# Magic Quadrant for Security Information and Event Management

Gartner RAS Core Research Note G00156945, Mark Nicolett, Kelly M. Kavanagh, 8 May 2008, R2725 05092009

## Broad adoption of SIEM technology is driven by compliance and security needs. New use cases in areas such as application activity monitoring are emerging.

### WHAT YOU NEED TO KNOW

Funding for security information and event management (SIEM) technology deployments is driven in large part by the need to quickly address regulatory compliance issues, but most organizations also want to improve security monitoring capabilities. An optimal solution will support the 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. Ease of deployment, ease of support and log management functions are weighted more heavily than advanced event management functions or the ability to heavily customize an SIEM deployment.

SIEM technology projects are typically oriented to one of three major use cases: compliance reporting, threat management or a general SIEM deployment that implements both capabilities. The SIEM market is comprised of vendors with products that are optimized for a specific use case, provide a mix of “good enough” functions for the most common use cases, or are broad and flexible but complex.

This year's Magic Quadrant for SIEM evaluates the most-common situation: An SIEM project that is funded to solve a compliance reporting issue, but has project leaders that also want better security monitoring and event management. 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; the ease and speed of deployment; the IT organization's support capabilities; and integration with established network, security and infrastructure management applications.

### MAGIC QUADRANT

#### Market Overview

The SIEM market is being driven by three factors: the emergence of user and resource access monitoring as the primary customer problem to be solved, the demand for the technology from a broad set of customers, and the availability of the technology from large vendors that also sell related products or services. SIEM is one of the fastest-growing security markets, with a growth rate of more than 50% in 2006, 30% in 2007 and estimated revenue reaching more than $800 million in 2007. Nonetheless, there are more than 20 vendors that compete in the segment, and viability is a concern for some privately held vendors that have not recently received funding but face competition from much larger vendors. There were no further acquisitions of SIEM vendors in 2007.

Gartner

## Customer Requirements – Compliance, Log Management, Security and Fraud Detection

The primary driver of the North American SIEM market continues to be regulatory compliance. European SIEM deployments have been focused primarily on external threat monitoring, but compliance has recently emerged as a strong driver in Europe as well. More than 80% of current SIEM deployment projects are funded to close a compliance gap. 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 deployments of SIEM technology are focused on user activity and resource access monitoring for host systems, but real-time event management for network security remains a common requirement.

The compliance driver has also changed the buyer profile, which is now extended to organizations that have smaller security staffs and more-limited system support capabilities. For these buyers, predefined functions and ease of deployment and support are valued over advanced function and extensive customization.

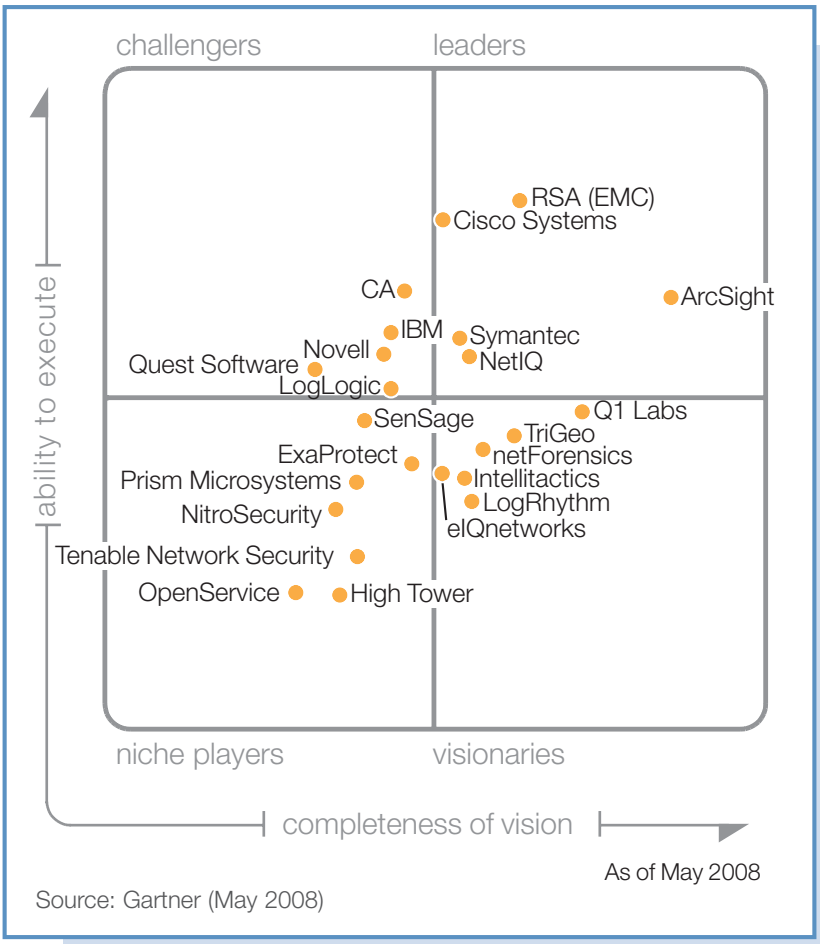
Log management functions have become a more important customer requirement because of the following factors:

- 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
- The ability to employ log management in front of a SEM-focused deployment to enable more-selective forwarding of events to correlation engines (thereby, reducing the load on the event manager)

Some product architectures natively provide log management (for example, eIQnetworks, High Tower, LogLogic, LogRhythm, Prism Microsystems, Q1 Labs, RSA, SenSage and Symantec); others (such as ArcSight, IBM, Intellitactics, netForensics, NetIQ and TriGeo) provide a log management tier that is integrated with a SEM back-end. Other vendors have development initiatives under way and are expected to announce log management extensions during 2008.

Application layer monitoring for fraud detection or internal threat management is emerging as a new use case for SIEM technology. Some customers are paying incumbent SIEM vendors for services to assist in projects to collect and analyze application-level events or transaction logs for the purpose of discovering combinations of transactions that are indicators of fraud or misuse.

**Figure 1. Magic Quadrant for Security Information and Event Management**




Source: Gartner (May 2008)

SIEM technology is being deployed alongside fraud detection and application monitoring point solutions as a complementary technology. These projects have been undertaken by large companies in industry vertical markets such as financial services and telecommunications as an internally justified security measure. An external regulatory driver for the fraud detection capability may begin to emerge during 2008 because of the 2007 release of the Public Company Accounting Oversight Board (PCAOB) version 5 auditing standard, which emphasizes anti-fraud controls. A number of SIEM vendors are beginning to position their technologies as “platforms” that can provide security, operations and application analytics.

## The Changing Vendor Landscape

The way that SIEM products are sold is also changing, because large vendors have integrated their SIEM technology with related products in their portfolios. 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. CA, IBM and Novell have integrated their SIEM products with related identity and access management (IAM) offerings, and are selling their SIEM solutions as part of an IAM-related deal. CA and IBM are also integrating their SIEM technology with related system management functions, such as configuration management and configuration management databases (CMDBs). NetIQ has integrated its SIEM technology with its event management and IT governance, risk and compliance management (GRCM) offerings. Symantec sells SIEM to large enterprises that use its endpoint security products, and has integrated its SIEM and IT GRCM offerings. 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 are part of an equipment acquisition.

In addition to the 23 vendors evaluated, a number of other companies' solutions have SIEM capabilities but do not fully meet inclusion criteria. However, these vendors sometimes compete with the SIEM vendors in this Magic Quadrant. NetPro provides Windows-oriented log management and event monitoring software for use by the IT operations and IT security organizations. During 2008, NetPro will extend full capabilities to non-Windows platforms.

Fair Warning provides user activity and resource access monitoring at the application layer for the healthcare vertical market. Splunk provides event collection and search technology that is sometimes used by customers to gain some of the capabilities provided by SIEM technology. Splunk's 3.2 release provides predefined reports for security and compliance use cases.

Two vendors are not included in the Magic Quadrant because of their focused regional market presence. S21Sec provides a SIEM solution to Spain and Latin America, and is planning to expand to additional geographies. Tier-3 is an Australian-based company that provides SIEM technology to the Asia/Pacific region and is increasing its visibility in Europe.

A growing number of vendors also sell solutions that are based on licensed SIEM technology. Q1 Labs licenses its technology to companies that implement the Q1 Labs technology on their own appliances and add specific integrations with their respective management infrastructures. The Enterasys Dragon Security Command Console integrated with Q1 Labs QRadar in 2005 and delivers workflow integrations with Enterasys NAC and NetSight Automated Security Manager for Distributed Intrusion Prevention. The Juniper Networks Security Threat Response Manager is an appliance solution that was released early in 2008 that uses the QRadar technology and is also integrated with Juniper's policy management sub-system. Nortel offers QRadar for Nortel as an appliance solution and as a software solution optimizing larger-size deployments. HP entered the SIEM market late in 2007 with two appliance-based offerings that use technology licensed from SenSage. The HP Compliance Log Warehouse (CLW) solution is targeted at the broad compliance market. Another version of the product – Trusted Compliance Solution for Energy (TCS-e) – adds digital signing, encryption, strong authentication and document management functions needed by the energy industry for North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC), and similar compliance requirements in other geographies.

## 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 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

This year's SIEM Magic Quadrant adds evaluations for the following vendors:

- elQnetworks has begun to compete in the enterprise SIEM market with sales of its SecureVue offering to enterprise customers.
- NitroSecurity has recently entered the SIEM space with a product that uses its core data storage and analysis technologies.
- Prism Microsystems has gradually built security and compliance capabilities into its event and log management software offering.

### Dropped

No vendors were dropped from this update of the SIEM Magic Quadrant.

## Evaluation Criteria

### Ability to Execute

- **Product/service** evaluates 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 provider's 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 functions when they are 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. It uses feedback from Gartner clients that are using or have completed competitive evaluations of the SIEM offering.

### Completeness of Vision

- **Market understanding** evaluates the ability of the technology provider to understand buyers' needs and translate those 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 vendor's 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 vendor's approach to product development and delivery that emphasizes functionality and feature set as they map to current requirements for SIM and SEM. Development plans during the next 12 to 18 months are also evaluated.
- **Innovation** evaluates the vendor's development and delivery of SIEM technology that is differentiated from the competition in a way that uniquely solves critical customer requirements.

**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 | |

**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

ArcSight continues to be the most visible SIEM point solution vendor in competitive evaluations and has the largest installed base of its point solution competitors. ArcSight provides Enterprise Security Manager (ESM) software, which is oriented to large-scale, SEM-focused deployments, and a line of log management and collector appliances that are oriented to simpler deployments and which can be implemented stand-alone or in combination with ESM. The vendor continues to develop sales channels and product simplifications to address the broader market. ArcSight plans to introduce an appliance-based offering for ESM during 2008. In March 2007, the company became the first SIEM vendor to complete an initial public offering. Although this provides ArcSight with some capital for expansion, the company must adjust to a new set of pressures from shareholders.

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. The technology provides a combination of SEM, SIM and network behavior analysis (NBA) capabilities, but it is limited in heterogeneous network device support and in its support for event analysis and reporting across appliances. Cisco MARS can be deployed for SIM and compliance reporting use cases that do not require extensive report customization. Cisco has a large effect on all other SIEM vendors because of its SIEM technology presence in such a large number of customer sites.

The RSA security division of EMC sells the enVision appliance, which provides a combination of SEM, SIM and log management. Although enVision is not as capable in SEM as best-of-breed (and more-complex) point solutions, it provides function in all three areas that is “good enough” for common deployment scenarios in an appliance form factor that is easy to deploy. enVision has one of the largest installed bases, and RSA uses its direct sales force and its channel partners to sell enVision. EMC is developing new, dedicated tiering options for SIM and SEM.

Symantec's Security Information Manager (SSIM) appliance provides SIM, SEM and log management capabilities. SSIM appliances are dynamically updated with threat and vulnerability data content from Symantec's security research and managed security areas. Symantec also provides managed service offerings that use the appliance for on-site data collection and analysis.

NetIQ's Security Manager has a large installed base that is primarily oriented to SIM, user activity monitoring and compliance reporting. Recent architectural changes (which minimize the use of relational database management system technology) have simplified deployment and greatly improved scalability. The technology can be used for network and security device sources, but it is not widely deployed for this use case because NetIQ does not typically sell to the network security buying center. NetIQ sells its security management products primarily into its operations management installed base, but also to new accounts. The company plans a 2008 release of an enhancement that provides integrated workflow between the two technology sets.

## Challengers

IBM has distinct SEM and SIM technologies, and has begun the work of merging them into a single offering that will ultimately be comprised of separately deployable SEM, SIM and log management components. IBM Tivoli Security Operations Manager (TSOM) is SEM-focused, and IBM Tivoli Compliance Insight Manager (TCIM) is SIM-focused (primarily oriented to user activity monitoring and compliance reporting). In January 2008, IBM released Tivoli Security Information and Event Manager (TSIEM) – an integrated bundle of TSOM and TCIM that enables select event sharing and common reporting from TCIM. In February, IBM released Tivoli Event Log Manager (TELM) – a log management sub-set of TCIM. The fully integrated modular offering is planned for the version 2 release of TSIEM.

CA has two products in the SIEM space: CA Audit provides basic log data collection and analysis for host systems; Security Command Center (SCC) provides SEM functions. CA has achieved a large installed base by selling CA Audit to its IAM customers. There are also some SEM-focused deployments of SCC in large environments, but SCC is not widely deployed. CA must develop capabilities to simplify deployment and to support log management use cases. CA plans to introduce a log management appliance in 2008.

LogLogic has established itself as the primary provider of log management functions in the SIEM market. The company's appliance technology is a log management platform that provides data analysis and real-time alerting to IT security and IT operations. An increasing percentage of organizations express log management requirements ahead of SEM, and LogLogic continues to increase sales. The appliance is sometimes installed as a data collection and analysis tier in conjunction with another SIEM product because of its limited SEM capabilities. Although LogLogic has partnerships with many SEM software and security service providers, customer demand and LogLogic's success have caused other SIEM vendors to (gradually) develop competing solutions.

Novell's Sentinel software offering is integrated with Novell's IAM solutions, and Novell is actively selling Sentinel as a complementary monitoring and automated remediation technology to its IAM customers. The technology is also designed for large-scale deployments that require broad and flexible SEM capabilities. The May 2007 release of Sentinel version 6 implemented changes intended to reduce deployment efforts and simplify administration.

Quest Software's InTrust is comprised of a compressed log data repository in combination with a data analysis and reporting tier. InTrust is typically deployed in combination with plug-ins for Microsoft platforms (such as Active Directory, Exchange or file servers), which replace and enhance native audit functions. The technology is primarily oriented to host log data, but a limited number of network and security devices are supported. The November 2007 release of version 9.6 extended real-time alerting to include multisource data correlation. Quest has a large installed base for InTrust, but narrow source support limits its applicability to a subset of SIEM technology buyers.

## Visionaries

Q1 Labs' QRadar product provides a combination of SIEM and NBA capabilities. The technology 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 2007, Q1 introduced Simple Log Management Information Manager (SLIM) – an entry-level log management

appliance tier. Q1 labs positions QRadar as a competitive alternative to Cisco MARS, and licenses the technology to some Cisco competitors (such as Juniper Networks, Nortel and Enterasys).

LogRhythm provides appliances that deliver a mix of log management and SEM functions with agent-less and agent-based collection options for many sources. The vendor targets midsize organizations that require SIM and SEM capabilities, but also has some larger production deployments. The 1Q08 version 4 release includes an expansion of the taxonomy to support anomaly detection and broader database management system source support.

Intellitactics' SIEM offering is comprised of two main components: Intellitactics Security Manager (ISM) software and the SAFE LA log management appliance for ISM. ISM provides broad-scope SIEM functions that are highly customizable and optimal for large-scale deployments. The 2007 version 5.6 release of ISM provided major and much needed usability and stability improvements, but the ISM technology still requires the support capabilities typically found in larger organizations. Intellitactics has begun the rollout of additional appliances (not available at the time of this writing) to provide stand-alone logging, and logging plus SEM capabilities without a dependency on ISM. The new appliances are intended to address current market requirements for simplification and rapid deployment.

NetForensics' SIEM solution is comprised of three components: 1) nFX SIM One software provides full-function SEM that has traditionally competed with point solutions from ArcSight, Intellitactics and Novell; 2) nFX Log One log management (appliance or software) can be deployed stand-alone or loosely coupled with other nFX components; and 3) nFX Data One – database activity monitoring (appliance or software) – can be deployed stand-alone or loosely coupled with other nFX components.

eIQnetworks has begun to build an installed base in the enterprise SIEM market with its SecureVue software and appliance. It also licenses SEM functions to network security vendors that don't have their own “vendor-specific SEM” and need to compete with vendors such as Cisco, ISS or Check Point Software. eIQnetworks' SecureVue offering is unique in that it provides broad capabilities that include SEM, SIM, security configuration policy compliance, operational performance functions and some NBA capabilities in a single product. eIQ's competitive challenges are to build its sales capability to compete with established vendors and to convince prospects that are focused on a single problem of the value of this breadth of function.

TriGeo's Security Information Manager appliance has been designed for ease of deployment and support. It provides a combination of SEM and SIM function, and is oriented to midsize companies that need SEM and compliance reporting. TriGeo has released a log archive and reporting function that is based on embedded technology from Splunk. TriGeo needs to continue its efforts to develop sales channels to sustain growth in a competitive segment.

## Niche Players

ExaProtect's appliance provides a combination of SEM, SIM and log management functions. The majority of ExaProtect's customers are in Europe, but the company is gradually expanding its U.S. customer base, initially selling to customers gained through its acquisition of Solsoft (a North American network configuration management vendor). Although ExaProtect has won competitive evaluations against major SIEM vendors in Europe and has sold SIEM to a few of its North American Solsoft customers, the company has recently taken major steps to strengthen its North American presence to become more visible in competitive evaluations of SIEM technology.

High Tower revamped its SIEM appliance technology with the January 2008 release of the Cinxi SIEM product line, which implements collection and aggregation tiers to support midsize and large distributed deployments. The vendor has also improved compliance-oriented reporting. High Tower needs to continue its development of sales capabilities.

During 2007, NitroSecurity expanded into the SIEM market from its position as an intrusion detection system (IDS)/intrusion prevention system (IPS) vendor with the introduction of the NitroView line of appliances. NitroView Receiver provides log collection and event correlation. NitroView ESM provides cross-source correlation and a consolidated back store to support high-speed search and reporting. The vendor has begun its entry into the SIEM segment by selling SIEM technology into its IDS/IPS installed base and by selling both solutions to new customers.

OpenService's InfoCenter software solution is composed of the InfoCenter console, event collectors, ThreatCenter (which provides SEM) and LogCenter (which provides log management functions). Although InfoCenter is easy to deploy and low in server resource requirements, OpenService has lost ground to competitors in key functional areas such as user and resource access analysis for compliance. In addition, the vendor has not been visible on client shortlists in competitive evaluations.

Prism Microsystems has gradually increased the compliance reporting and SEM capabilities of its EventTracker software offering. The vendor sells primarily to midsize enterprises that value a solution that can provide security and operations event management in a single deployment.

The SenSage solution is optimized for analytics and compliance reporting against a large log event data store, and the company has successfully pursued large deployments that require this capability. SenSage provides explicit audit support for multiple packaged applications, and has OEM arrangements with Cerner (healthcare applications), Symantec (e-mail archive) and HP (the HP Trusted Compliance Solution appliance). SenSage's version 4 release (2Q08) is intended to provide improvements in real-time event management and ease of use that are designed to expand solution applicability to a broader market.

Tenable Network Security'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 capabilities and interface of Security Center.

## Vendor Strengths and Cautions

### ArcSight

**Strengths**

- ArcSight continues to be the most visible point solution vendor in competitive evaluations, and it provides the broadest SIEM function set.
- Its log management and collector appliances provide capabilities that address common compliance use cases and simpler, lighter-weight deployment options that complement its SEM-focused ESM software.

**Cautions**

- ArcSight ESM software 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.
- Although ArcSight plans a May 2008 release of an appliance offering to provide log management and simplified SEM functions, customer references were not available at the time of this evaluation.

### 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.
- Its SIEM solutions are tightly integrated with the IAM solutions provided by CA.
- CA's SIEM solutions are especially well-suited for organizations that have already implemented other CA IAM or system management products that integrate with SCC or are willing to implement the CA suite to address requirements beyond SIEM.

**Cautions**

- Deployments of SCC for the network security use case are not widespread.
- To meet requirements for the majority of SIEM buyers, CA needs to provide simplified deployment options for use cases that require a combination of compliance reporting, log management and “light” SEM.

### Cisco Systems

**Strengths**

- The MARS SIEM appliance provides “out of the box” network SEM capabilities and is integrated with Cisco Security Manager.
- MARS should also be considered by organizations that want to gain some NBA capabilities from their SIEM deployments.

**Cautions**

- Although MARS supports basic compliance monitoring for servers, it is not optimal for SIM deployments that require highly customized audit/reporting functions.
- Larger enterprises with heterogeneous network device data source requirements, and those that require consolidated correlation or reporting across multiple appliances will find MARS insufficient for their specific needs.

### eIQnetworks

**Strengths**

- The SecureVue offering provides network SEM and compliance-oriented SIM capabilities that are easy to deploy.
- SecureVue provides a broad function set that includes SIEM, performance, security asset and configuration policy compliance capabilities.

**Cautions**

- eIQnetworks is establishing a market presence for enterprise SIEM and needs to develop broader sales capabilities.
- SecureVue capabilities are broader than the typical SIEM problem set, and eIQnetworks needs to convince prospects of the value of expanded functions in competitive evaluations.

### ExaProtect

**Strengths**

- ExaProtect's appliance-based offering is oriented primarily to large and midsize 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**

- Although ExaProtect has established an installed base in Europe, the company needs to continue executing its plans to expand in the North American SIEM market.

### High Tower

**Strengths**

- High Tower's new line of appliances provides a combination of SEM and SIM capabilities that are easy to deploy.
- It has improved event management capabilities and provides predefined reports for common compliance use cases.

**Cautions**

- Now that High Tower has competitive SIEM appliance technology, the company needs to develop its sales capabilities.

### IBM

**Strengths**

- IBM TCIM provides strong reporting capabilities for compliance and user activity, while IBM TSOM provides SEM functions.
- IBM has completed an initial integration between TSOM and TCIM that enables consolidated reporting and limited event sharing.

**Cautions**

- Although Tivoli (TSIEM) V1 provides basic integration between TSOM and TCIM, organizations that need real-time event monitoring of host log events still need to deploy two IBM products.

- Customers that are considering IBM's offerings will need to evaluate IBM's integration road map against the timing of their requirements for log management, SIM and SEM.

## Intellitactics

**Strengths**

- The current release of Intellitactics Security Manager contains user interface improvements and expanded, predefined functionality that reduces deployment and support labor when compared with previous releases.
- Intellitactics log aggregation appliance – in combination with Security Manager's proprietary, compressed back store – enables for efficient collection and online storage of large amounts of log data in combination with function event management.

**Cautions**

- Intellitactics must continue to reduce the technical skill requirements needed to provide a better match to the requirements of the broader SIEM market.
- Intellitactics needs to find ways to reach the broader market as it simplifies its offerings for expanded use cases.

## LogLogic

**Strengths**

- LogLogic has established itself as the primary provider of log management functions 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 capabilities usually preclude the use of LogLogic appliances as the sole technology when SIM and SEM functions are needed.
- Organizations that require log management and SEM should evaluate LogLogic against the log management capability of the SEM vendor under consideration.

## LogRhythm

**Strengths**

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

**Cautions**

- LogRhythm needs to establish sales capabilities to enable sustained growth in the face of competition from larger competitors.

## netForensics

**Strengths**

- netForensics nFX SIM One software is best-suited for deployments where real-time monitoring is required, flexible reporting is needed, and modest resources exist for customization and support.
- The nFX Log One and nFx Data One appliance components broaden supported use cases to those that require basic log management and database activity monitoring capabilities.

**Cautions**

- netForensics also needs to execute on its plans to simplify deployment and support requirements for the nFX Open Security Platform. The recent nFX SIM One v4.0 release is intended to address these issues.

## 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 integrated log data collection and archiving capabilities can be used to collect and analyze all log data from every source.

**Cautions**

- NetIQ is not optimized for deployments that are primarily focused on event management for network and security devices.

## NitroSecurity

**Strengths**

- NitroView provides a mix of SIM and SEM, and its repository can sustain high real-time event insert rates while supporting report generation and analytics.

**Cautions**

- NitroView lacks some SEM capabilities, such as embedded incident management support and vulnerability assessment technology integration.

## Novell

**Strengths**

- Sentinel is most appropriate for large-scale deployments that require 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**

- Deployments that require log management functions will need to be augmented with third-party log management technology.
- The technology is not a good fit 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**

- OpenService needs to improve its sales and marketing capabilities.

## Prism Microsystems

**Strengths**

- Prism Microsystems offers a software solution optimized for midsize businesses that require log management, SEM, compliance reporting and operations monitoring in a single product.
- Prism's EventTracker is easy to deploy and maintain for the SIM and SEM use cases.

**Cautions**

- EventTracker is not well-suited for implementations that require security operations center (SOC)-level event management capabilities.
- EventTracker does not integrate vulnerability assessment data.

## 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**

- InTrust, in combination with Quest plug-ins for Windows servers and applications, provides enhanced audit and reporting capabilities for the Windows platform that are not dependent on native Windows audit capabilities.

**Cautions**

- Organizations that need to enable a full-function security console for an SOC should consider solutions that provide more function or flexibility in this area.
- Organizations that require broad network and security device coverage, or that host coverage beyond Windows and the major Unix variants, will find InTrust to be a poor match to their requirements.

## RSA (EMC)

**Strengths**

- RSA enVision should be considered in cases where all data needs to be collected and available for analysis, and where a need exists for SEM and SIM capabilities.
- Because of its ease of deployment, the appliance should also be considered in environments where customers have limited personnel resources to manage servers and databases as part of their SIEM implementation.

**Cautions**

- Organizations that need to enable a full-function security console for an 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 application providers, and its technology supports precise analytics needed for use cases such as fraud detection.

**Cautions**

- Organizations that have a strong focus on real-time event management will need to validate scalability with SenSage reference customers until version 4 is more widely deployed in production environments.
- Organizations that require only basic log management functions should consider simpler and less-expensive offerings that focus on collection and basic reporting.

## Symantec

**Strengths**

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

**Cautions**

- Symantec needs to improve reporting and analytics functions to accommodate the needs of stakeholders outside the IT security technical areas.

## 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 used 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 that are looking to satisfy a mix of regulatory reporting and SEM requirements.
- The appliance provides a mix of SIM and SEM functions. It also provides automated responses through a TriGeo host agent, and intrusion detection capabilities through a bundling in the Snort open-source IDS.

### 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.

## 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.