Solutions Review

Security Information and Event Management

Buyer's Guide

Includes a Category Overview
The Top 10 Questions to Ask
Plus a Capabilities Reference of
the Leading 24 SIEM Solutions

INTRODUCTION

We are living in the age of the data breach. As of December 2016, there have been over 980 data breach incidents in 2016, putting us on track to eclipse 2014's record high 783 data breaches.

The average cost of those breaches? $3.8 to $4 million, according to research from the Ponemon institute. And, beyond the immediate financial cost, data breaches can cause an unquantifiable loss in customer confidence.

But IT organizations aren't just fighting hackers and malware—they're also battling a torrent of data from their own networks. Information is pouring in. A fortune 500 enterprise's infrastructure can easily generate 10 terabytes of plain-text data per month. Logs, threat intelligence feeds, forensics, IAM- if improperly managed these systems can create such a deluge of data that many enterprises end up underwater while the pertinent security data floats by.

So how can enterprises effectively log, monitor, and correlate that data to obtain actionable insight? Enter the Security Information and Event Management (SIEM) solution.

Coined by Gartner analysts Mark Nicolett and Amrit Williams in 2005, SIEM is, in simple terms, a security solution that combines Security Event Management (SEM), which focuses on log collection and report generation, with Security Information Management (SIM), which focuses on analyzing real-time events using event correlation and event mechanisms.

SIEM solutions help enterprises manage the increasing volumes of logs coming from disparate sources and lessen the damage of sophisticated cyber-attacks by proactively monitoring networks for suspicious activity in real-time.

"SIEM solutions help enterprises manage the volumes of log data coming from disparate sources."

Traditionally, SIEM is deployed for two use cases: threat management: the real-time monitoring and reporting of activity and access, or Compliance reporting, which helps businesses meet stringent compliance requirements such as HIPAA, PCI DSS, SOX, and more.

However, as information security has evolved, so have SIEM capabilities. Today's SIEM systems are quickly embracing new capabilities such as behavioral analytics, which can help enterprises detect potential threats and eliminate them before they turn into costly breaches.

In 2017, SIEM is seen as a necessary part of any significant enterprise security effort, but choosing the right SIEM solution for your organization isn't easy. SIEM has a reputation as a complex and convoluted product, and implementation is a daunting process that can take weeks or even months to complete. Rush that process and you could end up with massive cost overruns or worse, an expensive, failed deployment.

To complicate things further, SIEM is a mature market full of vendors capable of meeting the basic log management, compliance, and event monitoring requirements of a typical customer, but whose points of differentiation may not be obvious to the untrained eye. However, as similar as they may seem, many SIEM solutions are optimized for drastically different use-cases, and one size almost never fits all.

This guide includes both pure SIEM solutions and more specialized solutions, as a full-blown SIEM may not be the best option for an organization. We've also included the new-guard— Big Data Analytics security platforms such as Splunk.

When evaluating the 24 solutions listed in this guide and others not listed, it's important to consider the tradeoffs that come with each kind of solution. Will you be focused on compliance or threat detection or incident response? Do you want a solution that comes prebuilt for today's threats, or one that, through customization, can adapt to new threats? What kind of solution does your team want? What can they handle? These are the questions you need to ask yourself.

Whatever your decision, one thing is certain: whether you are a publicly traded corporation, a government institution or even a small to medium-sized business, the benefits of SIEM are worth investigating today. In this Buyer's Guide there's a solution for everyone, from small groups to multi-national organizations.

"In this Buyer's Guide there's a solution for everyone, from small groups to multi-national organizations."

Solutions Review is not in the business of picking winners and losers in a technology solution sector; we'll leave that to others. Our job is to help you get started evaluating providers. In this Buyer's Guide, we've selected 24 SIEM and Security Analytics solutions as a way to narrow things down a bit for potential buyers.

In order to help you start the process of sorting all this out, below are 10 questions, five for yourself, and five for a prospective solutions provider to your SIEM needs. These questions will help you walk through what you want in a solution, what it's supposed to do for you, as well as evaluating the solution's offerings, services and staying power.

Jeff Edwards
Editor
Solutions Review

5 Questions You Should Ask Yourself Before Selecting an SIEM Solution

QUESTION #1 How will we support our SIEM Solution?

SIEM only works if you work it, and a typical SIEM deployment can require a team of up to eight full-time employees to properly manage it. SIEM without a dedicated team of security analysts is like an empty castle: it may seem imposing, but it's not stopping anybody. SIEM is not a substitute for a security department, it's a tool, and it needs a good technical expert and ongoing to work properly and deliver value. Before considering which SIEM is right for you, make sure your organization is prepared to properly manage one. Do you have the resources and personnel to effectively manage SIEM? Can you hire and train the staff necessary to support SIEM? If not, you may be better off considering a managed services offering.

QUESTION #2 What does my organization want to get out of SIEM?

It may seem obvious, but you must know your requirements when evaluating SIEM or Security Analytics solutions. Before beginning the evaluation process you should rank your needs and your business drivers for adopting SIEM. What data sources do you need to log? Do you need real-time collection? Do you need to collect all security data or just a subset? What do you need to archive? For how long? How will you use data once collected? For Forensics? Detecting threats? Auditing and Compliance?

QUESTION #3 Do we need a full SIEM solution? Or is log management sufficient?

SIEM systems are highly capable, but they're also costly and complex. If your organization is window shopping for complex SIEM solutions without a complex use case, then you may want to reconsider. For example, many regulatory compliance requirements can be met with traditional log management solutions. If you find yourself more concerned with log management than with correlation, SEM, and SIM, this may the right move for you.

QUESTION #4 Do we need 'Security Analytics' or traditional SIEM?

"Security Analytics" solutions, which leverage big data technologies and new analytic algorithms, are making a major impact on the SIEM market. They are extremely effective solutions, but they are also quite complicated. Organizations with mature, well-funded and dedicated security operations teams should investigate these kinds of solutions, which can recognize security threats better and reduce the workload on the analysts tasked with monitoring your systems. Be wary, though—if your organization is having trouble with its current SIEM deployment, it's doubtful that you could handle a big data security analytics system. As Gartner Analyst Anton Chuvakin has said, "do not pay for the glamour of big data if there's a low chance of benefiting from the investment."

QUESTION #5 How much are we willing to spend?

Enterprise SIEM requires a significant budget. There are the initial license costs, often arranged as base price plus user or node, there are database costs for servers, the costs of training personnel, and often additional external storage. Then there's the ongoing cost of the personnel required to operate a SIEM effectively. A full-blown, enterprise-grade SIEM system can cost your business hundreds of thousands of dollars when all is said and done, and while that will give you top-of-the-line capabilities, not all business are capable of spending that kind of money. Some SIEM vendors offer a lightweight version that gives basic log management and reporting capabilities without the advanced analytic capabilities and other features that other SIEMs support. These lightweight SIEMs are considerably less expensive to acquire than other SIEMs, and could be a good alternative for businesses looking to save money.

And 5 Questions You Should Ask Your Potential SIEM Solution Provider

QUESTION #6 How will your product meet our auditing and regulatory compliance needs?

Compliance management is one of the most frequent use cases for SIEM solutions, and as such, most SIEMs have built-in support for the most common compliance efforts, such as HIPAA, PCI DSS, and SOX. Your organization can save time and resources by using a SIEM to meet its compliance reporting requirements, but before you can do so you need to make sure that a potential solution is compatible to your specific industry regulations.

Ask your potential vendor to demonstrate a clear relationship between your industry compliance needs and their policies and rule sets. What out-of-the-box compliance reports are available? What level of customization is available for reporting?

QUESTION #7 Do you offer assistance with deployment? What about training for personnel?

SIEM is a complex technology, and so naturally, SIEM deployment is a complex process. In fact, SIEM is notoriously difficult to deploy-- In a 2014 Report, Gartner analyst Oliver Rochford estimated that somewhere between 20% and 30% of SIEM deployments among his client base fail. Once successfully deployed, a SIEM solution requires a dedicated team of skilled analysts and technicians to manage the software and ensure effective use. Ask prospective vendors what kind of support they will provide during the deployment process, and what, if any, training is available for your team.

QUESTION #8 Do you support public and private cloud platforms and big data environments? If not, do you have plans to do so?

Whether you're there yet or not, there's a strong chance that Public Cloud Computing and Big Data Solutions will play a prominent role in the future of your organization's IT environment. If you're spending top dollar on an SIEM solution today, you'll want to know that it will integrate with the systems you use tomorrow. Ask prospective vendors how their solutions support cloud and big data platforms that you currently use, or may use in the future.

"Will the SIEM system you buy today integrate with the systems you use tomorrow?"

QUESTION #9 How well does your SIEM handle the log sources? Is there extensive native support, or will custom development work be required?

Your SIEM isn't worth much if it can't understand the log data from the important log-generating sources in your organization. Make sure your potential SIEM solution supports your organization's security systems, such as firewalls, intrusion prevention systems, VPNs, email gateways, and antimalware products.

Any prospective SIEM solutions should also support log files from the operating system (both type and version) that your organization uses.

QUESTION #10 What features does your product provide for data analysis?

Aside from the SIEM's alerts and reporting, an SIEM used for incident detection and response should provide features that help your security analysts review and analyze log data.

Even the smartest, best-configured SIEM is worse than the best analyst--a highly accurate SIEM can still misinterpret events, so make sure your team can vet the SIEM's results. Strong search and data visualization capabilities can also help facilitate the investigation of incidents.

Solution Provider Profiles

Alert Logic

Alert Logic provides Security-as-a-Service (SaaS) for on-premises, cloud, and hybrid infrastructures, delivering security insight and protection. The company partners with cloud platforms and hosting providers, protecting 3,000+ organizations. Built for cloud scale, Alert Logic's patented platform stores petabytes of data, analyzes events, and identifies security incidents, all of which are managed by their Security Operations Center.

Key Features

- Threat Manager – A network-based intrusion detection system and vulnerability scanning product that monitors network traffic around the clock in order to identify known incidents, vulnerabilities and misconfigurations.
- Log Manager – A log management solution designed to collect, aggregate and normalize log data from any environment in order to meet compliance mandates and identify security issues.
- Web Security Manager – A managed Web Application Firewall (WAF) that detects and protects applications from advanced web application attacks to ensure uninterrupted availability.
- ActiveWatch – A managed service that provides 24 X 7 monitoring of Alert Logic products, including a core team of security and compliance experts that investigate security incidents identified by the Alert Logic platform, and work with each impacted customer to provide recommendations for neutralizing the threat.
- LogReview – Daily event log monitoring and review designed to help meet PCI DSS, HIPAA, SOX, and other compliance mandates; a team of certified security analysts acts as an extension of your team to expertly review your log data daily and alert you whenever suspicious activity or possible security breaches are detected.
- Cloud Defender – All the individual products can be purchased together in Cloud Defender.

Bottom Line

Alert Logic is well-suited for small to midsize companies, and is mainly used by Public and Hybrid Service Providers, and on-premises implementations.

AlienVault

AlienVault Unified Security Management (USM) is an all-in-one platform designed and priced to ensure that mid-market organizations can effectively defend themselves against today's advanced threats. It significantly reduces complexity and deployment time so users can go from installation to first insight in about an hour. AlienVault prioritizes risk through correlation of reputation, threat severity, and asset vulnerability.

Key Features

Unified Security Management – AlienVault includes five essential security capabilities in a single solution:

- Asset Discovery – This feature provides built-in passive and active network asset discovery, asset inventory, and software inventory. Infrastructure.
- Vulnerability Assessment – This feature enables organizations to scan assets to identify vulnerabilities that can be exploited by a bad actor.
- Intrusion Detection – A vital part of AlienVault's USM platform is to monitor the network and assets for threats with Network IDS, Host IDS, File Integrity Monitoring, Registry Monitoring, and Rootkit Detection capability.
- Behavioral Monitoring – AlienVault has built-in log management, netflow analysis, service availability monitoring, and network packet capture.
- Security Intelligence – This feature allows for correlation of data produced by the built-in tools and external data sources, incident response, and reporting to support threat detection and compliance use cases.

Integrated Threat Intelligence – AlienVault Labs Threat Intelligence drives the USM platform's threat assessment capabilities by identifying the latest threats, resulting in the broadest view of threat vectors, attacker techniques and effective defenses. Unlike single-purpose updates focused on only one security control, AlienVault Labs regularly delivers eight coordinated rule set updates to the USM platform.

Bottom Line

AlienVault's focus on ease-of-use and speed-to-deployment makes it a good fit for enterprises with a smaller staff and limited security programs at a lower cost.

Assuria

Assuria uses Amazon Web Services (AWS) to deliver a range of IT security monitoring solutions for enterprises. CSS provides an easy path for AWS customers to benefit from corporate data center levels of security and compliance monitoring in their AWS cloud platforms. CSS works in public cloud environments, enabling AWS customers to exploit the security monitoring, forensic investigations, operational efficiency, and compliance purposes. Products are sold worldwide, especially to the financial and government sectors.

Key Features

- Protective Monitoring – Provides automated monitoring and analysis of audit logs to provide visibility of IT system activity in order to enable protection and SOC (Security Operations Center) services.
- Enterprise-Wide Log Collection – Collects logs from almost any system into a central store.
- Forensic Readiness – Logs are collected in a secure and forensically sound manner, retaining their original form, complete with relevant metadata, thus allowing repeated examination, re-analysis, and use of the logs by other applications and processes.
- Real-time Event Alerting – Configurable to specific log events sent via email and/or SNMP traps.
- Agent-Based Log Management – Ensures the security, continuity, and integrity of all collected logs and alerting at the source.
- Digitally Signed – An RSA/SHA256 digital signature is calculated, and the log digitally signed before transfer. The transfer is authenticated and encrypted using TLS.
- Secure Storage – Log cataloging, chain of custody records, archive creation, and management. Archive to secure long-term storage, complete with a digitally-signed manifest.
- Scalable and Modular Architecture – Designed to support almost any sized IT environment up to the thousands of log sources. Supports multiple collection points; load balancing and resilience built-in.

Bottom Line

Assuria caters to enterprises of all sizes and works in both private and public sectors. They also provide reliable and simple security and compliance monitoring in their AWS cloud operations.

BAE Systems

BAE Systems is one of the United States' largest defense contractors, and also offers a wide variety of security capabilities such as threat analytics, threat intelligence, and advanced threat detection. BAE acquired SilverSky in 2014, and has since rebranded its solution as BAE Systems Applied Intelligence, and now offers specialized solutions in network security monitoring, Threat Analytics, Threat Intelligence, and Threat Detection. Many of BAE Systems' products can be delivered as a managed service.

Key Features

- Network Security Monitoring – Network Security Monitoring is a managed security service (MSS) provided by BAE Systems, that captures the logs and events from the devices on your network and then allows our cyber security experts to process and analyses them on your behalf.
- Threat Analytics Engine – The BAE Systems Threat Analytics Engine provides a scalable platform that supports massive scale data ingress, storage, fast querying, retrieval and analysis.
- Threat Intelligence Management –BAE's platform implements a workflow that provides automation for repeatable processes, whilst supporting rapid real-time analysis by experienced human operators.

Bottom Line

BAE Systems' customer portfolio includes small to medium-sized businesses as well as Fortune 500 enterprises, but their background as a defense contractor makes them particularly well suited to government and national security organizations.

BlackStratus

BlackStratus provides reliable and innovative security information event management (SIEM) and services, and offers security and compliance management. Their three offerings are Log Storm, SIEM Storm, and CYBERShark, a cloud-based SIEM-as-a-service. BlackStratus is built on a multi-tiered, distributed architecture to diminish the chance of missing a threatening event, saving downtime and information loss. They offer a simplified licensing model based on back-end storage, rather than an EPS-based model.

Key Features

- Log Storm – Log management capabilities aimed at MSSPs and small- to mid-size enterprises. Available as virtual and hardware appliances.
- SIEM Storm – Provides features such as multitenancy and SEM capabilities, including analytics, historical correlation, and threat intelligence integration. It is deployable as software or virtual images, and can be used in combination with LogStorm as the storage and collection tier.
- Compliance Storm – Cloud-based service for long retention and scheduled reporting for meeting regulatory and compliance mandates.
- Vulnerability Correlation – Integrate data from CVE-compliant intrusion detection systems, therefore eliminating false positives and freeing up time for your team to focus on real threats.
- Visibility – Within distributed networks, correlate activity in individual customer environments, identifying hidden threats, suspicious trends, and other potentially dangerous behavior.
- Reporting Tools – For compliance standards, including ISO, PCI, HIPAA, SOX, etc.
- Historical Correlation – Repeated attack patterns that might be hidden within raw security events can be quickly detected despite being previously recognized. This way, your analysts are better positioned for real-time detection for future zero-day attacks.

Bottom Line

BlackStratus Storm is compatible with 1,000+ network devices, operating systems, servers, and other appliances. It is a good fit for service providers requiring a customizable SIEM platform, and for service-centric end-user organizations looking for well-formed multitenancy support.

CorreLog

CorreLog is a web-based message aggregation and correlation system designed to acquire high-speed, real-time information in the form of event logs, syslog messages, and SNMP traps.

It also creates actionable tickets, and uses neural-network technology, auto-learning algorithms, semantic sensors, and other components to make sense from raw log file messages.

Key Features

- Message Reception – Suitable to operate as the single SNMP Trap and Syslog receiver for all devices on the networks of large enterprises. Able to process more than 2000 messages per second, and can handle burst traffic of more than 10,000 messages in one second (depending upon the supporting hardware). Tracks and catalogs devices on the network without hard upper limit.
- Message Correlation – CorreLog uses an advanced correlation engine, which performs semantic analysis of your messages in real-time. The system employs correlation threads, correlation counters, correlation alerts, and correlation triggers.
- Flexible Reporting – CorreLog incorporates various reporting facilities, including an Excel-based reporting facility that populates spreadsheets with summary and detailed event information, and an ODBC reporting facility that populates one or more databases with report information to support third-party report writers.
- Data Aggregation and Archiving Functions – The CorreLog system can collect in excess of 1 Gigabyte of data each day at a single site, and save this data online for up to 500 days (given enough storage). Additionally, CorreLog compresses and archives and retains users' data for a period of more than 10 years. To assist in forensics and long-term analysis, CorreLog generates archival data such as MD5 checksums and Security Codes.
- Taxonomy, Ontology, and Catalog Functions – Automatically catalogs information by IP address, username, facility, and severity. Users can further create catalogs of information based upon simple or complex match patterns. Data is categorized based upon specifications consisting of simple keywords, wildcards, and regular expressions, logical expressions of wildcards, macro-definitions of regular expressions, and logical combinations of macros.

Bottom Line

An affordable and easy to implement SIEM solution, CorreLog is a good option for smaller to mid-sized businesses.

EiQ Networks

EiQ NetWorks' origins are in the analysis of log files across web servers, file servers, firewall, and other network devices. Having recently moved into SIEM market, EiQ reduces cyber risk, and enables you to implement strategies to combat risk by combining security programs with insurance coverage. EiQ offers SOCVue, a security hybrid SaaS offering, and provides 24x7 security operations for Small to Medium enterprises who need to protect themselves against cyberattacks but lack resources or on-staff expertise.

Key Features

- Correlation – EiQ Networks correlates and analyzes event patterns across your network systems, as well as data types, such as network traffic, security events, user account activity, and host vulnerabilities to improve incident detection.
- Alerts – EIQ provides real-time alerting for visualizing information security to ensure that compliance personnel can address problems quickly and efficiently.
- Centralization – Events from advanced security technology (e.g., IDS, VA scanners, etc.) enable organizations to quickly isolate advanced threats, including DDOS, insider theft, brute force attacks, worms, and botnets.
- SecureVue's ComplianceVue® – EiQ utilizes an add-on module that provides comprehensive configuration auditing for workstations, servers, and network devices. ComplianceVue also identifies vulnerabilities caused by weak security settings and misconfigured systems. The solution automatically collects configuration data from across the computing environment without the need to install an agent on individual devices.
- SOCVue – EiQ offers SOCVue, a SaaS offering, to provide security and resources to businesses that lack on-staff expertise.

Bottom Line

EiQ is a good option for small and mid-sized enterprises. Their solutions help manage IT infrastructure costs while improving their IT security.

EventTracker

EventTracker targets its SIEM software and service offering primarily at midsize commercial enterprises and government organizations with SEM and compliance reporting requirements.

Available as software only, it provides support for file integrity monitoring and USB control. The EventTracker agent offers support for file integrity monitoring and USB control. Add-ons are available for vulnerability and configuration assessment while basic profiling capabilities are provided through a behavior module.

Key Features

- EventTracker Control Center (EEC) – The ECC provides system administration, including software updates, service and knowledge packs, new release upgrades, and licensing key installations. EEC also executes health checks, storage projections, and log volume/performance analysis.
- Analyze Alerts – EventTracker allows you to analyze alerts, incidents, anomalies, reports, and to escalate all of the above as needed.
- Reports – EventTracker delivers Critical Observations Reports, as well as monthly or quarterly Management Executive Dashboard Powerpoints.
- Compliance – EventTracker's software has the ability to review top level summary reports, and can maintain auditor-ready artifacts.
- Correlation – The SIEM simplified team provides on-demand expert services on an annual retainer. Advanced correlation and Behavior Analysis Configuration, custom alerts and scripts, as well as the configuration of FLEX Reports and Top Level Summaries.

Bottom Line

EventTracker is easy to deploy and maintain, and is a good choice for midsize businesses that require a software-based solution for log and event management, compliance reporting, and operations monitoring via on-premises or cloud-hosted SIEM, with optional basic monitoring services.

Fortinet (AccelOps)

Fortinet entered the SIEM in June 2016 when it acquired AccelOps and rebranded its product as FortiSIEM. Fortinet provides SIEM, file integrity monitoring (FIM), configuration management database (CMDB) and availability and performance, capabilities. This allows for monitoring of Data Center Infrastructure from network devices, environmental equipment, servers, storage, hypervisors, and applications. Analytics-driven IT operations and cloud management are also provided, helping companies manage and monitor network performance, security, and compliance requirements. FortiSIEM detects network services and profile network traffic from network flow and firewall logs.

Key Features

- Statistical Anomaly Detection – Machine-learning algorithm profiles traffic and metrics on all the devices on your network, triggering alerts when anomalies are detected or thresholds are reached.
- External Threat Feed API – Allows users to integrate any public or private threat feed into FortiSIEM, and cross-correlate with users' own networks and security data.
- Acceleport – Enables users to "tunnel in" between the AccelOps Collector and Supervisor to reach any server on the system, making it ideal for organizations with remote sites, managed service providers (MSPs), and managed security service providers (MSSPs).
- Threat Management and Compliance – Supports cross-domain patterns and time-based operators to codify and detect sophisticated threats. When combined with performance and configuration metrics from FortiSIEM Performance and Availability Monitoring, consumers can detect Advanced Persistent Threats and mitigate risks from a single platform. FortiSIEM has a knowledgebase of more than 1,700 reports, including automated compliance reports covering HIPAA, PCI DSS, SOX, and other compliance standards.

Bottom Line

FortiSIEM's Collector and Supervisor is unique to this vender, which is good for organizations with remote sites, MSPs, and MSSPs. Their solution is a well-suited for enterprises and MSSPs that need a combination of security monitoring and APM with integrated CMDB capabilities. It is also a good fit for IT teams with combined operations and security function.

Hewlett Packard Enterprise (HPE)

HPE's ArcSight includes Enterprise Security Manager (ESM) software for large-scale, SEM-focused deployments. They also offer ArcSight Express, which is an appliance-based solution for the midmarket with pre-configured monitoring and reporting. It provides advanced security analytics to identify threats, manage risk, and also includes Real-Time Threat Detection, Simplified Compliance, risk management, insider threat detection, application monitoring, and the ability to identify APTs. HP's Cyber Security Company provides data security analytics, intelligence software for security information, event management, and log management solutions.

Key Features

- Real-Time Threat Detection – Transforms data into actionable security intelligence by using real-time correlation combined with powerful security analytics with ArcSightESM and ArcSight Express.
- Simplified Compliance – Reduces cost and effort needed to meet compliance and regulatory requirements via ArcSight Logger and/or Compliance Insight Packages.
- Managed Risk – Manages security risks specific to users' business with ESM Risk Insight.
- Insider Threat Detection – Monitors user behavior and prevents threats to sensitive data.
- Application Monitoring – Eliminates application blind spots and gains full visibility into user apps with ArcSight Application View.
- Identify APTs – Identifies and reacts to Advanced Persistent Threats (APTs) via suspicious pattern and automated response.

Bottom Line

HPE's ArcSight ESM is best for large-scale deployments with in-house support. ArcSight Express is a good fit for midsize deployments.

IBM QRadar

IBM Security's QRadar Platform can be deployed as an appliance, a virtual appliance, or a SaaS infrastructure as a service (IaaS). They also deliver a hybrid option, with on-premises QRadar deployment – a SaaS solution hosted on their IBM Cloud, which includes optional remote monitoring from their managed security service operations centers. IBM products provide a unified architecture for integrating security information and event management, log management, anomaly detection, incident forensics, and configuration/vulnerability management.

Key Features

- Visibility – Provides real-time threat detection, delivering surveillance throughout the entire IT infrastructure. IBM QRadar helps to detect and track malicious activity over extended periods of time and uncover advanced threats. With QRadar VFlow Collector appliances, more visibility into business application activity allows for better security monitoring, analysis, and anomaly detection.
- Reduction and Prioritization of Alerts – Focuses investigations on an actionable list of suspected incidents, reducing the thousands of events into a manageable list.
- Threat Management Produces detailed data access and user activity reports and detects insider fraud with advanced options.
- Activity Reports – Manages compliance effectively and efficiently while integrating log management and network threat protection technologies within a common database and shared dashboard user interface.
- Master Console – Provides security intelligence solutions in a cost-effective manner in order to assist managed service providers.

Bottom Line

IBM's QRadar is best suited for midsize to large enterprises with general SIEM requirements, and those who use cases that require behavior analysis, network flow, and packet analysis.

McAfee Enterprise Security Manager

Intel Security delivers a real-time understanding of threat data, reputation feeds, and vulnerability status. It also brings event, threat, and risk data together to provide security intelligence, incident response, log management, and compliance reporting. McAfee Enterprise Security Manager (ESM) consolidates, correlates, assesses, and prioritizes security events for both third-party and Intel Security solutions. It also provides integrated tools for configuration and change management, case management, and centralized management of policy to improve workflow and efficiency.

Key Features

- Advanced Threat Intelligence – ESM calculates baseline activity for all collected information and provides alerts of potential threats before they occur. It also analyzes data for patterns that may indicate a larger threat, and leverages contextual information (i.e., vulnerability scans, identity and authentication management systems). Intel Security enriches each event with context for a better understanding of how security events might impact business processes.
- Critical Facts – Database appliance collects, processes, and correlates log events from multiple years with other data streams efficiently. It is also able to store events and flows, keeping all information available for immediate queries, forensics, rules, validation, and compliance.
- Built for Big Data – Leverages large volumes of security data to provide long-term indicators of compromise and actionable threat intelligence.
- Simplify Compliance – Eliminates time-consuming manual processes with centralized and automated compliance monitoring and reporting. Integration with the Unified Compliance Framework (UCF) enables a "collect once, comply with many" methodology for meeting requirements and keeping audit efforts and expense to a minimum.
- Connecting IT Infrastructure – Active integrations with ePolicy Orchestrator (Intel Security ePO) for policy-based endpoint management, Intel Security Network Manager for intrusion prevention, and Intel Security Vulnerability Manager for vulnerability scanning and remediation.

Bottom Line

McAfee Enterprise Security Manager is a good option for enterprises that use other Intel Security technologies, as well as those looking for an integrated security framework that includes advanced threat defense or monitoring of industrial control systems.

Logentries

Logentries is a real-time log management and analytics service built for the cloud for securely collecting log data while preventing unencrypted sensitive data from leaving your environment. Their SIEM products include search and analysis tools, alerts to identify security threats and investigate malicious activity. With an open API, Logentries brings the value of log-level data to any system. Logentries provides an alternative designed for managing huge amounts of data, visualizing insights that matter, and automating in-depth analytics and reporting across its global user community.

Key Features

- Data Collection & Aggregation – Centralizes your log data, integrates will all your major platforms, and enables you to stream data from any source.
- User Identification & Monitoring – Tracks users by unique ID and associating key events to specific users, which is necessary for identifying the source of suspicious user behavior.
- Instant Alerting - Set notifications that alert internal teams in real-time, as well as zero-delay alerting for instant notification of suspicious behavior.
- Analysis & Data Visualizations – Logentries visualizes data from multiple sources, which can reveal previously undiscovered insights.
- Data Compliance – Filter and obfuscate sensitive information, searches and analyzes all log data in one place.
- Live Forensic Analysis & Incident Investigation – Leverage aggregated live-tail searches of all log data simultaneously. Custom tags make it easy to spot important events.
- Auditing & Reporting – Logentries allows you to automate unlimited S3 archiving for easy log retrieval and exporting of log files for on-demand reporting.

Bottom Line

Logentries is a good solution for companies that want aggregated logging across their infrastructure. Because it is easy to use, it can appeal to small businesses, as well as large and mid-sized enterprises. Logentries also offers a low-cost option that still provides a complete set of logging, auditing, and mentoring capabilities.

LogPoint

LogPoint's SIEM Solution extracts events and incidents from logs existing in IT infrastructures of any size. Filtered and correlated real-time results are displayed in dashboards that can be configured based on the specific roles and responsibilities of each user. Real-time, actionable insights from raw machine data help increase operational efficiency and streamline compliance for regulatory mandates to strengthen security posture. LogPoint gives IT teams insight into all incidents across the infrastructure.

Key Features

- Scalability – Centralized reporting, analysis, and management speed up the process to quickly locate the event source.
- Transparent Search and Analysis – Users are able to carry out analysis centrally or conduct searches across the entire enterprise.
- Big Data Storage – Allows enterprises to fully utilize any storage system, ensuring prioritization of the amount and use of critical storage systems (NAS) and any protocol or interconnection within the infrastructure.
- Platform Flexibility – LogPoint can be delivered in three different ways to suit a user's needs: appliance (combined software and hardware package); virtual (utilizes existing infrastructure and enables a platform for easier and faster scalability); self-contained software package (allows for flexibility in terms of deployment scenarios or existing hardware within the enterprise).
- Data and Information – LogPoint supports network and security devices, operations management suites, identity and access management solutions, and enterprise-wide deployments of ERP systems.
- Data Enrichment – Provides full data enrichment capabilities, allowing LogPoint to produce a message about a critical transaction in an ERP system, investigate if the user is authorized to conduct the operation in the HR system, and raise alerts if a discrepancy is discovered.
- Swift Processing – Processes data before storage, attaining real-time analysis of events.

Bottom Line

LogPoint offers SIEM solutions to smaller companies with limited budgets and operational capabilities, as well as large, complex multinational enterprises. While they mostly operate in Europe, they also have partnerships across the globe and continue to grow.

LogRhythm

LogRhythm combines SIEM, Log Management, File Integrity Monitoring and Machine Analytics with Host and Network Forensics in a unified Security Intelligence Platform. Its SIEM solutions are mostly accommodating for midsize to large enterprises. Their SIEM consists of several unified components: the Event Manager, Log Manager, Advanced Intelligence Engine (AI Engine), and Console. It combines SIEM capabilities with endpoint monitoring, forensics, and management abilities to ease with deployment.

Key Features

- A1 Engine – LogRhythm attains visibility by analyzing all available log and machine data with forensic visibility at the endpoint and network levels. This insight is then leveraged by A1 Engine, their Machine Analytics technology, to perform continuous, real-time analysis of all activity observed within the environment. A1 Engine also helps to identify previously undetected threats and risks.
- LogRhythm Labs™ – Delivers out-of-the-box functionality that expedites threat detection and response. This includes log parsing and normalization for 700+ operating systems, applications, databases, devices, etc. Additionally, provides Compliance Automation Modules for 14+ regulatory frameworks, as well as Threat Management Modules.
- Detects – LogRhythm detects custom malware tied to zero-day attacks and is created to evade traditional security solutions that are built to detect specific signatures and known malicious behavior
- SmartReponse™ – Automatically disable an account or queue up a response for validation pending a more detailed forensic activity into questionable activity.
- Network Monitor – LogRhythm's Network Monitor provides visibility at network ingress/egress points with SmartFlow™ data providing deep packet visibility into each network session observed and the application in use. This establishes behavioral baselines across observed network activities, leveraging the extensive packet metadata delivered.
- SmartCapture™ – LogRhythm's SmartCapture™ automatically captures all packets associated with suspicious sessions for full packet forensics.

Bottom Line

LogRhythm primarily sells caters to companies that require an integrated combination of endpoint monitoring, SIEM, and value ease of deployment and function abilities.

Logsign

Logsign is a company focused on next-gen SIEM (Security Information and Event Management) solutions. Based in İstanbul, Logsign offers a security driven logging solution that can integrate with hundreds of vendors over tens of protocols. As a vendor agnostic company, they supply vast support to new/custom logging formats. Logsign installations can scale from a single server installation to tens of servers both vertically and horizontally in an almost linear fashion.

Key Features

- Compliance – Logsign helps to automate compliance needs and maintain a good-enough security posture to adapt to regulations such as PCI, HIPAA, ISO, FISMA, SOX, NERC, GLBA. Logsign fulfills compliance needs through Log Management and Security Information Management.
- Comprehensive Data Collection– Logsign collects terabytes of logs and events in real time from hundreds of physical, virtual and cloud data sources via enterprise wide log collection techniques. Normalization of logs and events provide a clear understanding and makes it easy to understand and work on.
- Scalability – Logsign installations can scale from a single server installation to tens of servers both vertically and horizontally in an almost linear fashion.
- Real-Time Monitoring– Logsign provides fast and clear identification with its high performing search capability. HDFS and NoSQL architecture enables faster search and indexing than traditional solutions with responses in seconds revealing reliable and accurate results.
- Threat Intelligence – Logsign's Threat Check Service offers integrated threat intelligence feeds that improve threat detection and empower cybersecurity defenses.

Bottom Line

Whether you be an end user or a security partner, Logsign's mission statement, "your teammate in Security," rings true. The company's SIEM platform offers scalable and easy-to-use security intelligence, log management, and compliance reporting for companies of all sizes. The freemium community edition is an good way to test the solution before investing.

ManageEngine

ManageEngine simplifies IT management with affordable software that offers the ease of use SMBs need and the powerful features the largest enterprises demand. ManageEngine® EventLog Analyzer is a web-based, agent-less syslog and windows event log management solution for security information management that collects, analyses, archives, and reports on event logs from distributed Windows host and, syslogs from UNIX hosts, Routers & Switches, and other syslog devices.

Key Features

- EventLog Analyzer – Aggregates logs from heterogeneous sources (Windows, Unix/Linux, Applications, Databases, Routers, Switches, and other Syslog devices) at a central place. EventLog Analyzer, using its Universal Log Parsing and Indexing (ULPI) technology, allows users to decipher any log data, regardless of source and log format.
- Log Forensics – EventLog Analyzer allows users to use log search functionality to search on both raw and formatted logs and instantly generate forensic reports based on the search results.
- File Integrity Monitoring – EventLog Analyzer facilitates real-time file integrity monitoring (FIM) by protecting sensitive data and meeting compliance requirements. With EventLog Analyzer's file integrity monitoring capability, security professionals can now centrally track all changes happening to files and folders when created, accessed, viewed, deleted, modified, renamed, etc.
- Log Analysis and Dashboards – EventLog Analyzer performs log analysis in real-time and displays the analyzed log data into easy to understand charts, graphs, and reports. Users can easily drill down through log data shown on the dashboard to get more insights and do a root cause analysis within minutes.
- User Monitoring – Provides reports for user monitoring by EventLog Analyzer, thereby enabling the tracking of suspicious behavior of users including privileged administrative users (PUMA).

Bottom Line

ManageEngine is a cost effective solution that is a good option for small and mid-sized businesses and enterprises. They also have a pay-as-you-go pricing model coupled with the ability to scale services up or down as needed, which offers flexibility to customers.

NetIQ (Micro Focus)

Micro Focus's Sentinel simplifies the deployment, management, and day-to-day use of SIEM. It adapts to dynamic enterprise environments and delivers the "actionable intelligence" security to help users understand their threat posture and prioritize responses. NetIQ integrates identity information with security monitoring to detect and respond to abnormal activity that signals a data breach or compliance gap. Their solutions provide visibility and control over user activities, security events, and critical systems to help quickly address evolving threats.

Key Features

- Virtual Appliance Packaging –Sentinel's virtual appliance packaging allows for fast, easy, and cost-effective deployment. As opposed to hardware based options, you can quickly ramp deployment handle growth and additional capacity as security needs change. Sentinel employs a searching and event forwarding mechanism to allow the deployment architecture to adapt to your environment.
- Anomaly Detection –Sentinel's anomaly detection enables you to automate identification and anomalous activity without needing to know exactly what you are looking for. Sentinel also allows you to automatically identify inconsistencies in your organization's environment without having to build correlation rules. Baselines for your organization's environment are established to deliver better intelligence and faster detection. Comparing trends enables you to develop models of typical IT activities to easily spot potentially harmful trends.
- Visibility into User Activities –Sentinel simplifies the process of collecting, monitoring, and analyzing system log data to speed up the discovery of data security threats to enable immediate remediation measures. Greater visibility and understanding of potential threats; responds and mitigates threats quickly; understands how users make use of access privileges. Implementing the industry's only seamless integration with identity management ties users to specific activities across the enterprise.

Bottom Line

Sentinel is well-suited to enterprises that are looking for large-scale security event processing. Its strengths will adequately assist those organizations that have deployed NetIQ IAM infrastructure, and need network monitoring with an identity context.

RSA Security (Dell Technologies)

The RSA NetWitness suite provides visibility from logs, full network packet, NetFlow, and endpoint data capture. The NetWitness Logs facilitates the automated collection, analysis, alerting, auditing, reporting, and secure storage of all logs. Organizations can simplify compliance by using regulation-specific, out-of-the-box reports, alerts, and correlations rules. Reports can be scheduled to be delivered at a specific time or run on an ad-hoc basis. Alerts can be delivered through the intuitive user interface, via SMS, or email, and auditors can even be granted read-only access to the enVision platform so that they can access the reports whenever they need them.

Key Features

- RSA Live – Provides automatic content updates, including correlation rules, reports, and threat intelligence feeds.
- Visibility – Allows you to spot advanced attacks with complete visibility across logs, networks, endpoints, and cloud data. Users can inspect networks, packet sections, and log events for threat indicators at the time of collection with capture time data enrichment, along with the ability to augment visibility with additional compliance and business context.
- Analysis – RSA allows you to detect and analyze attacks in real time, to discover attacks missed by signature-based tools to correlate network packets, and to find incidents immediately with out-of-the-box reporting, intelligence, and rules. Capture Time Data Enrichment amplifies the value of your data by generating metadata fields that can be used for both detection and investigation.
- Action – RSA allows users to prioritize actions and enable incident responses in order to increase workflow productivity. Users can separate the most critical threats from those of less importance, which makes for easier compliance to proactively defend your network and assets.

Bottom Line

RSA is best-suited for security-conscious companies that need log-based and network-level monitoring for threat detection and investigation, and have an incident response team (or SOC), or a related provider for configuring and tuning a complex technology.

SolarWinds

SolarWinds' all-in-one SIEM combines log management, correlation, reporting, file integrity monitoring, and active response in a virtual appliance. Its LEM (Log & Event Manager) deploys with ease and uses SIEM for smaller security teams that do not require big data analytics or malware detection integration. This relieves them of the complexity and cost of other solutions. SolarWinds allows companies to monitor network performance, optimize applications and systems, accelerate database performance, and enhance security and compliance.

Key Features

- Easy Compliance Reporting – Automates key compliance reports for HIPAA, SOX, NCUA, STIG, GLBA, PCI, NERC, etc. SolarWinds' Log & Event Manager collects and catalogs log and event data in real-time from wherever data is generated within your IT infrastructure.
- Log Compression and Retention – Log & Event Manager stores terabytes of log data at a high compression rate for compliance reporting, compiling, and off-loading to reduce external storage requirements.
- Built-In Active Responses – SolarWinds' Log & Event Manager enables you to immediately respond to security, operational, and policy-driven events using built-in active responses that take actions such as quarantining infected machines, blocking IP addresses, killing processes, and adjusting Active Directory® settings.
- USB Defender – The Log & Event Manager eliminates endpoint data loss and protects sensitive data with real-time notification of USB devices, the ability to automatically block their usage, and built-in reporting to audit USB usage.
- Out-of-the-Box Security and Compliance Reporting Templates – Log & Event Manager makes it easy to generate and schedule compliance reports using 300+ audit-proven templates and a console that lets you customize reports to your organization's specific compliance needs.

Bottom Line

SolarWinds is best suited for small to midsize organizations looking for easy deployment capabilities, and especially those who use other SolarWinds monitoring components.

Splunk

Splunk provides pre-packaged dashboards, reports, incident response workflows, analytics, and correlations to identify, investigate, and respond to internal and external threats. It employs a query language that supports visualization with more than 100 statistical commands. Splunk also provides out-of-the-box support for the most common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence to accelerate deployment and adoption.

Key Features

- Reports and Security Metrics – Splunk offers the ability to leverage dozens of out-of-the-box reports, dashboards, and metrics. Any search result can be created as a graphic, dashboard or table to turn raw unstructured data into analytics, and export raw data as a PDF or CSV.
- Incident Review and Classification – For governance, auditing, and protection against tampering, the Splunk App for Enterprise for Security provides reports on all users and system activities for a complete audit trail. This allows for bulk event reassignment, changes in status and criticality classification, with all analyst activity available for auditing purposes.
- Security Analytics, Correlation, and Response – Optimizes security monitoring, prioritization, response, containment, and remediation processes by analyzing machine data to understand the impact of alerts or incidents.
- Threat-Intelligence Sources – Includes free threat-intelligence feeds, third-party subscriptions, law enforcement, FS-ISAC Soltra (via STIX/TAXII), internal and shared data.
- Threat-Intelligence Framework – This framework supports multiple sources of threat feeds, including open-source feeds in the form of flat files via an API service; a subscription-based feed in the form of TCP streaming; feeds from law enforcement or local environment in the form of manual download; and shared threat feeds in the form of STIX or OpenIOC document via TAXII protocol.

Bottom Line

After recent acquisition of Caspita, Splunk is adding machine learning-based user behavioral analytics to better detect threats. Companies looking for a customizable SIEM platform in order to support analytics functions and log formats would largely benefit from Splunk, particularly those with cases that span security and IT support.

Sumo Logic

Sumo Logic enables enterprises to build analytical power that transforms daily operations into intelligent business decisions. They offer customers cloud-to-cloud integrations to simplify setup, and deliver business operational insights.

Sumo Logic's purpose-built Cloud-native service scales to over 4 Petabytes of data, and delivers data-driven insight.

Key Features

- Collect and Centralize – Sumo Logic collects terabytes of data from any app, cloud, device, custom hardware, sensor, server, and network sources. Centralized logging eliminates the need for additional archiving, backups, and restores. Data can be pre-parsed and partitioned immediately.
- Search and Analyze – Administrators can run searches and correlate events in real time across the entire application stack using an easy-to-use search-engine-like syntax. The patent-pending LogReduce™ technology reduces log events into groups of patterns. By filtering out this noise, LogReduce can help reduce the MeanTime to identification of issues by 50% or more. Transaction Analytics capability automates processes for collection and analysis of transactional context to decrease time associated with compiling and applying intelligence across distributed systems.
- Detect and Predict – Sumo Logic's Anomaly Detection technology is powered by machine-learning algorithms and detects deviations to uncover unknowns in data. Outlier Detection is powered by a unique algorithm, analyzes data streams with a single query, and determines baselines and outliers in real-time. The Predictive Analytics capability extends and complements Anomaly and Outlier Detection by predicting future KPI violations and abnormal behaviors through a linear projection model.
- Alert and Notify – Custom alerts proactively notifies you when specific events and outliers are identified across your data streams. The patent-pending Push Analytics™ technology leverages LogReduce to establish a baseline of application, system, and infrastructure activity. Proactive notifications are generated when your data deviates from calculated baselines or exceed thresholds to help address potential issues properly.

Bottom Line

Sumo Logic offers a pay-as-you-go solution, which works well with small to medium-sized organizations. It can be deployed instantly, scales easily, and requires very minimal maintenance.

Tenable Network Security

Tenable's SIEM leverages the log management capabilities of the Log Correlation Engine (LCE) to collect all logs, software activity, user events, and network traffic. IT analyzes data for correlated events and impact on security and compliance posture. Event context and threat-list intelligence about any system is provided by Tenable Nessus vulnerability and configuration scans and real-time monitoring with the Tenable Passive Vulnerability Scanner (PVS).

Key Features

- Event Correlation – Multiple forms of event correlation available for all events, including statistical anomalies, associating IDS event with vulnerabilities, and alerting on 'first time seen' events.
- Log Normalization – Normalize, correlate, and analyze user and network activity from log data generated by any device or application across your enterprise in a central portal.
- User Monitoring – Tenable monitors user activity, and associates events such as NetFlow, IDS detection, firewall log activity, file access, system error, or login failure with specific users for easy reporting and insider threat detection.
- Full Log Indexing & Search – All logs are compressed and stored, and by using full-text search, you can search logs for keywords, user names, IP addresses, etc. Log searches are stored with an independent checksum and can be re-launched at any time.
- NetFlow Analysis – In each instance of the Tenable LCE, there are agents for many different platform technologies that can collect NetFlow traffic logs from routers, switches, and other network devices.
- Network Content Analysis – Tenable is able to analyze network traffic in real-time with Tenable PVS, and can produce an accurate vulnerability report and real-time forensic log of network events such as shared files, DNS lookups, and social network activity.

Bottom Line

Tenable is a good option for organizations of all size, from small businesses to large enterprises. For the most part, it is used by large enterprises, companies, and organizations.

Trustwave

Trustwave Managed SIEM services provide threat intelligence, efficiency, and automation to organizations. Their service includes the Payment Card Industry Data Security Standard (PCI DSS).

Trustwave works with point-of-sale (POS) vendors to develop specific logging support for in-store payment solutions. Their appliances offer capabilities for additional correlation, reporting, and ad-hoc analysis, both locally on the appliance and via services provided through Security Operations Centers.

Key Features

- TrustKeeper Platform – Trustwave Managed Security Services are available through the Trustwave TrustKeeper cloud and managed security services platform. Businesses can access a variety of subscription-based Trustwave offerings, ranging from enterprise-grade managed security services to compliance and automation tools for small- and medium-sized businesses.
- Integrated Threat Intelligence: Spiderlabs, Trustwave's advanced threat research team, increases your business' uptime by preventing infections and keeping malware out.
- Compliance – Trustwave offers support for regulations and industry standards, including PCI, FFIEC/GLBA, SOX, HIPAA, etc.
- Threat Correlation – Includes 19 SIEM correlations which leverage Open Source, Crowd Source, and Enterprise Source intelligence.
- Portal User Interface – A configuration and management web-based portal. Users can test the service, review statistics on synchronized and updated threat intelligence through dashboards, and manage configuration of the service using the Trustwave Cloud.
- Forensics – Employs Boolean logic, enabling consumers to search for in-depth data, and save, share, and reuse searches, filters, lists, and reports.

Bottom Line

Trustwave would be a good choice for midsize organizations seeking SIEM that will offer a variety of technologies and service options to meet compliance and threat management requirements.

About Solutions Review

Solutions Review is a collection of technology news sites that aggregates, curates and creates the best content within leading technology categories. Solutions Review mission is connect buyers of enterprise technology with the best solution sellers.

Over the past three years, Solutions Review has launched ten tech Buyer's Guide sites in categories ranging from Cybersecurity to Wireless 802.11ac as well as Mobility Management and Business Intelligence, Data Analytics, Data Integration and Cloud Platforms.

Information for this report was gathered via a meta-analysis of available online materials and reports, conversations with vendor representatives, and examinations of product demonstrations and free trials. Solutions Review does not endorse any vendor, product or service depicted in this publication and does not advise technology users to base their vendor selection entirely on this research. Solutions Review disclaims all warranties, expressed or implied, regarding this research, including any warranties of merchantability or fitness for a particular purpose.