CASE STUDY

Global Manufacturer MAUSER Realizes Dream of Interconnected, Adaptive Security a Reality

McAfee provides a trusted partnership for this agencies security infrastructure

MAUSER Group

Customer Profile
Global industrial packaging company

Industry
Manufacturing

IT Environment
1,200 endpoints across 80 production sites in 16 countries, four regional data centers

This German-based global manufacturing company is well on its way to achieving its goal of adaptive threat defense. Unlike point solutions, this security model integrates data, workflows, and management dashboards into a centrally managed and extensible environment that simplifies and accelerates operations.

For a long time, Thomas Langer, head of networks and IT security for the European operations of global industrial packaging manufacturer MAUSER Group, had been looking for an appropriate solution for the company's security infrastructure. In his ideal environment, threat intelligence and other relevant information would be actively exchanged among all of the company's endpoints, networks, gateways, and so on—across all 80 locations and four data centers worldwide—and then immediately and automatically analyzed and acted upon as needed, with minimal human intervention. This interconnected system would continually learn from past incidents, creating a smart, adaptive defense against future cyberthreats.

The Only Vendor that Could Support a Long-Term Vision

In 2013, MAUSER decided it was necessary to consolidate security vendors and have one integrated security solution. Langer and others in the network and security team looked around to see which vendors could help implement the vision of an open, connected security system.

"McAfee was the only company that could help us optimize our medium-range and long-term strategy," says Langer. "The breadth of McAfee solutions and the market power of Intel gives us confidence that McAfee could deliver on its integrated security promise and even define security standards. No other vendor is in the same position."

Langer also notes that all the headlines about major data breaches since then have further confirmed that MAUSER is moving in the right direction with its information security strategy. "Even the most powerful point solutions are limited in their effectiveness," he declares," Unless they can share relevant information and learn from one another."

Connected Solutions and McAfee Threat Intelligence Exchange

In keeping with its new overarching strategy, MAUSER purchased and implemented McAfee Enterprise Security Manager as its security information and event management (SIEM) solution, along with McAfee Advanced Threat Defense appliances, which use dynamic and static code sandbox analysis to detect evasive threats, McAfee Threat Intelligence Exchange, and McAfee Application Data Monitoring. McAfee Threat Intelligence Exchange shares global, local, and third-party threat intelligence and organizational knowledge among all security solutions connected to the McAfee Threat Intelligence Exchange ecosystem. This ecosystem runs on the Data Exchange Layer, a bi-directional, efficient messaging layer for exchanging data and processes. In addition, McAfee Application Data Monitoring monitors important network services like DNS.

The integrated security framework inherent in MAUSER's existing McAfee endpoint protection solutions has always included automation and integration capabilities, but integrating McAfee Advanced Threat Defense, McAfee Enterprise Security Manager, and McAfee

Challenges

- First and foremost, a need for faster detection
- Increasing volume of malware attacks through MPLS network
- Compliance with legal requirements, country regulations, and ISO certifications
- Pressure from global customers and shareholders to protect against a data breach

McAfee Solution

- McAfee® Advanced Threat Defense
- McAfee Application Data Monitor
- McAfee Complete Endpoint Protection Enterprise—Advanced
- McAfee Enterprise Security Manager
- McAfee Global Threat Intelligence
- McAfee Threat Intelligence Exchange

Threat Intelligence Exchange takes the company's threat defense to a whole new level. McAfee Advanced Threat Defense makes it easier to detect the most difficult, targeted types of attacks, McAfee Enterprise Security Manager enables faster detection and visibility into threats and risk, and McAfee Threat Intelligence Exchange collects and shares this information plus other contextualized information to make protective decisions across the enterprise in real time. Systems integrated with McAfee Threat Intelligence Exchange also learn from one another, adapt, and improve protection and detection over time.

By integrating McAfee Threat Intelligence Exchange with McAfee Enterprise Security Manager, McAfee Advanced Threat Defense, and McAfee® ePolicy Orchestrator® (McAfee ePO™) software, the console used to manage the company's endpoint solutions, MAUSER was well on its way to making its security vision a reality.

Justification for the CIO and CFO

According to Langer, justifying the McAfee purchase to the CFO of MAUSER was not difficult. "We explained how the products were critical to our long-term strategy for safeguarding the company, and we also emphasized how they were necessary to meet current legal and compliance requirements," explains Langer. "We told the CFO we can either purchase this system or hire two new employees that add head count, can't be depreciated, and are not nearly as effective as this system, which analyzes more than 24 million entries daily. He got it."

To help the MAUSER's CIO better understand the proposed information security strategy and the role of McAfee, the security team invited him to the McAfee Executive Briefing Center (McAfee EBC) in Amsterdam. In his meeting at the McAfee EBC, the MAUSER CEO met with McAfee executives, viewed a demonstration of our interconnected system, and had his questions and concerns addressed by experts. He left fully on board with our integrated approach to security.

Automation for a Sustainable Threat Defense

One of Langer's favorite aspects of the open and connected McAfee system is automated incident response. If an infected computer attempts to spread malicious software, it is automatically disconnected from the network and quarantined. Furthermore, a firewall rule is automatically created to block that computer from accessing the network or the internet by any means.

"Our computers are scattered around the world, and I cannot be at work 24/7," explains Langer. "If the McAfee system detects something suspicious, I am very comfortable with it taking countermeasures automatically and leaving the details in a report for me to view when I return to the office."

Langer looks forward to using the McAfee system to automate workflows as well in the future—for example, updating Microsoft Windows machines with new service packs. Given that MAUSER has limited staff dedicated purely to security, automation is essential for a sustainable threat defense.

Results

- Blocked at least one extremely sophisticated targeted attack with 12 hours of deployment
- Decreases time to malware discovery, containment, and remediation
- Reduces number of security incidents
- Increases efficiency of day-to-day operations

Compressed Time to Response Thwarts Malicious Attacks

"With the McAfee SIEM, McAfee Advanced Threat Defense, and the McAfee Threat Intelligence Exchange system in place, the time to detect and analyze threats of all kinds has shrunk tremendously," asserts Langer. "And faster detection and analysis equates to faster response."

Just 12 hours after going live with McAfee Enterprise Security Manager, McAfee Advanced Threat Defense, and McAfee Threat Intelligence Exchange and creating a watch list, the system thwarted a serious malicious attack. "When we came in the morning after deployment, the log files showed that our systems tried to access malicious software from an Internet source. At our branch in China, an external employee connected to the MAUSER network without permission. The laptop was contaminated with malware, which wanted to contact a command and control server. Our firewall recognized it and blocked it. McAfee Enterprise Security Manager recognized the firewall log as dangerous and raised an alarm, so that we could start the analysis promptly. Given the volume of log files, we simply wouldn't have been able to detect this malware in such short time without the McAfee system."

Besides McAfee Enterprise Security Manager, McAfee Advanced Threat Defense also proved itself effective. It detected extremely advanced targeted malware before it could wreak havoc. "This malicious software was so advanced, it took more than three minutes to analyze, and the analysis produced more than 35 pages of information," states Langer. "That incident showed us just how powerful the McAfee system is. We hate to think what would have happened had it not been implemented."

Central Management and Fewer Incidents Also Saves Time

In addition, since leveraging McAfee products intelligent incident prioritization capabilities, MAUSER now investigates fewer security incidents in its network. And, notes Langer, the incidents can be explained afterward—something that wasn't always possible in the past. The network also runs much more smoothly. Fewer incidents and network issues mean even more savings in time and energy.

The ability to see all-important data from one centralized dashboard also saves the security team time and increases efficiency. From his desktop, Langer can view both the SIEM dashboards and the McAfee ePO software console from which he manages network security and a colleague manages endpoint protection. Langer uses the easily customized dashboards he built and reviews them several times a day. He can also conduct historical forensics, which was previously exceedingly time-consuming or impossible. Now he can investigate long-term historical data for patterns that help optimize systems or processes.

> "McAfee was the only company that could help us optimize our medium-range and long-term strategy. The breadth of McAfee solutions and the market power of Intel gives us confidence that McAfee could deliver on its integrated security promise and even define security standards. No other vendor is in the same position."
>
> —Thomas Langer, Head of Networks and IT Security, Europe, Network and Security Engineer, MAUSER Group

McAfee Threat Intelligence Exchange and Data Exchange Layer—The Standard of the Future

The next step for MAUSER is to connect additional security solutions to its integrated security framework, starting with McAfee Web Gateway appliances. "We will definitely be looking for products that work with McAfee Threat Intelligence Exchange and Data Exchange Layer," asserts Langer. "In our minds, they are already the standard and are a prerequisite because buying new products that cannot exchange information with the McAfee platform just doesn't make sense."

"The Integrated Security approach works 100% with our strategy—a strategy we truly believe is the most effective way to secure our global organization now and in the future," concludes Langer.

McAfee
Together is power.

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

62441cs_mauser_0516
MAY 2016