Critical Capabilities for Security Information and Event Management

21 September 2015 ID:G00267508

Analyst(s): Oliver Rochford, Kelly M. Kavanagh

VIEW SUMMARY

Security information and event management technologies vary widely in their focus and functionalities, with vendors offering divergent security monitoring visions. This research helps IT security managers align their needs with one of the three most common use cases to choose the best SIEM solution.

Overview

Key Findings

- The threat management use case is supported by capabilities that enable high-performance, real-time event processing and correlation, and the integration of contextual and threat intelligence data. Analytics, behavior profiling, anomaly detection and network activity monitoring data are required for advanced threat detection.
- Log management and reporting, and out-of-the-box reporting templates for a broad range of regulatory frameworks, are the primary capabilities for compliance.
- Deployment and support simplicity is important for all use cases, due to the resource constraints of most IT security organizations. This can be achieved by vendor-supplied correlation rules, alerts, reports and other content that require only light customization to provide early value. It is supported by providing ways to scale the deployment and incorporate advanced analysis, without requiring substantial additional resources.

Recommendations

- IT security managers should form core security information and event management project teams that include stakeholders from security, operations, compliance and legal.
- IT security managers should develop two- to three-year roadmaps for their SIEM deployments to ensure that all functional and scalability requirements are assessed for the initial buying decision. Focus on deploying critical use cases and quick wins first.
- IT security managers should select a technology with deployment and support requirements that align with the IT organization's project and support capabilities. Organizations may need to consider services to cover project and operational capability gaps — e.g., project-based services may be needed to expand monitoring scope and depth to address additional use cases. Managed services may be needed to allow 24/7 monitoring, analysis and response.

What You Need to Know

Organizations evaluating security information and event management (SIEM) tools should begin with a requirements definition effort that includes IT security, IT operations, internal audit and compliance. Organizations must determine deployment scale, real-time monitoring, postcapture analytics and compliance reporting requirements. Gartner recommends a use-case-based, output-driven approach (see "Planning for SIEM Deployment: Establish Scope and Requirements for Successful Implementation"). In addition, organizations should identify products with deployment and support requirements that align well with internal project and support capabilities.

Gartner recommends developing a set of requirements that focus initially on the most critical drivers and on quick-wins; however, we also anticipate broader implementation of SIEM capabilities in subsequent project phases. Developing a two- to three-year roadmap for all requirements will ensure that the buying decision considers longer-term functional and scaling requirements (see "How to Deploy SIEM Technology"). The plan must also adapt to changes in the IT environment, business requirements and threats.

Analysis

Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for the Compliance Use Case

CRITICAL CAPABILITIES METHODOLOGY

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor’s product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor: most or all defined requirements not achieved

2 = Fair: some requirements not achieved

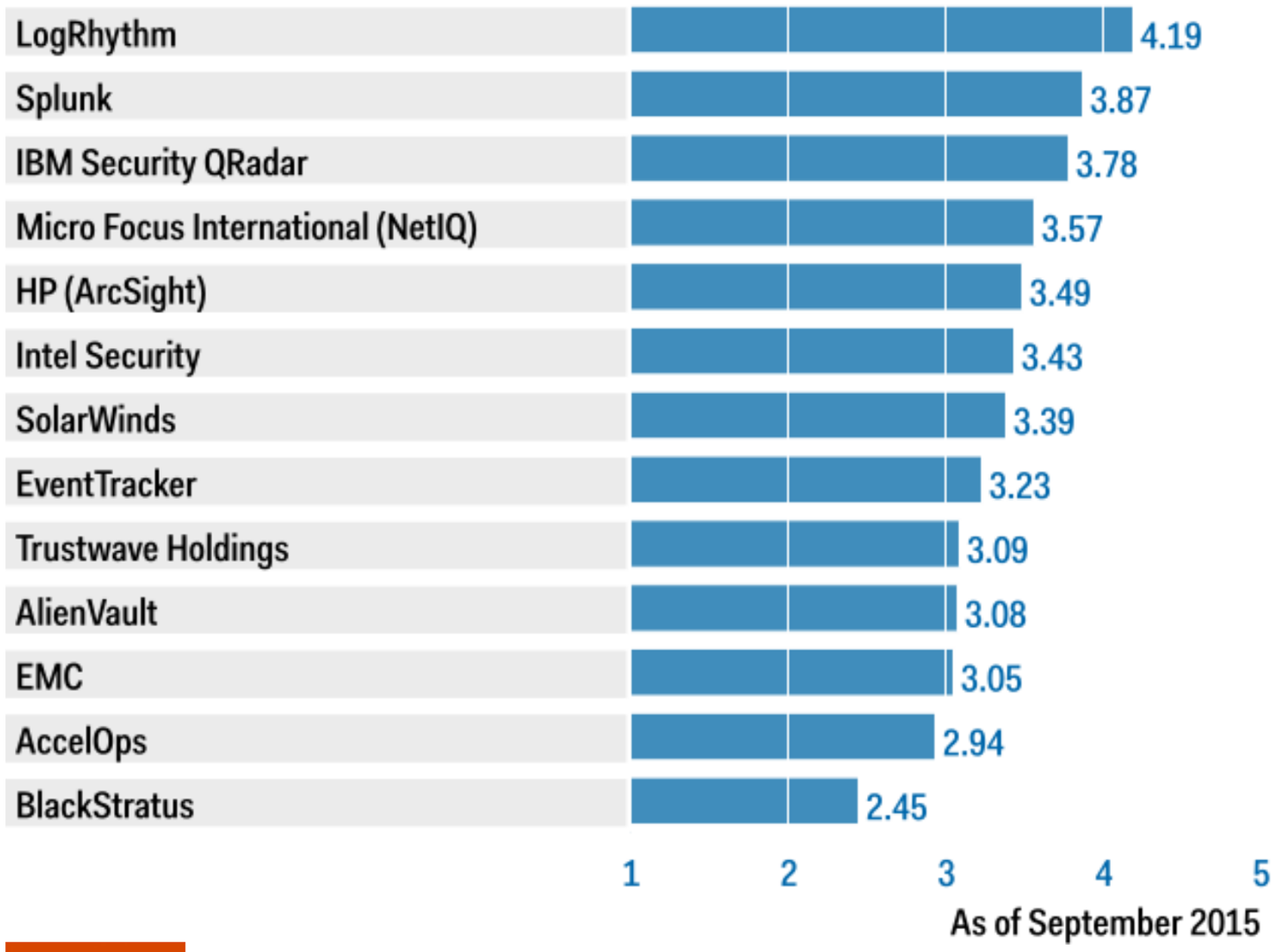
3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

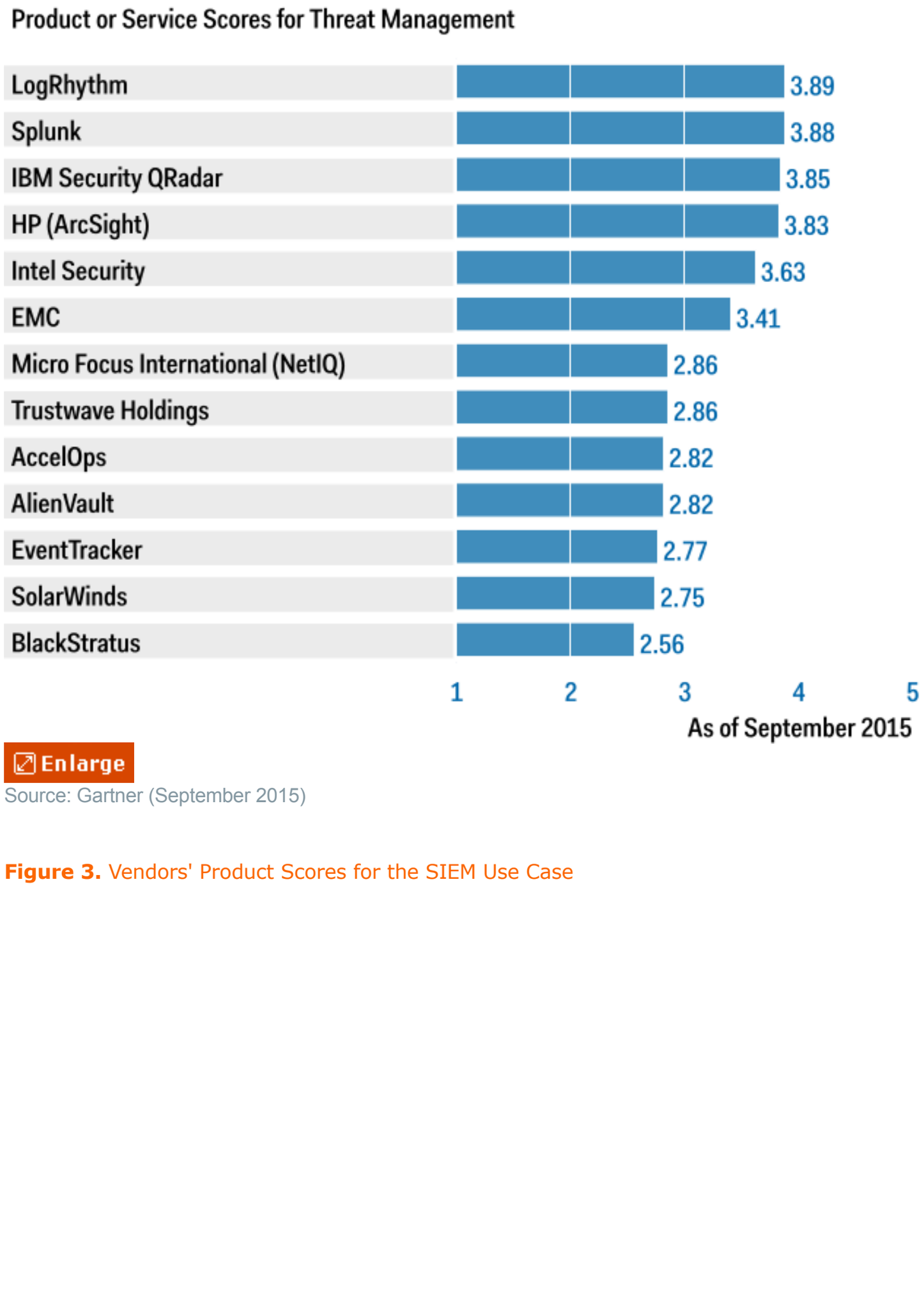
The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.



Enlarge

Source: Gartner (September 2015)

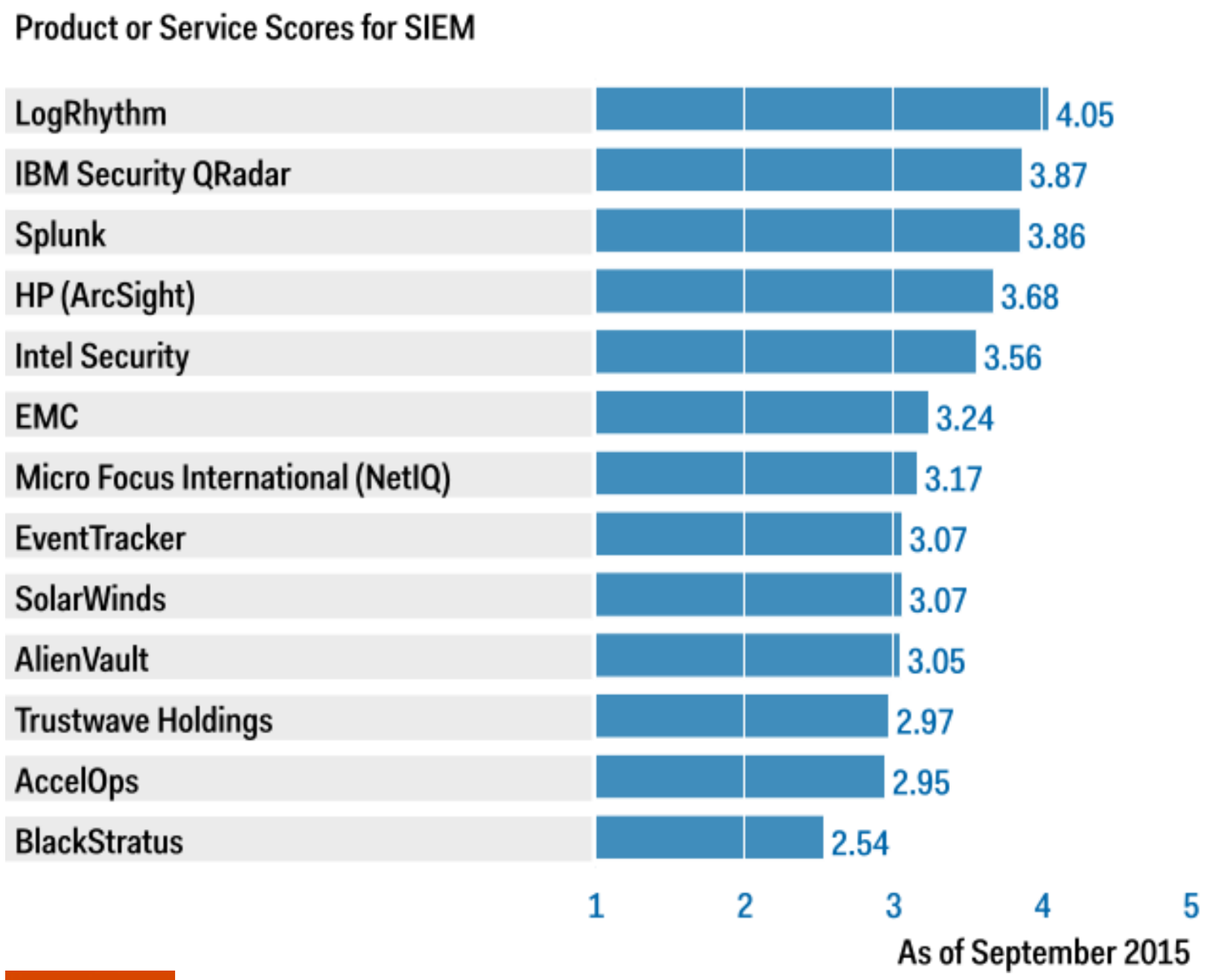
Figure 2. Vendors' Product Scores for the Threat Management Use Case



Enlarge

Source: Gartner (September 2015)

Figure 3. Vendors' Product Scores for the SIEM Use Case



Enlarge

Source: Gartner (September 2015)

The weighted capabilities scores for all use cases are displayed as components of the overall score.

Vendors

AccelOps

AccelOps primarily provides SIEM capabilities to the security organization and, secondarily, provides availability monitoring and application and performance monitoring (APM) to IT operations. File integrity monitoring (FIM) and configuration management database (CMDB) capabilities are integrated into the solution. SIEM and APM functions are delivered via a unified collection infrastructure and a common dashboarding environment. AccelOps is most often deployed by IT operations teams with a security function to do log management and monitoring for security-oriented use cases. Because of the APM and CMDB capabilities, the technology is sometimes championed and selected by the operations area as well.

Real-Time Monitoring: The AccelOps correlation rule language provides a unified framework for detecting patterns across security, performance, availability, compliance and change management scenarios.

Threat Intelligence: AccelOps can ingest various external threat data feeds, supporting such use cases as evaluating Domain Name System (DNS) lookups and outbound flows to known malicious IP address ranges. External customer threat data can also be integrated via an open API.

Behavior Profiling: AccelOps provides statistical analysis that can be used to identify anomalies and deviations from normal behavior.

Data and User Monitoring: Identity and access management (IAM) integration is limited to a collector for Active Directory; however, user and group information is appended to events. AccelOps provides basic change detection functions via its FIM technology and through integration with the Honeycomb FIM agent; however, there is no integration with third-party FIM solutions. Basic support for database activity monitoring (DAM) is provided; however, it's oriented toward availability and performance monitoring. There is no integration with third-party DAM tools.

Application Monitoring: AccelOps lacks specific support for application monitoring and does not support integration with third-party packaged applications.

Analytics: AccelOps provides standard support for the drill-down and display of event data in the context of event analysis, including data visualizations via heat maps, tree maps and scatter plots. AccelOps also offers Visual Analytics, an add-on that provides interactive dashboards and dynamic widgets.

Log Management and Reporting: AccelOps uses a relational database to store structured data (such as device configuration and network topology) and indexed flat files for events. The log management function is designed to be tightly integrated with the SIEM and cannot be installed as a stand-alone. A large number of predefined reports are provided, covering security, availability and performance use cases. AccelOps Visual Analytics is an add-on reporting server that provides executive- and management-level reporting.

Deployment/Support Simplicity: AccelOps has strong support for deployment in a virtualized environment, as well as public, private and hybrid clouds. AccelOps offers an API for workflow integration and supports built-in integration with several help desk applications. The product ships with a large number of predefined reports and correlation rules. The correlation rules are categorized as access/authentication, exploits, anomaly, policy violation and vulnerabilities.

Use Cases: AccelOps is a good fit for enterprises and managed security service providers (MSSPs) that require a combination of security monitoring and APM, as well as integrated CMDB capability.

AlienVault

AlienVault's security management software and appliance offerings provide SIEM, vulnerability assessment, NetFlow, network and host intrusion detection, and file integrity monitoring. AlienVault's commercial offering — the Unified Security Management (USM) platform — extends the open-source SIM (OSSIM) foundation with scaling enhancements, log management, consolidated administration and reporting, and federation for MSSPs. USM is available as a physical and virtual appliance, as well as for Amazon EC2.

Real-Time Monitoring: The AlienVault Correlation Engine provides real-time monitoring and correlation. Predefined correlation rules are provided for the intrusion detection system (IDS) sensor data, with some predefined rule content for third-party commercial products.

Threat Intelligence: AlienVault Labs provides threat intelligence content on a subscription basis for the commercial offering which is based on several open-source and commercial threat feeds, as well as AlienVault Labs generated content. AlienVault Labs provides feeds to its commercial products, including updates to signatures, vulnerabilities, correlation rules, reports and incident response content. The company also hosts and supports Open Threat Exchange, a free crowdsharing threat intelligence service that supports the sharing of IP and URL reputation information.

Behavior Profiling: Statistical analysis is applied to about 50 parameters and based on the Holt-Winters Exponential Smoothing algorithm and can be used to detect deviations from baseline and outliers. This capability complements rule-based correlation.

Data and User Monitoring: The AlienVault identity management (IdM) component is included as part of the suite, and it enables integrated monitoring with identity context. There is integration to provide monitoring for Active Directory and Lightweight Directory Access Protocol (LDAP), but not for monitoring other IAM technologies. Local account changes can be monitored if AlienVault's host-based intrusion detection system (HIDS) agent is installed, as well as via syslog for third-party agents. There is no productized integration with third-party FIM and data loss prevention (DLP) products; however, the HIDS agent provides FIM and some basic and limited DLP functions. DAM is supported through direct monitoring of major database management system (DBMS) logs. The integrated service monitoring component, which is based on open-source Nagios, provides DAM that requires native audit functions to be enabled, and there is integration with Imperva.

Application Monitoring: There is integration with major Web application firewall and Web server technologies. Application integration is primarily with open-source applications. Enterprise applications — such as ERP, or governance, risk and compliance (GRC) systems — do not have adequate out-of-the-box support.

Analytics: Search and structured analysis are provided from the alert investigation panel (the primary console) and the raw event panel, and operate against the primary event data store.

Log Management and Reporting: Log management capability is provided as a function of the logger component. Reporting is provided via an interface from the USM server.

Deployment/Support Simplicity: AlienVault provides wizards and dashboards to support initial deployment, configuration and ongoing management of the included controls and sensors. Content updates for signatures for sensors, correlation rules, reports and incident response templates are available through the threat intelligence feed. There is a basic, integrated workflow management system, but there are no integrations with external directories for workflow assignments.

Use Cases: The AlienVault USM platform should be considered by organizations that need a broad set of integrated security capabilities at relatively low cost, compared with other commercial offerings, and by organizations that will accept a commercially supported product that is based on open source.

BlackStratus

BlackStratus offers Log Storm, SIEM Storm and Compliance Storm. Log Storm provides log management capabilities aimed at MSSPs and small and midsize businesses (SMBs), and is available as virtual and hardware appliances. SIEM Storm provides multitenancy and security event management (SEM) capabilities, such as analytics, historical correlation and threat intelligence integration. It is deployable as software or virtual images. SIEM Storm can be deployed with Log Storm, using it as the storage and collection tier, Compliance Storm is a cloud-based service for log retention and scheduled reporting to meet regulatory and compliance mandates.

Real-Time Monitoring: Log Storm provides 66 predefined correlation rules, SIEM Storm 21, covering high-level categories, such as access/authorization, exploits and suspicious activity. A wizard can be used to create custom correlation rules. Nonevent data, such as threat intelligence watchlists and vulnerability scan data, can also be included. SIEM Storm contains a built-in incident management system based on the SANS Institute's seven-step incident remediation process. The integrations are provided by the vendor with Remedy and Service Desk. Active Directory and LDAP can be used to populate workflow assignments. NetFlow collection is supported, for nonevent data collection from the network, but feedback indicates it's only a basic implementation.

Threat Intelligence: Open-source threat intelligence feeds, such as DShield, Shadowserver and Spamhaus, are supported.

Behavior Profiling: Log Storm and SIEM Storm provide basic statistical anomaly detection capabilities.

Data and User Monitoring: Integrations with McAfee, Fortinet, Sophos and GFI Software DLP solutions, as well as with Tripwire, Sophos and McAfee FIM, are supported. DB2, Oracle and SQL database can be monitored via audit trail logs and database collector agents, but third-party DAM integrations are not available. Out-of-the-box, third-party IAM integrations are not available.

Application Monitoring: Log Storm and SIEM Storm can monitor Apache and IIS Web server logs. Integrations with FireEye and Mandiant, as well as Web application firewalls from F5, Barracuda Networks and Imperva, are supported. Nonsupported third-party applications can be included via

custom API scripts.

Analytics: Tabular views can be filtered by event fields and support nested conditional expressions. Visualizations are provided in the form of bar and pie charts, and network maps. SIEM Storm can also replay and apply correlations to historical data.

Log Management and Reporting: Log Storm is a full-fledged log management solution, with features including chain-of-custody compliance and digital signing. Both Log Storm and SIEM Storm are shipped with a large number of predefined report templates covering compliance standards and common security use case, and Crystal Reports templates can be imported.

Deployment/Support Simplicity: SIEM Storm and Log Storm can be deployed as virtual machines (VMs), and include an installation wizard and a passive autodiscovery feature for data source integration. A Web Services API is available to import user, contact, asset and similar information. The Vertical Analytics Database also required installation and maintenance if used for back-end storage for SIEM Storm. There are limited integration partnerships for deep, third-party technology integrations.

Use Cases: BlackStratus is a good fit for service providers that require a customizable SIEM platform, and end-user organizations or MSSPs looking tor well-formed multitenancy support.

EMC

The security division of EMC, RSA, offers RSA Security Analytics (SA), which provides visibility from log, full network packet, NetFlow and endpoint data capture. RSA SA performs real-time monitoring and alerting, forensic investigation, analytics and incident management.

RSA SA is made up of the following components:

- Decoders perform network capture or log ingestion and enrichment.
- Concentrators index the collected data in real time.
- Brokers distribute and aggregate results from multiple concentrators for analytics and reporting.
- The Event Stream Analysis server does complex correlation, event processing, alerting and incident management.
- Archivers provide long-term storage for reporting and forensic investigation purposes.
- The Security Analytics Server provides the analyst user interface, reporting and rule configurations, as well as systemwide administration.

The components of SA are available as physical or virtual appliances, and can be combined in one appliance or distributed over multiple appliances to meet customer deployment requirements. A cloud-based feed called RSA Live provides automatic content updates, including correlation rules, reports, parsers and threat intelligence feeds.

Real-Time Monitoring: The Event Stream Analysis engine for RSA SA provides more than 400. rules for correlating logs, events and packet data. RSA SA provides basic team-oriented workflow and incident management capabilities, but there is also an integration with the RSA Security Operations Management module for additional capabilities.

Threat Intelligence: RSA Live provides aggregated threat intelligence from multiple sources, including RSA 18 feeds from RSA numerous open-source feeds. Other feeds that support comma-separated values (CSV) or XML formats can be integrated.

Behavior Profiling: Behavior profiling is available through comparisons of deviation from baselines for short-time-frame analysis, through reporting trends on a recurring basis and via analysis of data in the Security Analytics Warehouse, with data science models provided through RSA Live.

Data and User Monitoring: RSA SA integrates with many third-party IAM technologies to enable the monitoring of identity-centric events, and provides more than 140 predefined user activity monitoring reports. For data monitoring, SA integrates with RSA, McAfee and Symantec DLP technologies. There is support for direct monitoring of database audit logs and integration with a few DAM products.

Application Monitoring: RSA SA integrates with a wide variety of Web server and Web application firewalls, and has a specific integration with SAP. There is also integration with SAP/Secude Security Intelligence for enhanced SAP activity monitoring, and with FairWarning for electronic health record monitoring and integrating third-party packaged applications used by the healthcare industry.

Analytics: RSA SA provides keyword search and pivot navigation through raw packet and log data and metadata, with basic data visualization capabilities to support investigations.

Log Management and Reporting: Log management functions are provided by its decoders and concentrators for collection. Archiver is used for long-term log archiving, reporting and forensics. SA provides about 200 predefined reports for compliance, user activity and suspicious activity.

Deployment/Support Simplicity: RSA continues to refine packaging and deployment features in RSA SA, including packaging to support deployments focused on log management and those focused on network/packet data. Feedback from clients, and prospects indicates that SA deployments are more complex than those for competing SIEM products, and they require technical expertise.

Use Cases: RSA SA is ideally suited for organizations that have advanced security monitoring requirements and a need for forensics analysis and reporting for both log and network/packet data. It is also appropriated for organizations with a well-staffed security organization that's capable of configuring and maintaining a complex monitoring technology.

EventTracker

EventTracker's SIEM software solution is targeted at SMBs and provides real-time monitoring and log management. The EventTracker Windows agent provides support for file integrity monitoring and USB control. Agents are also available for Solaris and AS/400. EventTracker also offers SIEM Simplified, a set

of services (daily incident review, daily or weekly log review, weekly configuration assessment review, incident investigation and audit assistance), delivered via remote access to the EventTracker instance running on customer premises. There is an option for continuous monitoring via a service provider partner.

Real-Time Monitoring: EventTracker provides SEM functions that are easy to customize and deploy. Although the primary focus is security monitoring, there is also support for basic availability and performance monitoring.

Threat Intelligence: EventTracker provides integration with threat intelligence feeds, including feed management. Malicious IP addresses, domain names, hashed executables and URLs can be correlated with event data.

Behavior Profiling: EventTracker includes a behavior analysis module that provides profiling and anomaly detection functions.

Data and User Monitoring: EventTracker provides an Active Directory Knowledge Pack that contains real-time alerts for user administration events. There is also integration with standard network authentication technologies. These limited IAM sources are dominant in the SMB space. The Windows agent provides USB device audit and control functions. File integrity monitoring is provided for the Windows platform via an optional Change Audit function. Integration with multiple third-party FIM solutions is also provided. EventTracker can directly monitor database audit logs. There is also integration with Imperva.

Application Monitoring: Integrations with packaged applications are provided for a variety of third-party vendor and technologies, including Web servers (e.g., Apache and IIS) and applications (e.g., SharePoint and Exchange).

Analytics: Support for analytics is provided through keyword search functions and via a data mart feature called EventVault Explorer, where data is exported into an external Microsoft SQL database to provide role-specific dashboards and also enables drilldown analysis and searching via the search interface or directly via SQL.

Log Management and Reporting: Log management capabilities are provided, and they are integrated with the solution. A large number of predefined reports are provided for compliance reporting.

Deployment/Support Simplicity: EventTracker provides technology that is well-suited to its target market, requiring only light customization through easy-to-use interfaces. A simplified licensing model based on monitored devices, rather than EPS, simplifies scoping and scaling. In addition, EventTracker offers SIEM Simplified, a low-cost, co-managed SIEM service offering that provides basic remote monitoring and incident management.

Use Cases: EventTracker is suited for midsize businesses that require log management, SEM, compliance reporting and operations monitoring via a software-based solution, as well as midsize businesses that require on-premises or cloud-hosted SIEM in combination with basic monitoring services. It has an especially good fit for small organizations that also need endpoint control functions or co-managed services.

HP (ArcSight)

HP ArcSight provides three SIEM offerings:

- ArcSight Enterprise Security Manager (ESM) software for large-scale event management
- The ArcSight Express appliance for SIEM functions for SMB deployments
- The ArcSight Logger line of appliances, software and connectors for log management and reporting

The capability to deploy Logger in combination with ArcSight Connectors provides additional options for normalized data analysis and application-layer data collection. HP is using ArcSight to unify event management across its security technologies, and to provide an integrated view of operations and security events. There is integration among ArcSight, Fortify, TippingPoint and IT Performance Suite (Operations Manager and Network Node Manager) products.

Real-Time Monitoring: ArcSight ESM provides the capabilities needed for large-scale, SEM-focused deployments. In addition to real-time event correlation and NetFlow network traffic monitoring, ArcSight ESM supports anomaly detection and statistical analysis capabilities across a variety of attributes. Dynamic dashboards and event visualization tools, as well as a fully implemented case and incident management workflow, are included, ArcSight Express is an appliance-based offering for ESM that's designed for the midmarket, with preconfigured monitoring and reporting, as well as simplified data management.

Threat Intelligence: ArcSight provides its own content and threat categorization model. There is also integration support for third-party feeds, such as iDefense and DeepSight, as well as HP's own ThreatCentral. HP Reputation Security Monitor (RepSM) is an optional component that receives near-real-time reputation feeds from HP research labs. Threat response manager is an add-on component that can perform network threat mitigation based on event triggers from ArcSight RepSM and other third-party security solutions.

Behavior Profiling: ArcSight provides two functions for behavior analysis. ArcSight User Behavior Analytics (UBA) has replaced IdentityView, providing full UBA capabilities, including user risk scoring, abnormal behavior detection and privileged user monitoring, based on Securonix. The second is ThreatDetector, which performs historical analysis of logs to detect and graphically display statistically significant patterns (groupings of events). The engine offers the option of autocreating a rule to detect future forming of this pattern.

Data and User Monitoring: In addition to typical integrations with Active Directory and network

authentication sources, HP ArcSight User Behavior Analytics is a separately chargeable module that provides connectors to many IAM systems, adds actor attribution to events and augments Arcsight ESM with true UBA capabilities. ArcSight maintains connectors with major DLP, FIM, and database audit and protection (DAP) products, and supports direct collection from database audit logs. There is no native FIM or DLP capability.

Application Monitoring: Connectors are provided for major packaged and SaaS applications, including Oracle, SAP and Salesforce. There is support for event collection from custom online applications and correlation across other fraud products to evaluate device, destination, account and transaction risks. HP also offers Application View, which enables application activity monitoring by interfacing with a Java or .NET application's runtime environment. HP Fortify Runtime technology is used to gain visibility without access to log or event data. It monitors method calls by the application, with more than 40 discrete activities monitored out of the box. There is also a customization interface for transaction monitoring.

Analytics: ESM provides trend analysis functions, event graphs, and map-based event and pattern visualizations. ArcSight has integrations with Business Service Management, and there are ArcSight connectors for Hadoop and Autonomy. Risk Insight is an ESM add-on and a visualization tool for security event analysis. It offers visualizations such as heat and asset maps, as well as risk scoring.

Log Management and Reporting: The ArcSight Logger line of appliances, software and collectors provides log management as a discrete component. ArcSight Logger can be implemented stand-alone or in combination with ArcSight Connectors and/or ESM software or appliances. ArcSight provides more than 900 predefined and configurable reports. In addition, there are separately chargeable Compliance Insight Packages, which provide rules, reports and dashboards for specific regulations (such as Sarbanes-Oxley Act [SOX], PCI, North American Electric Reliability Corp. [NERC] and the U.S. Federal Information Security Management Act [FISMA]). These packages are installed on top of Logger or ESM.

Deployment/support simplicity: ArcSight ESM is frequently cited by end users as a powerful, but complex solution to deploy, manage and maintain. A new Web-based management console to perform administrative tasks, as well as the new ArcSight Management Center (ArcMC) permitting unified and centralized management of the infrastructure have been released to simplify large-scale deployments

For less complex deployments, ArcSight Express provides predefined monitoring rules and reports, as well as a simplified data model, integrating SIEM, RepSM threat intelligence, IdentityView and connector management in a single appliance.

Use Cases: ArcSight provides comprehensive coverage for the compliance, threat management and SIEM use cases. Organizations seeking to build a Security Operations Center should consider ArcSight ESM. Organizations that require a full UBA integration, should consider ArcSight ESM in conjunction with the ArcSight UBA module. ArcSight Express should be considered by organizations seeking extensive third-party connector support.

Organizations that do not require full-function event management may be able to deploy a simpler and less expensive alternative. Users of HP security and operations technologies should expect an ongoing expansion of integrations with the ArcSight suite.

IBM Security QRadar

IBM Security's QRadar Platform includes the QRadar SIEM, Log Manager, Vulnerability Manager, Risk Manager, QFlow and VFLow collectors, and Incident Forensics. QRadar can be deployed as an appliance, a virtual appliance or as SaaS/infrastructure as a service (IaaS). Components can be deployed in an all-in-one solution or scaled by using separate appliances for different functions.

Real-Time Monitoring: The QRadar technology provides an integrated view of the threat environment using log-based event sources, NetFlow, full packet capture, in combination with threat intelligence, and vulnerability and asset data.

Threat Intelligence: QRadar includes an automatic update service that maintains current threat information (such as top targeted ports, botnets, emerging threats, bogon IPs, hostile nets, darknets and anonymous proxy). In addition, IBM Security provides an integration of X-Force IP Reputation data into QRadar, which can be refreshed in real time. Third-party feed integration is supported via API import.

Behavior Profiling: Behavior analysis capabilities can be applied to all supported sources (i.e., events and flow) in real time and on historical data. This capability complements rule-based correlation. QRadar can also determine baseline behavior of assets, users and applications, then alert on deviations.

Data and User Monitoring: QRadar provides predefined, user-oriented activity reports and console views to track user authentication activity in real time. In addition to standard integration with Active Directory and network authentication devices, QRadar also integrates with IAM technologies from IBM, CA Technologies, Novell and others. DAM is supported through direct monitoring of major DBMS logs and through integration with third-party database monitoring products from IBM InfoSphere Guardium, Imperva, McAfee and Application Security. This also integrates with third-party FIM and DLP products.

Application Monitoring: There is integration with a variety of applications, including major Web application firewall and Web server technologies. Support for SaaS applications, for example Salesforce, is included. There is also an integration with the SAP audit log, and a capability to monitor application behavior from the network using QFlow sensors.

Analytics: Analytics are supported directly from QRadar distributed event and flow data in real time and against historical data. QRadar has two-way integration with InfoSphere BigInsights (IBM's commercialized Hadoop offering) and with IBM's analytics and data visualization technologies (InfoSphere BigSheets and i2 Intelligence Analysis).

Log Management and Reporting: This capability is available as a function of a SIEM appliance, as a specialized function in a tiered deployment or as a stand-alone capability via the QRadar Log Manager appliance (which can be upgraded to QRadar SIEM via a license key upgrade). Included in the base

technology are a large number of predefined reports covering all major regulatory requirements, as well as data obfuscation support. These reports can be augmented with security configuration compliance reporting via Risk Manager and vulnerability reporting with Vulnerability Manager (or third-party vulnerability-scanning products).

Deployment/Support Simplicity: Customer feedback reveals that the technology is relatively straightforward to deploy and maintain across a wide range of deployment scales.

Use Cases: QRadar can support a wide set of threat management and compliance use cases for modest, as well as large-scale, deployments. In addition, the technology supports security-oriented use cases that benefit from network flow analysis and threat detection via broad-scope network, server, user and application behavior analysis.

Intel Security

Intel Security's McAfee Enterprise Security Manager (ESM) combines SIM and SEM functions and is available as a physical, virtual or software appliance. ESM architecture comprises the Enterprise Security Manager (ESM), the Event Receiver (ERC) and the Enterprise Log Manager, which can be deployed together as an all-in-one, stand-alone instance, or separately for distributed or large-scale environments. Capabilities can be extended and enhanced for additional cost with a range of specialized add-on products, such as the Advanced Correlation Engine (ACE), adding advanced correlation capabilities, Database Event Monitor (DEM), which provides DAM and analysis, and Application Data Monitor (ADM) for application monitoring.

McAfee ESM further provides integrations with McAfee's Advanced Threat Defense (ATD), an appliance-based malware analysis and sandboxing solution, and the Threat Intelligence Exchange, a threat intelligence platform for automated security defense, based on allowing security technologies to collectively detect and block threats.

Real-Time Monitoring: McAfee ESM supports rule-based and risk-based correlation. Data from event and log sources, dynamic watchlists and threat intelligence can be used for correlation. The McAfee Advanced Correlation Engine (ACE) adds the capability to correlate NetFlow and event data, and run correlations against historic data.

Threat Intelligence: McAfee Global Threat Intelligence for ESM provides threat context and is available as an additional module. McAfee ESM also supports the integration of third-party threat intelligence services via dynamic watchlists. Threat Intelligence data can be used for historical and real-time correlations.

Behavior Profiling: The McAfee ESM correlation engine supports statistical and baseline anomaly detection, as well as risk-based correlations. McAfee Application Data Monitor provides network anomaly detection, and McAfee Advanced Correlation Engine can be used to correlate and profile network and event data.

Data and User Monitoring: ESM provides policy monitoring of Active Directory and LDAP, and uses integrations with Exabeam, Securonix and Gurucul to provide identity cross-referencing and behavior profiling from major identity management products. The ADM component can extract identity information from monitored network traffic. Identity and access policy data can be automatically polled and imported for use in correlation rules and in reporting. The DEM provides network- and agent-based DAM functions. McAfee ESM can also directly monitor database audit logs, and ESM is integrated with McAfee Vulnerability Manager for databases, McAfee Virtual Patching for Databases, as well as IBM Guardium and Imperva, using Common Event Format. For FIM, there is integration with McAfee Application Control and with several third-party FIM products. The McAfee ADM component provides network-based monitoring of data access, and there is also integration with all major third-party DLP products.

Application Monitoring: The McAfee ADM component provides network-based activity monitoring for an extensive list of applications. Direct Web server log integration is limited to Apache and Microsoft IIS. SAP and Oracle's PeopleSoft are supported via a direct integration. Support for industrial control systems and supervisory control and data acquisition (SCADA) servers is also provided.

Analytics: ESM provides a range of features to allow the analysis of event, network and incident data, including data pivoting and drill-down views from dynamic and customizable dashboards. Visualizations for data include charts, graphs and tables, and prebuilt dashboards are provided for all available predefined reports. An HBase connector is available to enable bidirectional exchange between ESM and Hadoop.

Log Management and Reporting: The McAfee Event Receiver component is an event log collector, and McAfee Enterprise Log Manager (ELM) provides log management. More than 700 customizable predefined reports are available, covering a range of different compliance regimes and security use cases.

Deployment/Support Simplicity: Reference feedback indicates that ESM is relatively easy to deploy and maintain. Users give ESM high marks for out-of-the-box correlation rules, dashboards and reports. Deployment complexity can be increased when using multiple add-on products, but all-in-one appliances are offered for smaller deployments. User feedback regarding support has been positive.

Use Cases: McAfee ESM provides good support for the compliance, threat management and SIEM use cases. ESM capabilities are well-matched with deployments that require DAM, or monitoring of industrial control systems. Organizations looking to build an integrated security framework to protect against advanced threats should also consider McAfee ESM. The technology should also be evaluated for use cases that require heavy ad hoc query and historical analysis. Users already using McAfee ePolicy Orchestrator (ePO) and other McAfee products should also consider McAfee ESM.

LogRhythm

LogRhythm provides SIEM appliance and software technology to midsize and large enterprises. The SIEM technology can be deployed as a single appliance or software instance in smaller environments —

configured to provide log management, event management and real-time analytics. In larger environments, it can be scaled as a set of specialized appliances and/or software instances (log management, event management and real-time analytics). Network forensic capabilities, such as deep packet inspection and flow monitoring, are supported via LogRhythm's Network Monitor. The technology also includes optional agents for major OSs that can be used for filtering at the source and to provide capabilities such as file, process and host activity monitoring.

Real-Time Monitoring: LogRhythm provides almost 900 out-of-the-box correlation and detection rules, with additional modules focusing on specific use cases or verticals, such as privileged user monitoring, advanced persistent threats or retail point of sale (POS) monitoring. Network Monitor adds network traffic monitoring and forensic capabilities and allows correlation with log-based sources. Case and incident management capabilities for computer security incident response (CSIRT) teams and security operations center (SOC) environments were added in 2014, including a centralized "evidence locker" feature, tamperproof audit trail and real-time status tracking of ongoing incidents.

Threat Intelligence: LogRhythm provides an integration interface for open-source, as well as commercial threat intelligence, sources. Direct integrations of commercial threat intelligence vendors, such as Norse, Webroot or Crowdstrike, are provided through the LogRhythm Threat Intelligence Ecosystem. LogRhythm also provides its own threat intelligence content, but this requires the LogRhythm AI Engine. Threat intelligence data can be referenced in correlation and analytics rule sets, alarm rules and reports. LogRhythm also offer the Honeypot Analytics Suite, designed to collect and generate local threat intelligence gathered via honeypots that can be used to aid in threat detection.

Behavior Profiling: Behavioral profiling and anomaly detection are supported via event, log and endpoint sources, as well as network activity based on flows and deep packet inspection via Network Monitor. Monitoring against whitelists, average trends, rate trends and histogram trends is supported, as is the ability to create behavioral whitelists and baselines from host, application and user data, as well as Network Monitor session data.

Data and User Monitoring: In addition to integration with Active Directory and standard network authentication sources, there are integrations with IAM technologies, including CA Technologies, IBM, RSA and Oracle. LogRhythms AI Engine provides some UBA capabilities, focused on access and authentication policy monitoring, as well as establishing user profiles and baselines and applying anomaly detection methods. The Identity Inference Engine adds missing identity information to anonymous log data. An agent upgrade is available that provides file integrity and system process monitoring for Windows, Unix and Linux. Integrations for DLP technologies include McAfee, RSA and Symantec. LogRhythm can directly monitor database audit logs, and there is integration with third-party DAM technologies.

Application Monitoring: LogRhythm integrates with a large number of packaged applications, including SAP, Oracle's PeopleSoft, and a variety of other ERP and HR applications. There are also integrations with Web application servers and firewalls. Network Monitor adds application awareness via deep packet inspection and application identification for more than 2,500 applications. POS system monitoring is a further supported use case, aided by the availability of a Windows-embedded agent and corresponding dashboard, reporting and correlation rule module.

Analytics: Search and structured analysis can be done directly via the integrated Lucene query language, or by drilling down from customizable dashboard widgets. These can be customized to provide use-case-specific views, visualizations and analytics, and can accommodate data point pivoting and filtering. Additional features to aid in analysis include the Investigator Tool, a wizard for quickly creating forensic investigations, and 25 customizable, prebuilt analytics widgets.

Log Management and Reporting: LogRhythm's appliances provide horizontally scalable log management functions. Knowledge Base has more than 1,300 predefined security monitoring and compliance reports, plus more than 170 additional report templates that can be used to create custom reports, including executive, trending, auditing and security operations reporting.

Deployment/Support Simplicity: Feedback from LogRhythm customers has remained positive for its high level of predefined functions, ease of deployment, and presence of straightforward interfaces for tasks such as customizing reports and developing customized correlation rules. End users highly value the usefulness and effectiveness of predefined correlation rules and report templates.

Use Cases: LogRhythm is optimal for organizations that require balanced SIEM capabilities combined with endpoint and network monitoring to support security operations and compliance use cases. Organizations seeking good predefined use cases should also consider LogRhythm.

Micro Focus International (NetIQ)

Micro Focus International's NetIQ Sentinel is composed of three packages: the Sentinel Server, Sentinel Log Manager and Change Guardian. All three are offered as software, as well as virtual appliance deployments. Optional host agents are also available. NetIQ Sentinel integrates with other NetIQ products, including AppManager, Identity Manager, Access Manager, Directory and Resource Administrator and Secure Configuration Manager.

Real-Time Monitoring: Sentinel supports the rule-based correlation of event data and context data, such as asset, user identity, vulnerability and geolocation information. In addition to ad hoc queries, dynamic lists and user-defined thresholds can also be used.

Threat Intelligence: Sentinel provides threat intelligence integrations with Webroot, Palevo and Zeus, in addition to providing an API to integrate HTTP-based threat intelligence sources as dynamic watchlists.

Behavior Profiling: Sentinel detects anomalies through the statistical analysis of baseline deviations, and provides visual representation of baselines and deviations. Anomaly rules can be created based on visual exploration of statistical data.

Data and User Monitoring: Sentinel provides integrations with active directory and some of third-party IAM solutions, such as RSA, SailPoint and Novell, to add user context and monitor authentication

and access activity, Statistical anomaly detection techniques are applied to user data. Sentinel is also integrated with NetIQ's IAM technologies, which enables policy-based user activity monitoring, and provides competitive differentiation for use cases where NetIQ IAM products are deployed. Change Guardian for Active Directory (an optional component) provides agent-based, real-time monitoring that augments native audit functions. Sentinel provides database audit functions and also integrates with some major third-party DAM products, such as Imperva and IBM InfoSphere Guardium. In addition, Sentinel provides a portfolio integration with NetIQ Change Guardian for real-time FIM for Windows Unix and Linux, plus Active Directory, and there is also an integration with Tripwire FIM.

Application Monitoring: Sentinel integrates with SAP for monitoring of transaction activity, identity and access policy changes in SAP, and also integrates with Oracle's PeopleSoft. Sentinel can monitor a number of Web application servers, including Microsoft IIS and Apache.

Analytics: Analysis capabilities include dashboards containing alert-views-based correlation and anomaly detection rules and dynamic, customizable dashboards, containing charts, graphs and other visualizations. Ad hoc and drill-down searches are also supported.

Log Management and Reporting: Sentinel Log Manager provides log data collection, storage, archiving and reporting as a subset of Sentinel. NetIQ offers a package that includes only Log Manager to address stand-alone log management use cases. Sentinel includes more than 1,200 reports, sorted into solution packs covering specific use cases — for example, Payment Card Industry Data Security Standard (PCIDSS) or Network Security.

Deployment/Support Simplicity: Sentinel is available as software, supporting Red Hat or SUSE Linux as a base system, or as a virtual image. Solution packs, containing correlation rules, dashboards and reports by topic or use case, support rapid deployments.

Use Cases: Sentinel is a good option for small to midsize SEM deployments for threat monitoring. There is also a good fit for compliance use cases, when Sentinel Log Manager provides adequate coverage of compliance reporting requirements, or when additional NetIQ technologies are deployed, Sentinel is also a good fit for SIEM combined with FIM or identity context.

SolarWinds

SolarWinds Log & Event Manager (LEM) software is a virtual appliance. The vendor positions LEM as an easy-to-deploy and use SIEM for resource-constrained security teams that have no requirements for big data advanced analytics or malware detection integration. An optional Windows and Linux endpoint agent provides endpoint monitoring and control functions that are in widespread use within the installed base. SolarWinds LEM has integrations with SolarWinds other products for operations monitoring to support activities such as change detection and root cause analysis.

Real-Time Monitoring: SolarWinds LEM provides a library of more than 700 predefined correlation rules covering common security and some operational use cases. They can be reused as templates for custom rules.

Threat Intelligence: SolarWinds provides a small number of watchlists, such as known bad/good process names, bad IP addresses and common administrative account names. These are included with product updates. SolarWinds LEM users can import threat feed and watchlist information for use in correlation rules, real-time monitoring or queries.

Behavior Profiling: LEM provides basic profiling capabilities based on identifying statistical deviations from baselines on a number of data attributes.

Data and User Monitoring: SolarWinds LEM can derive user context from Active Directory and standard network authentication technologies. These limited IAM sources are dominant in the SMB space. Correlation rules are provided to facilitate authentication and access policy monitoring. The SolarWinds LEM agent provides file integrity monitoring, configuration and file access audit functions. The endpoint agent also provides some DLP capabilities. There are also integrations with a few third-party products. The SQL auditor agent provides DAM capabilities, and SolarWinds LEM can directly monitor database audit logs. There is also integration with third-party DAM products, such as Imperva and Sentrigo.

Application Monitoring: SolarWinds Server and Application Monitor (SAM) or SolarWinds Web Performance Monitor (WPM) can provide application activity data to SolarWinds LEM. SolarWinds LEM also integrates with a variety of Web infrastructure technologies, but provides limited integration with packaged applications. The vendor indicates its customers have shown no interest in support for ERP and GRC platforms.

Analytics: Support for some analytics is provided through visualization and investigation tools that are built into the SolarWinds LEM console, and through the reporting interface. SolarWinds LEM provides no support for integration with external data warehouse or big data technologies, and SolarWinds cites lack of customer demand for these capabilities.

Log Management and Reporting: Log management capabilities are provided through a proprietary data store. The reporting engine is an external component that is not fully integrated into the SIEM console; however, users indicate that predefined reports are close to what is needed for compliance reporting, and that, when light customization is needed, it is easy to accomplish.

Deployment/Support Simplicity: SolarWinds provides technology that is well-suited to its target market, requiring only light customization through easy-to-use interfaces. SolarWinds offers online training videos, but does not provide on-site implementation support services to its customers.

Use Cases: SolarWinds LEM is well-suited to SMBs that require simple, but effective threat monitoring and compliance reporting. Operationally focused and resource-restrained security teams should also consider LEM. There is an especially good fit for small organizations that also need endpoint monitoring functions.

Splunk

Splunk Enterprise provides search, alerting, real-time correlation and a query language that supports visualization using more than 100 statistical commands. The Splunk App for Enterprise Security extends Splunk Enterprise with predefined dashboards, searches, reports and alerts, to support security monitoring and analytics, as well as compliance use cases. Splunk Enterprise is widely deployed by IT operations organizations and application support teams for log management and analytics for availability-oriented use cases, contributing to the vendors' high visibility on SIEM shortlists with their Splunk App for Enterprise Security.

Real-Time Monitoring: The Splunk App for Enterprise Security includes predefined mapping for security event sources, security-specific correlation searches, reporting and security monitoring dashboards and visualizations.

Threat Intelligence: The Splunk App for Enterprise Security includes a threat intelligence framework to import and manage a variety of external threat data feeds. The framework supports STIX/TAXII, CybOX and Open IOC formats. Users can search external and internal data sources for known malicious spyware and adware IP address ranges, malicious IP addresses and bogon lists.

Behavior Profiling: Splunk's statistical analysis functions can be used to identify anomalies and deviations from normal behavior, and includes automated pattern detection capabilities.

Data and User Monitoring: Splunk provides a Windows Management Instrumentation collector for Active Directory, integration with LDAP and specific support for a few other IAM event sources. As with any SIEM technology that supports keyword search, users with knowledge of log source formats can define their own searches to develop identity context. Splunk's agent for Windows and Linux/Unix provides basic FIM functions (essentially change detection), as well as providing rudimentary endpoint behavior information (such as process, application execution path, registry information, port/traffic information and user/account/login information). Splunk also integrates with a variety of endpoint detection/endpoint detection and response (ETD/ETDR) solutions, such as Tanium, Ziften, Digial Guardian, CarbonBlack/Bit9, Tripwire, OSSEC and FileTrek. Splunk has mapping support for third-party DLP products from RSA and Symantec. For DAM, Splunk has predefined mapping support for the major third-party DAM products, and the Splunk DB Connect app provides predefined mapping support for Oracle, Microsoft SQL Server, IBM DB2, SAP Sybase and others.

Application Monitoring: A common use case for Splunk is application management — monitoring in-house-developed and commercial applications through keyword searches to correlate and visualize data from multiple sources. Splunk provides specialized add-ons for a number of commercial applications; however, only a few of these sources are supported with event mapping, predefined searches and reports. Customers can build their own add-on to provide application coverage. Splunk —supported apps for Netflow stream collection enable analysis and correlations for performance and security use cases. The free Splunk App for Stream, which can be deployed on-premises or in the cloud, enables customers to collect and analyze data from streaming network packets.

Analytics: The Splunk App for Enterprise Security provides predefined dashboards that support drill-down to intermediate data aggregations, drill-down to the raw data and pivoting to look at the data from different perspectives. Splunk has released enhancements to visualizations for security metrics, threat analytics and predictive analytics. Hunk: Splunk Analytics for Hadoop and NoSQL Stores uses batch loading and does not require Splunk event collection infrastructure.

Log Management and Reporting: There is continued deployment of, and interest in, Splunk Enterprise as a companion technology to existing SIEM deployments, and as a SIEM. Security organizations use Splunk to provide log management functions for SIEM deployments, ad hoc query for investigation and reporting for compliance. The Splunk App for Enterprise Security provides functionality to enable deployment as a SIEM, including predefined reports, dashboards, searches, visualization and real-time monitoring to support security monitoring and compliance reporting use cases. Reporting has been improved through predefined data models and pivot tables.

Deployment/Support Simplicity: Splunk has improved the ease of data acquisition in the base Splunk Enterprise product, providing guides and tools to streamline the process of working with new data sources. Splunk continues to add and refine security content to the Splunk App for Enterprise Security, Splunk App for PCI Compliance and Splunk App for FISMA. An active user and partner community also provides additional content (e.g., Cisco Security Suite and Splunk for Palo Alto Networks App). Splunk provides a wide range of configuration options and a growing number of wizards for the automated support of customization, dashboards, queries and report creation. Users report that more customization is usually required than with other SIEMs, and proficiency is required to perform extensive customization.

Use Cases: Splunk is a good fit for security organizations that need powerful drill-down search and ad hoc query investigative capabilities, in combination with real-time monitoring, visualization and correlation, and that have users with knowledge of event formats with sufficient deployment and customization expertise. Splunk supports a wide range of additional use cases, which include application monitoring, data analytics and IT operations management (ITOM). Splunk provides out-of-the-box use-case support for several security and use cases through the Splunk App for Enterprise Security, and the product can be extensively customized by skilled users.

Trustwave Holdings

Trustwave offers managed security services, vulnerability assessment and compliance services. Trustwave also offers a broad portfolio of security products, including secure Web and email gateways, DLP, a Web application firewall, network access control, unified threat management (UTM), security scanning and encryption technologies. Its threat and research capabilities include SpiderLabs, which provides research on security threats and vulnerabilities in support of service delivery and product development. The core of this portfolio is a SIEM deliverable in several configurations to meet diverse requirements, from large enterprise, SEM-oriented deployments to midsize deployments with more-modest SEM needs.

Trustwave has two SIEM options: Log Management Appliances and SIEM Enterprise. SIEM Enterprise and Log Management Appliances are available as physical or virtual appliances. The vendor also offers

managed security services for both solutions through its security operations centers. In April 2015, The Singtel Group announced that it intended to acquire Trustwave, and that Trustwave would continue to operate as a stand-alone business. At the time of this writing, the deal is pending regulatory approval.

Real-Time Monitoring: Trustwave SIEM Enterprise and Operations Edition (OE) support event and log data via agent and agentless collection, NetFlow data, as well as contextual information, such as threat intelligence and vulnerability assessment results for real-time correlation and alerting. Trustwave SIEM Enterprise includes 90 customizable correlation templates.

Threat Intelligence: Trustwave Threat Correlation Services is available as an add-on product for Trustwave SIEM Enterprise, SIEM OE and Log Management Enterprise. The service provides threat intelligence from a mix of open-source, crowdsource and commercial feeds, and contributions from Trustwave SpiderLabs research.

Behavior Profiling: SIEM Enterprise and OE provide basic statistical analysis, trending, profiling and deviation from baseline anomaly detection capabilities.

Data and User Monitoring: Trustwave SIEM Enterprise and SIEM OE integrate with Microsoft Active Directory and Oracle Identity Analytics to support user and identity mapping, and IAM policy change monitoring. Trustwave DLP can be integrated, and FIM is included with the Log Management Appliance. DAM is supported via Java Database Connectivity (JDBC) connectors and audit trail logs.

Application Monitoring: Third-party application monitoring capabilities are based on syslog and flat file ingestion, with the Active Response API available for deeper integrations.

Analytics: Customizable dashboards and visualization, as well as investigation tools (e.g., LogExplorer and EventExplorer) provide access to raw and normalized log and event data. SIEM Enterprise and SIEM OE also support post hoc statistical analysis, trending and profiling.

Log Management and Reporting: Trustwave's Log Management Enterprise and SIEM Enterprise both deliver log management and compliance capabilities. Log Management Enterprise can be upgraded to SIEM Enterprise. Agent and agentless collection are supported, with FIM capabilities included in the agent. Log Management Enterprise includes 153 report templates, including compliance, event and statistical reporting.

Deployment/Support Simplicity: Trustwave SIEM Enterprise and Log Management are available as virtual and physical appliances. Deeper third-party integrations require an API, but Trustwave also provides appropriate professional services.

Use Cases: Users deploying SIEM for threat management and compliance use cases, especially in conjunction with PCI requirements, should consider Trustwave. Use cases where automated response capabilities are required should also review Trustwave SIEM and Trustwave's self-healing network offering.

Context

SIEM technology is an important element of an organization's security strategy, because it establishes a centralized orchestration point for security monitoring, and it may be used to detect an ongoing attack in its early phases to minimize damage. SIEM tools provide user activity monitoring and DAM, as well as reporting for threat detection and to satisfy audit requirements.

Historically, the driver for many SIEM deployments has been satisfying regulatory requirements. Gartner has seen a strong shift in focus in the client base to threat monitoring in the past year, with compliance taking a secondary position. Vendors have addressed this change in demand in different ways, with analytics, network monitoring, and enhanced incident management and workflow capabilities the most common. A few vendors are offering deep UBA integrations. This research will help IT security organizations better match SIEM vendors with their requirements.

SIEM technology provides a set of common core capabilities that are needed for all cases. Other SIEM capabilities are more critical for the threat management use case or the compliance use case. Many organizations will apply SIEM technology broadly across their IT infrastructures and implement most SIEM capabilities, but they typically start with a narrow deployment that implements a subset of functions to resolve a specific compliance gap or security issue.

In addition to the eight critical capabilities described in this research, organizations should evaluate the following four additional SIEM capabilities.

Scalable Architecture and Deployment Flexibility

These are derived from vendor design decisions in the areas of product architecture, data collection techniques, agent designs and coding practices. Scalability can be achieved by:

- A hierarchy of SIEM servers — tiers of systems that aggregate, correlate and store data.
- Segmented server functions — specialized servers for collection correlation, storage, reporting and display.
- A combination of hierarchy and segmentation to support horizontal scaling.
- During the planning phase, many organizations underestimate the volume of event data that will be collected, as well as the scope of analysis reporting that will be required. An architecture that supports scalability and deployment flexibility will enable an organization to adapt its deployment in the face of unexpected event volume and analysis.

Real-Time Event Data Collection

SIEM products collect event data in near real time in a way that enables immediate analysis. Data collection methods include:

- Receipt of a syslog data stream from the monitored event source

- Agents installed directly on the monitored event source or at an aggregation point, such as a syslog server
- Invocation of the monitored system's command line interface
- APIs provided by the monitored event source
- External collectors provided by the SIEM tool
- Network traffic monitoring (e.g., via NetFlow)

The technology should also support batch data collection for cases in which real-time collection is impractical or not needed.

Filtering options at the source are important methods of data reduction, especially for distributed deployments with network bandwidth constraints. Agent-based collection options and virtualized SIEM infrastructure options will become more important as organizations move workloads to virtualized and public infrastructure as service cloud environments. A growing number of organizations that have deployed SIEM technology must integrate data sources that aren't formally supported by the SIEM vendors. SIEM products should provide APIs, graphical user interfaces and wizards for parser creation to support the integration of unsupported data sources. This capability becomes crucial as organizations apply SIEM technology for application-layer monitoring.

Event Normalization and Taxonomy

This is a mapping of information from heterogeneous sources to a common event classification scheme. A taxonomy aids in pattern recognition, and also improves the scope and stability of correlation rules. When events from heterogeneous sources are normalized, they can be analyzed by a smaller number of correlation rules. This reduces deployment and support labor. In addition, normalized events are easier to work with when developing reports and dashboards.

Incident Management Support

Specialized incident management and workflow support should be embedded in the SIEM product primarily to support the IT security organization. Products should provide integration with enterprise workflow systems and support ad hoc queries for incident investigation.

Product/Service Class Definition

SIEM technology supports threat management and security incident response through the collection and analysis of security events from a wide variety of event and contextual data sources in real time. It also supports incident investigation and security policy compliance monitoring through the analysis of and reporting on historical data from these sources. The core capabilities of SIEM technology are the broad scope of event collection and the ability to correlate and analyze events across disparate information sources. The technology is typically deployed to:

- Discover external and internal threats
- Monitor the activities of privileged users
- Monitor server and database resource access
- Monitor, correlate and analyze user activity across multiple systems and applications
- Provide compliance reporting
- Provide analytics and workflow to support incident response

SIEM technology aggregates and analyzes the event data produced by devices, systems and applications. The primary data source is log data; however, SIEM technology can also process other forms of data to obtain network context about users, IT assets, data, applications, threats and vulnerabilities. The data is normalized, so that events from disparate sources can be correlated and analyzed for specific purposes, such as network security event monitoring and user activity monitoring for the early detection of breaches or misuse.

Critical Capabilities Definition

Real-Time Monitoring

This is important for threat management, to track and analyze the progression of an attack across components and systems, and, for user activity monitoring, to track and analyze a user's activity across applications or to track and analyze a series of related transactions or data access events.

Event correlation establishes relationships among messages or events that are generated by devices, systems or applications, based on characteristics such as the source, target, protocol or event type. There should also be a library of predefined correlation rules and the ability to easily customize those rules. A security event console should provide the real-time presentation of security incidents and events.

Threat Intelligence

Up-to-date data on threats and attack patterns help organizations recognize abnormal activity — e.g., outbound activity to an external IP address might look normal and be overlooked. This changes if threat intelligence indicates the destination is associated with a botnet command and control center.

Intelligence about the current threat environment exists in a variety of sources, including open-source lists, the threat and reputation content developed and maintained by security research teams within security vendors, and data developed by managed security and other service providers. Two related standards — Structured Threat Information Expression (STIX), for the structured representation of cyberthreat information, and Trusted Automated Exchange of Indicator Information (TAXII), for the exchange and transport of cyberthreat information — are also gaining traction.

Threat intelligence data can be integrated with a SIEM in the form of watchlists, correlation rules and queries in ways that increase the success rate of early breach detection.

Behavior Profiling

Well-defined abnormal conditions support correlation rules that seek a specific set of conditions to be defined. Anomaly detection can complement rule-based approaches, because it alerts organizations to deviations from normal. Profiling and anomaly detection also complement rule-based correlation.

Behavior profiling employs a learning phase that builds profiles of normal activity for various event categories, such as network flows, user activity and server access.

The monitoring phase alerts on deviations from normal.

Data and User Monitoring

User activity monitoring and DAM that includes user and data context is needed for breach and misuse discovery. Privileged user and sensitive data access monitoring is also a common requirement for compliance reporting.

This capability establishes user and data context, and enables data access and activity monitoring. Functions include integration with IAM infrastructure to obtain user context and the inclusion of user context in correlation, analytics and reporting.

Data access monitoring includes monitoring of DBMSs and integration with FIM and DLP functions. DBMS monitoring can take three forms — parsing of DBMS audit logs, integration with third-party DAM functions or embedded DAM functions. FIM can be provided by the SIEM product directly or through integration with third-party products.

Application Monitoring

This is critical because application weaknesses are frequently exploited in targeted attacks, and abnormal application activity may be the only signal of a successful breach or of fraudulent activity.

The ability to parse activity streams from packaged applications enables application-layer monitoring for those components, and the ability to define and parse activity streams for custom applications enables application-layer monitoring for in-house-developed applications. Integration with packaged applications, an interface that enables customers to define log formats of unsupported event sources, and the inclusion of application and user context are important capabilities that support the monitoring of application activities for application-layer attack detection, fraud detection and compliance reporting.

Analytics

When security monitoring/activity reporting reveal suspect activity, the ability to analyze user and resource access via an iterative approach that starts with a broad query about an event source, user or target, and then increasingly focus queries to identify the source of the problem is crucial.

Security event analytics comprise dashboard views, reports and ad hoc query functions to support the investigation of user activity and resource access to identify a threat, a breach or the misuse of access rights.

Log Management and Reporting

Log management has become part of the standard of due care for many regulations. Compliance-oriented deployments are simplified when the SIEM technology includes predefined and modifiable reports for user activity, resource access and model reports for specific regulations.

Functions supporting the cost-effective storage and analysis of a large information store include collection, indexing and storage of all log and event data from every source, as well as the capability to search and report on that data.

Reporting capabilities should include predefined reports, as well as the ability to define ad hoc reports or use third-party reporting tools.

Deployment/Support Simplicity

Compliance and security requirements have extended the SIEM market to organizations with smaller security staffs and more-limited system support capabilities. For these buyers, predefined functions and ease of deployment and support are valued over advanced functionality and extensive customization.

Deployment and support simplicity is achieved through a combination of embedded SIEM use-case knowledge and a general design that minimizes deployment and support tasks.

Embedded knowledge is delivered with predefined dashboard views, reports for specific monitoring tasks and regulatory requirements, a library of correlation rules for common monitoring scenarios, and event filters for common sources. There should also be an easy way to modify the predefined functions to meet the particular needs of an organization.

Use Cases

Although most SIEM projects have been funded to resolve compliance issues, this has changed noticeably during the past 24 months. New and evolving threats, better situational awareness about adversaries and a growing number of high profile breaches have made compliance a secondary consideration. Most organizations know that they need to improve security monitoring and incident response. IT security organizations evaluate and deploy SIEM tools for three primary use cases.

Compliance

The SIEM technology deployment is tactical, focused on log management, specific compliance reporting requirements and a subset of servers that is material to the regulation.

Log management is weighted heavily, because it provides the basic "check box" that a superficial audit would require. User and resource access reporting is important, because SIEM technology is commonly deployed as a compensating control for weaknesses in user or resource access management. The

implementation time frame is typically short, so simplicity and ease of deployment are valued over advanced functions and the capability to customize heavily.

Threat Management

The IT security organization has obtained funding for a SIEM deployment by making the case for improved threat management, breach detection and incident response capabilities.

There's higher weighting to real-time event management and correlation, threat intelligence, anomaly detection, and support for high-performance and large-scale historical data analysis.

SIEM

In this use case, there is a need to improve breach detection and incident response capabilities, and also a need for reporting to close compliance gaps.

The SIEM technology must support rapid deployment for compliance reporting, and provide for subsequent deployment steps that implement SEM capabilities.

Vendors Added and Dropped

Added

No vendors were added.

Dropped

- ManageEngine
- Tenable Network Security
- Tibco Software (LogLogic)

Inclusion Criteria

In this research, we've included software products for evaluation, based on the following criteria:

- The products must cover the core SIEM functions.
- The products must have been in general availability and deployed in customer environments as of March 2015.
- The products must target the SIEM market segment and the security buying center.
- Gartner must have determined that the participants are the largest players in the market, based on Gartner estimates of the SIEM customer base size and SIEM revenue.

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Compliance	Threat Management	SIEM
Real-Time Monitoring	2%	18%	15%
Threat Intelligence	2%	9%	10%
Behavior Profiling	2%	10%	7%
Data and User Monitoring	10%	10%	8%
Application Monitoring	2%	10%	6%
Analytics	2%	23%	8%
Log Management and Reporting	55%	10%	26%
Deployment/Support Simplicity	25%	10%	20%
Total	**100%**	**100%**	**100%**
As of September 2015			

Source: Gartner (September 2015)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighted in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated (see Table 2) on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

This year, capabilities provided by add-on products were not weighted as much as last year. The availability of additional products that extend the SIEM's capabilities have been given some credit, but Gartner has considered that these involve additional cost and complexity. To facilitate a better assessment of the technical capabilities, Gartner also weighted insights gained from structured vendor demos.

Table 2. Product/Service Rating on Critical Capabilities

Critical Capabilities	AccelOps	AlienVault	BlackStratus	EMC	EventTracker	HP (ArcSight)	IBM Security	Int Sec

							QRadar	
Real-Time Monitoring	3.0	3.0	3.3	3.3	2.5	4.0	4.0	
Threat Intelligence	3.5	3.8	2.5	4.0	3.1	4.0	3.8	
Behavior Profiling	2.5	2.8	2.0	4.0	2.8	4.0	4.5	
Data and User Monitoring	2.4	2.0	2.0	3.5	3.0	4.2	3.3	
Application Monitoring	2.5	2.0	2.0	3.7	2.7	4.1	3.7	
Analytics	2.6	2.5	2.8	3.4	2.0	3.8	3.7	
Log Management and Reporting	2.8	3.0	2.5	3.2	2.8	3.5	3.6	
Deployment/ Support Simplicity	3.5	3.8	2.5	2.3	4.5	3.0	4.3	
As of September 2015								

Source: Gartner (September 2015)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3. Product Score in Use Cases

Use Cases	AccelOps	AlienVault	BlackStratus	EMC	EventTracker	HP (ArcSight)	IBM Security QRadar	Int Se
Compliance	2.94	3.08	2.45	3.05	3.23	3.49	3.78	3
Threat Management	2.82	2.82	2.56	3.41	2.77	3.83	3.85	3
SIEM	2.95	3.05	2.54	3.24	3.07	3.68	3.87	3
As of September 2015								

Source: Gartner (September 2015)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.