

TTUHSC Reliance on McAfee to Connect Security and Compliance

Improving Security Management



Texas Tech University Health Sciences Center

Customer Profile

A leading teaching and research university located in Lubbock, Texas

Industry

Healthcare

IT Environment

- 400 servers
- 10,000 endpoints
- Seven schools across six campuses, research facilities, and healthcare clinics

Texas Tech University Health Sciences Center (TTUHSC) offers programs in medicine, nursing, pharmacy, biomedicine, and health sciences. The university has trained more than 10,000 healthcare professionals since 1969. TTUHSC is a leader in education and patient care with research specialties in the study of aging, cancer, reproduction, genetic diseases, and rural health.

CASE STUDY

Compliance and Productivity

Through research, education, and health care clinics, the University serves patients in more than 100 counties in West Texas and beyond. The University's security team has to ensure that TTUHSC complies with HIPAA regulations, as well as Chapter 202 of the Texas Administrative Code (commonly known as TAC 202) to protect electronic medical records and health information.

Before turning to McAfee for a solution, TTUHSC was using multiple devices from different vendors that did not integrate with each other. "Performing an investigation or audit was extremely time-consuming," says information and security officer Andrew Howard. "Additionally, the SIEM product we were using at the time was very difficult to manage."

Centralized Management and Advanced Correlation

The security team needed a better security information and event management (SIEM) solution not only for log management, but also as a means to correlate events in the environment. The University selected products included under the Security Connected framework to protect their endpoints, data, and web environments. TTUHSC chose SIEM solutions from McAfee for situational awareness, centralized management, and advanced correlation.

Additionally, McAfee® Enterprise Security Manager features pre-built dashboards, complete audit trails, and intelligent log management for compliance management. "The correlation is fantastic," explains Andrew. "Data is easier to consume, and we can see full spectrum across the infrastructure."

Phased Approach to Transforming Security at TTUHSC

When Andrew joined TTUHSC, the environment had nearly 10,000 endpoints with only basic virtual-scan and anti-malware protection. "There are not a lot of standards in this type of setting," maintains Andrew. "Endpoint access depends on the department and role."

To minimize disruption, the security team used a phased approach to implement new security solutions. They began by testing each product by department and then by campus before going live. If they thought a solution would have low impact on users, the team would start the rollout, such as McAfee Complete Endpoint Protection—Enterprise, on a large campus. If they thought that a product rollout would have a higher impact on users, the team would start the deployment on a smaller regional campus with only a few hundred endpoints at a single campus.

After implementing McAfee Complete Endpoint Protection—Enterprise, Andrew and his team continued the evolution of their security strategy by replacing the existing end-of-life intrusion prevention systems (IPS)

Challenges

- HIPAA and Texas Administrative Code TAC 202 compliance.
- Improve security management and situational awareness
- Replace legacy and/or under-performing, third-party network, web, and email solutions

McAfee Solutions

- McAfee Advanced Correlation Engine
- McAfee Complete Endpoint Protection—Enterprise
- McAfee DLP Endpoint
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator® (McAfee ePO™) software
- McAfee Global Threat Intelligence
- McAfee Host Intrusion Protection
- McAfee Network Data Loss Prevention
- McAfee Network Security Platform
- McAfee Web Gateway

CASE STUDY

with McAfee Network Security Platform and enabling smart blocking. “We were impressed by the demo for McAfee Network Security Platform,” says Andrew. “It’s a great way to get edge protection and leverage McAfee Global Threat Intelligence (McAfee GTI) for inbound and outbound traffic.” TTUHSC uses the McAfee Advanced Correlation Engine for risk-based correlation and set-up rules to compare source IP and destination IP against the malicious McAfee GTI database.

Blocking Network-Based Threats and Policy Violations

TTUHSC followed up their IPS rollout with McAfee Web Gateway almost immediately. As a state institution, there is no right to privacy unless it’s related to HIPAA, PCI, banking, or other regulations. The university is responsible for student, faculty, and administrative accounts and monitors all traffic.

“There was no existing proxy environment, and malware viruses and vicious code are more difficult to remediate on an endpoint,” describes Andrew. “Now we are catching malicious code before it reaches an endpoint. In eight months, McAfee Web Gateway has caught and blocked thousands of malicious viruses, code, and websites.”



Figure 1. The McAfee Enterprise Security Manager dashboard.

Central Management Provides Performance and Speed

After McAfee Web Gateway, TTUHSC deployed McAfee ePO software as a centralized solution to manage endpoints, build and deploy policy, and to generate reports. The team integrates McAfee ePO software with McAfee Risk Advisor for insights into system vulnerabilities. They also use McAfee ePO software in another dashboard to monitor the web environment. “We can observe how students are streaming video and catch video copyright issues, for example,” Andrew explains. “We use McAfee ePO software for state reporting every month. It’s our central management point, without a doubt.”

Results

- Extensible compliance reporting
- Block thousands of attacks
- Security audits in minutes
- Improve visibility and productivity

CASE STUDY

Realization of CIO's Vision

For TTUHSC, the ability to integrate security and manage security solutions centrally is a key benefit of McAfee. "My advice to anyone looking at security solutions is to focus on integration," says Andrew. "Now that we're using McAfee, we can go to McAfee ePO software and pull mountains of data or use the SIEM solutions from McAfee to quickly and efficiently find the root cause of an issue. The time-to-value is almost instant—and that is beyond beneficial."

Andrew is also pleased with the improvement in productivity as a result of using McAfee solutions. With its previous SIEM solution, if the security team wanted six months or a year's worth of data for a historical investigation, it would take days to retrieve the data. Then the team would have to go through a CSV file

and correlate the data themselves. There was no automation. Now they use McAfee Enterprise Security Manager, which acts as a central point of management, saving time and alleviating work for the security team as they review logs, web traffic, and inbound traffic.

Why McAfee?

"It used to take weeks to perform a comprehensive review," says Andrew. "With McAfee, we can use a centralized management point to input criteria and obtain actionable data within a matter of minutes." When we started down this path, the CIO and I had a vision of true centralized management and fast reporting," concludes Andrew. "Working with McAfee helped us realize the end goal in implementing our security and compliance strategy."

"Now that everything is connected, productivity has increased greatly and time to value is very beneficial."

—Andrew Howard, Information Security Officer



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

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2018 McAfee, LLC.
61136cs_texas-tech_0614B
JUNE 2014