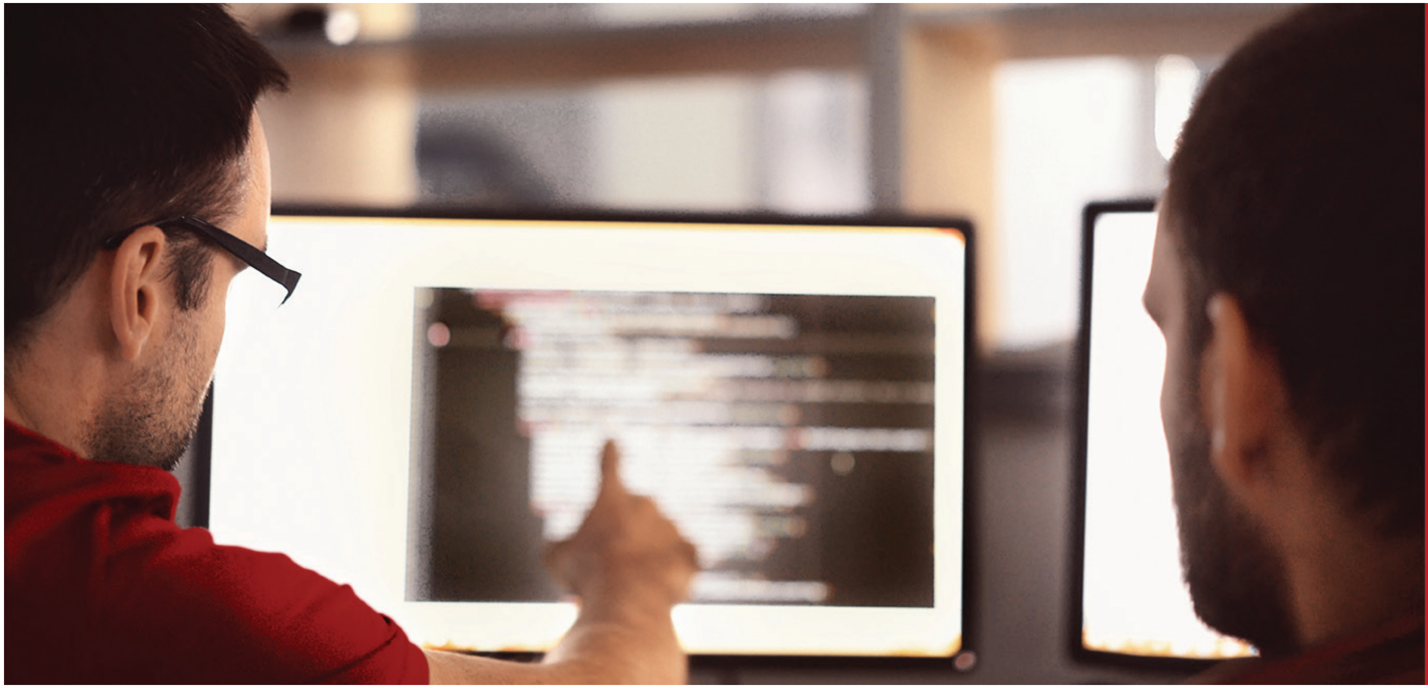
CASE STUDY

Multilayered Defense Fortifies Federal Agency's Security Posture

Germany's Federal Employment Agency (Bundesagentur für Arbeit) simplifies security administration and strengthens defenses with the McAfee integrated security platform



Federal Employment Agency for Germany (Bundesagentur für Arbeit]

Customer profile
Federal agency responsible for social security benefits payments, employment services and other employment-related issues

Industry
Government

IT environment
160.000 endpoints across Germany

The Federal Employment Agency is a knowledgeable contact for finding employment and training. They provide advice on the topic of work and support millions of citizens with financial compensation such as unemployment and child benefits every day. By implementing an integrated security infrastructure featuring McAfee Endpoint Security, McAfee Threat Intelligence Exchange, and McAfee Advanced Threat Defense, along with the McAfee SIEM solutions, the agency has built a multilayered defense that is shrinking the gap to containment and improving its overall security posture.

Connect With Us

Shielding 160.000 Endpoints from Sophisticated Malware Attacks

Every day, the Computer Emergency Response Team (CERT) at the Federal Employment Agency for Germany (Bundesagentur für Arbeit) report to work not knowing exactly what the day will bring. With 160.000 endpoints and more than 100.000 internal users within the corporate network to protect and the sensitive data of the country's citizens at stake, they know their role is critical and will only become more so as cyberthreats continue to grow and become more evasive.

"In recent years, we've seen a considerable uptick in the number of threats we face, such as ransomware and distributed denial-of-service attacks," says Peter Neuhauser, head of the CERT. "Our enterprise experiences 300 million security incidents daily. Knowing which incidents need remediating and how best to protect our huge enterprise is a challenge and not for the faint of heart. We need to be on guard all the time, especially against advanced, zero-day threats."

Protection Against WannaCry Ransomware Catches Management's Attention

The Federal Employment Agency has been relying on McAfee solutions for more than 20 years, starting with McAfee antivirus software. These solutions provide protection that is consistently reliable and also keep up with the changing threat landscape, as well as the increasing number and sophistication of possible threats.

"WannaCry attacked us too, but, unlike many large organizations in the Europe and US, we were not a victim," recalls Peter Neuhauser. "That our operations were not impacted at all was very good for the security department. It got us noticed by top management and increased awareness of the importance of cybersecurity across the agency."

Simplified Security Management and Reduced Operational Overhead

In addition, the McAfee ePolicy Orchestrator (McAfee ePO) central management console has proved invaluable for the federal agency's CERT team in managing and protecting so many endpoints. The team uses McAfee ePO software to manage a wide range of security software, from antivirus protection and host intrusion prevention to encryption and vulnerability management, for the agency's entire physical and virtual infrastructure.

"McAfee ePO software simplifies our lives because it enables us to manage multiple security products with one platform and one interface," explains Peter Neuhauser. "Its customizable dashboard and reports make it easy for my operational team to protect such a huge number of endpoints. Almost every server task is automated and scheduled. The team's job is simply to improve the automation or to manually intervene if the automation doesn't work for some reason."

Challenges

- Provide robust defense against sophisticated attacks, including ransomware and advanced malware
- Reduce administrative burden of protecting infrastructure and 160.000 endpoints
- Comply with ISO 27001 and federal regulations for critical infrastructure

McAfee solution

- McAfee® Advanced Threat Defense
- McAfee® Endpoint Security
- McAfee® ePolicy Orchestrator® (McAfee ePO™)
- McAfee® Threat Intelligence Exchange
- McAfee SIEM solutions: McAfee® Enterprise Security Manager, McAfee® Log Manager, McAfee® Advanced Correlation, McAfee® Event Receiver, McAfee® Global Threat Intelligence for McAfee Enterprise Security Manager
- McAfee® Network Security Platform

The Federal Employment Agency CERT team uses several of the McAfee ePO software reports frequently, such as one depicting the update rate of software being pushed out across the enterprise and another listing all suspicious or malicious interceptions. The team uses the latter to help determine exactly what needs attention or remediation and to monitor security posture. Typical monthly incident findings include:

- 2,000 viruses/malware on endpoint
- 5,000 detections on network
- 30 million suspicious emails
- 1,000 spyware instances.

Advanced Endpoint Protection Bolsters Defenses and Makes Users Happier

To take advantage of newer technologies for endpoint protection, the Federal Employment Agency decided to upgrade its endpoint protection to McAfee Endpoint Security. After thorough testing and staging over several months, the CERT operational team migrated most of the organization's 160.000 endpoints from McAfee® VirusScan® Enterprise endpoint protection to McAfee Endpoint Security in one weekend, with help from McAfee® Professional Services.

With McAfee Endpoint Security, the organization augmented threat detection capabilities beyond signature-based scanning. The solution's state-of-the art machine learning techniques identify malicious code based on appearance and behavior. Neuhauser was particularly keen to deploy enterprisewide the solution's Adaptive Threat Protection module, which includes Real Protect technology. Real Protect draws upon real-time cloud-based intelligence, garnered from millions of malicious samples and static and dynamic behavioral analysis, to automatically match attributes and behaviors of unknown files against threat models to effectively convict zero-day malware.

In addition to providing a more robust defense, the migration to McAfee Endpoint Security made users happier. Now malware scans are much faster and primarily occur in the background when systems are idle. The massive reduction in CPU impact has increased user satisfaction and productivity.

Results

- Easier security administration, thanks to single console for breadth of solutions
- Superior defenses, faster workstation performance, and happier users with advanced endpoint protection
- Reduced incident response time with bi-directional sharing of threat intelligence
- Actionable intelligence and visibility into security incidents

Integration of Security Tools Via DXL Blocks Malware Faster, Shrinks the Gap to Containment

Along with McAfee Endpoint Security, the Federal Employment Agency implemented McAfee Threat Intelligence Exchange, which uses Data Exchange Layer (DXL), an open source platform that connects security components to share local and global threat information bi-directionally among all DXL-connected systems within the environment. Since McAfee Endpoint Security is built to leverage DXL, when an agency endpoint encounters a suspicious or malicious file, that information is immediately conveyed to McAfee Threat Intelligence Exchange, which compares it to its reputation database. If the file is deemed malicious, it is immediately blocked, not only at "patient zero" but also across all endpoints. As soon as new threats are discovered, whether in the local environment or external sources, that information is added to the McAfee Threat Intelligence Exchange database.

If McAfee Threat Intelligence Exchange does not find a match to an unknown file, then the file is automatically forwarded to one of the agency's McAfee Advanced Threat Defense appliances for in-depth static and dynamic analysis (malware sandboxing). If McAfee Advanced Threat Defense concludes the file is malicious, that information is instantly shared with all systems in the environment connected via DXL.

"The integration of McAfee Endpoint Security, McAfee Threat Intelligence Exchange, and McAfee Advanced Threat Defense gives us a critical, multilayered defense against zero-day attacks," notes Peter Neuhauser. "Real-time information from the cloud combined with bi-directional sharing of threat information via DXL helps us stop malware at 'patient zero.'"

Innovative Security Check Mailbox Tests Questionable Emails for Users

In addition to using McAfee Advanced Threat Defense to analyze files directed to it via DXL, the CERT team realized it could leverage the appliance and its XMODE capability to create a "Security Check Mailbox" for Federal Employment Agency employees to help them contribute to keeping the agency secure. "The XMODE of McAfee Advanced Threat Defense is a unique feature. I have not seen it in any other sandboxes," claims the endpoint security product manager at the agency. "It makes it easy to manually analyze suspicious files in a safe space whenever needed."

If any agency employees receive an email that they are uncertain is legitimate—for instance, if it is in a language other than German or contains an unknown URL link or attachment—they can forward it to a specific email address, also known as the Security Check Mailbox. A CERT analyst receives the e-mail and lets you analyze suspicious attachments via McAfee Advanced Threat Defense's intuitive user interface. The analysis takes place in a secure environment and the appliance provides the CERT Analyst with the results.

McAfee SIEM Provides Actionable Intelligence and Facilitates Regulatory Compliance

The Federal Employment Agency also utilizes the McAfee SIEM solution, consisting of McAfee Enterprise Security Manager, McAfee Log Manager, McAfee Advanced Correlation Engine and other related products, which meet the requirements of the Agency as far as possible and integrate seamlessly with the McAfee ePO Software and the Network Security Platform.

"The McAfee SIEM solution gives us visibility into each of the 300 million security incidents logged daily," says Neuhauser. "With it we have actionable, intelligent reports all in one place. The dashboards and reports make our security measures visible and help us meet compliance requirements."

A Strategic Partnership of "Good Guys"

Peter Neuhauser considers McAfee to be a vital partner in the IT Security environment. The Federal Employment Agency for Germany uses numerous McAfee products and taps into McAfee Professional Services when needed, for instance, to help with the migration to McAfee Endpoint Security and to assist in creating incident response plans. "The bad guys are collaborating on a highly professional level. I think 'Together is Power' is the right way for the good guys to work together," concludes Peter Neuhauser.

> "...The integration of McAfee Endpoint Security, McAfee Threat Intelligence Exchange, and McAfee Advanced Threat Defense gives us a critical, multilayered defense against zero-day attacks. Real-time information from the cloud combined with bi-directional sharing of threat information via DXL helps us stop malware at 'patient zero'."
>
> — Peter Neuhauser, Head of the Computer Emergency Response Team, Bundesagentur für Arbeit, Germany

McAfee™
Together is power.

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