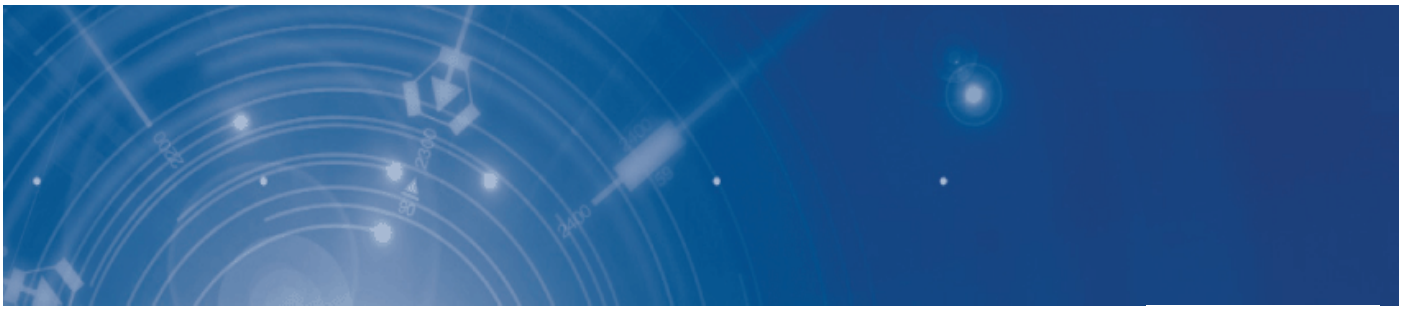


Gartner

Magic Quadrant for Security Information and Event Management

13 May 2010

Mark Nicolett, Kelly M. Kavanagh

Gartner RAS Core Research Note G00176034

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

What You Need to Know

Security information and event management (SIEM) technology provides two major functions for security events from networks, systems and applications:

- Security information management (SIM) — log management and compliance reporting
- Security event management (SEM) — real-time monitoring and incident management

SIEM deployments are often funded to address regulatory compliance reporting requirements, but organizations should also use SIEM technology to improve threat management and incident response capabilities.

SIEM technology can be deployed to support three primary use cases: SIM, SEM or a general SIEM deployment that implements a mix of log management, reporting and real-time event management capabilities. As a companion to this research, we also evaluate the SIEM technologies of 12 vendors with respect to these three use cases. Organizations require a general SIEM deployment, but there are variations in use-case priority and capability requirements.

The SIEM market has matured, and is composed of vendors with products that can provide basic support for all three use cases; however, there are variations in the relative level of capability for each use case, in the architectural approach, in deployment and support complexity, and in support for emerging use cases (such as application and user activity monitoring).

This Magic Quadrant evaluates technology providers with respect to the most-common technology selection scenario: an SIEM project that is funded to resolve a compliance reporting issue, but with secondary requirements for effective threat monitoring and SEM.

Organizations may need to evaluate SIEM products from vendors in every quadrant of this Magic 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; identity and application monitoring requirements; and integration with established network, security,

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

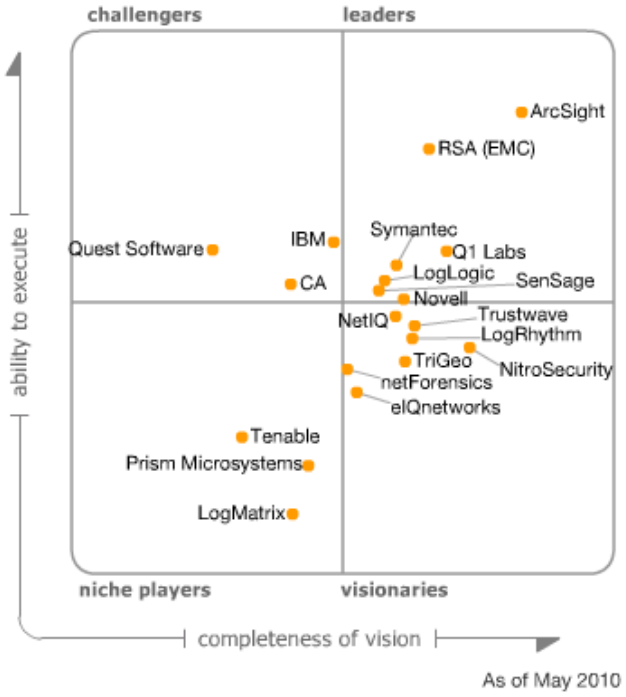
infrastructure and identity management applications.

Security managers considering SIEM deployments should first define the requirements for SIM and SEM. The requirements definition effort may need the input of other groups, including audit/compliance, identity administration, IT operations and application owners. Organizations should also describe their network and system deployment topologies, and assess event rates so that prospective SIEM vendors can propose solutions to company-specific deployment scenarios (see Figure 1).

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (May 2010)

Return to Top

Market Overview

In 2009, demand for SIEM remained very strong. The number of Gartner inquiry calls from end-user clients with funded SIEM projects grew by more than 35% over 2008, and many vendors reported substantial increases in customers in 2009; however, revenue growth was less than 15%. We think that the size of initial deployments was much smaller in 2009 than in 2008, due to budget constraints and the continued adoption of the technology by smaller organizations.

The market is bifurcating, with a relatively small number of vendors that are very visible in competitive evaluations and are growing ahead of the market, and other vendors that are growing much slower or are stalled or shrinking. Many of the larger vendors in this space now exhibit multiyear patterns of poor visibility in competitive evaluations, as well as slow responses to core requirements. As a consequence, we have adjusted our Ability to Execute rating such that the absolute size of the vendor's overall customer base and revenue stream has less influence than in previous years.

The market is maturing and very competitive. We are now in a broad adoption phase in which multiple vendors can meet the basic log management, compliance and event monitoring requirements of a typical customer. In the early days of this market, vendors scrambled to meet

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 website, 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.

customer requirements. In the current market, vendors are developing capabilities for a narrow segment of forward-thinking customers and proactively marketing those capabilities to the rest of their customers.

In the past four years, the North American market has been the source of most of the demand, driven by regulations or security standards such as Sarbanes-Oxley and Payment Card Industry (PCI). There had been a lower level of demand in Europe and Asia/Pacific, driven mostly by the SEM use case; however, we have recently seen a marked increase in demand from clients in Europe and Asia/Pacific, driven by a combination of security standards (like PCI), a variety of regional regulations and the threat management use cases that we have seen in the past.

SIEM Vendor Landscape

Twenty vendors met Gartner's inclusion requirements for the 2010 SIEM Magic Quadrant. Nine are point-solution vendors, and 11 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 strategies. SIEM vendors are increasingly focused on covering additional use cases so that they can continue to sell additional capabilities to their existing customer bases. Large vendors are positioning SIEM as a platform that can unify adjacent security and operations technologies within their portfolios. Many SIEM vendors are developing sales channels that can reach the midsize market in North America. Sales effectiveness in Europe and Asia/Pacific is becoming increasingly important 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 technologies. 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 (GRCM) offerings. During the latter half of 2009, Cisco decided to freeze support for non-Cisco security devices within its Security Monitoring, Analysis and Response System (MARS), effectively withdrawing itself from the SIEM market.

In addition to the 20 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.

Tripwire entered the SIEM space in January 2010 with technology from the acquisition of a small SIEM vendor. Tripwire Log Center provides log management and security event management in a single solution. Tripwire's VIA technology provides tight integration with the company's core file integrity monitoring and security configuration assessment technologies. Although we have evaluated customer references, the technology did not yet meet minimum sales revenue inclusion criteria.

Splunk provides event collection, log management and search technologies that are often used by customers for forensic investigations or to provide log management functions for SIEM deployments, and also for ad hoc compliance reporting. Splunk is gradually expanding its support for SIEM use cases. The company provides predefined reports for security and compliance use cases. In 2009, Splunk announced Splunk Enterprise Security Suite — a collection of security applications consisting of packaged searches, correlations, reports, dashboards, visualization and analyses 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 it is in the process of introducing real-time monitoring, and we were unable to validate its production deployments at the time of this research effort.

AlienVault provides AlienVault Professional SIEM, which is a framework (available as software or an appliance) that integrates open-source and proprietary components. The company launched in 2007, but its Open Source SIM (OSSIM — the open-source software components) has been available since 2003. AlienVault Professional SIEM provides SIEM functionality as well as integrated intrusion detection, vulnerability

assessment, and other network and security monitoring and detection components. AlienVault was initially based in Madrid, Spain, but is now incorporated in the U.S. Customer references indicate that the software is much less expensive than most competing products in the SIEM space.

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

- S21sec provides an SIEM solution that incorporates endpoint control technology and a cyberintelligence service. Geographically, the largest installed bases are in Europe and Latin America; however, S21sec is also becoming active in projects in the Middle East and Africa. Industry verticals include financial services as well as those that require operational control system monitoring.
- Tango/04 provides SIEM, operations monitoring and business process monitoring solutions with customer concentrations in Europe and Latin America.
- Tier-3 is an Australia-based company that provides SIEM technology to the Asia/Pacific region. It is increasing its visibility in Europe.
- FairWarning provides privacy breach detection and prevention solutions for the healthcare market that entail user activity and resource access monitoring at the application layer.

A few vendors sell solutions that are based on licensed SIEM technology. Q1 Labs licenses its technology to vendors that implement its technology on their own appliances, and add specific integrations with their respective management infrastructures. The Enterasys Security Information & 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. The Juniper Networks Security Threat Response Manager, released in early 2008, is an appliance solution that uses the QRadar technology, and is also integrated with Juniper's policy management subsystem.

HP has an appliance-based offering that uses technology licensed from SenSage, and has a growing installed base that also includes an increasing number of its outsourcing customers. 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.

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

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 also becoming a strong driver in these regions. Adoption of SIEM technology by a broad set of companies has fostered demand for products that provide predefined compliance reporting and security monitoring functions, as well as ease of deployment and support. Log management functions have become a more important customer requirement because of the following factors:

- PCI Data Security Standards' (DSS's) 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 an 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)

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 applications, as well as requirements for real-time event management for network security. Application layer monitoring for fraud detection or internal threat management continues to evolve as a use case for SIEM technology. This 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. We also see demand for application layer monitoring in the energy vertical (driven by the North American Electric Reliability Corporation's [NERC's] Critical Infrastructure Prevention [CIP]), and we are beginning to see some initial interest in the healthcare industry in anticipation of requirements for the Health Information Technology for Economic and Clinical Health (HITECH) Act. 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 and support, log management functions, and application and user monitoring capabilities are weighted more heavily in this year's Completeness of Vision evaluation.

SIM as a Service

Most managed security service providers (MSSPs) 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 MSSPs in this Magic Quadrant. However, we do note SIEM product vendors that offer remote management of their SIEM products.

Return to Top

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. The vendors that are included in our analysis have technologies that have been designed for this purpose, and they actively market and sell these technologies to the security buying center. 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, as well as 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 responses. SEM supports the external and internal threat monitoring activities of the IT security organization, and improves incident management capabilities.

Return to Top

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, including network devices, security devices, security programs and servers.
- 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:

- They provide SIEM functions that are oriented primarily to data from their own products.
- They position their products as an SIEM offering, but the products do not appear in the competitive shortlists of end-user organizations.
- They have less than $4 million in SIEM product revenue.
- The solution is delivered exclusively as a managed service.

Return to Top

Added

Trustwave has been added to this update of the SIEM Magic Quadrant due to its acquisition of Intellitactics.

Return to Top

Dropped

Cisco has been dropped from the SIEM Magic Quadrant due to its decision to freeze support for most of the non-Cisco event sources that have been supported by MARS.

Intellitactics has been dropped due its acquisition by Trustwave.

Return to Top

Evaluation Criteria

Ability to Execute

- **Product / service** evaluates product functions in areas such as SIM, SEM, log management, incident management, workflow and remediation support, and reporting capabilities.
- **Overall viability** includes an assessment of the organization's financial health, the financial and practical success of the overall company, and the likelihood that the business unit will continue to invest in the SIEM technology segment.
- **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 size, growth rates for SIEM revenue and the installed base, 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 in

combination with 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
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 2010)

Return to Top

Completeness of Vision

- **Market understanding** evaluates the ability of the technology provider to understand buyers' needs and to 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.
- **Marketing strategy** evaluates the vendor's ability to effectively communicate the value and competitive differentiation of its SIEM offering.
- **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 sets 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 meets 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 2010)

Return to Top

Leaders

The SIEM Leaders quadrant is composed of vendors that provide products that are a good functional match to general market requirements, as well as vendors that have been the most successful in building an installed base and revenue stream within the SIEM market, and have a relatively high viability rating (due to SIEM revenue, or SIEM revenue in combination with revenue from other sources). Companies in this quadrant offer functionality that is a good match to current customer requirements, and they also show evidence of superior vision and execution for anticipated requirements. Leaders typically have relatively high market share and/or strong revenue growth, and demonstrate positive customer feedback for effective SIEM capabilities and related service and support.

Return to Top

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-size 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. Companies in this quadrant typically have strong execution capabilities, as evidenced by financial resources, a significant sales and brand presence garnered from the company as whole, or other factors. However, Challengers have not demonstrated as rich a capability or track record for their SIEM technologies as vendors in the Leaders quadrant have.

Return to Top

Visionaries

The Visionaries quadrant is composed of vendors that provide products that are a good functional match to general SIEM market requirements, but have a lower Ability to Execute rating than the Leaders. This lower rating is typically due to a smaller presence in the SIEM market than the Leaders, as measured by installed base or revenue size or growth, or by smaller overall company size or general viability.

Return to Top

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. Niche Players focus on a particular segment of the client base or a more-limited product set. Their ability to outperform or innovate may be affected by this narrow focus. Vendors in this quadrant may have a small or declining installed base, or be limited, according to Gartner's criteria, by a number of factors. These factors may include limited investments or capabilities, a geographically limited footprint, or other inhibitors to providing a broader set of capabilities to enterprises now and during the 12-month planning horizon. Inclusion in this quadrant does not reflect negatively on the vendor's value in the more narrowly focused service spectrum.

Return to Top

Vendor Strengths and Cautions

ArcSight

ArcSight is the most successful and visible SIEM point solution vendor with a 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; ArcSight Express, an appliance-based offering for ESM that's designed for the midmarket with preconfigured monitoring and reporting; and a line of log management and collector appliances that can be implemented as stand-alone or in combination with ESM. ArcSight's development plans include expansion of application monitoring capabilities, further simplifications to deployments, and better integration between the log and event management tiers.

Return to Top

Strengths

- ESM provides a complete set of SEM capabilities that can be used to support a security operations center.
- ArcSight Logger provides log management capabilities, and ArcSight Express provides a simplified option for SEM deployment.
- Optional modules provide advanced support for user activity monitoring, IAM integration and fraud management.
- ArcSight continues to be the most visible SIEM point solution vendor in competitive evaluations.

Return to Top

Cautions

- ArcSight's ESM software is oriented to environments that need capabilities to support a security operations center, and it requires substantial end-user expertise in areas such as database tuning.
- Organizations that do not require full-function event management may be able to deploy simpler and less expensive alternatives than ArcSight ESM, and should consider ArcSight Express along with competing alternatives from other vendors.

Return to Top

CA

CA's overall SIEM product strategy is to focus on IAM, user activity and compliance reporting. The company has successfully sold its CA Audit and CA Enterprise Log Manager solutions to its IAM customers, but is not visible in competitive evaluations and currently lacks a viable SEM solution. CA's primary offering for the SIEM market is CA Enterprise Log Manager, which is a software appliance that provides log management, basic real-time monitoring, 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 long-term replacement for CA Audit. While CA supports an existing customer base for its Security Command Center (SCC) SEM technology, SCC is no longer being sold by CA, and CA does not have a replacement technology for SEM. There is an alert-forwarding integration with CA Spectrum Infrastructure Manager. The next release of Enterprise Log Manager (planned for 2010) will provide real-time correlation capabilities and enhancements to user activity monitoring.

Return to Top

Strengths

- CA's SIM solutions are tightly integrated with the IAM technology provided by CA, are especially well-suited for organizations that have already implemented other CA IAM or system management products, and are most commonly deployed for user activity monitoring on host systems.
- 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.

Return to Top

Cautions

- Enterprise Log Manager's network device support and security device support are extremely limited.
- Enterprise Log Manager currently lacks incident management support, but can be integrated with CA or third-party incident management systems.
- Organizations that require external threat monitoring or SEM capabilities beyond user activity monitoring should evaluate SEM alternatives from other vendors.

Return to Top

eIQnetworks

eIQnetworks targets enterprise security and compliance buyers with its SecureVue product. The company also licenses SEM technology to MSSPs, and to network security vendors that use it to build SEM capabilities for their product sets. A distinguishing characteristic of SecureVue is its functional breadth — with capabilities that include SEM, SIM, security configuration policy compliance, file integrity monitoring, operational performance functions, and some network behavior analysis capabilities. SecureVue is composed of a hierarchy of server and collector components, with a minimal deployment consisting of a global central server and a data collector. Additional tiers of optional servers (regional, local and data processing) and optional agents can be added to scale deployments. The server components are available as software images or appliances, while collectors and agents are software only.

Return to Top

Strengths

- SecureVue augments SIEM functionality with additional operational performance, as well as asset and configuration policy compliance capabilities. eIQnetworks has been able to win competitive evaluations against other SIEM vendors, especially when the customer has a need for capabilities in these adjacent areas.
- Customer feedback indicates that SecureVue is easy to deploy.
- SecureVue's role-based access and tiered deployment architecture support federated enterprise and service provider requirements.
- eIQnetworks has bolstered its system integrator and technology partnerships for channel and OEM deals.

Return to Top

Cautions

- eIQnetworks is establishing a market presence for enterprise SIEM and needs to develop broader direct sales capabilities.
- SecureVue capabilities are broad in areas that are not part of the typical SIEM problem set, and eIQnetworks needs to continue finding prospects that value expanded functions in competitive evaluations.

Return to Top

IBM

IBM's overall SIEM strategy continues to be focused on integration with its IAM, security and service management technologies; its leverage of Internet-Security-Systems-managed services; and its development of appliance-based offerings. The company indicates a large and growing installed base, but IBM's SIEM technology is not often on the shortlists of companies that are doing competitive evaluations. IBM has three SIEM offerings:

- 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) provides log management and integration between TCIM and TSOM. TSIEM Version 1 provides a loose integration between TSOM and TCIM that enables select event sharing and common reporting from TCIM. In 2009, enhancements included direct reporting from log storage and further expansion of localization support. In February 2010, IBM released TSIEM Version 2 and indicated that it provides more scalable log management and a tighter integration of SIM and SEM functions, but we have not spoken with customers that have deployed it.

Return to Top

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, and also is providing a variety of blended or hybrid technology/managed service offerings that use TSIEM as the base.

Return to Top

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, and SEM capabilities are not best in class. TSIEM Version 2 is positioned as a fully integrated offering, but we have not been able to validate this with customer references.
- Although TSIEM implements a log management tier via software, a log management appliance is not available from IBM.
- IBM is not very visible in competitive evaluations.
- IBM customer feedback on product function and support is mixed.

Return to Top

LogLogic

LogLogic has seen its position as the pioneering log management provider challenged by SIEM vendors that now provide their own log management capabilities. In 2009, LogLogic expanded its functional capabilities to include SEM and network security configuration management (via the Exaprotect acquisition), and database activity monitoring (via a licensing arrangement). In addition to its log management appliance line, LogLogic provides Security Event Manager, Database Security Manager and Compliance Manager (which provides compliance dashboards and workflows). In 2010, LogLogic plans to release two new functions, "Log Labels" and "Unified Collection Framework," that will provide the ability to integrate with unsupported data sources — an important capability for application layer integration that many competitors already have.

Return to Top

Strengths

- The LogLogic line of log management appliances provides competitive log management capabilities that can be integrated with a wide variety of third-party event managers.
- The LogLogic Security Event Manager can be loosely coupled to the log management appliances via the log routing function, which can be configured to send a filtered subset of log data to the event manager.
- LogLogic provides the capability to monitor and shield Oracle, SQL

Server and Sybase DBMS through the use of specialized agent technology.

Return to Top

Cautions

- In 2009, LogLogic was not as visible in competitive evaluations among Gartner clients as it was in the past, and it needs to continue its efforts to extend SEM knowledge to its sales force, sales channels and presales support.
- LogLogic needs to improve its support for application layer integration, which the vendor plans to address with the release of a user interface that will allow a customer to define the formats of unsupported log sources.
- The company needs to deepen the integration between the log management appliances and its Security Event Manager so that the customer does not have to move between interfaces when doing investigative work.

Return to Top

LogMatrix

In 2009, the recently installed LogMatrix (formerly OpenService) management team continued the restart of the company, which began in 2008. Late in 2009, the company name was changed from OpenService to LogMatrix as part of a rebranding effort. The company has retained a core set of large customers and is focusing on building sales and marketing. EventCenter and LogCenter form the core of the LogMatrix SIEM solution. These components provide real-time correlation and log storage, and are managed by the CommandCenter console, which also provides reporting. Although the product offers traditional rule-based correlation capabilities, LogMatrix emphasizes a separate risk-weighting correlation approach to identify and rank events.

Return to Top

Strengths

- The risk-based correlation feature provides a user-configurable evaluation of events that includes threats as well as the attributes and vulnerabilities of target assets.
- Customers with sufficient expertise can access EventCenter and LogCenter data, and can develop custom reporting, dashboards and integration with other enterprise management technologies.
- LogMatrix has demonstrated its ability to provide fast response in implementing customer requests for enhancements and new features.

Return to Top

Cautions

- LogMatrix continues to have limited visibility among Gartner customers in competitive evaluations, and must develop greater direct sales capabilities and broader sales channel partnerships.
- The company's rapid responses to customer requests for incremental product enhancements have sometimes resulted in the need to patch or correct those enhancements shortly after release — a need to which LogMatrix has consistently responded.

Return to Top

LogRhythm

LogRhythm sells its SIEM appliance offering primarily to midsize businesses, but also has some large deployments that we have verified through customer references. The SIEM offering is composed of appliances that can be deployed in smaller environments in an all-in-one mode (a single

appliance provides log management and event management), or it can be scaled as a set of specialized appliances (log management, event management and centralized console). The technology also includes optional agents for major operating systems that can be used for filtering at the source. An agent upgrade is available and provides file integrity monitoring for Windows and Unix. In the past year, LogRhythm has continued to grow its installed base, increased staffing in several areas and added channel partners.

Return to Top

Strengths

- LogRhythm provides a balance of log management, reporting, event management, privileged user and file integrity monitoring to support security operations and compliance use cases.
- The appliance format and configuration wizards allow for fast deployment with minimal resources.
- The predefined reports included with the product and the custom report creation features get good marks from users.
- LogRhythm has added resources in sales, channel and professional services to address enterprise market requirements.

Return to Top

Cautions

- LogRhythm is relatively new in supporting large enterprise deployments.
- As a smaller vendor, LogRhythm must continue its efforts to increase its visibility to enterprise buyers.

Return to Top

netForensics

netForensics sells its SIEM technology to enterprise and service provider customers, but has not been as visible in the market as it has broadened to smaller companies. In 2009, netForensics focused more effort on expanding its service provider customer base, and that strategy is working well. netForensics' SIEM solution is composed of two components:

- nFX SIM One software provides full-function SEM for large environments.
- nFX Cinxi One (from the January 2009 acquisition of High Tower Software) is a hardware appliance for midsize environments that combines log management, event correlation, alerting, remediation workflow and reporting.

In 2009, netForensics introduced basic integration between Cinxi One and SIM One to allow the former to forward events to the latter. Development plans include an expansion of event collection to include application layer sources, and further integration between nFX Cinxi One and nFX SIM One to expand the former's capabilities as a log collector for the latter.

Return to Top

Strengths

- The nFX SIM One software is best suited for larger deployments in which customizable event correlation, dashboard views and incident management are required, and where appropriate resources exist for customization and support.
- netForensics is successfully expanding its customer base of MSSPs.
- The nFX Cinxi One appliance is best suited for midsize environments that can use out-of-the-box log management, event correlation, remediation workflow and reporting.

Return to Top

Cautions

- netForensics needs to broaden its presence in competitive evaluations.
- netForensics needs to expand support for user activity monitoring beyond standard user activity reports to include predefined, user-oriented views or correlation rules.
- Application layer event source support and analytics are currently limited and should be expanded.

Return to Top

NetIQ

NetIQ provides a portfolio of security and operations technologies, and has a moderately sized SIEM customer base. The company's operations and security management software products are integrated, but typically deployed individually over time. The NetIQ Security Manager SIEM software product is typically deployed for SIM, user activity monitoring and 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. 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. In the past 12 months, NetIQ released a new version of NetIQ Security Manager that contains major performance and scalability improvements. The vendor also released updates to its NetIQ Change Guardian family of monitoring software, and introduced a database activity monitoring offering (based on licensed technology). The company plans an expansion of the NetIQ Change Guardian line to cover more platforms and applications.

Return to Top

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, especially in cases where the agent technology needs to be used as an alternative to native platform audit functions.
- The technology is also a good fit when there is a need to filter data at the source to reduce event collection network and server resource requirements.
- NetIQ Security Manager is tightly integrated with the NetIQ Change Guardian product line, which provides monitoring and change detection for Active Directory file integrity monitoring and database activity monitoring for host systems.

Return to Top

Cautions

- NetIQ can be successfully used in event management for network and security devices, but it is not optimized for deployments that are primarily focused on this use case.
- NetIQ is not very visible in competitive evaluations, and, despite its capable technology, it is not growing with the market.

Return to Top

NitroSecurity

In the past 12 months, NitroSecurity has achieved a credible position as an innovator in the SIEM market. The company's NitroView line of appliances combines SIM and SEM functions with in-line network monitors, which implement deep packet inspection to obtain data and application context and content for security events. In addition, the company continues its intrusion detection system (IDS)/intrusion prevention system (IPS) business

with a common platform for SIEM and IPS.

NitroView is composed of the following components:

- NitroView Enterprise Security Manager provides the primary interface for SIEM functions.
- NitroView ELM provides log management.
- NitroView DBM provides database monitoring and policy enforcement.
- NitroView ADM provides application data inspection and monitoring.
- NitroView Receiver is an event log collector.

The NitroView line of appliances uses NitroSecurity's high-speed event storage and query technology. In May 2010, NitroSecurity will introduce focused solutions for critical infrastructure.

Return to Top

Strengths

- In addition to competitive SIEM functions, NitroView provides application and data context via network monitors and integrated database activity monitoring.
- NitroView's back store supports high-performance, ad hoc queries for forensic analysis and reporting.

Return to Top

Cautions

- NitroSecurity needs to continue its expansion of channel partnerships and its development of broader sales capabilities.
- While NitroView provides standard support for user activity monitoring, integrated third-party IAM products are still narrow.

Return to Top

Novell

Novell is primarily focused on using SIEM to provide activity monitoring to its IAM customers, but it is beginning to sell to a wider set of prospects. Novell's Sentinel software offering is integrated with Novell's IAM solutions, and Novell is actively selling Sentinel as a complementary monitoring and audit technology to its IAM customers. In 2009, Novell released the Sentinel Rapid Deployment option, which packages a complete, single-system instance of Sentinel and provides predefined correlation rules, dashboards and workflows. Novell also released Log Manager — a log management tier for Sentinel. Novell is beginning a channel expansion effort as a means of reaching the broader SIEM market with products that are easier to deploy.

Return to Top

Strengths

- Sentinel and Sentinel Log Manager are appropriate for large-scale, SEM-focused deployments.
- Sentinel is based on a message bus architecture that provides flexibility and scaling for large deployments.
- Sentinel RD and Sentinel Log Manager are well-suited to deployments that need a combination of event management and compliance reporting, and for organizations that use Novell IAM products and need broader audit capabilities.

Return to Top

Cautions

- Sentinel provides user and resource access monitoring reports that are ultimately adapted to compliance reporting. Although predefined compliance reports cover all major regulations, coverage for other regulations is narrower in comparison to competing products that are

best of breed in this area.
- While the Sentinel 6.1 Rapid Deployment release provides simplified deployment and support, a deployment that includes log management and event management requires multiple software components to install and configure, so the technology is still more complex to deploy and manage than all-in-one appliance solutions.

Return to Top

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. The EventTracker agent also provides support for file integrity monitoring and USB control. In the past year, Prism added a number of enhancements to EventTracker, including support for virtualization, Web services integration, a Web-based user interface, Security Content Automation Program (SCAP) support, and risk-based alerting. Prism also enhanced its event correlation with Cisco NetFlow support and behavioral and statistical analysis.

Return to Top

Strengths

- Prism's EventTracker is suited for midsize businesses that require one product that provides log management, SEM, compliance reporting and operations monitoring.
- EventTracker is easy to deploy and maintain, especially in Windows environments, where EventTracker supports centralized agent deployment and management.
- Knowledge packs provide prebuilt correlation, alerting and reporting for operations use cases, and for compliance regimes, such as U.S. Federal Information Security Management Act (FISMA) requirements.

Return to Top

Cautions

- EventTracker's capabilities are limited in specific areas that are more typical in larger enterprises' deployments. There is a lack of integration with enterprise configuration management database products and IAM products, and limited capabilities to monitor application-level activity.
- Prism must grow its sales capabilities with direct and channel partners to establish greater visibility in the midsize market.

Return to Top

Q1 Labs

Q1 Labs' SIEM appliances provide log management, event management, reporting and behavioral analysis for networks and applications. In 2009, Q1 Labs continued its rapid growth and became more visible in competitive evaluations. The company continues to sell its SIEM appliances directly to large customers, but is now focused more on enabling its channel partners. Q1 Labs also licenses its technology to Juniper and Enterasys, which implement the software on their own appliances. The QRadar appliances can be deployed as all-in-one solutions for smaller environments, or can be horizontally scaled in larger environments using specialized event collection, processing and console appliances. A distinguishing characteristic of the technology is the collection and processing of NetFlow data to provide network and application behavior analysis.

Return to Top

Strengths

- The QRadar technology provides an integrated view of the threat

environment using NetFlow and direct network traffic monitoring, in combination with log data from monitored sources.
- Customer feedback indicates that the technology is relatively straightforward to deploy and maintain across a wide range of deployment scales.

Return to Top

Caution

- While Q1 Labs provides basic integration with SAP, organizations that require an SIEM solution that provides comprehensive SAP user activity monitoring should consider alternatives, such as SenSage.

Return to Top

Quest Software

Quest Software's InTrust SIEM software provides functionality that is complementary to Quest's Active Directory and Windows Server management products. Typical InTrust deployments are with customers that have Microsoft environments and have deployed other Quest products to extend the monitoring functionality of Microsoft products. InTrust is primarily oriented to host log data, but has some narrow support for network devices and network-based security technologies. Quest Software has a large installed base for InTrust, but narrow source support and basic real-time monitoring capabilities limit its applicability to a small subset of SIEM technology buyers.

Return to Top

Strengths

- Quest Software provides monitoring capabilities for Microsoft Active Directory, Exchange and file servers that do not rely on native logging and can be applied to user activity reporting.
- The integration of InTrust with other Quest products enables customers to enhance the audit capabilities of Microsoft products.
- InTrust's automated software wizard assists in deploying agents to servers and establishing initial configuration settings.

Return to Top

Cautions

- Support for network devices and network-based security technologies is very limited, and the product lacks integration with vulnerability assessment and endpoint protection data sources.
- The technology is unsuitable for external threat monitoring or SIEM use cases that require more than the most basic support for network and security event sources.
- Organizations that require robust, real-time event management and a full-function security console for a security operations center should consider solutions that provide more function or flexibility to meet those requirements.

Return to Top

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 channel partners to sell enVision. For smaller deployments, a single appliance can provide log collection, event management and reporting. For larger deployments, appliances can be configured for specialized functions (collector, management, analytics) and scaled horizontally. RSA has improved its SEM capabilities in the past few years, and is in the middle of a major effort to integrate enVision with the EMC technology portfolio. EMC

has completed an integration with RSA's Data Loss Prevention (DLP) technology, and is working on integrations with the recently acquired Archer Technologies' IT GRCM technology.

Return to Top

Strengths

- RSA's enVision should be considered in cases where all data needs to be collected and available for analysis, and also where there's a need for SEM and SIM capabilities in a single appliance.
- The appliance should also be considered in environments where customers have limited personnel resources to manage servers and databases as part of their SIEM implementations.

Return to Top

Cautions

- Organizations need to ensure that adequate appliance resources are available for later-stage deployment phases, when additional resources will be needed for real-time correlation, and for ad hoc queries to support investigative analysis.
- enVision collector appliances may not "scale down" enough to be cost-effective in highly distributed deployments.

Return to Top

SenSage

In 2009, SenSage continued its rapid growth, mostly through large deals for specific use cases within such verticals as U.S. and European federal governments, large telcos and financial services, using a combination of direct and partner sales. The SenSage solution is optimized for precision analytics and compliance reporting for a large event data store, and the company has successfully pursued large deployments that require this capability. SenSage has also successfully pursued use cases that require application layer and/or user-oriented monitoring. In 2009, HP emerged as SenSage's most important sales channel as HP continued to ramp up its sales capabilities for the HP CLW (which uses software licensed from SenSage). In 2009, SenSage released Continuous Monitoring and Auditing for SAP, which provides user activity and transaction monitoring for SAP.

Return to Top

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 investigations.
- SenSage has explicit support for SAP, Oracle (PeopleSoft and Siebel), Lawson, Cerner and other packaged application providers, and its technology supports the precise analytics needed for use cases, such as fraud detection.
- SenSage is a good fit for use cases that require compliance reporting or security analytics for a large event store with basic real-time monitoring requirements.

Return to Top

Cautions

- Organizations that require only basic log management functions should consider simpler and less-expensive offerings that focus on collection and basic reporting.
- SenSage's technology is not the best fit for use cases that are focused on SEM. Although SenSage has improved its real-time monitoring capabilities, the technology still has scalability limitations in this area

(many customers implement a combination of real-time and short-cycle monitoring), and there is no native incident management capability.

Return to Top

Symantec

Symantec typically sells its SIEM technology to its existing endpoint protection customers. Symantec Security Information Manager (SSIM) is delivered as a software appliance and provides SIM, SEM and log management capabilities. Symantec has integrated SSIM with its Security Endpoint Protection (SEP), IT GRCM and DLP technologies. Symantec also has managed service offerings that use the soft appliance for on-site data collection and analysis. In addition, SSIM is dynamically updated with threat and vulnerability data content from Symantec's DeepSight security research and managed security area.

Return to Top

Strengths

- SSIM provides good support for a wide variety of use cases that require a mix of log management, compliance reporting and very scalable security event management functions.
- The SSIM appliance provides SIM, SEM and log management functions that are scalable and easy to deploy. Customers have the option to outsource security monitoring or the management of appliances to Symantec's managed security organization.
- The dynamic integration of Symantec's DeepSight content enables real-time identification of active external threats and known malicious sources.

Return to Top

Cautions

- Symantec's SIEM technology provides good support use cases that are very common in today's market, but the company has not been very visible in the competitive evaluations of SIEM technology that we have seen from Gartner clients. The company needs to improve its sales and marketing of the technology in the general market.
- The technology is not a good fit for implementations that require integration with specific IAM technologies beyond the narrow set of directory and network authentication technologies that is currently supported.

Return to Top

Tenable

Tenable's SIEM software is tightly integrated with the company's active and passive vulnerability scanner products, and its SIEM customers tend to use the vulnerability scanning and configuration assessment technologies. Tenable's SIEM software solution includes the SecurityCenter 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 to correlate events with data from Tenable's vulnerability scanning and security configuration assessment products. SecurityCenter integrates Tenable's LCE and vulnerability scanning products to provide unified asset discovery, vulnerability detection, event management log collection and reporting. Windows and Unix log collection agents can also provide file integrity monitoring. At the time of our request for submission, the SecurityCenter Version 3 console environment was generally available, and was evaluated for this Magic Quadrant.

The Tenable SecurityCenter console and the LCE now include log search capabilities. Security Command Center and Nessus can be deployed as software or as physical or virtual appliances. The LCE is available as software, but will be available as physical or virtual appliances in 2010.

SecurityCenter includes basic NetFlow monitoring capabilities. In April 2010, Tenable released SecurityCenter Version 4.0 and indicated that there is an improved user interface, as well as improvements in identity, database and application monitoring. The vendor also indicates improvements in real-time monitoring. Tenable also plans a hosted SecurityCenter offering, as well as an increased capability to deliver professional services to assist in sizing and configuring customer deployments.

Return to Top

Strengths

- SecurityCenter and LCE are tightly integrated with Tenable's active and passive vulnerability scanner and configuration assessment products, and SIEM customers reference that quality as a strength for the products. The integration enables users to correlate alerts with vulnerability scan results. The SecurityCenter upgrade will bring a consistent interface to the SIEM and vulnerability scanning technologies.
- SecurityCenter and LCE offer excellent coverage of firewalls, intrusion detection and prevention products, and network devices, and Tenable provides better integration with DLP technologies than several other SIEM providers.
- A scripting capability that spans the SecurityCenter and vulnerability scanning products offers customization options within and between those products to users with sufficient technical expertise.
- Tenable has significantly increased the number of its direct sales staff.

Return to Top

Cautions

- SecurityCenter Version 3 does not score as well as some competitors' products in addressing user identity monitoring, database monitoring and application monitoring. We have not been able to evaluate the capabilities of Version 4.
- Other SIEM products provide more capabilities related to remote data collection requirements, such as bandwidth management.
- The company should expand its efforts to improve awareness of its SIEM capabilities to potential buyers, and should also continue to expand its channel's sales programs.

Return to Top

TriGeo

TriGeo has designed its appliance-based SIEM solutions for midsize organizations (with limited deployment and management resources) that need a combination of external threat monitoring and compliance reporting. TriGeo's SIEM appliance incorporates event correlation and analysis, log management and search, reporting, database activity monitoring and endpoint monitoring/control. The appliances are offered in four tiers, and specific functions can be segmented to specific appliances.

Return to Top

Strengths

- TriGeo's appliance is easy to deploy and provides integrated functions with extensive, predefined correlation and compliance reporting templates that are well-matched to midmarket buyers' requirements.
- The TriGeo Windows agent can be configured to provide active response and USB control capabilities within the core SIEM product. This provides additional endpoint monitoring and automated threat response functions.

Return to Top

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 technologies.
- TriGeo targets the small and midsize business market, and must develop more sales capabilities to sustain growth. Larger competitors, as well as similarly sized vendors, are selling easy-to-deploy and managed integrated SIEM offerings into the midsize market.

Return to Top

Trustwave

In March 2010, Trustwave acquired Intellitactics, one of the founding vendors of the SIEM space. Trustwave is primarily a security service provider that delivers PCI assessment services, vulnerability assessment services, managed security services and security consulting, but it has also built a security product portfolio through the acquisition of IT GRCM, DLP, network access control and encryption technologies. The SIEM technology is composed of two components:

- The Trustwave SIEM Operations Edition (SIEM OE) software is highly customizable and optimal for large-scale, SEM-focused deployments. Trustwave will sell this to its large customers, and we expect that it will also instrument its own security operations center with the technology.
- Trustwave SIEM is a customer-managed appliance that provides data collection, log management and basic SEM for midsize deployments. Trustwave Managed SIEM is a version of the appliance that provides on-premises log collection and event forwarding for Trustwave's Managed SIEM service.

Return to Top

Strengths

- Trustwave now offers a wide choice of SIEM sourcing options, and would be optimal for customers that want a mix of SIEM managed services and self-managed technologies, or the ability to move from one sourcing option to another.
- SIEM OE is a good fit for large-scale, SEM-focused deployments in which a high degree of customization is required and for which capable support resources are available.
- Trustwave SIEM is suitable for midsize environments that require predefined functions and simplified deployments.

Return to Top

Cautions

- Potential buyers and current users that are interested in mixing deployment modes (products and managed services) will need to carefully track Trustwave's progress in integrating the various product and service options, and in providing unified administration and functional capabilities.
- Trustwave now has a diverse software portfolio to manage, in addition to its core security service business. It will be difficult for Trustwave to maintain the focus required to sustain new functional developments across the portfolio with the resources available to a company of its size.

Return to Top