FOCUS ON FIVE

SIEM REQUIREMENTS
1 BIG SECURITY DATA
2 CONTENT AND USER AWARENESS
3 DYNAMIC CONTEXT
4 SOLUTION CUSTOMIZATION
5 BUSINESS VALUE
SIEM: Solve for the Bigger Business Issues

After more than a decade functioning in production environments, security information and event management (SIEM) solutions are now considered mature. Capabilities such as event collection, correlation, alerting, and demonstrating compliance with regulatory mandates are table stakes, and most SIEM solutions address these needs. But the landscape is changing. Organizations face new threats such as targeted and persistent attacks, new trends like mobile, cloud, and virtualization, and shifting business priorities around customer acquisition, operational efficiencies and cost savings. As a result, SIEM use cases require more advanced capabilities to solve bigger business issues.

McAfee talked to customers and asked them to tell us about their primary issues with SIEM. Here are the top five issues as explained to us:

- Big Security Data
- Content and User Awareness
- Dynamic Context
- Solution Customization
- Business Value

In order for SIEM to help usher in more effective security and risk management strategies—particularly as they relate to threat mitigation, embracing trends, and aligning with business priorities—these five issues must be solved. Each issue is described here along with corresponding customer case studies and use cases.
Big Security Data can be extremely valuable—if you’re able to use it. Legacy SIEM solutions weren’t designed to integrate with such a broad number of endpoint, network, and data sources, nor intended to process such high event rates or maintain such long retention policies. As a result, relational databases and similar SIEM shortcomings designed primarily with network-centric events in mind simply don’t work in today’s environments. They lack the speed, extensibility, and scalability to be effective and usable.
USE CASES

Expanding event feeds from more relevant sources
Building larger datasets in which to perform analytics
Continuing to reduce resources needed for reporting
Increasing employee and process efficiencies

CASE STUDY

Federal Government

A large government agency was interested in applying advanced analytics to the Big Security Data stored within its SIEM’s multi-petabyte, relational database. But even simple reports took hours to render and some took more than a day, making the agency’s SIEM unusable for forensics.

By switching to a SIEM solution from McAfee, the agency was able to expand the number and types of integrated devices—adding more data- and user-centric context to its analytics. The agency also increased event rates and stored data. Now, reports render in minutes, improving the entire approach to forensic analysis.
There was once a time when SIEM was simply a tool to correlate events across firewalls and intrusion detection systems, and then maybe apply some vulnerability assessment data. Even today, there are some SIEMs that rely primarily on network flow data. While all of these sources are important, they need to be enriched with application, data content, and identity information. Without that, it’s virtually impossible to understand events with enough empirical evidence to be actionable.
A regional healthcare provider embraced the idea of “bring your own device” (BYOD) to increase staff agility by supporting personal tablets. Because of past incidents, the provider was concerned about insider abuse. The existing SIEM solution lacked the ability to understand which users were interacting with sensitive data regardless of the device—laptop, desktop, tablet, or virtual desktop. With the McAfee® SIEM solution, the healthcare provider connected with identity and mobility management, active directory, and LDAP products to gain user and device awareness. Because of integration with structured and unstructured data stores such as native database support, as well as integration with data loss prevention (DLP) and database active monitoring (DAM), there was more complete situational awareness and improved insider threat mitigation.
One of the earliest SIEM use cases was log management—collect, store, and query with a few extra bells and whistles. Logs are still a foundational component of SIEM, but today’s SIEMs also need dynamic context.

Examples of dynamic context are McAfee Global Threat Intelligence™ (McAfee GTI™) and McAfee Risk Advisor. McAfee GTI provides a real-time, cloud-based reputation service and Risk Advisor collects organizational information about attacks, vulnerabilities, and deployed countermeasures.
USE CASES

**Understanding** threats inside and outside the environment

**Improving** SIEM capabilities with dynamic context

**Reducing** incident identification time and response times

**Prioritizing** future security investments by understanding countermeasures juxtaposed with SIEM information on targets and attacks

CASE STUDY

**Retailer**

A Fortune 100 retailer without a production SIEM and no McAfee solutions conducted a proof of concept. Within the first week, the retailer identified that over 30 percent of the traffic attempting to enter its network was from malicious sources and/or contained malicious payloads.

Utilizing SIEM to correlate existing event information with McAfee GTI, the retailer quickly identified which assets were being targeted across all their store locations and data centers, as well as understanding the types of attacks. By consuming McAfee Risk Advisor countermeasure information, the SIEM determined the highest level of severity and then prioritized a response. SIEM paired with dynamic context allowed for more rapid threat acquisition, prioritization, and remediation.
Legacy SIEMs have very rigid architectures and lack a few essential capabilities. For example, they don’t easily integrate with previously unsupported devices to make information usable. But a next-generation SIEM, on the other hand, is like soft clay—there are many ways to mold it to fit any given environment. This is exactly what makes a next-generation SIEM strategic for so many organizations.
USE CASES

Deploying SIEM with dynamic whitelisting and hardware-assisted security to protect fixed-function devices

Centralizing the enforcement of policies across all three zones

Integrating SIEM with firewall and IPS for rapid incident response

Gaining more life from legacy assets because of improved security

CASE STUDY

Utility

A major utility company needed to employ security controls to address Stuxnet-like attacks from impacting the infrastructure and causing blackouts for millions of customers. With a McAfee SIEM, the utility achieved situational awareness across corporate IT, SCADA, and industrial control system (ICS) zones with native device, application, and protocol support.

The McAfee SIEM provided the customer with the tools to do their own custom integration with the SCADA and ICS devices. That in turn allowed correlation, anomaly detection, and trend analysis across all three zones. Beyond customized event collection, the customer quickly and easily built unique dashboards, reports, correlation rules, and alerts. This made the SIEM an invaluable tool for security, demonstrating compliance with regulatory mandates and availability—in other words, keeping the lights on.
SIEM is an important component of any strategic security initiative, but it’s still just one of many. In fact, the sheer number of security and compliance solutions has created added cost and their non-integrated architecture has created complexity. Exactly why security has remained largely tactical instead of becoming more strategic and aligned with business priorities.
USE CASES

Reducing security-related helpdesk tickets
Monitoring all headquarter and branch locations with fewer FTEs
Redeploying FTEs, formerly focused on monitoring, more strategically
Leveraging integrated security to help streamline business initiatives such as business merger integration, cost reduction through datacenter consolidation, and customer acquisition, retention through mobile solution support

CASE STUDY

Financial Services

A multinational banking customer owned a wealth of disparate products from various vendors. Some products were in production, but many were not regularly used or maintained because of limited resources. The bank determined that by leveraging SIEM in conjunction with integrated endpoint, network, and data controls it could more effectively mitigate risk and reduce costs while also making security more business-relevant.

The bank reduced the number of vendors and gained economies of scale—reducing training costs, reducing agents, consoles, servers, and more. This also lowered contract costs and a multitude of associated expenses. Beyond cost savings, the bank ensured that all existing and future solutions were fully integrated with McAfee SIEM to ensure better controls and visibility to its security posture.
What worked in the previous decade with legacy SIEMs simply doesn’t address today’s requirements. From Big Security Data, content and user awareness, and dynamic context, to solution customization, and business value, SIEM use cases have matured. Organizations should demand more from their SIEM solutions. SIEMs should be fast and easy to use. They should reduce complexity, not create it.

Today’s SIEMs need to operate as part of a larger, connected security framework where security and business priorities are aligned. SIEM plays an important role in making security more strategic and providing real business value. As security professionals continue to be more essential in broader business deliberations, SIEM will act as one of their trusted solutions for making timely, relevant decisions.

**TAKE ACTION**

- How much are existing SIEM or manual information management process delays costing your security team?
- Who are the stakeholders of security visibility in your organization? Are they getting the data they need when they need it?
- Does your organization have the visibility it needs to identify attacks, internally and externally?
- What are the top three time delays that increase time-to-respond?
- What are the primary barriers to the collection, storage, and analysis of the security data we need?
Security Connected

McAfee SIEM is part of the Security Connected framework from McAfee that enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.
Focus on Five

1. Big Security Data
2. Content and User Awareness
3. Dynamic Context
4. Solution Customization
5. Business Value