McAfee
Together is power.

SIEM Solutions from McAfee

Monitor. Prioritize. Investigate. Respond.

Today's security information and event management (SIEM) solutions need to be able to identify and defend against attacks within an ever-increasing volume of events, sophistication of threats, and infrastructure. These attacks come from a constantly evolving threat landscape, hiding behind normal enterprise activity. You need a SIEM that can quickly detect emerging threats so that you can investigate and respond faster and with fewer resources. SIEM solutions from McAfee provide an intuitive interface, actionable intelligence, and the factory-built integrations required for you to prioritize, investigate, and respond to threats efficiently and effectively. While complementing the urgency of threats, we also enable the operational and compliance tasks: the embedded compliance framework and ready-to-go content packs speed time-to-value for key use cases and simplify security operations.

SIEM Foundation

McAfee® SIEM solutions bring event, threat, and risk data together with an optimized user experience, leveraging the latest technology, open source, and McAfee and partner innovations to provide the strong security insights, rapid incident response, seamless log management, and compliance reporting required for optimized security operations. The analyst-centric user experience offers increased flexibility, ease of customization, and faster response to investigations. Streamlined workflows allow for more timely and effective incident management. With fast and smart access to threat information, every level of analyst will find it easier to prioritize, investigate, and respond to evolving threats.

McAfee Enterprise Security Manager

As the foundation of the McAfee SIEM solution portfolio, McAfee Enterprise Security Manager expedites data handling and security operations to help analysts prioritize, investigate, and respond more effectively in less time, despite increasing threat volumes and operational pressures. The extensible McAfee Enterprise

Connect With Us

Security Manager solution can process big security data at the speed and scale required to identify, triage, and intervene against threats, while the embedded compliance framework simplifies audits and governance. This balanced system optimizes your security operations efforts through continuous visibility into changing risk, actionable analysis to speed investigations, and orchestration of security remediation.

McAfee Enterprise Security Manager offers a distributed design that integrates with dozens of partners, hundreds of standardized data sources, and industry threat intelligence. The solution delivers the scale and intelligence needed to support your organization's current and evolving security and compliance goals. Hybrid delivery choices give you the flexibility to choose physical and virtual appliances, as well as managed security services provider (MSSP) offerings. Flexible and extended horizontal storage allows organizations to rapidly query billions of events. Storage is more resilient, as data can be replicated to multiple locations immediately, improving business continuity. McAfee Enterprise Security Manager integrates security intelligence with enterprise-wide information management, including a real-time view of the systems, data, risks, and activities inside your enterprise, delivering critical threat and compliance insights to optimize security operations.

McAfee Log Management Solutions

McAfee log management solutions provide you with the increased flexibility you need to align your log management needs with your business needs. The open and scalable data bus shares huge volumes of events and allows threat hunters to simultaneously conduct rapid searches of recent events while efficiently retaining data long term for compliance and forensics.

- McAfee Enterprise Log Search is optimized for fast investigations, leveraging Elasticsearch to perform high-speed searching across raw data. Near real-time retrieval of insights from high volumes of events, logs, flows, and threat intelligence provide timely and prioritized threat detection and investigation value from your data.
- McAfee Enterprise Log Manager is optimized for data retention. It efficiently collects, compresses, hashes, and stores all original events, supporting chain-of-custody and non-repudiation efforts. Security events are collected and linked directly to the original record stored on McAfee Enterprise Log Manager, enabling one-click access for event management, forensic investigations, and compliance monitoring. McAfee Enterprise Log Manager accommodates different log management needs via flexible storage pools spanning local or remote storage devices and configurable retention periods.

McAfee Event Receiver for scalable event collection

To enable a single view across IT devices, McAfee Event Receiver appliances collect security event and network flow data from hundreds of third-party sources. Data sources can include firewalls, VPNs, switches, routers, IPS, applications, identity and authentication systems, servers, NetFlow, sFlow, and much more. Appliances scale to tens of thousands of events per second, providing dedicated, reliable collection for distributed sources. Event and flow data from different vendor products are correlated into a normalized event taxonomy to make it possible to detect larger incidents. All data collected is cached locally to preserve data in the event of network communication error or outage.

McAfee Advanced Correlation Engine for rule-based and rule-less correlation and threat detection

McAfee Advanced Correlation Engine provides dedicated correlation horsepower that enables rapid threat detection. Just tell the McAfee Advanced Correlation Engine what's important to you—users or groups, applications, specific servers or subnets, virtually anything—and the McAfee Advanced Correlation Engine will start scoring threat activity against it. As the score grows, yellow, orange, or red alerts can be generated to notify you of increasing threats against those key systems and services. It also produces complete audit trails—supporting internal security plan reviews and compliance reporting.

For Deeper Insights

McAfee Application Data Monitor for monitoring the application layer

Helping you understand exactly how your valuable networked applications are being used, McAfee Application Data Monitor delivers full visibility into the application layer, examining the underlying protocols and analyzing the full application session. This fully integrated appliance decodes the entire application session—going beyond flow monitoring all the way to Layer 7 to detect advanced application-layer threats. It also tracks all use of sensitive data on the network—supporting your compliance efforts with monitoring, logging, and auditing of access with all details of an application session.

McAfee Database Event Monitor for detailed security logging of databases and applications

McAfee Database Event Monitor provides a complete audit trail of all database activities, including queries, results, authentication activity, and privilege escalations. Predefined rules and reports, along with privacy-friendly logging features, make it easy to comply with regulations while strengthening your overall security profile. After McAfee Database Event Monitor for SIEM discovers sensitive databases and consolidates database activity into a central audit repository, it provides this information for normalization, correlation, and real-time analysis to enable improved security operations and compliance auditing.

Integrate and Extend

McAfee Global Threat Intelligence for enhancing situational awareness with threat intelligence data

Enabling rapid discovery of events involving communications with suspicious or malicious IP addresses, McAfee Global Threat Intelligence (McAfee GTI) for McAfee Enterprise Security Manager delivers a constantly updated, rich threat feed. Your organization can harness the power of McAfee GTI to quickly identify attack paths and past interactions with known bad actors and increase threat detection accuracy while reducing response time.

Connecting Your IT Infrastructure

Integration across your security infrastructure delivers an unprecedented level of real-time visibility into your organization's security posture. McAfee Enterprise Security Manager can collect valuable data from hundreds of third-party security vendor devices, as well as threat intelligence feeds. Integration with McAfee GTI brings in data from more than 100 million McAfee Labs global sensors, offering a constantly updated feed of known malicious IP addresses. Furthermore, McAfee Enterprise Security Manager can ingest threat information reported via Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) and/or third-party web URLs and take action based on analysis.

McAfee Enterprise Security Manager also offers active integrations with other McAfee solutions and McAfee Security Innovation Alliance partner solutions. For example, McAfee Threat Intelligence Exchange, based on endpoint monitoring, aggregates low-prevalence attacks, leveraging global, third-party, and local threat intelligence. McAfee Threat Intelligence Exchange can also utilize other integrated products, such as McAfee Advanced Threat Defense, to further analyze and convict files. Incident response teams and administrators can use McAfee Active Response to hunt for malicious zero-day files that lay dormant on systems, as well as active processes in memory. McAfee Active Response also uses persistent collectors to continuously monitor your endpoints for specific indicators of compromise (IoCs), automatically alerting you if an IoC appears somewhere in your environment. Unlike standard security approaches, this combination provides organizations with detailed, closed-loop workflow—from discovery to containment and remediation.

Analysts also benefit from integration with McAfee Behavioral Analytics, a dedicated user and entity behavior analytics solution that distills billions of security events down to hundreds of anomalies to produce a handful of prioritized threat leads and allows analysts to discover unusual and high-risk security threats, often unidentifiable by other solutions. Similarly, McAfee Enterprise Security Manager integrates with McAfee Investigator, to help transform analysts into expert

investigators and allow them to close more cases faster with higher confidence that they've determined root cause.

McAfee delivers an integrated security system that empowers you to prevent and respond to emerging threats. We help you resolve more threats faster and with fewer resources. Our connected architecture and centralized management reduce complexity and improve operational efficiency across your entire security infrastructure. McAfee is committed to being your number one security partner, providing a complete set of integrated security capabilities.

Scalable Deployment Options

SIEM solutions from McAfee can be deployed all in one or distributed over multiple appliances, providing flexibility and scalability for your current or future needs. Hybrid delivery choices include physical and virtual appliances with high-availability options. McAfee Professional Services is available to help meet your organization's deployment objectives, accelerate time to protection, and enhance your security technology investment.

Learn More

For more information on SIEM solutions from McAfee, visit **www.mcafee.com/siem**.

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com