for the integration of customer-defined data sources, over simple interfaces and pre-defined functions.
- Security Manager ships with a large number of pre-defined compliance reports and incorporates a proprietary compressed back store that allows for efficient online storage of large amounts of log data.

Cautions

- Intellitactics must continue to reduce the technical skill requirements needed to provide a better match to the requirements of the broader SIEM market.

LogLogic

Strengths

- LogLogic has established itself as the primary provider of log management function in the SIEM segment and should be considered when there is a need to collect and analyze all log data from every source, in combination with basic event alerting.
- The technology can be deployed in combination with SEM-focused technology in the same environment, providing log management functions that complement SEM and reduce SEM resource requirements.

Cautions

- Limited SEM capability usually precludes use as the sole technology when both SIM and SEM functions are needed.
- LogLogic is challenged to address real-time collection for non-syslog event sources.

LogRhythm

Strengths

- LogRhythm's appliances provide a combination of log management and basic SEM functions that are most appropriate for midsize organizations that require both functions but have limited support capabilities.

Cautions

- While real-time event display capabilities exceed those of competitors such as LogLogic, LogRhythm needs to continue development of real-time event management functions to reach parity with competitors such as TriGeo and RSA.
- LogRhythm is a recent market entrant that needs to establish sales capabilities to enable sustained growth in the face of competition from more-established competitors.

netForensics

Strengths

- The netForensics nFX is best-suited for deployments where real-time monitoring is required, flexible reporting is needed, and modest resources exist for customization and support.
- The recently announced nFX Log One log management functions have the potential to broaden appropriate use cases to those that require simplified deployment and basic log management and monitoring capabilities.

Cautions

- netForensics also needs to execute on its plans for further integration of nFX Log One with the nFX Open Security Platform.

NetIQ

Strengths

- NetIQ Security Manager is most appropriate for deployments that are focused primarily on host log analysis for user and resource access monitoring and regulatory compliance reporting.
- The core offering is designed to process a filtered subset of log data, but this can be augmented with a log data collection and archiving component that can be used to collect and analyze all log data from every source.

Cautions

- NetIQ is inappropriate for deployments that are primarily focused on event management for network and security devices.
- NetIQ needs to simplify its log management component.

Novell

Strengths

- Sentinel is most appropriate for large-scale deployments that require both SIM and SEM functions but where selective collection and analysis of event data is acceptable.
- The solution is especially well-suited to organizations that use Novell IAM products.
- Sentinel is based on a message bus architecture that provides flexibility and scaling for large deployments.

Cautions

- The offering is not appropriate for deployments that require the processing of all log records, and for organizations that lack database support capabilities.

OpenService

Strengths

- OpenService is a good choice for organizations that are looking for an out-of-the-box SIEM solution with modest upkeep and server-side resource requirements.

Cautions

- Organizations that require extensive pre-defined compliance reporting functions should also evaluate other products.

Q1 Labs

Strengths

- Q1 Labs' QRadar provides a combination of SEM, SIM and NBA capabilities, which can be used by IT security and network operations.
- NBA capabilities can be applied to host breach discovery.

- The collection tier can be used to provide log management functions, and the log data is indexed and accessible for reporting.

Cautions

- Other appliance-based solutions are more appropriate when only log management and/or basic event management is required.

Quest Software

Strengths

- Organizations that require analysis and reporting on a small subset of host log records and do not require real-time data collection and correlation can implement InTrust at a relatively low cost.

Cautions

- InTrust's limited support for real-time event management, in combination with a design that requires selection and secondary data movement before analysis is possible, limits the applicability of InTrust to very specific customer use cases.
- Organizations that require continuous log data collection or event monitoring, or analysis of all log records, will find InTrust to be a poor match to their requirements.

RSA (EMC)

Strengths

- RSA enVision should be considered in cases in which all data needs to be collected and available for analysis and a need exists for both SEM and SIM capabilities.
- Because of its ease of deployment, the appliance should also be considered in environments that are constrained in areas such as server and database support.

Cautions

- Organizations that need to enable a full-function security console for a security operations center (SOC) should consider solutions that provide more function or flexibility in this area.

SenSage

Strengths

- SenSage is optimized for organizations that require high-volume event collection, monitoring, analytics and reporting for large amounts of log data over long periods, for audit, compliance and internal investigation.
- SenSage has explicit support for SAP, Oracle (PeopleSoft and Siebel), Lawson, Cerner and other packaged applications, and the technology is embedded in solutions from Cerner, Intec, HP and Sendmail.

Cautions

- Organizations should consider alternatives when there is a strong focus on real-time event management.

- SenSage's current technology is more complex and costly than log management offerings from some competitors, and SenSage needs to demonstrate that its planned appliance offering and recent improvements in the reporting interface will simplify and lower the cost of deployment.

Symantec

Strengths

- Symantec's Security Information Manager provides SIM, SEM and log management functions that are scalable and easy to deploy.

Cautions

- Organizations that have existing network systems and security infrastructure from SIEM competitors, such as Cisco, IBM and CA, should also evaluate potential benefits of integrated SIEM offerings from these vendors against the capabilities of the Symantec SIEM appliance and the appliance's integration with other Symantec security products.

Tenable Network Security

Strengths

- Tenable's Security Center integrates Tenable's Log Correlation, Nessus Vulnerability Scanner and Passive Vulnerability Scanner products to provide unified asset discovery, vulnerability detection, event management and reporting.
- Security Center is a software solution that can be deployed at a low overall cost, which also includes basic NetFlow collection and anomaly detection functions that can be utilized for host breach discovery.

Cautions

- Alternative offerings are better-suited for deployments that are focused on regulatory compliance reporting requirements related to host identity and access activity.

TriGeo

Strengths

- TriGeo provides a low-cost, easy-to-deploy SIEM appliance that is targeted at and well-suited for midsize organizations that have limited deployment and support resources and are looking to satisfy a mix of regulatory reporting and SEM requirements.
- The appliance provides a mix of SIM and SEM functions, and it also provides automated response through a TriGeo host agent and intrusion detection capabilities through a bundling in the Snort open-source intrusion detection system.

Cautions

- TriGeo's appliance is not designed for large-scale deployments that require aggregation and analysis of data from a large number of collection points.

RECOMMENDED READING

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills, etc., whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements, etc.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen

and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the Web site, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling product that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

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
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509