CASE STUDY

Vidant Health Shifts from Security Alert Overload to Automated Detection and Correction

Small security team implements a McAfee integrated and connected ecosystem

Vidant Health

Customer Profile
Regional healthcare provider in North Carolina

Industry
Healthcare

IT Environment
13,000 endpoints across 80 locations

Burdened with cryptomalware and on an unsustainable trajectory toward attack fatigue, Vidant Health found actionable intelligence and adaptive automation that protects, detects, and corrects. The result: faster threat identification, expedited remediation, and freedom to focus on core activities.

To Kirk Davis, Director of Information Security at Vidant Health, an eastern North Carolina regional not-for-profit healthcare company, with eight hospitals and 80 clinics, a tough day at work is spent reacting to security events, whether large or small. One particularly challenging Monday, a Cryptowall Trojan encrypted half a million files and directories before his team could identify the attack source and mount an effective response. A good day, on the other hand, is as patient-focused as possible—for instance, helping to facilitate innovative clinical workflows that improve patient care and grow business securely. Unfortunately, tough days far outnumbered good ones.

Alert Overload Impaired Productivity and Protection

"Before we implemented a truly interconnected security infrastructure, it was extraordinarily difficult to get actionable information fast enough," explains Davis. "With conflicting [application programming interfaces] APIs or APIs not communicating very well with one another, we were basically on alert overload most of the time and were not in concert with our organizational objective of excellence."

The consequences of alert overload were not just less productive days for the information security team; the health of the entire organization and its patients was on the line. "For my team, just as for a medical team, how fast we can consolidate events and alerts and get actionable information can be the critical difference between very positive and very negative outcomes," says Davis. "We knew we needed to eliminate the overwhelming amount of noise within our security environment so we could spend time dealing with the things that really matter, like securing and supporting the patient care lifecycle."

Automated Security Decision Support Platform

Davis knew that the only way his small team could truly protect the organization was with better technology: "We looked across the entire market for a technology solution that could provide a cohesive, automated security decision support backbone that would enable us to spend the majority of our time supporting patient-centered business innovation and growth—rather than dealing with the daily bombardment of security alerts."

After a comprehensive search, Vidant Health decided to implement the McAfee® SIEM solution: McAfee Enterprise Security Manager and McAfee Advanced Correlation Engine, as well as McAfee Advanced Threat Defense and McAfee Threat Intelligence Exchange. Leveraging the Data Exchange Layer, McAfee Threat Intelligence Exchange combines multiple internal and external threat information sources and instantly shares this data with all of the organization's other data exchange layer and connected security solutions, such as its previously implemented McAfee enterprise anti-virus software encompassing all endpoints, including those in virtualized and data center environments.

Challenges

- Talent supply shortage, very small information security team, and normal budget constraints
- Security alert overload, continual "firefighting"
- Need to shrink incident detection and response time
- Burdened with cryptomalware

McAfee Solutions

- McAfee Advanced Correlation Engine
- McAfee Advanced Threat Defense
- McAfee Complete Data Protection—Advanced
- McAfee Deep Command
- McAfee Endpoint Security
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator® (McAfee ePO™)
- McAfee Threat Intelligence Exchange
- McAfee Web Gateway

One of the key reasons the healthcare company chose McAfee was the effectiveness of its SIEM and out-of-the-box correlation engine that identifies and scores threat events in real time using both rule- and risk-based logic. "The [McAfee] Advanced Correlation Engine gives us a wealth of salient information without having to dig for it," says Davis. "Within days of deployment we were ingesting Netflow information from a wide range of sources, sharing context and threat intelligence, and picking up an amazing amount of actionable data."

Automated Detection and Correction Up and Running Within Days

Since Vidant Health deployed McAfee Advanced Threat Defense and McAfee Threat Intelligence Exchange, it has been enormously pleased with this integrated solution. "In less than a week we had McAfee Advanced Threat Defense and McAfee Threat Intelligence Exchange fully installed, and, within two weeks, we had done the lion's share of the tuning," states Davis. "Immediately afterward, we began catching malware, including Cryptowall variants."

Thanks to McAfee, Davis and his team could see "patient zero"—the first infected device—in its Microsoft Windows 7 environment, automatically quarantine it, and, via the McAfee ePolicy Orchestrator (McAfee ePO) central console, automatically push out a remediation script to all the Windows XP legacy machines. "While every once in a great while an XP machine gets hit, the vast majority of XP machines are protected automatically, thanks to the interconnectedness of the McAfee platform," claims Davis. "The transformation has been phenomenal. Instead of hundreds of thousands of files maliciously encrypted before we know about it, today a device is automatically quarantined as soon as it tries to write its first encrypted file."

Frees Up Resources, Pays for Itself

"Leveraging McAfee Threat Intelligence Exchange, we have pretty much everything feeding into McAfee Enterprise Security Manager—endpoints, web gateways, and so on—plus we have McAfee Advanced Threat Defense processing hundreds of files every day," says Davis. "All of that gives us an automated platform to protect, detect, and correct—a platform that allows us to not worry about the things that can best be handled by computers and focus on the things we do best."

"By enabling us to confidently automate processes," adds Davis, "this approach has allowed us to stop reacting as much. We have been freed up to add value in other areas where it supports the business. More time can be spent on improving the maturity of other security control objectives, as well as lend subject matter expertise when onboarding new projects, products, and services."

Less time on firefighting and remediation also equates to considerable cost savings. "When you consider how much time we had to spend on Cryptowall remediation in the past and how much productivity was lost, I would say that McAfee Threat Intelligence Exchange and McAfee Advanced Threat Defense paid for themselves

Results

- Automated security ecosystem with only critical threats requiring human interaction
- Much faster detection and remediation of cyberthreats
- More threats addressed with fewer resources
- IT staff freed to focus on core operations activities
- Time and cost savings

within the first six months," asserts Davis. "Plus, we've seen no impact whatsoever on system performance or network bandwidth."

Adding the Equivalent of Extra Staff with Dynamic Application Containment

After adding McAfee Threat Intelligence Exchange, Vidant Health also migrated the antivirus engine and host intrusion prevention components of its McAfee Complete Endpoint Threat Protection suite to McAfee Endpoint Security. "Our overarching reason to migrate to McAfee Endpoint Security was to add Dynamic Application Containment (DAC)," claims Davis. "That feature alone is the equivalent of adding a few staff to my team. No longer do they have to write individual access protection rules or mine through false positives. Files that the endpoint is not sure about are essentially gray-listed, set aside for deeper examination while protecting 'patient zero.' We're not always going to be able to prevent infection at 'patient zero'—that's why we have a layered architecture and DXL—but DAC really raises the bar."

Vidant Health migrated many antivirus and host intrusion prevention rules to the new endpoint protection's Threat Prevention and Firewall modules respectively. "Migration to McAfee Endpoint Security took three days and was flawless and reasonably effortless," claims Davis. "We were thrilled." The company did not implement the Web Control module because it had already deployed the McAfee Client Proxy associated with McAfee Web Gateway.

"With McAfee Endpoint Security, McAfee basically reengineered and rearchitected endpoint protection into modules that work extraordinarily well together, increasing performance and providing a much cleaner interface," explains Davis. "It also reduces complexity. It's easier to push out packages, make upgrades, troubleshoot, and so on."

Security That Continually Learns and Evolves

Davis recognizes that even sharing threat intelligence among all devices is not enough to protect an enterprise today. "Moving forward, we will be focused much more keenly on ensuring that we have an environment that can learn and automatically remediate threats when they do happen. Without a doubt, the most valuable aspect of the McAfee SIEM solution and integrated framework is its adaptability and flexibility. Its kernel-level access to nearly every device in our organization enables us to respond innovatively to threats today, as well as keep learning in an iterative cycle, which improves over time, so we can continue to respond appropriately in the future."

Furthermore, as Vidant Health continues to grow and as it considers moving services to the cloud, the McAfee infrastructure allows it to easily package and scale its infrastructure security and support services as needed. It is also easy to extend protection to newly acquired users and systems. "I think the majority of leaders in my position know that flexibility, celerity, and scalability are critical considerations in platform selection. Will all our compute resources move to the cloud? Not likely,

but I can promise you I was not willing to go with a system that wasn't able to move at the same pace as our business. We rolled out our laptop encryption package to more than 2,000 devices in less than 24 hours—McAfee ePO software is a backbone I know I can trust."

Effective technology alone is not enough, however. "Even more than the right technology, we need partners who are just as committed to our success as we are," claims Davis. "From my account representative all the way up to the C-level, the McAfee folks we interact with are 100% dedicated to us and the healthcare vertical. They understand that every dollar we spend ends up on a patient's bill and has to translate into value, ultimately, for our patients. They understand our workflows, jargon, regulatory scrutiny, and other challenges we face—and they are incredibly responsive. Having great business partners like McAfee is a competitive advantage for us."

More Than the Sum of Its Parts

"Prevention is becoming a commodity service," notes Davis. "Detection and correction were part of our dream roadmap from the start, which is why I was thrilled that the McAfee claim of interconnected, adaptive security actually works. It's pretty much the panacea that all security professionals have been looking for. I suspect a key component of this—Data Exchange Layer—will become an industry standard, just like USB or Wi-Fi. The technology is evolutionary."

Thanks to Vidant Health's investment in McAfee for security management, Davis and his team have gone from working in an environment without any real automation and efficiencies to one with continuous monitoring and faster remediation, all with unparalleled efficiency. "The McAfee solution is so much greater than the sum of its individual products," concludes Davis. "Having outstanding threat visibility and being able to remediate or guard against them with limited or no human intervention allows us to focus on our core business, which, believe it or not, is not running down malicious code."

"My team dedicates itself every day to doing whatever we can do to improve the health of the 1.4 million people we serve here in eastern North Carolina. It's a great feeling to know that what we have accomplished though our partnership with McAfee has supported us in that objective."

"The McAfee solution is so much greater than the sum of its individual products. Having immediate visibility to threats and being able to remediate or guard against them with little or no human intervention allows us to focus on our core business, which—believe it or not—is not running down malicious code."

—Kirk Davis, Information Security Director, Vidant Health

McAfee™
Together is power.

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