CASE STUDY

Intelligent, Collaborative Endpoint Security

Improves Detection and Protection and Slashes User Impact

US Insurance Company

Customer Profile
A leading American insurer

Industry
Financial

IT Environment
6,000 desktops and 2,000 servers across 12 locations

By migrating to McAfee® Endpoint Security, a leading insurance company fortified its security posture while reducing the impact on end users. As a result, the insurance company gained safer operations and data, hours each week freed up for security engineers, and happier, more productive business users.

"Our number-one objective is always security," says the lead information security engineer on a team that oversees all of the McAfee network and endpoint security solutions for a leading US insurance company. "However," he adds, "as at most organizations worldwide, we have other factors to consider as well."

Balancing Security without Impact on Users

"We absolutely need to provide the most effective controls possible to secure our customers' sensitive data. That means we need to defend against ransomware and zero-day threats, prevent accidental access to malicious websites, and so on. But we can't hinder business operations and productivity," continues the IS engineer.

In addition, security needs to be as efficient as possible. "There are only so many hours in a day and so many things our security team can attend to," he adds. "So dealing with users complaining about the impact of virus scans, or remediating after a malware attack that could have been prevented—or detected sooner—takes valuable hours away from projects that improve security."

Consolidation and Manageability Drive Migration to McAfee Endpoint Security

Furthermore, to reduce redundant technologies and complexity and ease security administration, the insurance company's information security leaders had recognized several years ago the need to consolidate security solutions and create a smaller, more manageable security footprint. "We had products all over the place, each with their own agent," explains the engineer. "And it worked, but it wasn't ideal."

As an existing user of McAfee Complete Endpoint Threat Protection, the company decided to move from its legacy McAfee endpoint products (McAfee VirusScan® Enterprise software, McAfee SiteAdvisor® software, and McAfee Host Intrusion Prevention) to the collaborative McAfee Endpoint Security framework, which consolidates and optimizes technologies as well as connects and enables more defenses to communicate. "Implementing McAfee Endpoint Security represents our first step toward establishing a more refined, smaller security footprint and easier management," says the IS engineer.

"McAfee Endpoint Security version 10.5 finally closes the endpoint protection gap," he continues. "It is a stable product that provides all the protection of the previous McAfee endpoint solutions as well as the adaptive threat protection and behavioral analysis necessary to defend against today's advanced and zero-day threats. That kind of coverage gives us a warm, fuzzy feeling."

The insurance company migrated the majority of its nodes to Endpoint Security version 10.2, including the endpoint protection framework's three core modules: Threat Prevention, Web Control, and Firewall. According to the information security engineer, he and his team used the McAfee Migration Assistant tool to copy security policies from the previous endpoint suite to Endpoint Security. Although migration can be done quickly, the team took advantage of the migration to 'clean house,' taking time to eliminate extraneous files and fine-tune policies and settings.

Challenges

- Secure customers' sensitive personal data
- Provide top security without compromising customer experience
- Minimize security footprint and impact on end users

McAfee Solution

- McAfee Advanced Threat Defense
- McAfee Complete Data Protection
- McAfee Complete Endpoint Threat Protection
- McAfee Data Loss Prevention
- McAfee Endpoint Security
- McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
- McAfee Web Gateway

The company then migrated all its 8,000 Microsoft Windows-based nodes to Endpoint Security version 10.5 in conjunction with an enterprise rollout of Windows 10. McAfee Endpoint Security version 10.5 was an essential component of the new corporate desktop image.

Significant Improvements in Defense and Performance

The insurance company's information security staff has been extremely impressed with the improvements in performance and adaptive threat prevention provided by McAfee Endpoint Security. "McAfee Endpoint Security is state-of-the-art," says the IS engineer. "It represents the next evolution of endpoint protection. It's more stable, more efficient, and more accurate. It is definitely worth the migration."

Even more impressive, however, has been the increase in CPU performance since migrating. With the legacy endpoint protection, some of the company's desktops would often experience up to 95% spikes in CPU utilization during antivirus scans. With McAfee Endpoint Security, those spikes have shrunk to at most 35%. Most of the time, end users are oblivious to security scans on their PCs and laptops. Zero-impact user scans only run when the device is idle and resume after shutdown or restart. Boot-up time is also much faster with the new endpoint security framework.

"In my mind, improved performance has been the biggest benefit of migration to McAfee Endpoint Security," says the information security engineer. "Users who didn't have issues with the impact of McAfee VirusScan software beforehand don't even realize a change has been made. But for the users who used to complain often—some daily—about the impact of antivirus scans on their PCs, the difference is enormous. On machines with tens of thousands of archive files and some other legacy devices, anti-malware scans could run for days," he says. "These users were the most vocal complainers, and the first we targeted for migration to McAfee Endpoint Security. As soon as their machines were upgraded, their calls to the IT help desk completely stopped."

After implementing McAfee Endpoint Security, the company's IT help desk also receives 80% fewer tickets. Previously, the help desk typically received five to 10 tickets each week, or more than 25 per month; with McAfee Endpoint Security, it receives at most five per month.

Superior Protection with Real Protect and Dynamic Application Containment

After deploying McAfee Endpoint Security version 10.5, the insurance company fully enabled the cloud-based Real Protect machine-learning behavioral analysis technology. "Real Protect gives us the behavioral threat detection that HIPS used to provide and more," says the IS engineer. "For example, signature-based protection can't prevent a system with compromised credentials from laterally attacking another system within our network, but Real Protect can."

Across its workstation environment, the company also deployed the endpoint protection framework's Dynamic Application Containment (DAC) functionality that traces and quarantines unknown files such as greyware so that they cannot infect 'patient zero,' whether or not users are connected to the network. As but one example scenario

Results

- CPU utilization spikes reduced from 95% to 30/35% and multiday scans to hours
- Numerous hours saved weekly by information security engineers
- Increased productivity of both end users and security operations
- Improved security posture thanks to a collaborative ecosystem

shared by the IS engineer, if a hacker tries to crack a password using an insecure LM hash, DAC will block the execution and contain the culprit file.

Initially, the IS team is running DAC in report mode, to build a baseline for quarantine exceptions. "We are evaluating containment rules in approximately 30 major categories," says the IS engineer. "After workstations, we'll deploy DAC on servers."

Huge Time Savings for Security Engineers

The company's IT help desk employees are not the only ones saving time thanks to the McAfee Endpoint Security rollout. Information security staff also save a tremendous amount of time. One reason is the significant increase in incident containment since the new endpoint protection framework was deployed. With improved protection at the endpoint, IS engineers spend fewer hours reimaging desktops and performing other remediation. "Furthermore, by eliminating the need to troubleshoot issues related to legacy software, the McAfee Endpoint Security framework has saved our team countless man-hours each week," states the information security engineer.

In addition, with the legacy McAfee Endpoint Protection, the IS team had to spend more time on manual activities, such as creating exception lists of processes to whitelist—one process at a time—and building complicated rule sets. Creating exceptions for an SQL server's 25 processes could take 40 hours. But with McAfee Endpoint Security, none of that time-consuming manual activity is necessary. The endpoint protection automatically 'knows' it can trust these processes based on the AMCore Trust Model and a host of other information it receives from shared local and global intelligence.

The overhauled administrative user interface for the new endpoint protection framework also helps IS staff save time. It is extremely easy-to-navigate, provides helpful at-a-glance visuals as well as the ability to drill-down to granular details, and communicates in language that engineers and executives can both understand—and all from one screen via the web-based McAfee ePolicy Orchestrator® (McAfee ePO™) central console.

Dramatically Bolstering Security with Collaborative Architecture

In addition to the McAfee Endpoint Security framework, the insurance company relies on a host of other McAfee products. These include McAfee Complete Endpoint Threat Protection Suite, McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus, McAfee Complete Data Protection, McAfee Network Security Platform for network intrusion detection and prevention, McAfee Web Gateway, McAfee Advanced Threat Defense for dynamic sandboxing and advanced detection of evasive threats, and McAfee Threat Intelligence Exchange, which shares threat intelligence from multiple sources across resources that use the Data Exchange Layer.

Because the McAfee Endpoint Security framework is connected by DXL, McAfee Threat Intelligence Exchange enables it to receive threat information directly from McAfee Advanced Threat Defense and vice versa, creating much stronger threat detection and enabling

> "McAfee Endpoint Security is state-of-the-art. It represents the next evolution of endpoint protection. It's more stable, more efficient, and more accurate. It is definitely worth the migration."
>
> —Lead Information Security Engineer, US Insurance Company

faster response. For example, if a questionable file attempts to execute on the insurance company's endpoint, it is immediately quarantined and sent securely to the McAfee Advanced Threat Defense sandbox for immediate inspection. If McAfee Advanced Threat Defense determines the file is malicious, that information is conveyed via McAfee Threat Intelligence Exchange to all DXL-connected devices that are connected, including all the company's endpoints and McAfee Web Gateway.

Being Prepared for the Future

With collaborative endpoint protection and an integrated security architecture, the insurance company's information security operations gain considerable peace-of-mind knowing that as threats evolve and security needs change, any future defenses can be integrated easily, without creating security silos or redundancies.

"If you want to stay in the security race, you have to keep your technology current, and that requires a layered defense," says the IS engineer. "McAfee Endpoint Security may not understand every threat it encounters, but if it sees something new, it knows to immediately notify other tools in the environment that can help. A collaborative security environment is a much more secure environment."

One Number to Call

On the rare occasion that there is an issue related to a McAfee product, the insurance company has a single number to call and a single point of contact—a dedicated support account manager who is, according to the IS engineer, "gold." He retells an instance when his team had trouble getting two different McAfee solutions to talk with each other. "It was a simple matter to have the two McAfee product managers talk and resolve the issue quickly," he recalls. "That just wouldn't have been the case if we had had two separate vendors to deal with."

"Furthermore," the IS engineer continues, "it doesn't matter how big or small a vendor is; every security product out there has issues—bugs, flaws, new vulnerabilities, and so on. McAfee has consistently supported our environment quickly and effectively to eliminate any such problems whenever they occur. To me, that's what defines a successful partnership."

> "In my mind, the biggest benefit of migrating to McAfee Endpoint Security has been improved performance. As soon as machines were upgraded, calls to the IT help desk stopped. By eliminating the need to troubleshoot issues related to legacy software, the McAfee Endpoint Security framework has saved our team countless man-hours each week."
>
> —Lead Information Security Engineer, US Insurance Company

McAfee
Together is power.

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