Gartner

Research

Publication Date: 29 May 2009 **ID Number: G00167782**

Magic Quadrant for Security Information and Event Management

Mark Nicolett, Kelly M. Kavanagh

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

Security information and event management (SIEM) technology provides real-time monitoring and historical reporting of security events from networks, systems and applications. SIEM deployments are often funded to address regulatory compliance reporting requirements, but organizations should also use SIEM to improve security operations, threat management and incident response capabilities.

SIEM technology can be deployed to support three primary use cases: compliance reporting/log management, threat management, or a SIEM deployment that covers both use cases. Most organizations require a general SIEM deployment that implements capabilities in all three areas, but there is variation in use case priority and capability requirements.

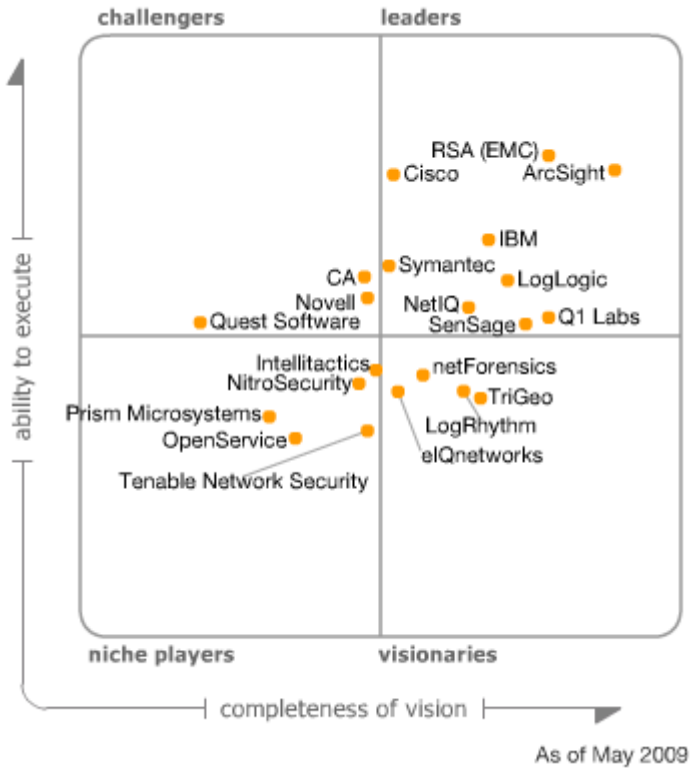
The SIEM market is composed of vendors with products that can provide at least basic support for all three use cases, but there is wide variation in the architectural approach and the relative level of support for security event management (SEM), security information management (SIM), user activity monitoring and compliance reporting. (For an evaluation of 11 SIEM products with the largest installed bases with respect to these use cases, see "Critical Capabilities for Security Information and Event Management Technology.")

Security managers considering SIEM deployments should first define the requirements for compliance reporting, log management, user and resource access monitoring, external threat monitoring, and security incident response. This may require the inclusion of other groups in the requirements definition effort, including audit/compliance, IT operations, application owners and line-of-business managers. Organizations should also describe their network and system deployment topology, so that prospective SIEM vendors can propose a solution to a company-specific deployment scenario.

The 2009 Magic Quadrant for SIEM evaluates technology providers with respect to the most-common technology selection scenario — an SIEM project that is funded to solve a compliance reporting issue, but with secondary requirements for effective threat monitoring and SEM. There are numerous variations in SIEM product architecture and deployment options, and wide variation in capabilities for log management, SEM and user monitoring.

Organizations may need to evaluate SIEM products from vendors in every quadrant to best meet specific functional and operational requirements. Product selection decisions should be driven by organization-specific requirements in areas such as the relative importance of SIM and SEM capabilities; the ease and speed of deployment; the IT organization's support capabilities; and integration with established network, security and infrastructure management applications.

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (May 2009)

Market Overview

The SIEM market grew about 30% in 2008, with total revenue at approximately $1 billion. Demand for SIEM remains strong (there is still a growing number of funded projects), but we are seeing a more tactical focus, with Phase 1 deployments that are narrower in scope. Despite a difficult environment, we still expect healthy revenue growth for 2009 in this segment.

The current economic situation constrains external funding for SIEM vendors and raises viability concerns for some privately funded vendors that:

- Are not yet cash-flow positive and will not receive further funding
- Have current investors that need to pull their money out

During 2008, High Tower ceased operations (its assets were acquired by netForensics), and a few smaller, privately held SIEM vendors pared back staffing and channel expansion initiatives to control costs.

SIEM Vendor Landscape

Twenty-one vendors meet Gartner's inclusion requirements for the 2009 SIEM Magic Quadrant. Nine are point-solution vendors, and 12 are vendors that sell additional security or operations products and services. Because SIEM technology is now deployed by a broad set of enterprises, vendors are responding with a shift in sales and product strategy. Larger vendors are working to integrate their SIEM technology with related products or service portfolios, so that they can sell SIEM to existing customers. Vendors of all sizes are developing sales channels that can reach the midsize market in North America, and are developing a presence in Europe, the Middle East and Africa, as well as the Asia/Pacific region, as SIEM deployments increase in these regions.

Some SIEM technology purchase decisions are noncompetitive, because the technology is sold by a large vendor in combination with related security, network or operations management 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. NetIQ has integrated its SIEM technology with its security configuration management and file integrity monitoring technologies. Symantec sells SIEM to large enterprises that use its endpoint security products, and has integrated its SIEM and IT governance, risk and compliance management 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 21 vendors evaluated, a number of other companies' solutions have SIEM capabilities but do not fully meet our inclusion criteria. However, these vendors sometimes compete with the SIEM vendors in this Magic Quadrant.

Splunk provides event collection, log management and search technology that is sometimes used by customers to investigate security incidents, to gain some of the capabilities provided by SIEM technology, or to complement their SIEM investments. Splunk has released predefined reports for security and compliance use cases. In April 2009, Splunk announced Splunk Enterprise Security Suite — a collection of security applications consisting of packaged searches, correlations, reports, dashboards, visualization and analysis that support security use cases, including compliance reporting, event monitoring, incident response, log management, user and system access reporting, and forensics. Splunk is not included in this evaluation because Enterprise Security Suite was released after our evaluation, and the monitoring Splunk provides is not in real time.

Four vendors are not included in the Magic Quadrant because of their regional or vertical market focus and/or SIEM revenue level:

- S21sec provides an SIEM solution, endpoint protection technology and managed security services to Spain and Latin America, and is planning to expand to additional geographies.
- Tango/04 provides SIEM, operations monitoring and business process monitoring solutions with customer concentrations in Europe and Latin America.
- Tier-3 is an Australian-based company that provides SIEM technology to the Asia/Pacific region. It is increasing its visibility in Europe.
- FairWarning provides user activity and resource access monitoring at the application layer for the healthcare vertical market.

A few vendors sell solutions that are based on licensed SIEM technology. Q1 Labs licenses its technology to vendors that implement the Q1 Labs technology on their own appliances and add specific integrations with their respective management infrastructures. The Enterasys Security Information and Event Manager appliance (also known as Dragon Security Command Console)

has been using the Q1 Labs technology since 2005, and delivers workflow integrations with Enterasys Network Access Control 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 subsystem. Nortel has discontinued the QRadar for Nortel appliance.

HP has an appliance-based offering that uses technology licensed from SenSage, and is building up an initial installed base. Although the HP Compliance Log Warehouse (CLW) solution is targeted at the broad compliance and SEM market, HP is also using the technology to enable SEM capabilities across its portfolio. HP has made CLW a core element of its Secure Advantage program, and has completed integrations with its ProCurve line of network and security devices, encryption, and software configuration management technologies. In April 2009, HP released an updated version of the CLW product that uses SenSage v.4, which provides major user interface and SEM improvements.

Customer Requirements — Compliance, Log Management, Security and Fraud Detection

Although compliance drives SIEM project funding, most organizations also want to improve external and internal threat-monitoring capabilities. As a consequence, there are requirements for user activity and resource access monitoring for host systems, and real-time event management for network security. Adoption of SIEM technology by a broad set of companies has fostered demand for products that provide predefined compliance reporting and security monitoring functions, and ease of deployment and support. The primary driver of the North American SIEM market continues to be regulatory compliance. More than 80% of SIEM deployment projects are funded to close a compliance gap. European and Asia/Pacific SIEM deployments have been focused primarily on external threat monitoring, but compliance is becoming a strong driver in these regions as well.

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

- Payment Card Industry Data Security Standards (PCI DSS) requirement for log management
- 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 and improving its scalability)

Application layer monitoring for fraud detection or internal threat management continues to evolve as a use case for SIEM technology. SIEM technology is being deployed alongside fraud detection and application monitoring point solutions to broaden their scope. These projects have been undertaken by large companies in industry vertical markets, such as financial services and telecommunications, as an internally justified security measure. A number of SIEM vendors are beginning to position their technologies as "platforms" that can provide security, operations and application analytics.

An optimal SIEM solution will:

- Support the real-time collection and analysis of log data from host systems, security devices and network devices
- Support long-term storage and reporting

- Not require extensive customization
- Be easy to deploy 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.

SIM as a Service

Most managed security service providers have service offerings for SIM, in addition to their long-standing SEM services. These new services include the collection, analysis, reporting and storage of log data from servers, user directories, applications and databases. SIM services typically forgo real-time monitoring and alerting, and focus on compliance-oriented reporting on exceptions, reviews and documentation, with the ability to store and archive logs for later investigation and for data retention requirements. These offerings are being driven by clients that need to meet compliance requirements and are seeking an alternative to buying and implementing an SIEM product. We do not include an evaluation of the service delivery capabilities of managed security service providers (MSSPs) in this Magic Quadrant.

Market Definition/Description

The SIEM market is defined by the customer's need to analyze security event data in real time for internal and external threat management, and to collect, store, analyze and report on log data for regulatory compliance and forensics. SIEM products provide SIM and SEM:

- SIM provides log management — the collection, reporting and analysis of log data (primarily from host systems and applications, and secondarily from network and security devices) — to support regulatory compliance reporting, internal threat management and resource access monitoring. SIM supports the privileged user and resource access monitoring activities of the IT security organization, and the reporting needs of the internal audit and compliance organizations.
- SEM processes log and event data from security devices, network devices, systems and applications in real time, to provide security monitoring, event correlation and incident response. SEM supports the external and internal threat monitoring activities of the IT security organization, and improves incident management capabilities.

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 supply production reference accounts for SIEM deployments.
- 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 vendor has less than $4 million in SIEM product revenue.
- The solution is delivered exclusively as a managed service.

Added

No vendors were added to this update of the SIEM Magic Quadrant.

Dropped

High Tower ceased operations in 2008 and has been dropped from this update of the SIEM Magic Quadrant.

Exaprotect was acquired by LogLogic in May 2009 and has been 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 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.
- **Sales execution/pricing** evaluates the technology provider's success in the SIEM market and its capabilities in presales activities. This includes SIEM revenue and the installed base, pricing, presales 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.
- **Operations** is an evaluation of the organization's service, support, and sales capabilities.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High

Evaluation Criteria	Weighting
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	High

Source: Gartner (May 2009)

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. Product capabilities and customer use in areas such as application layer monitoring, fraud detection and identity-oriented monitoring are evaluated, in addition to other capabilities that are product-specific, and are needed and deployed by customers.

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	No Rating
Vertical/Industry Strategy	No Rating
Innovation	High
Geographic Strategy	No Rating

Source: Gartner (May 2009)

Leaders

The SIEM Leaders quadrant is composed of vendors that have been the most successful in building an installed base and revenue stream within the SIEM market, have a relatively high viability rating (due to SIEM revenue or SIEM revenue in combination with revenue from other sources), and provide products that are a good functional match to general market requirements.

Challengers

The Challengers quadrant is composed of vendors that have a large revenue stream (typically because the vendor has multiple product and/or service lines), at least a modest-sized SIEM customer base, and products that meet a subset of the general market requirements. Many of the larger vendors in the Challengers quadrant position their SIEM solutions as an extension of related security and operations technologies.

Visionaries

The Visionaries quadrant is composed primarily of smaller vendors that provide SIEM technology that is a good match to general market requirements.

Niche Players

The Niche Players quadrant is composed primarily of smaller vendors that provide SIEM technology that is a good match to a specific SIEM use case or a subset of SIEM market requirements.

Vendor Strengths and Cautions

ArcSight

ArcSight is the most successful and visible SIEM point solution vendor with very broad function. ArcSight has the largest installed base of its point solution competitors. It 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 can be implemented stand-alone or in combination with ESM. In April 2009, ArcSight announced general availability of ArcSight Express, an appliance-based offering for ESM designed for the midmarket with preconfigured monitoring and reporting, and simplified data management. Version 3 of the ArcSight Logger appliance line (released in November 2008) provides reporting and collection performance improvements.

Strengths

- ArcSight provides the broadest SIEM function set.
- It has recently introduced an appliance that provides a simpler deployment option for SEM.
- ArcSight continues to be the most visible SIEM point solution vendor in competitive evaluations.

Cautions

- ArcSight's ESM software is oriented to environments that need capabilities that support a security operations center, and it requires substantial end-user expertise in areas such as database tuning.

CA

CA has been successful in selling its security information management (SIM) solution as an audit enhancement to its identity and access management (IAM) customers, but has not been competitive in use cases that require SEM. During 2008, CA sold two SIEM products: CA Audit (which CA has successfully sold to its IAM customers) provides basic log data collection and analysis for host systems; Security Command Center (SCC) provides SEM functions. On 20 April 2009, CA announced general availability of CA Enterprise Log Manager, a software appliance that provides log management, compliance reporting and analytics for applications, hosts, network devices and security devices. The product integrates with CA's IAM portfolio and is intended as a replacement for CA Audit. SCC is not widely deployed and requires extensive customization.

Strengths

- CA's SIM solutions are tightly integrated with the IAM technology provided by CA and are most commonly deployed for user activity monitoring on host systems.
- CA's SIM solutions are especially well-suited for organizations that have already implemented other CA IAM or system management products.
- Enterprise Log Manager provides simplified deployment options and better log management for use cases that require a combination of compliance reporting and general log management.

Cautions

- Organizations that require SEM capabilities should also evaluate SEM alternatives from other vendors.

Cisco

Cisco provides a widely sold solution that is primarily oriented to network security. Cisco has built the largest SIEM customer base for its Cisco Security Monitoring, Analysis, and Response System (MARS) appliance by positioning it as a component of its self-defending network strategy, and selling it to its network-focused buyers. The technology provides a combination of SEM, SIM and network behavior analysis (NBA) capabilities, and provides effective out-of-the-box network security monitoring and host activity monitoring for the platforms that it supports. Cisco has not done much to expand network device source support beyond its own devices, and MARS is limited in host platform, security device and application support. Cisco continues to have a large effect on all other SIEM vendors because of its SIEM technology presence in such a large number of customer sites.

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

eIQnetworks is building an installed base in the enterprise SIEM market with its SecureVue software and appliance. The company licenses SEM technology to MSSPs and also to network security vendors that use it to build SEM capabilities for their product sets. 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 has been able to win competitive evaluations against other SIEM vendors, especially when the customer has a need for capabilities in these adjacent areas.

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 broad in areas that are not part of the typical SIEM problem set, and eIQnetworks needs to continue to find prospects that value expanded functions in competitive evaluations.
- SecureVue does not yet have IAM integration beyond active directory and general Lightweight Directory Access Protocol support.

IBM

IBM's overall SIEM strategy is further integration with its IAM, security and service management technologies; leverage of ISS-managed services; and development of appliance-based offerings. IBM has three SIEM offerings. IBM Tivoli Compliance Insight Manager (TCIM) is SIM-focused and primarily oriented to user activity monitoring and compliance reporting. Tivoli Security Operations Manager (TSOM) is SEM-focused and primarily oriented to external threat management. Tivoli Security Information and Event Manager (TSIEM) is a loosely integrated bundle of TSOM and TCIM that enables select event sharing and common reporting from TCIM. Further integration is planned.

Strengths

- TSIEM integrates with a wide set of IBM and third-party IAM technologies and applications.
- TSIEM provides strong reporting capabilities for compliance and user activity monitoring.
- IBM is expanding the integration of its SIEM offerings with its operations management technologies.

Cautions

- Although TSIEM provides basic integration between TSOM and TCIM, organizations that need real-time event monitoring of host log events still need to deploy two technologies.
- Although TSIEM implements a log management tier via software, a log management appliance is not yet available from IBM.

Intellitactics

Intellitactics has rearchitected its SIEM offerings and now provides both software and appliance-based solutions for security event management compliance and log management. Intellitactics Security Manager (ISM) is a software offering that is highly customizable and optimal for large-scale SEM-focused deployments. The SAFE line of appliances provides data collection, log management and basic SEM. The new appliances address current market requirements for simplification and rapid deployment.

Strengths

- The current Intellitactics SIEM product line provides user interface improvements, and expanded, predefined functionality that reduces deployment and support labor when compared with previous releases.
- Intellitactics provides solutions for large-scale deployments that require customization and solutions for midsize companies that require predefined function and simplified deployment.

Cautions

- Intellitactics must continue its effort to develop sales channels that are effective in reaching a critical mass of midsize companies.

LogLogic

LogLogic has expanded from its position as the major log management provider, into direct competition with the broader SIEM providers. LogLogic has expanded its functional capabilities to include SEM, database activity monitoring and network security configuration management. In May 2009, LogLogic closed the acquisition of Exaprotect, which provided SEM and network security configuration management technology. Prior to the acquisition, LogLogic had released its Security Event Manager appliance, which used technology licensed from Exaprotect. In addition, LogLogic has released Database Security Manager, which provides database activity monitoring and security management. This solution uses agent technology in combination with a specialized appliance. LogLogic has also released the Compliance Manager appliance, which provides compliance dashboards and workflow.

Strengths

- LogLogic has augmented its log management functions with taxonomy-based event correlation and management through the acquisition of Exaprotect.
- LogLogic provides the capability to monitor and shield Oracle, SQL Server and Sybase DBMS through the use of specialized agent technology.

Cautions

- LogLogic needs to continue efforts to extend SEM knowledge to its sales force, sales channels and presales support.

LogRhythm

LogRhythm's SIEM technology provides SEM and log management capabilities, as well as compliance and security operations reporting. During the past 18 months, the company has expanded beyond its primary installed base of midsize organizations to include larger enterprises. The technology can be delivered in several formats. The Dashboard, Event Manager and Log Manager formats are available as software images, as an all-in-one appliance or as separate appliances for each function. LogRhythm supports agent-based and agentless collection for many host, network and application sources, and the agent also provides basic file integrity monitoring.

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

- Although LogRhythm is growing rapidly, the company is still among the group of smaller vendors in the market and needs to continue to develop its sales channels to maintain its growth.

netForensics

netForensics is a SIEM point solution vendor that has a mix of end-user and MSSP customers. Its SIEM solution is composed of three components: (1) nFX SIM One software provides full-function SEM that has traditionally competed with point solutions from vendors such as ArcSight, Intellitactics and Novell. (2) nFX Log One provides log management. (3) nFX Data One provides network and agent-based database activity monitoring. nFX log One and nFX Data One are available as software or an appliance and can be deployed stand-alone or loosely coupled with other nFX components. In January 2009, netForensics acquired the assets of High Tower and will position the Cinixi appliance as a combined log management and event management solution for the midmarket.

Strengths

- The 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 needs to broaden its presence on competitive evaluations.

NetIQ

NetIQ is a business unit of Attachmate. It has a portfolio of security and operations technologies, with a moderately sized SIEM customer base. NetIQ provides operations and security management software products that are integrated but typically deployed individually over time. NetIQ sells its security management products into its operations management installed base, but also to new accounts. The NetIQ Security Manager SIEM product has a large installed base that is primarily oriented to SIM, user activity monitoring and compliance reporting. 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. 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.

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.
- Security Manager is tightly integrated with the Change Guardian product line that provides monitoring and change detection for active directory and file integrity monitoring for host systems.

Cautions

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

NitroSecurity

NitroSecurity is expanding into the SIEM market from its core intrusion detection system (IDS)/intrusion prevention system (IPS) business. The vendor sells SIEM technology into its IDS/IPS installed base and is also selling both solutions to new customers.

The NitroView line of SIEM appliances uses the high-speed event storage and query technology from its IDS/IPS products. 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.

During 2008, NitroSecurity acquired Rippletech and integrated its database activity monitoring technology with NitroView. Early in 2009, NitroSecurity also acquired Chronicle and is working to enable its network data analysis capabilities with its real-time monitoring.

Strengths

- NitroView provides a mix of SIM and SEM, and its repository can sustain high real-time event insert rates, while supporting high-performance report generation and analytics.
- Database activity monitoring (network monitor and agent-based) is available as an integrated option.

Cautions

- NitroView's embedded incident management support is limited.

Novell

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. Novell's Compliance Management Platform is an integrated bundle of IAM and SIEM technology. Sentinel is designed for large-scale deployments that require broad and flexible SEM capabilities, but it is complex to deploy and, therefore, is not a good match to Novell's strategy of selling SIEM to its IAM customers. Late in 2008, Novell released the Novell Identity Audit package, which provides basic log management and reporting for Novell's IAM products. At the time of this evaluation, Novell was planning the release of two enhancements: (1) the Sentinel 6.1 Rapid Deployment option — intended to provide simplified deployment and support (2Q09 release); and (2) Sentinel Log Manager — a log management tier for Sentinel (release planned later in 2009).

Strengths

- Sentinel is most appropriate for large-scale SEM-focused deployments where selective collection and analysis of event data are acceptable.
- Sentinel is based on a message bus architecture that provides flexibility and scaling for large deployments.
- The Identity Audit solution is well-suited to organizations that use Novell IAM products and need broader audit capabilities.

Cautions

- Organizations that require log management functions will need to wait for Novell's Sentinel Log Manager release or will need to augment their SEM deployment with third-party log management technology.
- While the Sentinel 6.1 Rapid Deployment release is intended to provide simplified deployment and support, it was not generally available at the time we conducted our evaluation, and we had not yet spoken to production references.

OpenService

OpenService provides event management software that covers system management and security management use cases. The technology is scalable, easy to deploy and differentiated in its approach to correlation. Despite its differentiated technology and some very large referenceable customers, OpenService was slow to adapt to the shift in demand to a compliance focus, and has suffered from ineffective sales and marketing. In 2008, the company received additional funding and has a new management team in place. OpenService's InfoCenter is composed of the InfoCenter console, ThreatCenter (risk-based correlation/analysis), LogCenter (log storage), NerveCenter (availability and performance monitoring) and Event Collectors.

Strengths

- OpenService is a good choice for organizations that are looking for an out-of-the-box SEM solution with modest server-side resource requirements.
- OpenService has improved InfoCenter's reporting and user interface features.
- Risk-based correlation evaluates events with respect to threats, vulnerabilities and asset attributes, and is an alternative to rule-based approaches.

Cautions

- Open Service still has limited visibility among Gartner customers in competitive evaluations and must develop broader sales channel partnerships.
- OpenService needs to strengthen its direct sales and marketing capabilities.

Prism Microsystems

Prism Microsystems EventTracker software is targeted primarily at midsize commercial enterprises and government organizations with security and operations event management and compliance reporting requirements. Prism continues to improve the event management and compliance reporting capabilities of EventTracker, and the software now supports scalability through virtualization and through hierarchical or multisite deployment. EventTracker includes specific monitoring support for virtual environments. The EventTracker agent also provides support for file integrity monitoring.

Strengths

- EventTracker software is suited for midsize businesses that require one product that provides log management, SEM, compliance reporting and operations monitoring.
- Prism's EventTracker is easy to deploy and maintain, especially in Windows environments, where EventTracker supports centralized agent deployment and management.
- Knowledge Packs provide EventTracker with prebuilt correlation, alerting and reporting for specific compliance regimes or operations requirements.

Cautions

- EventTracker is not well-suited for implementations that require security operations center capabilities or integration with configuration/asset management databases.
- Some Windows vulnerability assessment functions are provided in EventTracker, but the product does not integrate vulnerability assessment data from other vulnerability assessment products.
- EventTracker does not have integration capability with IAM products.

Q1 Labs

Q1 Labs' QRadar appliance line provides a combination of SIEM, log management and NBA. The company is growing rapidly through direct sales to large customers, through the use of channel partners, and by licensing the technology to network and security vendors. While Q1 Labs competes in the overall SIEM market, the company also positions QRadar specifically as a competitive alternative to Cisco MARS, and licenses the technology to some Cisco competitors (such as Juniper Networks and Enterasys). The QRadar technology provides an integrated view of the threat environment using NetFlow and direct network traffic monitoring, in combination with host activity monitoring and reporting from log data. QRadar Simple Log and Information Management (SLIM) is a log management appliance that can be upgraded to full SIEM capabilities. The vendor has actively pursued deployments that require user-oriented monitoring and deployments that are compliance-focused.

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

- Organizations that are evaluating QRadar for identity-auditing-focused deployments should also evaluate the SIEM offerings of incumbent IAM vendors.

Quest Software

Quest Software provides an SIEM offering that is complementary to its line of Active Directory and Windows Server management products, and is typically implemented by customers that have deployed those products. The InTrust software solution for SIEM includes data analysis, reporting and log collection. The SIEM product favors Microsoft environments. Plug-ins and additional Quest Software products are often deployed to expand monitoring functionality specific to Microsoft platforms, including Active Directory, Exchange and file servers. InTrust is primarily oriented to host log data, but has some support for network devices and network-based security technology. Quest Software has a large installed base for InTrust, but narrow source support limits its applicability to a subset of SIEM technology buyers.

Strengths

- Organizations with a predominantly Microsoft-based IT environment will be able to extend the native audit capabilities of Microsoft products with InTrust and related plug-ins.
- Quest Software has extensive monitoring capabilities for Microsoft Active Directory, Exchange and file servers that can be applied to user activity reporting.

Cautions

- Organizations that need to enable a full-function security console for a security operations center should consider solutions that provide more function or flexibility in this area.
- InTrust is not well-suited where monitoring requirements include operating systems other than Windows and major Unix distributions, nor where monitoring firewall, IDS/IPS or a broad range of network devices is an important consideration.

RSA (EMC)

RSA, the Security Division of EMC, sells the enVision appliance, which provides a combination of SEM, SIM and log management. enVision has one of the largest installed bases, and RSA uses its direct sales force and its channel partners to sell enVision. Although enVision has not been as capable in SEM as best-of-breed (and more-complex) point solutions, it has provided function in all three areas that was "good enough" for common use cases in an appliance form factor that is easy to deploy. In March 2009, RSA released enVision v.4, which has improved correlation capabilities for external threat management, privileged user monitoring and system monitoring.

New correlation rules fully use the enVision taxonomy (as opposed to referencing source-level events).

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 in a single appliance.
- 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

- Application-layer monitoring is limited when compared with solutions that are best of breed in this area.

SenSage

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. The company has also successfully pursued use cases that require application layer and/or user-oriented monitoring. The 2008 release of SenSage v.4 enables the company to compete more broadly in the SIEM market, because it solved limitations in real-time collection and event management capabilities. Version 4 also delivered improvements to the user interface that ease deployment and administrative tasks, and has also improved the usability of report generation functions. SenSage has OEM arrangements with Cerner (healthcare applications) and HP (the HP CLW appliance).

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 require only basic log management functions should consider simpler and less-expensive offerings that focus on collection and basic reporting.

Symantec

Symantec Security Information Manager (SSIM) is delivered as a software appliance and provides SIM, SEM and log management capabilities. SSIM is dynamically updated with threat and vulnerability data content from Symantec's DeepSight security research and managed security areas. Symantec also provides managed service offerings that use the soft appliance for on-site data collection and analysis. Symantec has integrations between its SIEM and Security Endpoint Protection (SEP) technologies, and will focus on selling its SIEM offering into its SEP customer base.

Strengths

- The SSIM appliance provides SIM, SEM and log management functions that are scalable and easy to deploy.
- The dynamic DeepSight content enables real-time identification of active external threats and known malicious sources.

Cautions

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

Tenable Network Security

Tenable Network Security's SIEM solution is tightly integrated with the company's active and passive vulnerability scanner products, and its SIEM customers tend to also use the vulnerability scanning and configuration assessment technology. Tenable's SIEM software solution includes the Security Center console environment and the Log Correlation Engine (LCE). The LCE can be distributed in a network to collect logs from host and network devices, and also correlate events with data from Tenable's vulnerability scanning and security configuration assessment products. Security Center integrates Tenable's Log Correlation Engine and vulnerability scanning products to provide unified asset discovery, vulnerability detection, event management log collection and reporting.

Strengths

- The integration with Tenable's Nessus Vulnerability Scanner and Passive Vulnerability Scanner products can be beneficial to buyers seeking to address scanning and log collection, and reporting requirements, though a single user interface.
- Security Center's basic NetFlow collection and anomaly detection can be used for host breach discovery.
- A scripting capability offers customization options to users with sufficient technical expertise.

Cautions

- Other SIEM solutions provide a better fit for deployments that are focused on regulatory compliance reporting requirements related to host identity and access activity.
- Tenable needs to continue its efforts to expand its sales capabilities.

TriGeo

TriGeo has designed its appliance-based SIEM solutions for midsize organizations that need out-of-the-box external threat monitoring and compliance reporting. In addition to the Security Information Manager for information and event management, TriGeo offers distributed appliances for log collection and for network event collection, an appliance for business intelligence reporting, and an appliance for log searching/reporting, which includes embedded technology from Splunk.

Strengths

- TriGeo's appliance-based approach provides easy-to-deploy SIEM, with extensive predefined correlation and compliance reporting templates.
- Add-on appliances for log collection, network device alert collection, searching and reporting enable customers to add incremental capabilities.

Cautions

- Other SIEM solutions are a better fit for large-scale data collection and aggregation efforts, or where deployment requirements include extensive customization and integration with other IT management technology.
- TriGeo targets the small-to-midsize enterprise market, and must develop more sales channels to sustain growth, in the face of larger competitors that are beginning sell into the segment.

RECOMMENDED READING

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

Vendors Added or Dropped

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

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets and skills, 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 presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales 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 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 and service-level agreements.

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

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

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

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

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

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

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

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

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

REGIONAL HEADQUARTERS

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

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

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

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

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

Gartner