CASE STUDY

McAfee
Together is power.

Faster Time to Protection and Time Savings at Multinational Bank

Large Multinational Bank

Customer profile
Large multinational bank

Industry
Financial

IT environment
Approximately 45,000 endpoints across more than 40 countries and two data centers

With an integrated security platform and migration to McAfee® Endpoint Security, this global financial services institution has improved its overall security posture, including accelerating time from detection to protection.

Connect With Us

This large multinational bank offers a wide range of retail, direct, commercial, and other financial services. The company has operations in more than 40 countries. The global security architecture team that reports to the office of the CISO coordinates global security architecture, defines security standards, and sets policies and reporting and across the company's 45,000 endpoints.

Need for Updated Endpoint Protection

According to the global security architecture team's senior security architect, until a few years ago, each country in which the bank operates had a great deal of autonomy with respect to security operations, so the company had many different security solutions, versions, and vendors present across its extended enterprise. To reduce costs and overhead, the company decided to create a few central global hubs and began standardizing on fewer security vendors and products.

For endpoint protection, the global security architecture team felt it needed more than the standard, signature-based antivirus protection. "We wanted enterprise-ready endpoint protection that provides a higher level of protection than traditional signature-based antivirus protection," says the senior security architect.

The company had deployed McAfee VirusScan® Enterprise endpoint protection many years ago, then switched to another vendor. When that vendor's license neared renewal, the bank evaluated leading vendors and decided to return to McAfee. "We looked at some of the more specialized, newer endpoint security tools, as well as the standard signature-based technology, but we wanted both signature-based and non-signature based behavioral protection," explains the senior security architect. "McAfee covered both in a single product."

"We ultimately returned to McAfee for endpoint security because of the solution's technical functionality," he adds. "Price, ease of administration, and an integrated security framework also influenced the decision."

Migration to McAfee Endpoint Security to Stay Current and Bolster Protection Against Zero-Day Attacks

When McAfee introduced McAfee Endpoint Security, an intelligent, adaptive endpoint protection framework, the bank paid close attention. "[McAfee VirusScan Enterprise] was a useful product, but it is very mature. It is time for the next generation of endpoint protection, with technology that goes beyond signatures," notes the senior security architect. "McAfee Endpoint Security is way more appropriate for combatting today's threats."

Challenges

- Protect the organization from ransomware and zero-day threats
- Block threats caused by user behavior
- Manage security as efficiently as possible

McAfee solution

- McAfee Advanced Threat Defense
- McAfee Complete Endpoint Threat Protection
- McAfee® ePolicy Orchestrator®
- McAfee Threat Intelligence Exchange
- McAfee Web Gateway

Results

- Improved endpoint protection that catches more malware and defends better against zero-day threats
- Accelerated time to protection, thanks to integrated security solutions that share threat information in near real time
- Operational time savings from easier security administration and fewer incidents

The bank migrated to McAfee Endpoint Security v. 10.5 soon after the product was released. The company tested the new software for two to three weeks, and then rolled it out group by group over a couple weeks with help from McAfee Professional Services. The migration went smoothly, with no hiccups. Using the migration tool provided by McAfee, the McAfee VirusScan Enterprise antivirus engine and McAfee Host Intrusion Prevention policies in the McAfee Complete Endpoint Threat Protection suite were migrated to the Threat Prevention and Firewall modules respectively.

"With McAfee Endpoint Security, we catch significantly more malware than we did before," says the senior security architect. The company is also considering enabling the cloud-based Real Protect behavioral analysis technology, which could potentially boost threat detection even more.

Faster Time to Protection Through Integration

Since McAfee Endpoint Security is built to leverage Data Exchange Layer (DXL)—an open source platform that connects security components for automated, real-time data exchange—it augments the bank's existing DXL-connected systems. The company has multiple McAfee Advanced Threat Defense sandboxing appliances and is currently deploying McAfee Web Gateway as well. Two of the McAfee Advanced Threat Defense boxes and a McAfee Web Gateway appliance are currently connected via the DXL framework.

Consequently, if an endpoint with McAfee Endpoint Security encounters a known malicious file contained in the McAfee Threat Intelligence Exchange database, the file will immediately be blocked from executing not only on "patient zero," but across all endpoints and all DXL-connected devices in the company's environment. If the file is unknown, with no existing reputation data, it will be sent via McAfee Threat Intelligence Exchange to a McAfee Advanced Threat Defense appliance for in-depth analysis. Once analyzed, the file's reputation will be shared throughout the environment.

"In short, with integrated security solutions and McAfee Threat Intelligence Exchange, protection starts earlier in the chain than it would have, increasing effectiveness and reducing the likelihood of infection," explains the senior security architect. In addition, while McAfee Advanced Threat Defense is analyzing the suspicious file, Dynamic Application Containment (DAC) functionality in McAfee Endpoint Security quarantines the file at the endpoint so that it cannot infect its host machine or its neighbors.

The bank's security team also mines the trove of useful information contained within the McAfee Threat Intelligence Exchange database for further intelligence to help protect the organization's infrastructure. "From third-party and internal sources, we collect many IoCs [indicators of compromise]," says the senior security architect. "We run the IoC data against the data in the McAfee Threat Intelligence Exchange database. If there is a hit, we can follow up."

> "We looked at some of the more specialized, newer endpoint security tools, as well as the standard signature-based technology, but we wanted both signature-based and non-signature based, behavioral protection. McAfee covered both in a single product. We ultimately returned to McAfee for endpoint security because of the solution's technical functionality. Price, ease of administration, and an integrated security framework also influenced the decision."
>
> —Senior Security Architect, Large Multinational Bank

In the future, he hopes to add McAfee Endpoint Threat Detection and Response to the DXL-connected security infrastructure to obtain even greater depth of insight and superior forensic capabilities. McAfee Endpoint Threat Detection and Response continuously monitors endpoint processes to uncover hidden threats, automatically prioritizes suspicious activity, and provides live and historical threat data to determine the full scope of an attack before using one-click correction across the entire organization.

Time Savings from Easier Security Administration and Fewer Incidents

"Now we have fewer agents on the endpoint, which equals less work," states the senior security architect. "By consolidating all agents into one agent with more functionality, McAfee Endpoint Security saves us a significant amount of time. Having multiple agents on every endpoint impacts performance and requires more time and more overhead in general. With McAfee Endpoint Security, we spend less time managing and troubleshooting. Since implementing it, our incident response team also spends less time on endpoint-related issues."

In addition, the bank continues to benefit from the ease of use of McAfee ePolicy Orchestrator (McAfee ePO™) software, the central management console that enables management of multiple McAfee solutions from one screen. "With McAfee ePO [software] and the McAfee integrated security platform, we don't have to do the work ourselves to get all these solutions to talk to one another," notes the senior security architect. "The more tools you have, the more effort is involved. Going with McAfee saves us time and hassle."

McAfee™
Together is power.

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