Case Study

Making the Job of Security Operations Easier at Berkshire Health Systems

Berkshire Health Systems

Customer profile
Largest regional healthcare provider in Western Massachusetts.

Industry
Healthcare.

IT environment
5,100 endpoints across 20 locations.

Challenges
- Improve and accelerate detection of cyberattacks with limited staff.
- Comply with HIPAA and state privacy regulations.
- Block leakage of sensitive data, yet enable staff to work with data away from office.
- Compress incident response.

Intel Security solution
- McAfee Enterprise Security Manager
- McAfee Enterprise Log Manager
- McAfee Advanced Correlation Engine
- McAfee Complete Endpoint Protection—Enterprise
- McAfee Complete Data Protection—Advanced
- McAfee Host Data Loss Prevention

With total prevention of data breaches no longer a realistic goal, Berkshire Health System's Security Operations, the leading regional healthcare provider in Western Massachusetts, turned to McAfee® Enterprise Security Manager for security information and events management (SIEM), which offers a centrally managed, interconnected security architecture for improved cyberthreat detection and response and simpler, sustainable solution administration.

In today's threat climate, Paul Doucette, senior cybersecurity engineer at Berkshire Health Systems, knows that total prevention of data breaches is no longer possible: "It's more a question of when and how quickly can I detect and minimize impact to my business."

According to the Ponemon Institute's fifth annual benchmark study[1] on patient privacy and data security, more than 90% of healthcare organizations experienced a data breach in the past two years, and 40% experienced more than five data breaches within the same time period. With protection of patients' personal data his top priority, those are statistics that would keep anyone up at night.

Total Breach Prevention No Longer Realistic

For Doucette, who oversees day-to-day security operations for the growing, 5,400-employee organization with three hospitals and multiple clinics and physician offices, the key to a sustainable, effective defense against cyberattacks is the ability to detect threats and respond to them as fast as possible and to optimize his IT staff's resources and priorities.

"Prevention is still very important, but our biggest challenge has become detection—more specifically to immediately detect the threats attacking us and then to respond fast enough so that patient data and other sensitive information is not impacted," says Doucette. "We have a definite need to shift our focus from prevention and protection to detection and correction. Transforming your security defense to this new mode is not something you do overnight, however."

Assessment a Key First Step to Detect and Correct

As a first step, Berkshire Health Systems knew it should assess its security situation. "We needed to look more closely at the solutions we currently have and figure out where the technology gaps are," says Doucette. "In other words, we needed to know what we didn't know."

The company hired DynTek Services and Intel Security to perform a detailed data management security assessment prior to creating a layered, centrally managed security architecture. For the assessment, Dyntek interviewed Berkshire Healthcare Systems

intel Security

Berkshire Health Systems (continued)

Results

- Significantly simplifies security administration.
- Provides comprehensive control over sensitive data.
- Allows complete visibility into all endpoints and data.
- Saves time, thanks to centralized management and automated tasks.
- Enables fast historical analysis to optimize operations and set policies.

"Prevention is still very important, but our biggest challenge has become detection—specifically, being able to immediately detect the new threats attacking us and then to respond fast enough that patient and other sensitive data is not impacted. We have recognized a definite need to shift our focus from prevention and protection to detection and correction."

—Paul Doucette, Senior Cybersecurity Engineer, Berkshire Health Systems

employees at various levels and reviewed the organization's cybersecurity initiatives in detail, including vulnerabilities in the environment scored against HIPAA requirements and staff policies and behavioral controls. Dyntek also reviewed physical controls, such as facility access, device and media control, encryption, password management, security incident reporting, disaster recovery, and data backup plans. Assessment results indicated the need to implement a SIEM solution that integrates with and reinforces the company's current solutions.

Solution: Intel Security SIEM and an Integrated Security Platform

McAfee Enterprise Security Manager was the company's logical choice for a SIEM solution. The primary reason: its ability to seamlessly share pertinent information with other security solutions across Intel Security's integrated security platform. This open, unified framework enables central management and information sharing across hundreds of products and services, eliminating point solution silos and dramatically improving security posture.

Berkshire Health Systems already had McAfee Complete Endpoint Protection—Enterprise, which includes antivirus, host data loss prevention, SiteAdvisor®, and other endpoint protection functionality, all controlled by the McAfee® ePolicy Orchestrator® (McAfee ePO™) management console and part of the Intel Security integrated security framework. McAfee Enterprise Security Manager easily integrated with these solutions and could share data with all of the company's endpoints. McAfee Enterprise Security Manager collects data from the company's endpoints and then applies sophisticated correlation rules to help Doucette prioritize events that need investigation. A risk score unifies vulnerability status, asset criticality, and any countermeasure protection available for the threat to gauge the severity and risk of the threat.

"Makes My Job a Whole Lot Easier"

"The biggest benefit of the integrated Intel Security ecosystem to me personally is that it makes my job a whole lot easier," says Doucette. "I can see potential threat activity, push out updates or remediation, add devices to the network, manage data and endpoint protection policies, and so on, all from the McAfee ePO central console and the SIEM threat intelligence and risk-based dashboards."

He can also determine appropriate security policies much faster. "For example, we were having issues with employees being constantly locked out of their accounts—perhaps they changed a password on their laptops but forgot to change it on their mobile devices and then entered the incorrect password too many times," explains Doucette. "With the Intel Security SIEM, we were able to quickly and easily determine what the right threshold for lockouts should be in order to balance the twin needs for security and easy access."

Improved Enterprise Visibility and Faster Detection

Before deploying McAfee Enterprise Security Manager, Doucette took a training course offered by Intel Security Professional Services that helped him get up and running quickly—with no surprises. Intel Security Professional Services also helped him implement McAfee Enterprise Security Manager. In addition to McAfee Enterprise Security Manager, the company implemented McAfee Enterprise Log Manager, McAfee Advanced Correlation Engine, and physical and virtual McAfee Event Receivers. Doucette implemented many of the out-of-the-box policies and correlation rules, as well as some of his own customized correlation rules.

"With McAfee Enterprise Security Manager and McAfee ePO [software], I have much greater visibility into what is happening across the organization," says Doucette. "Having all events correlated quickly in one central location is huge. I can detect threats we had no idea were happening—for instance, that our passwords are being attacked 24/7 every day from other countries or the presence of CryptoLocker activity. Such dramatically improved visibility and rapid detection of threats means we can respond much faster."

DLP and Fast Historical Analysis Make Compliance Easier

Berkshire Health Systems must comply with HIPAA, Massachusetts state personal privacy laws, such as CMR 17, and other internal and external regulations concerning data security. However, even if such regulations didn't exist, data security would be of utmost importance. "Keeping all potentially sensitive patient data safe is our top priority," notes Doucette," from confidential patient medical information to credit card information."

To prevent data loss, the company uses McAfee Host Data Loss Prevention. McAfee Host Data Loss Prevention allows Doucette to quickly and easily monitor real-time, user activities and apply centrally managed security policies to regulate and restrict how sensitive data is transferred, without impacting employee productivity.

McAfee Enterprise Security Manager also helps Doucette determine appropriate policies. "The Intel Security SIEM enabled us to segment devices that take credit card information—whether PCs or kiosks or cafeteria cash registers—and manage our policies and reporting based on the various PCI subgroups," explains Doucette. "The ability to easily analyze historical credit card transaction data and segment it meant we could lock down point-of-sale devices and some workstations but use DLP for others. Previously, such historic analysis would have taken weeks or would have been impossible."

Sustainable Security Foundation for the Future

With its Intel Security integrated security platform, Berkshire Health Systems has laid the foundation for a sustainable protect-detect-correct threat defense lifecycle to safeguard the company and its patients today and in the future. Doucette has a much more effective approach to disrupt and investigate suspicious events and limit overall risk exposure and compress incident response.

When asked, "What would you do if you got a call from the FBI telling you your company was the victim of a data breach?" Doucette replies, "Most likely I'd already know about it, thanks to our integrated security system."

1. http://www.ponemon.org/news-2/66

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

Intel and the Intel and McAfee logos, ePolicy Orchestrator, McAfee ePO, and SiteAdvisor are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2016 Intel Corporation.
62364cs_berkshire-esm_0416_kgs