Case Study

Reducing Operational Costs and Combating Ransomware with McAfee SIEM and Integrated Security

Atrius Health

Atrius Health

Customer profile
Large regional healthcare provider in the northeastern US

Industry
Healthcare

IT environment
More than 65,000 users on 9,000 endpoints across more than 29 sites

Challenges

- Guard against ransomware and phishing attacks.
- Accelerate detection of and appropriate response to cyberthreats.
- Keep organization secure while enabling business growth.

Intel Security solutions

- McAfee® Enterprise Security Manager
- McAfee Enterprise Log Manager
- McAfee Event Receiver
- McAfee Advanced Correlation Engine
- McAfee Global Threat Intelligence (McAfee GTI) for SIEM
- McAfee Complete Endpoint Threat Protection
- McAfee Management for Optimized Virtual Environments (McAfee MOVE) AntiVirus
- McAfee Complete Data Protection

By adding a security information and event management (SIEM) solution from Intel Security and integrating it with McAfee® ePolicy Orchestrator® (McAfee ePO™) software, as well as non-Intel Security products, the largest independent physician-led healthcare organization in the northeastern US has significantly strengthened its ability to quickly protect, detect, and correct when facing cyberthreats.

Atrius Health Chief Information Security Officer Chris Diguette oversees security for Atrius Health, the largest physician-led healthcare provider in the northeastern US. The organization is recognized nationally for its use of health information technology. Diguette is also CIO of the VNA Care Network, a home healthcare provider and subsidiary of Atrius Health. As CISO, Diguette and his team work to implement and maintain a security infrastructure that safeguards the organization's critical health information systems and applications, such as its Epic Systems Electronic Medical Records (EMR) system and the personal data of more than 675,000 patients at 29 facilities in eastern and central Massachusetts.

Ransomware and Phishing Attacks Plague Healthcare Industry

When Diguette talks with other CISOs in the healthcare industry, one of their main themes is the dramatic increase in ransomware and phishing attacks. "Until we learned how to better detect and quickly disable ransomware, it was one of our biggest challenges," he notes, "and we are definitely not alone."

Compounding the challenge of increasing malware attacks is Atrius Health's rapid growth. The merger with VNA Care Network added 13,000 users, increasing the total number of users to 65,000. Such growth requires an information security infrastructure that can easily accommodate and, ideally, facilitate expansion to support more patients.

Diguette's team had been sending network and firewall logs to a third party that analyzed them and then alerted the company if it noticed any out-of-the-ordinary incidents. Once alerted, one or more analysts or engineers would manually research the incident to determine the appropriate response. For greater control and visibility and faster detection and response to security events, Diguette determined that Atrius Health needed an SIEM solution.

Why an Intel Security SIEM? Faster Speed and Superior Integration

Although Atrius Health had relied successfully on Intel Security for antivirus protection for many years, upgrading and expanding Intel Security endpoint and data protection along the way, Diguette's team still did its due diligence to select the best SIEM solution. After evaluating leading SIEM solutions, the team ultimately chose the Intel Security SIEM solution, including: two McAfee Enterprise Security Manager appliances, one McAfee Enterprise Log Manager appliance, two McAfee Event Receiver appliances, McAfee Advanced Correlation Engine, and McAfee GTI for SIEM.

Easily installed on the company's network, the Intel Security SIEM ingests data from numerous systems in the Atrius Health IT infrastructure, including: network access control (NAC), Citrix NetScaler devices, network scanners, DNS servers, firewalls, routers, web and email gateways, and 900 different servers. The Intel Security SIEM is also seamlessly integrated

intel Security

"With the Intel Security SIEM, we could more quickly and easily investigate the ransomware attacks, finding their targeted encryption keys and tracing them back to their point of origin. Initially, that information showed us which ports and IPs to shut down on our firewall, but it also led us rather quickly to a clear-cut decision to implement geographic blocking—since the vast majority of the ransomware originated from places such as Russia and the Middle East."

—Chris Diguette, Chief Information Security Officer, Atrius Health

Results

- Huge operational savings.
- Avoided hiring several full-time employees.
- Accelerated decision making, thanks to better visibility and correlations.
- Robust detection capability and faster response to threats.
- Improved security for virtual environment.

with Microsoft Active Directory and McAfee ePO software, the central console through which Atrius Health information security engineers manage Intel Security endpoint and data protection suites. On average, the system analyzes 24,000 events per second (EPS) each day.

"In our initial evaluations, we were impressed by the speed of the Intel Security SIEM and its tight integration with McAfee ePO software," says Diguette. "Since implementing the SIEM, we have also been pleased with how easily it integrates with non-Intel Security resources. For instance, when our non-Intel Security firewall registers something suspicious, our Intel Security SIEM automatically alerts us in near real time."

Intel Security SIEM Saves the Expense of Hiring Three to Four Full-Time Employees

As an alternative to purchasing an SIEM, Atrius Health also looked at the option of adding more information security experts and analysts to its headcount. "In our ROI analysis, we figure that we saved three to four full-time employees by going with the Intel Security SIEM," claims Diguette. "The operational savings from more robust protection, elimination of external log analysis, and avoidance of additional headcount is huge. In addition, our existing information security staff is now more effective and can respond appropriately to security events much more quickly."

Automation Accelerates Threat Response

Alerts automatically triggered by the detection of a potential threat on an Atrius Health endpoint or firewall contribute significantly to increased efficiency and reduced time to response. If ransomware is detected and blocked on the endpoint by McAfee VirusScan® Enterprise, for instance, McAfee ePO software instantly shares that information with the Intel Security SIEM, automatically triggering an alert that notifies someone on Diguette's team who can run a correlation right away to determine what action, if any, is needed.

"Using McAfee ePO software, we have built lots of rules based on file types, signatures, and other parameters to detect and block potential threats," explains Diguette. "As soon as an abnormal activity is detected on the desktop, McAfee ePO software reports it, and the SIEM sets off an alarm. Then the SIEM provides all kinds of pertinent information—such as whether and where the potential culprit 'phoned home,' what exactly it did, and to whom—to help us rapidly determine the appropriate response."

Diguette also notes that McAfee GTI—a cloud-based service that provides real-time intelligence on new and emerging threats across file, web, message, and network vectors—helps dramatically reduce security incidents in the first place. Atrius Health leverages McAfee GTI both on its endpoints and in the SIEM. "One time, we let our McAfee GTI license expire," remembers Diguette, "and we were hit by malware that we are sure McAfee GTI would have caught. It was just a minor incident, but it shows how McAfee GTI makes a significant difference."

Improved Visibility and Advanced Correlation Fast-Track Decision Making

Atrius Health has also found that the combination of widespread visibility, via out-of-the-box and customized Intel Security SIEM dashboards, and advanced correlation capabilities has streamlined decision making in

multiple ways. For example, thanks to the SIEM, it was easy for Diguette and other management at Atrius Health to determine that geographic blocking should be implemented to vanquish ransomware.

"With the Intel Security SIEM, we could more quickly and easily investigate the ransomware attacks, finding their targeted encryption keys and tracing them back to their point of origin," explains Diguette. "Initially, that information showed us which ports and IPs to shut down on our firewall, and it also led us rather quickly to a clear-cut decision to implement geographic blocking—since the vast majority of the ransomware originated from places such as Russia and the Middle East."

Thanks to more advanced correlation, it is also easier for the organization's NAC to determine if rogue devices attached to the network should be enabled or disabled. "Often the rogue devices are new clinical devices that have not yet been cleared through proper IT channels or are part of an onsite product demo by a clinical device company," explains Diguette. "The Intel Security SIEM's advanced correlation helps us make sure that the device in question is safe, has limited reach, and employs antivirus protection."

Protection for Data and Virtual Servers Facilitates Compliance and Savings

Like many organizations, Atrius Health has a hybrid environment of both physical and virtual servers. The organization also expects to expand its virtual environment as it moves to an active-active environment for continuous availability. Its Epic EMR application and several clinical applications that integrate with EMR currently run on a mix of physical and virtual servers. To secure these virtual servers, Diguette's team deployed McAfee MOVE AntiVirus. According to Diguette, the McAfee MOVE AntiVirus software was extremely easy to deploy using the McAfee ePO console, conserves virtual server resources, and saves on licensing costs compared to traditional antivirus software.

To protect its physical endpoints, Atrius Health uses McAfee Complete Endpoint Threat Protection suite, which detects approximately 100 viruses daily and includes functionality such as McAfee ePO Deep Command, for secure management of remote PCs, and McAfee SiteAdvisor®, which enables employees to surf the web safely. To comply with Massachusetts regulations and keep data safe, Atrius Health relies on aspects of the McAfee Complete Data Protection suite for comprehensive endpoint encryption. The organization uses the suite's enterprise-grade drive encryption to encrypt all of its more than 7,000 desktops and is in the process of moving from another solution to the suite's file and folder encryption and removable media protection.

Future Plans Include Intel Security

In the near future, besides continuing to educate staff and users to lessen the human component of the risk equation, Atrius Health plans to upgrade its Intel Security endpoint protection to McAfee Endpoint Security 10 for even more out-of-the-box functionality. Atrius Health also plans to integrate its Intel Security SIEM with its EPIC EMR system. Diguette says he also plans to investigate adding McAfee Threat Intelligence Exchange to further enhance their intelligent automation capabilities and McAfee Advanced Threat Defense dynamic sandboxing to simplify and fortify its threat defense lifecycle.

"Every time we have rolled out a new Intel Security product, we have seen huge system and network performance increases," claims Diguette. "I highly recommend considering Intel Security because of the robust protection and performance its products have provided us, as well as ease of deployment and superior integration with both Intel Security and non-Intel Security solutions. Intel Security is always looking forward—it has a strategic vision that keeps us coming back."

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