Case Study

The Standard for a Vastly Improved Security Posture

McAfee SIEM reduces administrative, analytic, and compliance time.

McAfee, Inc.

Profile
World's leading dedicated security vendor.

Industry
High technology.

IT environment
More than 14,000 endpoints and network devices spread across 60 countries.

Challenges
Provide the highest level of visibility and situational awareness to protect critical information and infrastructure, achieve PCI compliance, and leverage virtual machines in the McAfee security infrastructure.

Solutions
- McAfee First Program.
- McAfee Enterprise Security Manager.
- McAfee Enterprise Log Manager.
- McAfee Application Data Monitor.
- Integrated with McAfee® ePolicy Orchestrator® (McAfee ePO™) software, McAfee Network Security Platform, McAfee Vulnerability Manager, McAfee Firewall Enterprise, McAfee Email Gateway, McAfee Web Gateway.

McAfee, now a part of Intel® Security, provides system, network, and mobile security solutions that allow users to safely connect to the Internet, browse, and shop online. Backed by global threat intelligence, the company's innovative products empower home users and organizations by enabling them to prove compliance, protect data, prevent network disruptions, identify vulnerabilities, and monitor and improve their security. The company has approximately 8,000 employees and a network containing 14,000 endpoint and network devices spanning the US and 60 other countries.

Security Event Management and an Effective Security Operations Center

Several years ago, McAfee implemented a security information and event management (SIEM) solution to more efficiently analyze data from its various security solutions and to help the company be as proactive as possible at identifying and remediating threats. However, as the McAfee® security infrastructure matured and the number of security devices being monitored significantly increased, its SIEM appliances could not handle the exponential increase in data volume. Today, the McAfee Security Operations Center (SOC) records an average of 7.9 billion security events per month.

"As we started pumping more and more data into the SIEM, we found it almost impossible to get the data back out," explains McAfee SOC Manager, Robert Morris. "It could take up to a week to analyze an event. SIEM plays a critical role in the SOC, so having to wait that long simply wasn't acceptable. In addition, our SIEM queries would open a floodgate of data that would completely choke network bandwidth."

Superior SIEM Architecture Provides Multiple Benefits

After complaining to its SIEM vendor and being told that a $500,000 investment was required to make the existing solution meet requirements, the company began researching other options. After narrowing the field to four different vendors and thoroughly evaluating each of their solutions, McAfee chose NitroSecurity to replace their previous SIEM solution. McAfee was so pleased with the performance of the product that it bought NitroSecurity and renamed the solution McAfee SIEM.

"The architecture of the SIEM solution clearly stood out above the other vendors," notes McAfee Director of Security Engineering, Tony Gunn. "It was designed from the ground up to handle billions of events each month—50,000 each second—and to enable incredibly fast data query, retrieval, and analysis. We knew that it would be—and it was—many times easier to deploy and use than our previous solution. And, unlike the previous solution, we could use virtual machines where needed without having to manage them manually. Thanks to our McAfee First program, which positions McAfee as our first and most demanding customer, we rolled out McAfee SIEM in a controlled manner to help determine best practices."

intel Security

Results

- Significantly shortens time to analyze security events from four to six days to less than 10 minutes.
- Decreases time to produce PCI compliance reports from eight to 12 hours to 10 minutes.
- Saves administrative time and manual maintenance while eliminating unnecessary activities.
- Facilitates disaster recovery and allows for proper use of virtual machines.
- Improves the organization's overall security posture in the industry.

McAfee deployed three McAfee Enterprise Security Manager SIEM appliances and three McAfee Enterprise Log Manager SIEM appliances. Two of each at its SOC in the US and the others in a disaster recovery location on another continent, and 16 Event Receivers systems, 14 as appliances and two as virtual machines. The SIEM solutions were integrated with McAfee ePO software, McAfee Network Security Platform, McAfee Vulnerability Manager, McAfee Firewall Enterprise, McAfee Web Gateway, and McAfee Email Gateway solutions, as well as several non-McAfee solutions.

"Once the SIEM systems were physically hooked into our network, the team literally just plugged them into the McAfee Enterprise Security Manager, created a couple of dashboards for daily use, and modified maybe five policy rules," recalls Morris. "Implementation was substantially easier than with our previous SIEM solution."

Accelerating Event Analysis and Minimizing Response Time

"Before implementing the McAfee SIEM solutions, it used to take us four to six days to extract security event data for analysis," adds Gunn. "Now it takes three minutes, 10 minutes at most," he explains. "That's an extremely significant time savings. To be able to perform meaningful historical analysis, you need to have easy access to as much forensic data as possible, from all relevant data sources. And to react quickly and efficiently to a security incident, you need to have that information as fast as possible. The McAfee SIEM solution allows us to do both."

The SIEM system that McAfee has implemented is rated to handle 50,000 security events per second. It also automatically and very efficiently normalizes incoming data, taking event information from the various devices and different vendors' solutions and classifying all of it using common terminology— "virus," "buffer overflow," "web exploit," "email exploit," "potential vulnerability," and so on— and four levels of detail, so that any McAfee IT administrator can see instantly from the solution's dashboard what types of events are occurring, and drill down for more detail as needed. The McAfee SIEM system also assigns a level of severity to events more efficiently than the previous SIEM solution. "In short, not only do we retrieve the data much faster, we can use it much more efficiently once we have it," says Gunn. "We can look at all the data at a high level and then hone in on the specifics as needed from the dashboard. This information enables us to more rapidly assess our risk profile and security posture, as well as analyze and institute a range of corrective actions, such as issuing new configurations, implementing new policies, and deploying more recent software updates."

Slashing Administrative Efforts and Dramatically Improving Network Bandwidth

"From an administrative point of view, we save time every day simply by having one central place to manage and update all the SIEM receivers," explains Morris. "One person can now deploy a new patch across eight receivers worldwide in 15 minutes, leaving them the time to focus on other security tasks, whereas before, that person's entire work day would have been consumed."

As mentioned earlier, built-in normalization also aids in event analysis. "Previously, we had to manually create a lot of rules and dig through event data, worrying that we might not have parsed it out properly," states Morris. "The McAfee SIEM system's extremely effective normalization of data as well as some of its built-in tools eliminates previously manual activities. For example, we can populate watch lists and filters to tell the system to expect certain types of traffic from specific networks."

Not having to deal with overloaded network bandwidth is another time-saver. "Prior to implementing the McAfee SIEM system, every piece of uncompressed, raw security event data went into a single repository, and that flow of data literally flooded our network at times," declares Morris. Instead of moving gigabytes of raw data every time a query is conducted, the McAfee SIEM system transfers realtime indexes over the network. "We can still pull up specific event data when needed, but our network is no longer bombarded," concludes Morris. "The raw event data gathered from various devices is backed up daily from the eight receivers to the McAfee Enterprise Log Manager, but we can throttle the traffic and send the data whenever it makes the most sense," he adds. "And when it is sent, the impact is greatly reduced because the data compression ratio averages 17:1."

"An important feature of a SIEM is the ability to bring in new events quickly to be viewed. Our previous SIEM required events to be reviewed manually before conducting incident response. With McAfee SIEM we were able to push events in which were then normalized with standard categories (for example, Windows Exploit, Malware, etc.) and respond almost immediately."

—Robert Morris, Security Operations, Center Manager, McAfee, Inc.

Shrinking Time to PCI and ISO 27001 Compliance

The McAfee First team found that with the McAfee SIEM system, compliance reporting is also much easier. McAfee is a Level-One PCI merchant, so PCI compliance is mandatory. "The first time we did PCI gap analysis after implementing the McAfee SIEM system, we were delighted with how much easier it was to show security events hitting specific firewalls and that we were monitoring across all our important devices," says Morris. "To produce that report for our auditors took about 10 minutes, whereas with our previous solution, it would have taken eight to 12 hours to provide evidence of PCI compliance."

By retaining the raw packets of security event data, the McAfee SIEM system also facilitates compliance with ISO 27001. "As part of the ISO incident response processes, you need to be able to go back and examine all the different events surrounding an incident," explains Morris. "And the best way to do that is with events in raw format, because they are forensically sound."

Safer through Integration

Integration of the SIEM system with other McAfee security solutions enhances its predictive capabilities even further. For example, by pulling in vulnerability data gathered by McAfee Vulnerability Manager, the McAfee SIEM solution enables McAfee to map asset vulnerabilities against factors such as confidentiality, integrity, and availability, as defined by the company's governance, risk, and compliance policy. In addition to other McAfee solutions, the McAfee SIEM system is integrated with Microsoft Active Directory, Cisco Syslog, and Avaya Syslog events.

For compliance reasons, McAfee required SIEM functionality at its disaster recovery site. The McAfee SIEM system made disaster recovery redundancy easy to implement. "In the McAfee SIEM architecture, you can have receivers send event data to both ESMs and ELMs," explains Morris. "If one were to go down, we could just hit the other IP address and still access the system and review events."

Leveraging Virtual Machines

McAfee found that to reduce capital expenditures and footprint they could deploy receiver virtual machines globally. Before implementing the McAfee SIEM solution, updating the SIEM agents on each system was a tedious manual process. Any type of Microsoft Windows patches or SIEM agent revisions had to be implemented from the individual host device. "Today, all we have to do is upload the most recent patch or update and deploy it from a central console to multiple devices—whether physical or virtual—and, within minutes, the SIEM system will automatically apply it and restart the device for us," states Morris.

Solution's Effectiveness Leads to Acquisition

McAfee was so impressed with the NitroSecurity solution and how it enhanced and improved the effectiveness of its SOC that, after only a year of using the solution, McAfee acquired the company and all of its technology. NitroSecurity had already been part of the McAfee Security Innovation Alliance program for three years, complementing the extensive McAfee security portfolio and helping joint McAfee and NitroSecurity customers meet their risk and compliance needs. Using NitroSecurity's technology in its own SOC further drove the

"Searching for indicators of compromise (IOCs) in our previous SIEM was not a feasible option due to the time. With McAfee SIEM we are able to quickly locate an indicator, such as an IP, and then search over the course of a year or more within minutes."

—Robert Morris, Security Operations, Center Manager, McAfee, Inc.

strategic decision to fully incorporate the SIEM vendor's technology into the McAfee and Intel Security product offerings. As a part of the Security Connected framework, the Nitro solutions help provide McAfee customers with visibility into enterprise endpoint assets, underlying network infrastructure, specific security threats and risks, and system vulnerabilities across their entire IT environment.

Security Connected

The Security Connected platform from McAfee provides a unified framework for hundreds of products, services, and partners to collaborate with each other. With Security Connected solutions, such as McAfee Enterprise Security Manager, security teams can view context-specific data in real time, offering immediate visibility into an organization's security posture across their infrastructure to enable organizations to optimize response time from discovery to remediation.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

60543cs_siem_0913B_ETMG