

Magic Quadrant for Security Information and Event Management, 1H06

Gartner RAS Core Research Note G00139431, Mark Nicolett, Amrit T. Williams, Paul E. Proctor, 12 May 2006, RA2074 5/21/2007

The security information and event management market is driven by an increasing need for customers to meet compliance requirements as well as continued need for near-real-time awareness of external and internal threats. The market remains fragmented, with no dominant vendor.

WHAT YOU NEED TO KNOW

Gartner has defined evaluation criteria for a broad set of security information and event management (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 narrower 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) vs. security event management (SEM) capabilities, ease and speed of deployment, acquisition cost and the IT organization's support capabilities, and integration with existing system and application infrastructure.

Market Overview

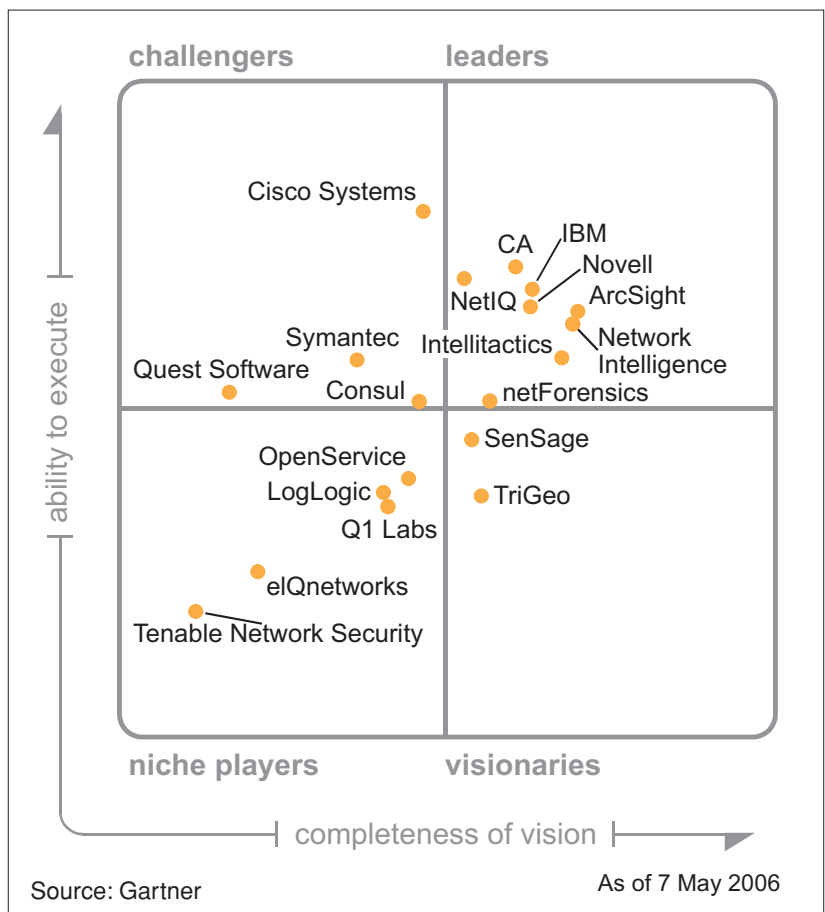
The SIEM market is driven by customer needs to analyze security event data in real time (for threat management, primarily in network events) and to analyze and report on log data (for security policy compliance monitoring, primarily in host and application events). SIM requirements (to support regulatory compliance initiatives) have replaced SEM as the primary driver for SIEM project funding. This means, fundamentally,

that organizations are placing more emphasis on watching the actions of authorized users on servers.

Nineteen vendors provide SIEM products, and significant variation exists in product delivery, functional capability, scalability, cost of deployment and support, and segment focus. Products are delivered as appliances or software. Some offerings are designed to deliver a mix of event management and information management capabilities, while others are optimized primarily for either SIM or SEM. A few vendors provide products that are narrow in function but optimized for scalability or for ease of deployment and support. A small but increasing

MAGIC QUADRANT

Figure 1. Magic Quadrant for Security Information and Event Management, 1H06



number of offerings are oriented to midsize IT organizations that have more-limited deployment and support resources. These offerings primarily help smaller organizations address auditor requirements for log centralization and correlation.

Technology providers include seven large network management and security vendors that integrate SIEM technology with related systems and security management products, and 12 point-solution vendors (some of which have driven technical innovation). 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 – Full-featured SIEMs designed to deliver a broad set of capabilities for large complex environments: ArcSight, CA, Novell, Intellitactics, netForensics, Network Intelligence and IBM.
- Use Case 2 – SIEM products that are integrated with an incumbent vendor's vulnerability management, and systems management products: CA, NetIQ, Symantec and IBM.
- Use Case 3 – Integration with identity and access management (IAM) products to monitor and record user activity as well as address compliance requirements: CA, IBM, Consul Risk Management and Novell.
- Use Case 4 – Host log analysis: NetIQ, Quest Software and Consul.
- Use Case 5 – SIEM integrated with network behavior analysis (NBA), primarily oriented toward network SEM: Cisco Systems and Q1 Labs. Tenable Network Security also offers some NBA functionality.

- Use Case 6 – Collect and analyze all log data primarily in ASCII through sysloglike centralization mechanisms: SenSage, LogLogic and Network Intelligence.
- Use Case 7 – Lower resource requirements: eIQNetworks, OpenService, Tenable, TriGeo and Quest.

Market Definition/Description

SIEM technology delivers two basic capabilities:

- SIM – 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 can be used to support the activities of the IT security, internal audit and compliance organizations.
- SEM – 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.

Although we estimate that 70 percent of current SIEM technology buyers require both capabilities within a single product, the SIM and SEM use cases drive different product capabilities and resource requirements. Early adopters of the technology tended to be very large organizations, but a wider variety of companies are now evaluating SIEM technology.

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 SEM and SIM capabilities.

The Magic Quadrant is copyrighted May 2006 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

© 2006 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

- The product must support data capture from heterogeneous data sources.
- The vendor must appear on the SIEM product evaluation lists of Gartner clients.
- 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 Gartner clients.
- The solution is delivered as a managed service.

Added

The current Magic Quadrant adds evaluations for the following vendors:

- Quest Software has recently expanded the host log analysis capabilities of its InTrust product to also encompass network and security devices and real-time alerting.
- Q1 Labs has recently expanded the scope of its QRadar NBA product to incorporate log data sources from network devices, security devices and host logs.
- Tenable has expanded the capabilities of its security event monitoring technology to include the aggregation and correlation of additional network device and host log data sources.
- On 19 April 2006, Novell announced that it acquired e-Security. e-Security's technology is now evaluated as an offering from Novell.

Dropped

Since the publication of the last SIEM Magic Quadrant, Micromuse acquired GuardedNet. This was followed by an acquisition of Micromuse by IBM. As a consequence, Micromuse and GuardedNet have been dropped from the SIEM Magic Quadrant, and IBM is evaluated with respect to the neuSecure technology from the Micromuse acquisition. In addition, e-Security has been dropped because of the acquisition by Novell.

Evaluation Criteria

Ability to Execute

Ability to Execute is evaluated on a combination of factors. SIEM technology is provided by large publicly traded companies with significant sales and development resources and smaller, privately held companies. Overall viability evaluates these differences. Sales execution and pricing evaluates the SIEM installed base size, growth rate and revenue stream. Also included is an evaluation of the effectiveness of the product in customer production and test environments. Changes in the method used for this year's evaluation have caused shifts in Ability to Execute (as compared with the previous Magic Quadrant's criteria) that are related more to relative capabilities among the vendors (as opposed to an absolute deterioration or improvement in a specific vendor's capability).

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	standard
Marketing Execution	standard
Customer Experience	standard
Operations	no rating

Source: Gartner

Completeness of Vision

Completeness of Vision for the SIEM market is evaluated on capabilities that are required for the SIM and SEM use cases, capabilities that are specifically required for either SIM or SEM, and capabilities that are required for regulatory compliance monitoring and reporting.

Common capabilities include:

- Product scope (supported devices, systems and applications)
- Data collection and reduction methods/autodiscovery
- Scalability and deployment flexibility
- Event correlation and taxonomy

- Incident management and workflow support
- Enterprise administration support
- Embedded security knowledge and asset classification

In addition, the SIM and SEM use cases each have a set of required capabilities.

- The SIM use case requires:
 - A data repository that supports the cost-effective long-term storage and analysis of historical data
 - Reporting that can be customized to the needs of a specific organization
- The SEM use case requires:
 - Collection and correlation of security events and data in near-real-time
 - A security-optimized console environment

There are additional capabilities that are needed for regulatory compliance reporting. SIEM technology use for regulatory compliance requires:

- Support for monitoring of user activity from system, application and object access logs
- Integration with IAM applications
- Support for integration of customer-defined data sources
- Ability to express and track compliance with customer-specific policies
- Mapping of events and reports to control frameworks and regulations

Table 2. Completeness of Vision Evaluation Criteria

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

Source: Gartner

Leaders

The Leaders quadrant contains a mix of large and point-solution vendors. Many of the SIEM offerings from these vendors have similarities in terms of design, focus and function, but differentiation also exists. All deliver a balanced mix of SEM and SIM capabilities. ArcSight, CA, Novell, Intellitactics, NetIQ, netForensics and IBM all provide software solutions. All seven of these SIEM products are typically deployed in a way that implements filtering at the point of collection, so that a subset of the event data is passed to real-time correlation and indexing for analytics. In contrast, Network Intelligence provides an appliance-based solution that is designed to collect and process all log events. NetIQ provides an implementation option that incorporates a log data collection and archiving tier for complete log data collection.

Three large vendors – CA, IBM and Novell – are capitalizing on their position as major providers of IAM technology and because of the compliance-driven focus on identity and access monitoring by integrating their IAM and SIEM offerings. CA, IBM and NetIQ also provide integration between their SIEM offering and their operations event management, workflow and vulnerability management products. IBM plans to transition current users of both the IBM Tivoli Risk Manager product (which has scalability and deployment issues) and the (Micromuse) Netcool for Security Management product to the (Micromuse) neuSecure SIEM technology. The acquisition of e-Security by Novell in April continues the trend toward consolidation within the SIEM market as small, privately held companies are bought out by large, broad-scope vendors with substantial development and sales resources. In addition, NetIQ will be taken private when the acquisition by Attachmate is completed.

The point-solution vendors – ArcSight, Intellitactics, netForensics and Network Intelligence – frequently compete against each other and also against the large SIEM vendors. They all provide full-function SIEM capabilities and have relatively large and established installed bases within large commercial and/or government accounts.

Challengers

The Challengers quadrant is composed of three large vendors and one smaller vendor that provide products, which are very different in terms of scope and focus.

Although the Cisco MARS appliance provides some SIM capability, the primary focus is SEM. Cisco has quickly built a large installed base, and MARS is very often evaluated against other SIEM offerings. Cisco is further developing MARS as a component of its security management infrastructure and is also developing automated remediation capabilities through integration with its networking equipment.

Consul is an established provider of identity and access audit functions, and its focus is in the audit and compliance aspects of SIEM. The InSight suite provides well-developed audit, regulatory compliance and privileged user-monitoring functions, and basic SEM. Consul has a codevelopment and sales relationship with BMC Software that is focused on the integration of BMC's IAM products with Consul's InSight audit product.

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

Late in 2005, Symantec released an SIEM appliance that is being further developed to provide balanced SIM and SEM capabilities. The appliance is a replacement for a marginal software offering that had scalability and functional limitations. Users that have evaluated the appliance indicate that a single instance of an appliance vastly exceeds the event-processing capability of single instance of the former software offering. However, this is a first-release product that needs function expansion to be competitive against best-in-class SIEM products.

Visionaries

The Visionaries quadrant contains two vendors that differ widely in product focus and target market. SenSage provides SIEM software to large organizations that are focused primarily on analytics,

audit, monitoring and compliance reporting against a large log data store. SenSage provides explicit audit support for multiple packaged applications. In contrast, TriGeo provides an appliance that delivers balanced SIM and SEM functions, primarily to midsize enterprises. TriGeo's installed base includes many smaller financial services organizations (for example, regional banks) that use the technology for SEM and compliance reporting.

Niche Players

The vendors in the Niche Players quadrant have products that focus primarily on a subset of possible SIEM functions, but they can potentially provide the best match of product capability to an organization's specific requirements. Placement with respect to ability to execute is based, in part, on total revenue, SIEM revenue and SIEM product installed base relative to other vendors in the market.

eIQnetworks introduced its host-based (System Analyzer) and network-based (Network Analyzer) SIEM solution in 2004. It introduced an enterprise-focused SIEM solution, Enterprise Security Analyzer (ESA), in the second half of 2005. ESA provides log management, real-time monitoring, correlated alerting, reporting and forensics capabilities. eIQnetworks has original equipment manufacturer (OEM) and reseller partnerships with companies such as Astaro (resold by Novell), NEC, Secure Computing, Fortinet, iPolicy Networks, Mirapoint, Sanmina-SCI, Top Layer Networks, Intoto and NetContinuum. OEM customers tend to apply the technology for network-oriented SEM.

OpenService has a smaller installed base than leading SIEM point-solution vendors; however, Security Management Center has been deployed in large environments. The primary use case for Security Management Center's installed base is network SEM, and the vendor is further developing the SIM capabilities that are already provided.

LogLogic is a well-funded and rapidly growing recent entrant to the SIEM market, and it is distinguished both by its focus on SIM capabilities and its lack of advanced SEM function. The company positions its appliance technology as a log management solution that provides data analysis and real-time alerting.

The appliance is sometimes installed as a data collection and analysis tier in conjunction with another SIEM product. During the past year, the company has aggressively grown sales channels in North America, Europe and Asia/Pacific.

Q1 Labs entered the SIEM market late in 2005, through an expansion of QRadar's NBA capabilities, to include a 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 firewall and intrusion-detection system data. Host log data analysis is also provided.

Tenable is focused primarily on SEM. The vendor provides the Security Center console environment (formerly named Lightning) and the Log Correlation Engine (formerly named Thunder), which gather host and network device logs and correlate events with data from their vulnerability assessment and security event monitoring technologies.

Vendor Comments

ArcSight

Differentiators/strengths: ArcSight's Enterprise Security Manager was one of the first SIEM products to provide advanced analytics, and the console environment is visually appealing and easy to navigate. ArcSight remains one of the most visible on Gartner's client shortlists and has many successful large-scale deployments.

Appropriate use cases: ArcSight is primarily focused on large-scale deployments and provides a fully featured SIEM that offers both event management and information management capabilities. It is best-suited for deployments that selectively collect event data, use the console for real-time monitoring, and require flexible reporting from the data collected.

Challenges: ArcSight's functional differentiation has eroded to some degree as competitors, such as e-Security, have added similar capabilities to their offerings. Enterprise Security Manager system and database resource requirements have been much greater than initially expected in some deployments.

Inappropriate use cases: ArcSight is not optimized for use cases that require collection and indexing of all log records. The product requires server and database tuning expertise, and the vendor is oriented to large sales. Therefore, the product is not suited for small and midsize business (SMB) clients, organizations looking for small regional deployments, or organizations focused solely on user access monitoring and offline archives.

CA

Differentiators/strengths: While eTrust Security Command Center (SCC) is a stand-alone SIEM product, it is also the anchor console for a suite that integrates CA's IAM products as well as its vulnerability and security policy management offerings. CA has also standardized on a common inventory and asset schema across its systems and security management product line, which allows an organization to incorporate asset classification data for risk analysis and reporting.

Appropriate use cases: SCC provides both event management and information management capabilities for stand-alone deployment. It is best-suited for large-enterprise organizations that have already implemented other CA products that integrate with SCC or are willing to implement the CA suite to address requirements beyond SIEM.

Challenges: The console interface does not compare well to competitors such as ArcSight. In addition, it requires setup work and so does not "Idemo well" in pilots with tight time frames. Despite CA's large installed base of network systems management and host security products, the vendor does not have a standing relationship with the network security buying center.

Inappropriate use cases: eTrust SCC is not optimized for use cases that require collection and indexing of all log records. The software requires server and database tuning expertise. The product is not suited for SMB clients, organizations looking for small regional deployments, or organizations focused solely on user access monitoring and offline archives.

Cisco Systems

Differentiators/strengths: Cisco's Security Monitoring and Response System (MARS) appliance is differentiated by its ability to provide SEM that integrates network flow information and log data, enabling management functions that can be used by both IT security and network operations. MARS also provides automated threat response through interaction with routers, firewalls and other network devices. Cisco is developing additional capabilities in this area by extending MARS capabilities and by incorporating more-granular change support within Cisco networking and security devices. Cisco has also integrated MARS with its security management suite. MARS is a comparatively inexpensive SIEM appliance that is easy to deploy and manage.

Appropriate use cases: MARS is most appropriate for organizations that are focusing primarily on network SEM and value pre-defined function over deployment flexibility. Cisco-centric midsize enterprises that are focused on network event analysis for both security and operations should be sure to include MARS on their shortlist. Any organization that wishes to gain some NBA capability from an SIEM investment should also consider the appliance.

Challenges: Organizations that want to customize event management and reporting functions have indicated that MARS is inflexible. This leads to limitations in the technology's use for regulatory compliance monitoring. Cisco must also balance the development of new capabilities enabled by the combination of MARS and Cisco devices, with the need for heterogeneous device support (developing and maintaining support for the network and security devices provided by its competitors).

Inappropriate use cases: Larger enterprises with data source requirements, such as host-based event logs and reporting that include user activity analysis for compliance, will find MARS insufficient for their needs.

Consul

Differentiators/strengths: InSight customers primarily use the product for host and application log data consolidation and security policy audit, but InSight also supports network and security device data sources, albeit, not as well. The technology is focused on privileged user monitoring and audit. Consul and BMC Software have completed an extensive integration of InSight with BMC's IAM products. Consul is one of the few SIEM companies with a core competency in mainframe data records.

Appropriate use cases: Organizations focused on compliance, identity and user activity monitoring should have Consul on their shortlist. If you are using BMC for identity management, it will be hard to find an equal to address SIM requirements. Also, if processing events from mainframe data sources is high on your priority list, then Consul should make your shortlist.

Challenges: The nascent SEM functions provided by Consul are relatively immature compared with their competitors. Consul has benefited from the market shift from SEM to SIM requirements, but it falls short of the ability to compete head-to-head with general-purpose SIEM products when an organization requires both SIM and SEM capabilities.

Inappropriate use cases: Organizations with substantial SEM network security monitoring requirements will find Consul less able to address their needs.

eIQnetworks

Differentiators/strengths: eIQnetworks' Enterprise System Analyzer provides SIM and SEM functions at a relatively low entry price. Reference customers indicate that the product is easy to deploy and operate. Product pricing is extremely low when compared with other products in this market, and server resource requirements are modest. eIQnetworks has OEM and reseller partnerships with companies such as Astaro, NEC, NetContinuum, Secure Computing, Fortinet, iPolicy and Top Layer.

Appropriate use cases: Organizations with limited budgets that are focused primarily on network security monitoring but also have basic requirements for host log analysis should put eIQnetworks on their shortlist.

Challenges: eIQnetworks will need to expand host log analysis capabilities to include integration with data sources, such as database management system (DBMS) and IAM solutions to expand their customer base.

Inappropriate use cases: Larger organizations that require significant host-oriented SIM capabilities will find that eIQnetworks' offerings fall short of their requirements.

IBM

Differentiators/strengths: neuSecure is offered as a software or an appliance and provides balanced SIM and SEM capabilities. IBM gained the neuSecure technology when it acquired Micromuse. IBM has begun to make enhancements to the neuSecure product lines to support a single event management framework and infrastructure that can capitalize on the Micromuse and IBM installed base.

Appropriate use cases: Organizations that are looking for both security event and information management capabilities should consider neuSecure. Current Netcool for Security Management and IBM Risk Manager customers can look forward to a more-scalable, all-purpose SIEM as well as future integration with IBM IAM and network and systems management (NSM) technologies.

Challenges: IBM will need to assimilate the recent acquisitions, including transitioning the Risk Manager and Netcool for Security Management customer bases. Integration with the IBM Tivoli Identity Manager and IBM Tivoli Security Compliance Manager products also needs to be completed.

Inappropriate use cases: Alternative solutions are more appropriate for small deployments, deployments that require the processing of all log records, and for organizations that lack database support capabilities.

Intellitactics

Differentiators/strengths: Intellitactics' Security Manager provides balanced SIM and SEM functions, and it is highly customizable. Intellitactics' customers tend to value deployment flexibility and well-developed functions for the integration of customer-defined data sources over simple interfaces and pre-defined function. The technology incorporates a proprietary compressed backstore that allows for efficient online storage of large amounts of log data.

Appropriate use cases: Intellitactics is a good choice for organizations looking for deployment flexibility and customization and a broad SIEM solution that has strong event and information management capabilities. Intellitactics provides customizable reports that are easily adapted to organizational requirements.

Challenges: Intellitactics will need to continue to reduce the technical skill requirements and customization needed for large enterprise deployments.

Inappropriate use cases: Companies with limited deployment and support resources that value simplified administration and pre-defined function may find Intellitactics inappropriate for their environment.

LogLogic

Differentiators/strengths: LogLogic's technology is agentless and appliance-based for scalable rollup of ASCII-based logs, primarily through sysloglike delivery mechanisms. The product architecture implements distributed collection and consolidated online storage tiers. Log data is collected in its entirety from each source and is stored in raw/indexed and summarized formats. Data stored in binary formats (such as Windows logs) must be exported in ASCII before centralization to the appliance. The indexing supports full-text search and high-performance reporting.

Appropriate use cases: LogLogic should be considered when there is a need to collect all log data and when full-function SEM is not a requirement. It is optimized for cases in which the

major customer requirements are collection and storage of all log records from each source, log analysis and reporting and only basic event alerting. The technology is sometimes deployed in conjunction with another SIEM product to provide log management capabilities that are more directly applicable and efficient than a more broadly featured SIEM product can deliver.

Challenges: LogLogic provides functions to analyze log data, but Gartner clients report mostly basic application of the analysis functions for forensic use. LogLogic seems comfortable in the role of “log management” ceding more-complex and more-expensive functions to more fully featured broad SIEM products.

Inappropriate use cases: 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 detection requirements, ability to gather data from sources that are not easily exported in ASCII (that is, mainframe system management facility [SMF] records, and so on), and processing custom non-ASCII sources (such as Solaris BSM).

netForensics

Differentiators/strengths: netForensics is an early entrant and a longtime provider of SIEM technology, and it has a large installed base for its nFX SIEM software offering. nFX provides balanced SIM and SEM functions, and it also has specific support for some Cisco initiatives, such as Cisco Network Admission Control.

Appropriate use cases: netForensics provides a fully featured SIEM product that offers both event management and information management capabilities. It is best-suited for large organizations that are looking to selectively collect event data, use the console for real-time monitoring, and require flexible reporting from the data collected.

Challenges: netForensics needs to improve its visibility in competitive evaluations. The company must also execute its product development plan, which will better differentiate its offering.

Inappropriate use cases: netForensics is not appropriate for small deployments, deployments that require the processing of all log records, and for organizations that lack database support capabilities.

NetIQ

Differentiators/strengths: NetIQ’s Security Manager has been widely installed by organizations that apply the SIEM technology to host log analysis for security policy compliance monitoring and regulatory compliance reporting. NetIQ is integrating its security management products with its AppManager Suite of systems management products. NetIQ Vulnerability Manager, which provides security configuration policy compliance functions, is integrated with Security Manager, and both products can aggregate their events and data into AppManager. 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 process all log data from every source.

Appropriate use cases: NetIQ is appropriate for SIEM deployments that are focused primarily on host log analysis but also have some limited network security event requirements.

Challenges: Although the product supports balanced SIM and SEM capabilities, large-scale deployments that include network and security device data sources are rare within the NetIQ installed base.

Inappropriate use cases: NetIQ is inappropriate for deployments that are primarily focused on event management for network and security devices.

Network Intelligence

Differentiators/strengths: Network Intelligence sells its enVision SIEM appliances to midsize and large businesses. The enVision technology is agentless, collects all log data from each source and provides a combination of SEM and SIM capabilities. Appliances are sized according to a guaranteed events-per-second processing rate (that is, events can be collected, correlated and inserted into the database with no message loss). A compressed backstore is implemented with a proprietary object-oriented database that allows for faster processing of event

data and lower storage costs when compared with products that use traditional relational database management systems (RDBMSs).

Appropriate use cases: Network Intelligence should be considered in cases in which all data needs to be collected, and there is a need for both SEM and SIM capabilities. The appliance should also be considered in environments that are constrained in areas such as server and database support. If an appliance-based solution is a requirement, Network Intelligence should be included on the shortlist.

Challenges: Network Intelligence's real-time event console and correlation capabilities are not as comprehensive as vendors that lead in this area, such as ArcSight, e-Security (now Novell), and Intellitactics.

Inappropriate use cases: Organizations that will staff for operational monitoring of a security event console and organizations that want a high degree of customization should consider alternatives that are stronger in these areas.

Novell

Differentiators/strengths: Novell has stated that it intends to continue to offer e-Security's Sentinel software package as a stand-alone SIEM technology. In the near term, however, it will focus on localization, repackaging and branding efforts, followed by integration with Novell IAM products and technologies. Sentinel is based on a message bus architecture that provides flexibility and scaling for large deployments.

Appropriate use cases: Sentinel is most appropriate for large-scale deployments that require both SIM and SEM capabilities and selectively collect event data. Novell intends to integrate Novell Identity Manager, Novell Access Manager and Novell eDirectory with Sentinel through Novell Audit.

Challenges: To remain competitive in the SIEM market, Novell will need to retain e-Security development, sales and sales engineer expertise and continue to enhance the network SEM aspect of Sentinel – an area that is not within the core competency of Novell.

Inappropriate use cases: The Sentinel software offering is not appropriate for small deployments, deployments that require the processing of all log records, and for organizations that lack database support capabilities.

OpenService

Differentiators/strengths: Security Management Center's differentiating characteristics are its focus on statistical correlation and low server-side resource requirements for SEM. Security Management Center implements statistical correlation that is effective in reducing message rates and generating appropriate security alerts, and it provides a correlation rules generator that can be used by customers to develop rules.

Appropriate use cases: OpenService is a good choice for organizations, with limited resources, that are looking for an "out of the box" SEM solution with modest server-side resource requirements.

Challenges: OpenService needs to expand its internal incident management function and its support for customized reports.

Inappropriate use cases: Organizations that are focused primarily on SIM or have compliance-oriented requirements should evaluate offerings that are more mature in these areas.

Q1 Labs

Differentiators/strengths: Q1 Labs' QRadar provides a combination of NBA and SIEM capabilities, which can be used by both IT security and network operations. As with Cisco MARS, QRadar collects and analyzes both NetFlow and log data. Q1 Labs has an OEM agreement with Enterasys.

Appropriate use cases: Current QRadar customers that require SIEM capability should evaluate the new QRadar function. Any organization that wishes to gain both NBA and SIEM capabilities from a single investment should consider the solution. We also believe that Q1 Labs has additional opportunities to manufacture/partner with Cisco competitors that need a competitive response to MARS.

Challenges: Q1 Labs is a new entrant in the SIEM market and will need to play catch-up to some of the market requirements, especially in SIM-related areas, such as expansion of supported host sources and monitoring at the application and database layers. Q1 Labs' primary competitor is Cisco's MARs product, which provides less-substantial NBA capabilities. Gartner clients report that QRadar is a "heavier" deployment and MARS is a "lighter" deployment. Q1 Labs needs to continue to improve its SIM functions while maintaining its fuller functionality in the NBA area.

Inappropriate use cases: SIEM deployments that are focused primarily on application or database log analysis, or compliance-oriented reporting that is dependent on integration with IAM products, will find alternatives that are better developed for these use cases.

Quest Software

Differentiators/strengths: Quest Software's InTrust offering is designed primarily for the periodic collection of host log data and the analysis of a subset of the data collected. Limited SEM support is provided through event alerts from the agent running on the platform of the data source.

Appropriate use cases: 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.

Challenges: 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.

Inappropriate use cases: Organizations that require continuous log data collection, event management beyond real-time alerting, or analysis of all log records, will find InTrust to be a poor match to their requirements.

SenSage

Differentiators/strengths: SenSage's strengths are in the collection, efficient archive, monitoring, analytics and reporting for large and diverse log data stores. SenSage has explicit support for SAP, Oracle (PeopleSoft and Siebel), Lawson, Cerner and other packaged applications. It also has OEM relationships with Cerner, EMC, HP and Sendmail. The software also employs a purpose-built analytics engine (non-RDBMS) and has integrated real-time event correlation.

Appropriate use cases: SenSage is optimized for organizations that require high-performance event collection, monitoring analytics and reporting for large amounts of log data over long periods of time, for audit, compliance and internal investigation. The system uniquely supports regulatory data retention and verification requirements, using an architecture that compresses the original source data, maintains its integrity and optimizes complex queries. This is useful for organizations that need all original event data to be available for analytics.

Challenges: SenSage will need to balance product development initiatives that support both the requirements of its current customers and new functionality to support its partner strategy. SenSage will also need to extend its incident management functions as it further develops SEM capabilities.

Inappropriate use cases: Organizations should consider alternatives when there is a strong focus on real-time event management, and they should consider appliance-based alternatives when support and customization resources are constrained.

Symantec

Differentiators/strengths: The Security Information Manager appliance is differentiated by the dynamic update of external threat information from Symantec's Global Intelligence Network (GIN) and correlation with internal event activity to identify external threats targeted to local enterprises. Symantec has also done some initial integration with its Enterprise Security Manager (ESM) and BindView products, which provides automated asset discovery, vulnerability assessment and security configuration policy compliance functions.

Appropriate use cases: Organizations that are currently using Symantec's previous SIEM offering, Symantec antivirus customers with strong antivirus monitoring requirements, and organizations that have deployed other Symantec security management products should evaluate Symantec's appliance, after consideration of the technology's current maturity level.

Challenges: The appliance offering is new to the market, and Symantec needs to continue to develop product capabilities so that the solution becomes competitive with alternatives in the market.

Inappropriate use cases: Organizations that require the ability to monitor for resource access attempts on host systems that are material to regulatory compliance should consider alternatives with more mature function in this area.

Tenable Network Security

Differentiators/strengths: Security Center console environment (formerly named Lightning) and the Log Correlation Engine (formerly named Thunder) are SEM-oriented and provide basic log and event analysis (rollup of ASCII-based logs, primarily through sysloglike delivery mechanisms). Tenable offers NBA functionality through NetFlow processing, but it is not a full NBA system.

Appropriate use cases: The solution provides better value when integrated with Tenable's other products, including Nessus, Passive Vulnerability Assessment Scanner (formerly named Nevo), and the vendor's NetFlow collectors.

Challenges: Tenable is challenged in its ability to gather data from sources that are not easily exported in ASCII (that is, mainframe SMF records, and so on), and processing custom non-ASCII sources (such as Solaris BSM).

Inappropriate use cases: Organizations that are not using Tenable's other products, or organizations that have regulatory compliance reporting requirements for host activity, should consider alternatives.

TriGeo

Differentiators/strengths: TriGeo is a small company that provides a low-cost, easy-to-deploy SIEM appliance that is targeted at midsize businesses. The appliance provides a mix of SIM and SEM functions, and customers tend to use the solution for both purposes in a single deployment. The appliance also provides automated-response capabilities and intrusion-detection capabilities through a bundling in the Snort open-source intrusion-detection system.

Appropriate use cases: TriGeo is 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.

Challenges: TriGeo's primary challenge is finding ways to grow its installed base at a faster rate. Channel development and OEM arrangements would make the company more visible to potential customers.

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

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.