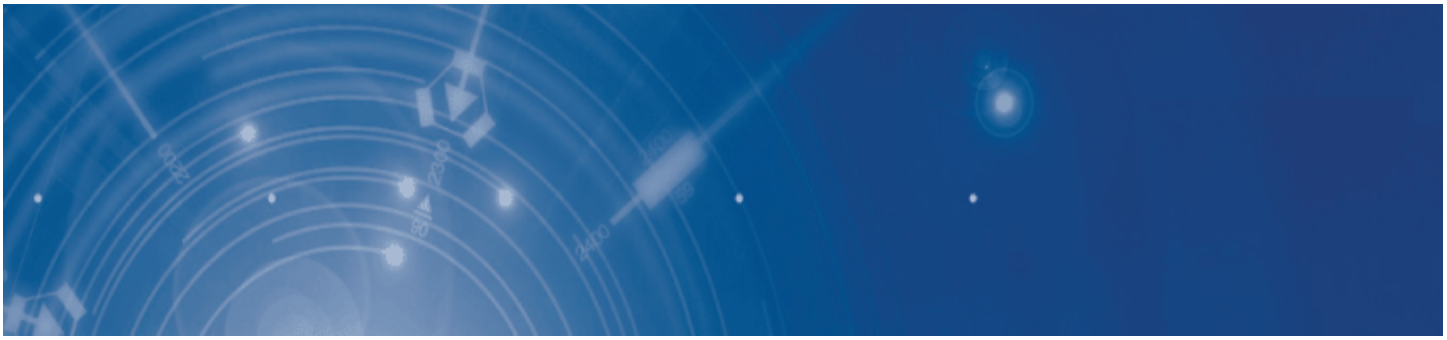


Gartner

Magic Quadrant for Security Information and Event Management

12 May 2011

Mark Nicolett, Kelly M. Kavanagh

Gartner Research Note G00212454

Broad adoption of SIEM technology is driven by both security and compliance needs. Targeted attack discovery requires effective user activity, data access and application activity monitoring. Vendors are now testing demand for broader-scope solutions.

What You Need to Know

Security information and event management (SIEM) technology provides:

- Security information management (SIM) — log management and compliance reporting
- Security event management (SEM) — real-time monitoring and incident management for security-related events from networks, security devices, systems, and applications

SIEM technology is typically deployed to support three primary use cases:

- Compliance — log management and compliance reporting
- Threat management — real-time monitoring of user activity, data access, and application activity and incident management
- A deployment that provides a mix of compliance and threat management capabilities

SIEM deployments are often funded to address regulatory compliance reporting requirements, but organizations are using this as an opportunity to deploy SIEM technology that will improve threat management and incident response capabilities. The SIEM market is composed of technology providers that support all three use cases; however, there are variations in the relative level of capability for each use case, in deployment and support complexity, in the scope of related functions that are also provided, and in product support for capabilities related to targeted attack detection (such as user activity monitoring, data access monitoring, application activity monitoring and anomaly detection). As a companion to this research, we evaluate the SIEM

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

technologies of 15 vendors with respect to the three major use cases.

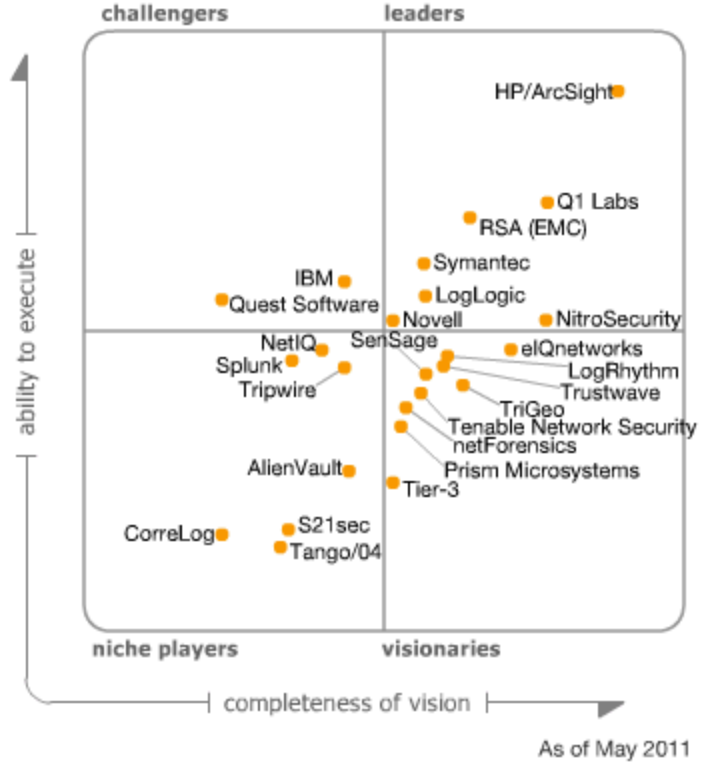
Organizations should consider SIEM products from vendors in every quadrant of this Magic Quadrant based on their specific functional and operational requirements. Product selection decisions should be driven by organization-specific requirements in areas such as the relative importance of compliance and threat management; the scale of the deployment; SIEM product deployment and support complexity; the IT organization's project deployment and technology support capabilities; identity, data and application monitoring requirements; and integration with established applications, data monitoring and identity management infrastructure.

Security managers considering SIEM deployments should first define the requirements for security event management and reporting. The requirements definition effort should include capabilities that will be needed for subsequent deployment phases. The project will benefit from the input of other groups, including audit/compliance, identity administration, IT operations and application owners. Organizations should also describe their network and system deployment topology, and assess event rates so that prospective SIEM vendors can propose solutions to company-specific deployment scenarios. The requirements definition effort should include later phase deployments beyond the initial use case. This Magic Quadrant evaluates technology providers with respect to the most common technology selection scenario — an SIEM project that is funded to satisfy a combination of threat monitoring/response and compliance-reporting requirements (see Figure 1).

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management



portfolio of products.

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

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

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

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

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

Completeness of Vision

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

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the 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.

Source: Gartner (May 2011)

Return to Top

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.

Market Overview

During the past year, demand for SIEM technology has remained steady. During this period, the number of Gartner inquiry calls from end-user clients with funded SIEM projects matched levels of the previous 12 months, and most vendors have reported increases in customers and revenue. During 2010, the SIEM market grew from $858 million to $987 million, achieving a growth rate of 15%. In North America, there continues to be many new deployments by smaller companies that need log management and compliance reporting. There are also new deployments by larger companies that are conservative adopters of technology. Both of these customer segments place a high value on deployment and operational support simplicity. Some large companies are also re-evaluating SIEM vendors in order to replace SIEM technology associated with partial, marginal or failed deployments. During this period, there has been a stronger focus on security-driven use cases from new and existing customers. There is growing demand for SIEM technology in Europe and Asia/Pacific, driven by a combination of compliance and threat management requirements. As a consequence, our overall evaluation of vendors in this Magic Quadrant now includes an evaluation of vendor sales and support strategies for these geographies.

The SIEM market is mature and very competitive. We are 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 customer requirements. In the current market, vendors are expanding the scope of their SIEM offerings to include additional capabilities in adjacent areas (such as file integrity monitoring, vulnerability assessment, security configuration assessment and data access monitoring), and proactively marketing those capabilities to their prospects and customers. Several SIEM vendors are beginning to position their technologies as "platforms" that can provide security, operations and application analytics. We now include an evaluation of the platform capabilities of SIEM technologies, but the weight we place on the capability is limited by the degree to which clients express requirements in this area. Most companies expand their initial SIEM deployments over a three-year period to include more event sources and greater use of real-time monitoring. SIEM vendors have large existing customer bases, and there is an increasing focus on selling more SIEM technology into existing accounts.

SIEM Vendor Landscape

Twenty-five vendors met Gartner's inclusion requirements for the 2011 SIEM Magic Quadrant. Sixteen are point solution vendors, and nine 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. RSA (EMC) is executing a strategy to integrate its SIEM technology with its storage, governance, risk and compliance (GRC), and security portfolio. 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. 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. NetIQ has integrated its SIEM technology with its security configuration management and file integrity monitoring technologies. HP's development strategy for ArcSight includes use of the technology to unify monitoring across its security portfolio and integration with its operations management technologies.

Several vendors are not included in the Magic Quadrant because of a specific vertical market focus and/or SIEM revenue levels:

- FairWarning provides privacy breach detection and prevention solutions for the healthcare market that entail user activity and resource access monitoring at the application layer.
- AccellOps provides event monitoring for IT operations and IT security, and is expanding its support for the security monitoring use case.

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 delivers workflow integrations with Enterasys Network Access Control and NetSight Automated Security Manager. The Juniper Networks Security Threat Response Manager is an appliance solution that uses the QRadar technology, and is also integrated with Juniper's policy management subsystem. SenSage licenses its SIEM technology to Cerner, which has integrated it with its packaged healthcare applications for application activity monitoring and audit.

Customer Requirements — Compliance Reporting and Security Monitoring for Systems, Users, Data, and Applications

While the primary source of funding for SIEM deployments continues to be regulatory compliance, security use cases are ascending in relative importance. In North America, more than 80% of initial SIEM deployments are funded to close a compliance gap, but the IT security organization owns the project and there is a strong motivation to improve security monitoring capabilities. The number of new European and Asia/Pacific SIEM deployments has been rising, and the initial focus (security monitoring or compliance) varies by region. 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 an expected and standard component of an SIEM technology architecture.

SIEM solutions should:

- Support the real-time collection and analysis of events from host systems, security devices and network devices combined with contextual information for users, assets and data
- Provide long-term event and context data storage and analytics
- Provide predefined functions that can be lightly customized to meet company-specific requirements
- Be as easy as possible to deploy and maintain

The security organization often wants to employ SIEM to improve capabilities for external and internal threat discovery and incident management. As a consequence, there are requirements for user activity and resource access monitoring for host systems and applications, as well as requirements for the early detection of data breaches. In this year's SIEM vendor evaluation, we have placed greater weight on capabilities that aid in targeted attack detection, including support for data access, user activity, and application activity monitoring, and development of profiling and anomaly detection.

SIM as a Service

Most managed security service providers (MSSPs) have service offerings for SIM in addition to their long-standing SEM services. These 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

These criteria had to have been met for vendors to be included in the 2011 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 solution must be delivered to the customer environment as a software- or appliance-based product (not a service).

Vendors were 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 had less than $4 million in SIEM product revenue during 2010.
- The solution is delivered exclusively as a managed service.

Return to Top

Added

- Tripwire's SIEM revenue now exceeds the threshold for the Magic Quadrant, and the company has provided adequate production references.
- During 2010, Splunk released specific support for the security monitoring use case, and now has enough support for security monitoring use cases to be included in the evaluation.
- AlienVault's SIEM revenue now exceeds the threshold for the Magic Quadrant, and the company has provided adequate production references.
- HP's acquisition of ArcSight has closed, and the designation on the SIEM Magic Quadrant is now HP/ArcSight.
- We now include three small vendors that have a regional focus — S21sec, Tango/04 and Tier-3. All three vendors have grown their SIEM revenue to meet our inclusion threshold, and all three operate in geographies where SIEM deployment activity is increasing.

Return to Top

Dropped

- In May 2010, the SIEM-oriented intellectual property of LogMatrix was acquired by NitroSecurity.
- In April 2011, CA Technologies notified customers of a change in strategy for CA Enterprise Log Manager. The technology is now called the User Activity Reporting Module, and there is a repositioning of Enterprise Log Manager from a general-purpose log management offering to a user activity and compliance reporting solution within CA's Identity and Access Management (IAM) portfolio.

Return to Top

Evaluation Criteria

Ability to Execute

- **Product/service** evaluates the vendor's ability and track record to provide product functions in areas such as log management, compliance reporting, security event management, and deployment simplicity.
- **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 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.
- **Marketing execution** evaluates the SIEM marketing message against our understanding of customer needs, and also evaluates any variations by industry vertical or geographic segments.
- **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, and includes an evaluation of these capabilities across multiple geographies.

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	Standard
Customer Experience	No rating
Operations	High

Source: Gartner (May 2011)

Return to Top

Completeness of Vision

- **Market understanding** evaluates the ability of the technology provider to understand buyer 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.
- **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.

  Because the SIEM market is mature, there is little differentiation between most vendors in areas such as support for common network devices, security devices, operating systems, consolidated administration capabilities and asset classification functions. In this evaluation, we neutralized relative ratings of vendors with capabilities in these areas, but there is a severe "vision" penalty for the few vendors that continue to have shortcomings in this area. This change has the effect of improving the visibility of relative differences in other functional areas.

  In this year's SIEM vendor evaluation, we have placed greater weight on capabilities that aid in targeted attack detection:

  - We evaluate data access monitoring capabilities, which are composed of file integrity monitoring (native capability and integration with third-party products), data loss prevention (DLP) integration, database activity monitoring (direct monitoring of database logs and integration with database activity monitoring [DAM] products).
  - We evaluate user activity monitoring capabilities, which include monitoring of administrative policy changes and integration with IAM technologies, for automated import of access policy for use in monitoring.
  - Our evaluation of application layer monitoring capabilities includes integration with third-party applications (e.g., ERP financial and HR applications, and industry vertical applications), for the purpose of user activity and transaction monitoring at that layer; the external event source integration interface that is used to define the log format of an organization's in-house-developed applications; and the ability to derive application context from external sources.
  - We evaluate vendor capabilities and plans for profiling and anomaly detection to complement existing rule-based correlation.

  Many SIEM vendors are now positioning the technology as a platform. There is a focus on expansion of function — security

configuration assessment, vulnerability assessment, file integrity monitoring, DAM and intrusion prevention system (IPS). This year, we have included an evaluation of SIEM vendor platform capabilities in our overall assessment of Completeness of Vision

Despite the vendor focus on expansion of capability, we continue to heavily weight deployment simplicity. Users still value this attribute over breadth of coverage beyond the core use cases. There is a danger of SIEM products (which are already complex) becoming too complex as vendors extend capabilities. Vendors that are able to provide deployment simplicity as they add function will ultimately be the most successful in the market.

- **Vertical industry strategy** evaluates vendor strategies to support SIEM requirements that are specific to industry verticals.
- **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.

  This year, we have made changes in the way we evaluate innovation. There is a stronger weighting of capabilities that are needed for security monitoring and targeted attack discovery — real-time event management, user activity monitoring, data access monitoring, application activity monitoring and capabilities/plans for profiling, and anomaly detection.
- **Geographic strategy.** Although the SIEM market is currently centered in North America, there is growing demand for SIEM technology in Europe and Asia/Pacific, driven by a combination of compliance and threat management requirements. As a consequence, our overall evaluation of vendors in this Magic Quadrant now includes an evaluation of vendor sales and support strategies for these geographies.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Standard
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	No rating
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Low

Source: Gartner (May 2011)

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, 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). In addition to providing a technology that is a good match to current customer requirements, Leaders also show evidence of superior vision and execution for anticipated requirements. Leaders typically have relatively high market share and/or strong revenue growth, and have demonstrated 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 a 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 are regional in focus, or provide SIEM technology that is a good match to a specific SIEM use case, 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

AlienVault

AlienVault is a relatively recent entrant to the commercial SIEM market and, in 2010, met the minimum revenue requirements for inclusion in this Magic Quadrant. The company launched in 2007. During 2010, the company received an initial round of venture capital funding and relocated its company headquarters from Spain to the United States. AlienVault's Unified SIEM provides SIEM, vulnerability assessment, network and host intrusion detection, and file integrity monitoring functions via software or appliance options.

AlienVault Unified SIEM is composed of proprietary and open-source components. Open Source SIM (OSSIM) is an open-source security management platform that has been available since 2003. AlienVault incorporates OSSIM into its SIEM solution, extending it with performance enhancements, consolidated administration, consolidated reporting, and multitenanting for MSSPs.

During 2010, the product has been updated to provide improved real-time dashboards and reporting. Support for NetFlow was also introduced. The company's 12-month development plan includes expansion of capabilities to solve existing competitive gaps in areas such as application, data and user monitoring. The two-year plan includes a dynamic monitoring alternative to rule-based correlation.

Return to Top

Strengths

- AlienVault Unified SIEM solution should be considered by organizations that need SIEM, file integrity monitoring, vulnerability assessment, endpoint control and IDS capabilities.
- AlienVault's solution should be considered by organizations that want a commercially supported product that is based on open source.
- Customer references indicate that the software and appliance offerings are much less expensive than corresponding product sets from most competitors in the SIEM space.

Return to Top

Cautions

- Unified SIEM currently lacks native support for DAM, and there is currently no integration with third-party DAM technologies.
- There is no IAM Integration beyond Active Directory monitoring, and application integration is primarily with open-source applications.
- Users report that there is frequently a need to dip below the product's management and administration interfaces into native Linux functions to deploy and customize the product.

Return to Top

CorreLog

CorreLog entered the SIEM market in 2008, and has recently met minimum revenue thresholds for inclusion in the SIEM Magic Quadrant. The company provides a Microsoft Windows-based software solution that has integrated log management and SEM functions and provides basic capabilities in both areas. CorreLog targets midsize businesses, and we have been able to validate small deployments in the range of 50 to 75 servers.

Return to Top

Strengths

- CorreLog provides basic SIEM software that is simple to deploy.
- The solution includes agent-based event filtering and file integrity monitoring for Windows, Unix, and Linux platforms.

Return to Top

Cautions

- CorreLog does not provide event source integration for packaged applications.
- CorreLog does not provide event source integration for third-party DLP or DAM technologies, but there is limited support for monitoring database activity through native audit functions.
- CorreLog's predefined compliance reporting is limited to Payment Card Industry (PCI) only.
- CorreLog is a small startup vendor, and is a late entrant in a mature market that needs to become more visible in competitive evaluations.

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 monitoring functions, and some network behavior analysis capabilities. Since our last evaluation, the company released ForensicVue, which improves search and ad hoc query capabilities. The company also released a custom report builder and additional policy content for security configuration assessment. The company is developing support for hypervisors beyond VMware, and plans to provide support for the collection of security and performance-related information from cloud environments.

Return to Top

Strengths

- SecureVue augments SIEM functionality with additional operational performance, as well as asset and configuration policy compliance

capabilities. The company has been able to win competitive evaluations against other SIEM vendors, especially when the customer has a need for capabilities in these adjacent areas.

- The vendor has found some demand for its combination of SIEM and security configuration assessment within the federal sector to satisfy Federal Information Security Management Act (FISMA) requirements.
- SecureVue's role-based access and tiered deployment architecture support federated enterprise and service provider requirements.

Return to Top

Cautions

- 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

HP/ArcSight

In 2010, HP acquired ArcSight — the largest and most visible SIEM point solution vendor. HP will continue to develop and sell ArcSight as an SIEM point solution, but will also use the technology to provide unified event management for its security technology portfolio. Integrations with HP business service management (BSM) technology are also in process. The goal is to integrate operational availability and performance events, asset inventories, and service dependency maps with ArcSight, and to integrate security events into HP's operational monitoring infrastructure.

ArcSight Enterprise Security Manager (ESM) software, is oriented to large-scale, SEM-focused deployments; ArcSight Express, is an appliance-based offering for ESM that's designed for the midmarket with preconfigured monitoring and reporting. ArcSight Logger is a line of log management and collector appliances that can be implemented as stand-alone or in combination with ESM. In addition to the HP integration plans outlined, during the past 12 months ArcSight has improved ESM user monitoring capabilities and provided a major new release of IdentityView. Logger enhancements included a software download option and the introduction of a Unix-like command line interface designed for IT operations searching and reporting.

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 vendor in competitive evaluations.

Return to Top

Cautions

- HP will need to manage the priority of HP technology integration and ArcSight development projects in a way that preserves capabilities in multivendor environments and must also manage the transition of ArcSight to its own sales channels and support infrastructure in a way that preserves the security expertise that has been built by ArcSight over time.
- 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 choose ArcSight most often cite deployment complexity as the reason. 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

IBM

IBM's Tivoli Security Information and Event Manager (TSIEM) v.2 software offering provides SIM and SEM functionality, and allows customers to have a starting point with log management. TSIEM provides capabilities for privileged user monitoring, compliance reporting, log management and basic real-time SEM. Tivoli also provides Tivoli Security Operations Manager (TSOM) to customers that also need additional security operations center capabilities. 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. A typical deployment is focused on user activity monitoring and involves 100 or fewer servers.

Since the writing of the last SIEM Magic Quadrant, IBM's TSIEM product updates have focused on maintaining integrations with updated versions of other Tivoli products and major third-party event sources. IBM's overall SIEM strategy continues to be focused on integration with its IAM, security and service management technologies and its leverage of Internet Security Systems-managed services.

IBM's development efforts are focused on the improvement of security analytics through the application of IBM business intelligence technologies such as Cognos and SPSS. There are also plans for additional integrations with IBM database and network security technologies.

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 provides a variety of blended or hybrid technology/managed service offerings that use TSIEM as the base.

Return to Top

Cautions

- Although there is loose integration between TSIEM and TSOM, organizations that need real-time event monitoring of host log events and security operations center functions still need to deploy two technologies, and SEM capabilities are not best in class.
- The technology is not well-suited for moderate or large deployments that require network security monitoring.
- IBM is not very visible in competitive evaluations.
- IBM customer feedback on product function and support is mixed.

Return to Top

LogLogic

LogLogic provides its core log management appliance line, and a number of appliance-based extensions: Security Event Manager (real-time monitoring and correlation), Database Security Manager (database activity monitoring and database protection), and Compliance Manager (compliance dashboards and workflows).

Since the last SIEM Magic Quadrant, LogLogic has released Universal Collection Framework, which provides a new protocol for secure transport of log data. Another component, Log Labels, provides users and partners with the ability to define the format of any event stream. Log Labels provides the ability to integrate with unsupported data sources — an important capability for application layer integration that brings LogLogic to parity with many competitors. The company also released improvements to its workflow component, and introduced basic support for NetFlow analysis. Development plans include scalability improvements and capabilities to enable the use of LogLogic SIM and SEM functions in virtualized and external cloud environments.

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

- While we have been able to validate Security Event Manager deployments in midsize environments, organizations that are considering larger-scale deployments should require customer

references from LogLogic that have deployed at the expected level of scale.

- LogLogic needs to continue its efforts to extend SEM knowledge to its sales force, sales channels and presales support.
- LogLogic does not provide event source integration for DLP applications or any of the major ERP applications.
- 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

LogRhythm

LogRhythm sells its appliance- and software-based SIEM solutions to midsize and large enterprises. The SIEM offering can be deployed in smaller environments with a single appliance or software instance that provides log management and event management, or it can be scaled as a set of specialized appliances or software instances (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 and system process monitoring for Windows and Unix. LogRhythm's recent 5.1 release includes the advanced intelligence engine, which provides support for compound correlation rules and contextual enhancement of events. Development plans include behavior profiling.

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.
- Its 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 needs to do a better job in describing the differentiating characteristics and benefits of its technology to prospective buyers.
- LogRhythm needs to continue development of its event correlation capabilities, and allow for more customization of its log taxonomy.

Return to Top

netForensics

This company declined to provide any information to Gartner for this research. We were able to locate two netForensics customers that have indicated that the company has provided maintenance updates to the product during the past year, but neither had knowledge of netForensics' plans for product development. Both customers indicated that netForensics' customer support continues to be good.

The company sells its SIEM technology to enterprise and service provider customers, but has not been as visible while the market has broadened to smaller enterprises. In 2009, netForensics focused more effort on expanding its service provider customer base. Its SIEM solution is composed of two components:

- Its nFX SIM One software provides full-function SEM for large environments.
- Its 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 then included 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. We have no information from netForensics or the two customers that we spoke with on progress during 2010 in these areas.

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.
- During 2009, netForensics successfully expanded 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.
- The company is one of five SIEM vendors (HP/ArcSight, LogLogic, netForensics, RSA [EMC] and Splunk) that have been named as ecosystem partners by Cisco and are working with Cisco to provide replacement functionality for users of the Cisco MARS product.

Return to Top

Cautions

- The company needs to broaden its presence in competitive evaluations.
- Organizations that have a requirement for user activity monitoring beyond standard user activity reports to include predefined, user-oriented views or correlation rules should contact netForensics to determine if any development work has been completed in this

area during the past year, or if there are any development plans for 2011.

- Organizations that have a requirement for application layer event source support and analytics should contact netForensics to determine if any development work has been completed in this area during the past year to expand what has been a limited capability.
- Prospective buyers should request information from netForensics on its product development road map.

Return to Top

NetIQ

NetIQ provides a portfolio of security and operations technologies, and has a midsize 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 on servers for user activity monitoring and compliance reporting. The technology can be used for network and security device sources, but is not widely deployed for this use case because NetIQ Security Manager's support for these event sources and use cases is basic, and 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.

During the past 12 months, NetIQ released an update to NetIQ Security Manager 6.5, which contained some performance and scalability improvements and event source support upgrades. The vendor also released updates to its NetIQ Change Guardian family of monitoring software. The company plans an expansion of the NetIQ Change Guardian line to cover more platforms and applications, and enhancements to user activity monitoring capabilities.

NetIQ has moved from the Visionaries quadrant to the Niche Players quadrant due to the increased emphasis that we have placed on broad scope security monitoring and limitations in NetIQ Security Manager event source coverage and SEM capabilities.

Return to Top

Strengths

- NetIQ Security Manager is most appropriate for deployments that are focused primarily on host log analysis for users, and data 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, and file integrity monitoring for host systems.

Return to Top

Cautions

- NetIQ parsing and correlation support for network and security devices is limited. Although the technology has been successfully used for the management of events from these sources, it is not optimized for deployments that are focused on this use case.
- NetIQ is not very visible in competitive evaluations, and, despite its strengths in server activity monitoring, it is not growing in the SIEM market.

Return to Top

NitroSecurity

During the past 12 months, NitroSecurity has expanded its sales channel, and has become more visible in competitive evaluations. 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 provides integrated DAM technology and continues its IDS/IPS business with a common platform for SIEM and IPS. During the past 12 months, NitroSecurity acquired the intellectual property for the LogMatrix SIEM technology and is integrating its statistical correlation and profiling capabilities into the NitroView platform. There was also a major release of function to support industrial control system, monitoring with specific event source support for supervisory control and data acquisition (SCADA) systems within the power generation industry. Development plans include integration with network IPS technology to support implementation of blocking based on NitroView event analysis.

Return to Top

Strengths

- In addition to competitive SIEM functions, NitroView provides application and data context via network monitors and integrated DAM.
- NitroView's event storage supports high-performance, ad hoc queries for forensic analysis and reporting. We have been able to validate this capability with large production deployments.

Return to Top

Cautions

- Non-English-language versions of NitroView are not available.
- Customer feedback indicates some issues with the maintenance of parsing support for the most current release of some data sources; however, the vendor reacted and successfully addressed the issues.

Return to Top

Novell

In February 2011, Novell's shareholders approved the acquisition of the

company by Attachmate. As with any acquisition of this type and at this early stage, there are unknowns about the acquiring company's funding of development plans within the various product lines, because U.S. Securities and Exchange Commission (SEC) regulations have placed constraints on Attachmate and Novell in terms of forward planning until the deal closes. Attachmate also owns NetIQ, another vendor that provides SIEM technology. Novell sells its Sentinel software and Sentinel Log Manager to customers of its IAM solutions, as well as to other enterprises and service providers. More recently, Novell has developed a system integrator channel that can sell to the security buying center. Sentinel is integrated with Novell IAM products. The Sentinel Rapid Deployment option, first introduced in 2009, provides a single-system instance of Sentinel with predefined correlation rules, dashboards and workflows.

Sentinel's event management capabilities remain a strong point, but planned improvements in application coverage and reporting capabilities have yet to be introduced. Sentinel provides integration with SAP for monitoring user administration activity, but overall application integration is not as strong as in competing products. Novell provides coverage for PCI-DSS monitoring and reporting with a solution package that provides predefined correlation and reporting. However, more-extensive reporting for other regulatory schemes remains in development.

In its planned version 7 release, Novell will introduce a two-tier storage architecture, with compressed flat file log storage and an embedded relational database management system (RDBMS) for reporting.

Return to Top

Strengths

- Sentinel and Sentinel Log Manager are appropriate for large-scale, SEM-focused deployments.
- Integration with Novell IAM products provides extensive user-based activity monitoring and reporting capabilities.
- Sentinel's two-way integration with SAP provides knowledge of SAP user and asset administration to Sentinel, and Sentinel-generated alerting to the SAP GRC solution.

Return to Top

Cautions

- Sentinel's compliance reporting capabilities have not been significantly improved, and lag those in best-of-breed SIEM products.
- Reference customers have been unable to provide validation that the Sentinel 6.1 Rapid Deployment release enables simplified deployment, because they have used professional services for installation and customization. Novell must continue its efforts to reduce deployment complexity for its version 7 release planned for 3Q11.

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. EventTracker can be deployed in a virtual environment, and supports risk-based alerting, statistical analysis and support for NetFlow data monitoring. The EventTracker agent also provides support for file integrity monitoring and USB control.

During the past year, Prism has added operations-focused network monitoring, a Federal Desktop Core Configuration (FDCC)/Security Content Automation Protocol (SCAP) option for configuration assessment, user-configurable features to its Web-based dashboards and behavior analysis capabilities, in addition to USB, writable media monitoring. Prism has added direct and partner sales resources in the U.S. and other regions.

Return to Top

Strengths

- Prism's EventTracker is suited for midsize businesses that require log management, SEM, compliance reporting and operations monitoring in physical and virtual environments.
- EventTracker is easy to deploy and maintain, with compliance and use-case-specific knowledge packs with prebuilt alerts, correlation rules and reports. EventTracker supports centralized agent deployment and management in Windows environments.
- EventTracker's Web interface supports role-based access to support security, compliance and operations use cases.

Return to Top

Cautions

- EventTracker's capabilities for application monitoring and integration with IAM products are more limited than other SIEM products targeting enterprise deployment. Prism must balance development resources to ensure that it expands capabilities that address current and emerging enterprise use cases, as well as those required by compliance-driven buyers.
- Other SIEM vendors are aggressively targeting the midsize, compliance-driven market. Prism must continue to expand its indirect sales channel to increase visibility in this market.

Return to Top

Q1 Labs

Q1 Labs' SIEM appliances provide log management, event management, reporting and behavioral analysis for networks and applications. Q1 Labs continues its rapid growth and continues to be very visible in competitive evaluations. The company continues to sell its SIEM appliances primarily through channel partners to the large enterprise and midsize markets. Q1 Labs also licenses its technology to Juniper Networks and Enterasys, which implement the software on their own appliances. Its 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. Q1 Labs recently announced an expansion

of behavior analysis capabilities to all event sources. The company also released its Risk Manager extension that analyzes security and network configuration, event and flow data to build a topology that is used to identify security gaps and risks. The company plans to introduce virtual appliances. Longer-term plans include the introduction of network forensic functions.

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

Cautions

- 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 provides two technologies for SIEM functions — InTrust and ChangeAuditor. Quest's 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. Quest's SIEM products are primarily oriented to host log data. There is some narrow support for firewalls, but the technology lacks specific parsing support for network devices, network-based security technologies and security software products. Quest Software has a large installed base for its Intrust and ChangeAuditor technologies, but narrow security event 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 Quest's monitoring technologies with other Quest products enables customers to enhance the audit capabilities of a Microsoft infrastructure.
- The technology can also be used to monitor Unix and Linux server environments.

Return to Top

Cautions

- Specific parsing support for network devices and for network security event sources is absent. Support for network security event sources 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 security event sources.
- Organizations that require broad-scope SEM should consider solutions that provide more function or flexibility to meet those requirements.

Return to Top

RSA (EMC)

RSA (EMC), also known as the Security Division of EMC, sells the enVision appliance, which provides a combination of SEM, SIM and log management. RSA (EMC) has one of the largest SIEM installed bases, but enVision has emerged as the most frequently displaced SIEM technology, primarily due to ad hoc query and report performance issues. 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 (EMC) has improved its SEM capabilities during 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 RSA Archer's GRC technology, and is working on integration with the recently acquired NetWitness network security analysis solution. The company is also working on an extension to support better performance for ad hoc queries against a large historical event store.

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

- Customers frequently complain of query performance issues as the size of the backstore grows.
- RSA has had some quality issues with recent maintenance upgrades.

- RSA needs to resolve performance and support issues to improve customer retention.

Return to Top

S21sec

S21sec is a security company based in Spain that provides a cyberintelligence service and the Bitacora SIEM solution, which incorporates its endpoint cyberintelligence agent. Geographically, the largest installed bases are in Europe (Spain) and Latin America (Brazil, Mexico and Panama); 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. The endpoint security technology is an agent that can implement endpoint control and also discover malware such as keyloggers and rootkits. Windows, Linux and Mac OSX systems are supported.

Return to Top

Strengths

- S21sec provides a combination of SIEM, endpoint security and security intelligence functions.
- Bitacora should be considered by companies that wish to acquire an SIEM solution from a vendor that is oriented to Spain or Spanish-speaking customers.
- S21sec should also be considered by financial services organizations that need endpoint malware detection, forensics and cyberintelligence capabilities to support fraud detection use cases.

Return to Top

Cautions

- S21sec does not have a sales and support presence in North America.
- Bitacora lacks integration with third-party DAM solutions.
- We have not been able to validate production deployments larger than a few hundred event sources with customer references.

Return to Top

SenSage

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 continues to pursue 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. SenSage has also successfully pursued use cases that require application layer and/or user-oriented monitoring.

With HP's acquisition of ArcSight, SenSage lost HP as a major sales channel to the general SIEM market. SenSage scores quite well in terms

of functionality. The areas that are a challenge are deployment simplicity. The largest inhibitor in terms of vision is that the company has not been able to effectively reach the "center of the SIEM market."

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. The technology is Linux-based, and the user needs to dip down into that interface for installation and tuning.
- SenSage's technology is not widely deployed for use cases that are focused on SEM. Although SenSage has improved its real-time monitoring capabilities, most customers continue to implement a combination of real-time and short-cycle monitoring, and there is no native incident management capability.
- Sales, marketing and technology "packaging" is oriented to larger environments that require large-scale security analytics — a specific use that is not at the center of the market.

Return to Top

Splunk

Splunk 4.1 was generally available with referenceable customers at the time of this analysis, when its capabilities were evaluated. Splunk 4.1 has the ability to test an event stream in real time and update a display, but lacks the ability to generate an alert in real time. Splunk refers to this level of capability as "real-time correlation." In this Magic Quadrant, we refer to this level of capability as "real-time monitoring." In March 2011, Splunk 4.2 was released and added the capability to generate an alert in real time — fulfilling the market's working definition of "real-time correlation," but we were not able to validate those capabilities with customer references. Spunk 4.1 provides real-time monitoring, log management and complex search capabilities that are often used by IT operations. Several hundred customers are now using Splunk for security use cases, typically to augment SIEM deployments. Splunk is gradually expanding its support for SIEM, and provides predefined reports and real-time monitoring for security and compliance use cases. Splunk also offers Enterprise Security Suite (ESS), which

provides predefined searches, reports, dashboards, visualization and real-time monitoring to support security use cases. Splunk's agent can also be used for file integrity monitoring. During the past 12 months, Splunk issued a minor update to ESS and Splunk version 4.2. Development plans include a major upgrade to Splunk for Security.

Return to Top

Strengths

- Organizations that need a combination of log management, forensics and real-time monitoring will find Spunk 4.1 a good match to their requirements.
- Splunk is often deployed by IT operations as log management infrastructure and is also used as log management infrastructure by IT security.
- Use cases that require analysis of a large number of data sources that are not formally supported by other SIEM vendors (for example, an organization's in-house-developed application portfolio) are ideal for Splunk's approach of normalization at the time of event data access.

Return to Top

Cautions

- Splunk does not have predefined parsing support for database management systems or specific integration with DLP technologies. The user must build its own keyword searches for these sources.
- Splunk does not have predefined parsing support for IAM infrastructure, beyond the use of a Windows Management Instrumentation (WMI) interface for Active Directory. The user must build its own keyword searches for these sources.
- We were not able to validate version 4.2 real-time correlation capabilities, because version 4.2 was not implemented in customer environments at the time the research for this Magic Quadrant was completed.

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. During the past 12 months, Symantec enhancements have included support for deployment in a VMware environment, enhancements to analytics for user activity, and improvements in archive/restore policy control. Development plans include the introduction of a no-charge unified collection architecture for all Symantec products.

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

- The company has not been very visible in the competitive evaluations of SIEM technology that we have seen from Gartner clients. Symantec 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 currently supported.

Return to Top

Tango/04

Tango/04 Visual Message Center provides operational event correlation, business process monitoring and SIEM solutions. Tango/04 is typically used by midsize financial institutions in Europe and Latin America (where the company is called Barcelona/04 due to trademark issues with the Tango name there). The company indicates that half of its customers use the technology for IT operations and IT security use cases. The technology can parse event data from major operating systems, network devices, vulnerability assessment programs and endpoint security programs.

Return to Top

Strengths

- The technology is a good fit for midsize companies within the geographic span of Tango/04 that want to use a common event monitoring technology for IT security and IT operations use cases.
- Data-monitoring capabilities include file integrity monitoring, database monitoring via standard audit logs, and modules that provide transaction-level monitoring for SQL Server and iSeries.
- The technology has been applied by many customers for application activity monitoring.

Return to Top

Cautions

- The primary orientation of the technology is for IT operations use cases such as availability and performance monitoring. Security-oriented dashboards are not provided out of the box.
- Its IAM integration is limited to Active Directory.
- Its security device support is very narrow when compared to the majority of established SIEM vendors.

Return to Top

Tenable Network Security

Tenable's SIEM software solution includes the SecurityCenter (SC) console and the Log Correlation Engine (LCE).The LCE provides log and event collection, analysis and reporting. SecurityCenter adds the ability to correlate events with data from Tenable's Nessus vulnerability scanner and Passive Vulnerability Scanner (PVS) to provide unified asset discovery, vulnerability detection, event management log collection and reporting. Windows and Unix log collection agents can also provide file integrity and change monitoring. Tenable's SIEM customers tend to use the vulnerability scanning and configuration assessment capabilities as components of their SIEM deployments.

SC, Nessus and PVS can be deployed as software or as physical or virtual appliances. The LCE is available as software, with planned physical or virtual appliances still in development. SecurityCenter includes basic NetFlow monitoring capabilities. PVS can monitor selected network traffic, such as file downloads, and generate alerts in SC.

During the past year, Tenable has released SC v.4, which includes a Web-based user interface with improved navigation, real-time dashboard capabilities and report templates. Users also report improved database-monitoring capabilities in version 4.

Return to Top

Strengths

- Customers cite the integration of SecurityCenter, and LCE with Nessus and PVS as a strength for SIEM deployment, and the combination of capabilities results in strong coverage of PCI and FISMA compliance requirements
- SecurityCenter and LCE offer excellent coverage of network-based security technologies including DLP, firewalls, and intrusion detection and prevention products.
- The SC user interface provides improved access to the product's searching, filtering, reporting and dashboard functions.
- Tenable has added management resources for service, including support and training, as well as for finance and marketing. Customers report strong satisfaction with Tenable's technical support.

Return to Top

Cautions

- SecurityCenter lacks the degree of workflow integration with corporate ticketing and directories found in competitive enterprise SIEM products, although SC has an internal ticketing capability and can initiate tickets by e-mail to corporate ticketing systems.
- LCE does not support data reduction, filtering and bandwidth management for low-bandwidth remote data collection deployments.
- Tenable must continue to refine and balance its marketing and messaging to focus on the distinct capabilities of the LCE, Nessus and PVS, and the value of the integration of those capabilities with SC.

Return to Top

Tier-3

Tier-3 is an Australia-based company that provides SIEM technology primarily to the Asia/Pacific region and the United Kingdom. The company has established offices in London and is increasing its sales focus on Europe. The company was founded more than 10 years ago, and is in this Magic Quadrant on the basis of its focus in geographies with increasing SIEM deployment activity. The company's Huntsman SIEM software is composed of three modules. Huntsman Log Analyzer provides log management and reporting. Huntsman Data Protector provides real-time monitoring and rule-based correlation. Huntsman Protector 360 provides behavioral anomaly detection.

Return to Top

Strengths

- We have validated use of a combination of rule-based correlation and anomaly detection in moderate deployments. Customers report that the anomaly detection can be effective (following the tuning effort that is required for any broad use of this method in any technology).
- The technology is oriented primarily to threat detection and security monitoring.

Return to Top

Cautions

- Organizations that are considering Huntsman should ensure that there is a good match with respect to Tier-3's regional presence.
- Huntsman uses a commercial relational database for parsed events, and users will need database administration and performance management skills to support the deployment.
- IAM integration is limited to Active Directory and a narrow set of network authentication sources.

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, DAM, and endpoint monitoring/control. The appliances are offered in four scalability tiers, and specific functions can be segmented to specific appliances.

During the past 12 months, the company has released virtual appliance options, substantial performance improvements for data analysis and new anomaly detection functions. TriGeo's development plans are focused on service enablement. The company is developing monitoring capabilities for customers with hybrid cloud environments and multitenant capabilities for managed security service providers.

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 buyer 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

Tripwire

Tripwire entered the SIEM space in late 2009, with technology from the acquisition of a small SIEM vendor. Tripwire Log Center (TLC) provides log management and SEM in a single solution. The technology scales horizontally and supports cross-event source correlation. Previous to the acquisition, the technology had been deployed primarily in managed security service providers for network security monitoring. Subsequent to the launch of the TLC product, Tripwire introduced a solution integrated with its Tripwire Enterprise product, a PCI-compliance package, and support for monitoring Oracle via native audit logs. Development plans include enhancement of the current taxonomy to make it Converged Enhanced Ethernet (CEE) compliant and support for anomaly detection.

Return to Top

Strengths

- Tripwire's Visibility, Intelligence, Automation (VIA) technology provides tight integration with the company's core file integrity monitoring and security configuration assessment technologies.
- The technology supports major network, security device and operating system event sources.

Return to Top

Cautions

- Support for DAM is currently limited to Oracle, and this was a recently released capability that we have not validated with customer references.
- IAM integration is limited to basic Active Directory monitoring.
- Organizations that are considering the technology for large-scale deployments should request customer references at the expected level of scale from the vendor.

Return to Top

Trustwave

Trustwave is primarily a security service provider that delivers PCI assessment services, vulnerability assessment services, managed security services and security consulting; however, it has also built a security product portfolio through the acquisition of IT GRCM, DLP, Web application firewall (WAF), network access control (NAC) and encryption technologies. The SIEM technology is composed of two components:

- The Trustwave SIEM Operations Edition (SIEM OE) software, which is highly customizable and optimal for large-scale, SEM-focused deployments. Trustwave will sell this to its large customers, and it has instrumented 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.

During the past 12 months, Trustwave transitioned its MSS operation to run on SIEM OE, and completed initial integrations with Trustwave DLP, FIM and NAC technologies. The company also released a large number of updates to device source support and updates to compliance reporting. Road map priorities include a user interface overhaul and a convergence of the Trustwave SIEM and SIEM OE code bases.

Return to Top

Strengths

- Trustwave 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 capable support resources are available.
- Trustwave SIEM is suitable for midsize and distributed environments that require configurable 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 has a diverse software portfolio to manage, in addition to its core security service business. Trustwave's challenge is to sustain new functional developments across the portfolio with the resources available to a company of its size.

Return to Top