



Adventist Health System Selects Trend Micro for Web Application Security

Trend Micro™ Deep Security for Web Apps provides a single, easy-to-manage solution for SSL certificates and application scanning

Overview

Today's healthcare organizations in the United States face a growing number of challenges that require innovative solutions. From implementing the Affordable Care Act, to compliance with HIPAA and other regulations, healthcare providers are looking for ways to increase the quality of care, increase meaningful use of technology, and reduce costs.

Adventist Health System is a faith-based health care organization headquartered in Altamonte Springs, Florida. A national leader in quality, safety and patient satisfaction, Adventist Health System's nearly 70,000 employees maintain a tradition of whole-person health by caring for the physical, emotional and spiritual needs of every patient.

With 45 hospital campuses and nearly 8,300 licensed beds in ten states, Adventist Health System facilities incorporate the latest technological advancements and clinical research to serve more than 4.5 million patients annually. The full continuum of integrated care also includes urgent care centers, home health and hospice agencies, and skilled nursing facilities.

Each Adventist Health System facility operates independently in delivering care and services to best meet the needs of the local communities they serve. While each entity is unique, all remain united in one mission: to extend the healing ministry of Christ.

AHS Information Services (AHS-IS) is a 695-person department of Adventist Health System that manages data centers, business applications, and IT applications across 32 of the 45 campuses. AHS-IS also acts as an information security provider for the corporate headquarters and individual campus operations. AHS works hard to maintain a high level of security and protection for patient health information accessed via web applications by both patients and healthcare staff.

Challenges

To help secure its web applications and portals, AHS-IS requires Secure Socket Layer (SSL) licenses for hundreds of domains. Their previous certificate provider required them to sign a yearly contract for a set number of licenses, but the frequent addition of new domains made it difficult for the IT team to accurately predict the number of licenses required in a given year. As a result, they often ran out of licenses part way into their yearly contract and had to open a new purchase order.

Managing licenses was also a challenge. With so many divisions using licenses, the process required to accurately track when SSL certificates were issued and when they would expire was time-consuming and labor-intensive.

"When we needed more licenses, we'd have to buy more at the last minute," said Mark Dunkerley, Messaging and domain services team lead for AHS-IS. "The inability to predict how many SSL certificates were needed created a budget issue for our annual SSL purchases."

Another challenge that AHS-IS faced was a lack of centralized management of their application security. With many web applications across their campuses, AHS-IS needed an application security solution that simplified monitoring and management across multiple locations.

For example, AHS-IS used a combination of Public-key Infrastructure (PKI) for internal apps and SSL certificates for external apps, forcing AHS-IS to monitor and manage multiple systems. "Trying to manage our PKI, SSL, and security for all of our websites and applications was very inefficient without a central management system," said Dunkerley.

AHS also needed to make sure patient information was secure, encrypted, and HIPAA compliant across hundreds of domains. This meant securing operating systems, web servers, and applications throughout its AHS divisions. "Providing PHI (Patient Health Information) electronically and through the web requires us to be extremely cautious. We have to ensure that information is always secured at the highest of levels," said Dunkerley.

>> Adventist Health System

Region

North America

Number of Employees

70,000

AHS Information Services

695

Sector

Healthcare

Trend Solution

- Deep Security for Web Apps

Business Benefits

- Simplified SSL purchases and delivered 70% in cost savings
- Reduced SSL domain approval time from up to two weeks down to minutes
- Increased confidence in the health of web applications through greater visibility into vulnerabilities

"When we needed additional credits for new domains, with our previous SSL vendor it could take days to get them published. With Trend Micro, all it takes is a simple email to the account team and it's done, which is significant for us."

Mark Dunkerley,
Messaging and domain
services team lead,
AHS Information Services



Solution

To find the right application security solution, AHS-IS initially focused on analyzing certificate authority vendors and considered analyst and peer recommendations. They selected Trend Micro Deep Security for Web Apps, which includes unlimited SSL certificates as well as application vulnerability detection and protection for a low, flat yearly fee.

Dunkerley says that his team at AHS-IS is looking forward to reducing the multiple vendors and their separate application security solutions with the centralized management provided by Deep Security for Web Apps. "The ability to track all of our SSLs and monitor them on one console will dramatically increase our IT productivity," said Dunkerley.

AHS-IS has started to leverage the solution's application and platform vulnerability scanning capabilities to increase the team's confidence in the security of their web applications. They are also planning to test and compare some of the protection capabilities like intrusion prevention and web application firewall (WAF) rule generation.

"Overall, we strive to be as proactive as possible with security," said Dunkerley. "Deep Security for Web Apps gives us greater visibility into our vulnerabilities and allows us to quickly address those issues and focus our IT efforts more efficiently."

To comply with regulations and protect patient information, AHS-IS needs to continually scan applications and platforms for vulnerabilities and mitigate those issues quickly. Deep Security for Web Apps meets those needs by continuously detecting vulnerabilities at the app and platform layer and automatically protects them with virtual patching of platform vulnerabilities or WAF rules.

The solution also removes distracting false positives found during web application scanning. "Trend Micro's vulnerability scanning solution provides a proactive solution instead of a reactive one," said Dunkerley. "It's important to protect both internal and external portals and comply with HIPAA regulations. Protecting personal health information for our patients is a very serious matter that demands our highest scrutiny."

Results

Trend Micro Deep Security for Web Apps simplified Adventist Health System's SSL purchases and delivered 70% in cost savings. AHS-IS no longer faces unnecessary and unpredictable purchase orders for SSLs thanks to the unlimited certificate model, including extended validation (EV) certificate capabilities found in Deep Security for Web Apps. "With Trend Micro's unlimited SSL model, we no longer have to worry about how many licenses we might need for an entire year, or scrutinize decisions about SSL because of the cost," said Dunkerley.

The Trend Micro solution also dramatically reduced the time AHS-IS had to wait for domain approvals. Prior to Trend Micro, AHS-IS would have to reach out to their different locations and collect paperwork in order to validate that they owned specific domains, a process that has taken up to two weeks in the past. "With Trend Micro, we've reduced our domain approval time from up to two weeks down to minutes," said Dunkerley.

Using Deep Security for Web Apps, AHS-IS can manage application security, including SSL certificates in a single, integrated web-based console. This eliminates unnecessary tasks and gives AHS-IS greater administrative access and flexibility. "The ability to manage multiple divisions under one account has given us significant cost savings," said Dunkerley.

With automated, continuous application and platform vulnerability scanning, and elimination of false positives, AHS-IS increased their confidence in the health of their web applications.

Dunkerley has also been impressed by the excellent customer support provided by Trend Micro throughout the entire implementation process. For example, Trend Micro detected an incorrectly issued 1024 bit SSL, and informed AHS-IS to help them resolve the issue the same day. "1024 bit SSLs were no longer going to be supported, so Trend Micro recommended we reissue it as a 2048 bit SSL. We quickly resolved what could have been an end-of-the-year problem," said Dunkerley.

Looking ahead, AHS-IS hopes to address mobile security issues and bring your own device (BYOD) trends, and to continue providing the best possible protection for its systems and patient information. "We look forward to working with Trend Micro to help solve challenges posed by consumerization and mobility," said Dunkerley.

“Trend Micro Deep Security for Web Apps gives us greater visibility into our vulnerabilities and allows us to quickly address those issues and focus our IT efforts more efficiently.”

Mark Dunkerley,
Messaging and domain services team lead,
AHS Information Services

“With the Trend Micro solution, we reduced our domain approval time from up to two weeks down to minutes.”

Mark Dunkerley,
Messaging and domain services team lead,
AHS Information Services