Case Study

Integrated Security Architecture Transforms Commercial Bank's Security Posture

Commercial bank

Customer profile
Regional commercial bank with clients across the US.

Industry
Financial.

IT environment
1,500 endpoints across headquarters and branch locations.

Challenges
- Multiple, siloed security solutions inhibited visibility.
- No simple fixes to protect against all advanced threats.
- Compliance with FFIEC, GLBA, Sarbanes-Oxley, and HIPAA.
- Employee behavior putting company at risk.

Intel Security solutions
- McAfee Enterprise Security Manager
- McAfee Advanced Threat Defense
- McAfee Threat Intelligence Exchange
- McAfee Global Threat Intelligence
- McAfee Complete Endpoint Protection—Enterprise
- McAfee Vulnerability Manager
- McAfee Network Data Loss Protection
- McAfee Network Security Platform
- McAfee Web Gateway

After attempting to rely on unintegrated point solutions, a CISO finds a more efficient, more sustainable way to tackle the ever-morphing advanced threat landscape.

Over the past seven years, the CISO for a US regional commercial bank witnessed the rise of ever-more sophisticated, targeted cyber threats. He also felt the increased pressure from the boardroom to ensure data privacy. He saw—and helped bring about—a remarkable transformation within the bank's own security environment, one that makes his 10-person information security and privacy team much more effective and the bank more secure.

No Silver Bullets, Just Point Solutions

Seven years ago the bank installed three different sets of leading antivirus software across its 1,500 endpoints. None of the software worked well or updated properly. For better visibility across endpoints, the company decided to consolidate to Intel® Security solutions, primarily because Intel Security sales reps were more responsive and willing to help solve problems. The bank then continued over the next few years to add best-of-breed products to address specific security concerns. Even though the chosen endpoint protection, intrusion prevention system (IPS), and security information and event management (SIEM) solutions were all from Intel Security, the bank had selected them independently and treated them as three distinct point solutions, along with a host of other point solutions from other vendors.

With advanced, targeted threats becoming the new normal, and very public, costly data breaches in the headlines, the CISO felt it was time to step back and reevaluate the bank's existing security environment. "I have been around long enough to know there are no silver bullets, no products that will protect against all threats," the CISO says. "I knew we needed more than point solutions. For starters, we needed to get our security solutions to talk to one another and work together so they could protect better and more efficiently."

Easy-to-Use SIEM

Consequently, with the help of Intel Security Professional Services, the CISO and his team leveraged the integrated security platform to enable McAfee® Enterprise Security Manager and McAfee Complete Endpoint Protection Enterprise software to communicate seamlessly with one another. Intel Security training also taught the team how to identify the types of behavior and activities to monitor, and how to create appropriate rules to set off alerts.

"If I had to start over from scratch, I would definitely choose the Intel Security SIEM solution again," claims the bank's CISO. "It is very intuitive and easy to use, as well as very customizable. We have even used it to diagnose non-security related network activity, such as misconfigured systems that resulted in network sluggishness."

More Effective Advanced Threat Detection

To improve detection of advanced, targeted threats and further overcome the effects of siloed point systems, the information security team added two additional solutions. The team chose McAfee Advanced Threat Defense for its dynamic sandbox technology to detect evasive threats, and McAfee Threat Intelligence Exchange because of it's global, local, and third-party threat intelligence that's instantly shared with all connected security solutions. McAfee

intel Security

Results

- Fast deployment and minimal maintenance.
- Better security event correlation, higher confidence in less time.
- Faster response and remediation.
- More efficient, sustainable defense against advanced threats.
- Blocked multiple sophisticated zero-day phishing attacks in one month period, saving support teams over 100 hours of work, and enabling them to focus on other matters.

"With the interconnected security approach, communication between solutions becomes a non-issue. I don't have to ponder, 'Can this product talk to that one?' I know they can … the fact that the Intel Security solutions are designed to work together makes so many activities easier. The planning, technical design process, deployment, implementation, maintenance … it has all become a whole lot easier."

— Chief Information Security Officer, Regional Commercial Bank

Threat Intelligence Exchange greatly enhances threat detection effectiveness, making it practical and possible for every security control that is integrated with it to leverage the strengths and experiences of the others around it.

According to the CISO, McAfee Advanced Threat Defense was much easier to deploy and cost less than competitive sandboxes. However, its integration with other systems via McAfee Threat Intelligence Exchange is what truly set it apart. "The combination of Advanced Threat Defense and Threat Intelligence Exchange is the glue that enables us to understand what's going on across all connected systems and informs us of any new threats or concerns," says the bank's CISO. "Even in observe mode, which is how we started, Advanced Threat Defense uses all that information and contextual insight to immediately analyze what's executing where and quickly respond. Threat Intelligence Exchange plus Advanced Threat Defense makes us better and more efficient at detecting malware of all kinds."

In addition to integrating Threat Intelligence Exchange with Advanced Threat Defense, the bank integrated McAfee Enterprise Security Manager and the McAfee ePolicy Orchestrator® (McAfee ePO™) central management console used to manage endpoint protection and other security solutions. In the future, the bank plans to also integrate additional security products, including McAfee Host Intrusion Prevention System, McAfee Web Gateway, and McAfee Data Loss Prevention Endpoint solution, as well as other third-party products.

Prevent, Detect, and Correct Faster, More Sustainably, and Efficiently

Today, the bank's security environment looks very different than it did just a few years ago. By providing an adaptive feedback loop whereby security evolves and learns in an iterative cycle that improves over time, the open, interconnected security infrastructure provides a much more sustainable advantage against complex threats. It is also much more efficient than the bank's previous traditional, unintegrated security architecture.

"We now have a security environment where critical information is continually shared internally among systems as well as externally," summarizes the CISO. "The result is better correlation, less false positives, greater confidence, and faster responsiveness—now and in the future. In other words, we can prevent, detect, and correct much more quickly and efficiently."

Zero-Day Phishing Attacks Become Practically Non-Events

The value of the Intel Security solutions became apparent very quickly. Shortly after installation, the bank was targeted by a zero-day phishing attack. Even though a small percentage of employees clicked on the malicious link, the security solutions detected the malware at the first download, automatically quarantined the infected PC, and blocked subsequent downloads, preventing infection of other systems. In the end, McAfee Advanced Threat Defense and McAfee Threat Intelligence Exchange did exactly what was expected—kept the bank safe. While systems and data were kept secure, the bank also appreciated the user

"We now have a security infrastructure where critical information is continually shared internally among systems as well as externally. The result is better ongoing correlation, less false positives, greater confidence, and faster responsiveness—now and in the future. In other words, we can prevent, detect, and correct much more quickly and efficiently."

— Chief Information Security Officer, Regional Commercial Bank

productivity and support time saved by having to reimage only one computer instead of many. Since that first targeted phishing attack, the bank has seen two more of similar size and sophistication. Each of them concluded in a similar manner—that is, almost a non-event.

Making a CISO's Life So Much Easier

"With the interconnected security approach, communication between solutions becomes a non-issue," says the CISO. "I don't have to wonder, 'Can this product talk to that one?' I know they can. If there is a problem, I don't have multiple vendors saying it's not their fault. The fact that the Intel Security solutions are designed to work together makes so many activities easier. The planning, technical design process, deployment, implementation, maintenance … it all has become a whole lot easier."

The CISO also adds that if he can find a product that 'plays nicely' with the Intel Security environment, that's worth a lot. "I will select an Intel Security, Cyber Threat Alliance, or other intelligence-sharing product over an equally competitive product because it makes my life easier. If it can plug into McAfee ePO software, deployment and maintenance are just so much easier."

Thanks to the greater efficiency enabled by the integrated system, day-to-day management and maintenance require minimal time. The bank's forensics and incident analysis team gathers the majority of information they need from McAfee ePO software or Enterprise Security Manager.

Long-Term Security Partner

"Intel Security has treated us as an important customer from the very beginning, when all we had was antivirus software," claims the CISO. "They have not tried to force products on us, but rather listened to what we want to accomplish and helped us figure out the best way forward. Their professional service people have been outstanding."

The CISO also highly values the Platinum Support the bank receives from Intel Security. "We call every other week," he says, "not because we have problems, but rather to understand how to get more out of what we have bought, to learn from the experts and others' experiences."

"A while ago, we chose a competitor's product, but now we are replacing that product with the Intel Security solution, largely because of the high level of support and high level of integration we have experienced," continues the CISO. "Our security transformation is still under way, but we are so much more secure now than we were before. I expect Intel Security to be partnering with us for the long haul, helping us tackle our strategic priorities, from better controlling employee behavior to securely leveraging the cloud."

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

62300cs_regional-comm-bank_0316_ETMG