

Organization

Adventist Health

Industry

Healthcare

Location

Roseville, California, USA

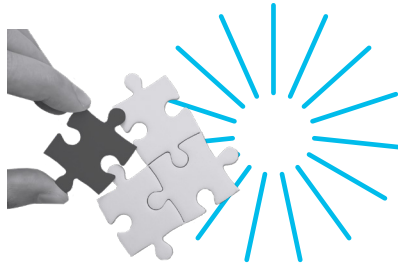
Employees

34,000 employees at more than
350 locations in four states

How a healthcare organization quickly consolidates multivendor firewalls to Cisco for streamlined management, consistent policies, and deep visibility across the environment

“Taking a comprehensive security approach with Cisco Security, including the integrated threat intelligence from Cisco Talos, keeps us up to date and enables us to detect emerging threats before we even know they’re an issue.”

–Ed Vanderpool, IT Technical Manager, Adventist Health



Objective

In a healthcare environment with 24 hospitals and more than 320 clinics across 80 communities, the complexity of the firewall infrastructure created inconsistent policy enforcement while making management time-consuming and inefficient. For Adventist Health's small team, the solution to simplifying firewall management while boosting the security posture was to standardize the firewall ecosystem.

Solutions

- [Cisco Secure Firewall](#)
- [Cisco Firewall Migration Tool](#)
- [Cisco Secure Network Analytics \(Stealthwatch\)](#)
- [Cisco Umbrella](#)
- [Cisco Identity Services Engine \(ISE\)](#)

Impact

- Simplified firewall management and streamlined maintenance while gaining threat protection with consistent network security policies, unified management, and deep visibility across all sites.
- Cisco's Firewall Migration Tool saved 144 hours (more than three weeks) during migrations at two sites, while minimizing downtime and eliminating the risk of human error.
- Improved ability to stop existing and future threats before they enter the environment.
- Implemented a comprehensive, integrated platform approach to security.

Simplifying firewall management and maintenance while securing networks and patient data across multiple environments and locations

Adventist Health, a faith-based nonprofit healthcare system, serves more than 80 communities on the West Coast and in Hawaii. The organization operates 24 hospitals and more than 320 clinics in four states, primarily in rural areas. Securing patient data and maintaining compliance are top priorities, but the hospital environment creates complexities, especially as the number of IoT devices proliferates.

“We need to make sure that data doesn’t leak out or go anywhere it shouldn’t be, and we need to have full control of our edge across the system, because we have many providers who need to access the internet directly at the edge,” explains Ed Vanderpool, IT technical manager at Adventist Health.

For many years, Adventist Health has successfully relied on Cisco Secure Firewall to defend its network against threats, prevent malware, detect intrusions, and control web traffic—not only protecting its infrastructure but also ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA). As the

organization grew and new locations expanded the firewall ecosystem, managing multiple vendors’ firewalls became time-consuming and inefficient for the small team and made policy enforcement inconsistent.

To simplify firewall management and maintenance while improving the consistency of policy controls, Adventist Health decided to consolidate vendors across all sites. After an extensive evaluation, the team again selected Cisco Secure Firewall.

“We chose Cisco, number one, because it’s the industry leader,” Vanderpool says. **“The Cisco solution overall had the most flexibility for deploying at the edge and at the data center. It was very manageable and our team didn’t have to learn something new.”**

After that decision, one challenge remained—transferring existing firewalls from Fortinet, Palo Alto, and Check Point to Cisco Secure Firewall, a process that would entail about 2,000 lines of code at each site. Manual migration would take as long as two weeks for each of the two hospital locations. But a migration tool that

Adventist Health used previously from another vendor created issues with the transfer of security policies. Vanderpool’s team needed a better firewall migration solution.

“We need to make sure that data doesn’t leak out or go anywhere it shouldn’t be.”

**Ed Vanderpool,
IT Technical Manager, Adventist Health**

Simplifying firewall migration and eliminating human error with Cisco Firewall Migration Tool

After discussing the challenge with the Cisco account team, Adventist Health decided to use the Cisco Firewall Migration Tool, which supports migration from Cisco Secure Firewall ASA and third-party firewall vendors to Cisco Secure Firewall Threat Defense solutions. Having performed manual migration before, Vanderpool knew that eliminating human error was especially critical when transferring existing security policies. **“Those errors could cause applications and other things to stop working, which has direct patient impact. For example, if you didn’t properly migrate the setup or made a mistake in coding, a blood pump wouldn’t work properly,”** he explains. **“The Cisco Firewall Migration Tool catches a lot of errors that we probably wouldn’t have caught if we were doing it manually.”**

With the Cisco Firewall Migration Tool, Adventist Health migrated each site in a day, saving as many as 144 hours (more than three weeks) total for the

two locations. **“The firewall migration speed was very fast and the complexity was cut by more than half,”** Vanderpool says. Using the tool, Vanderpool adds, made the process smooth and gave the team confidence they didn’t miss anything.

As the organization acquires new hospitals and clinics in the future, Adventist Health plans to continue standardizing with Cisco Secure Firewall Firepower 1000 Series, 2100 Series, or 4100 Series, depending on each location’s needs, and will use the Cisco Firewall Migration Tool to automate the process. **“My teams all know Cisco very well, and we’re all certified in Cisco,”** Vanderpool says. **“Standardizing on Cisco Secure Firewall makes it much easier to set up, implement, and maintain firewalls day-to-day without having to relearn a whole new product that may not integrate well into our overall strategy, monitoring, and maintenance.”**




Comprehensive security that meets existing and future needs

By deploying Cisco Secure Firewall, Adventist Health has simplified firewall management, streamlined maintenance, and boosted threat protection with consistent network security policies, unified management, and deep visibility across all sites. **“We have a very strong Cisco footprint and it’s something that we’ve been able to rely on and has taken very good care of us overall,”** Vanderpool says. **“And moving off a potentially outdated firewall product or a product that may have certain holes in it—and having a firewall migration tool to pull that information off, clean it up, and feed it into our Cisco infrastructure—has prevented security issues, guaranteed.”**

Consolidating firewall vendors also resulted in operational efficiencies. **“We have a consistent architecture from edge to edge—from our hospitals and other sites—all the way through our data center platform,”** Vanderpool says. **“We have consistency and standardization, and we need less staff overhead to maintain our firewalls. And our downtimes are pretty low.”**

Adventist Health recognized the importance of implementing a security platform that can meet existing and future needs. Cisco provides an integrated security platform that makes threat detection, protection, and response effective and scalable. Cisco security solutions also help to ensure that the organization remains HIPAA compliant. In addition to Cisco Secure Firewall, Adventist Health has implemented Cisco Identity Services Engine (ISE), Cisco Umbrella, and Cisco Secure Network Analytics (Stealthwatch). These solutions are underpinned by Cisco Talos, which provides industry-leading visibility, actionable intelligence, and vulnerability research to drive rapid detection and protection against known and emerging threats. **“Taking a comprehensive security approach with Cisco Security, including the integrated threat intelligence from Cisco Talos, keeps us up to date and enables us to detect emerging threats before we even know they’re an issue,”** Vanderpool says.

Vanderpool also looks forward to implementing Cisco SecureX, a cloud-native, built-in platform experience



that connects the Cisco Secure portfolio and the existing infrastructure. SecureX is integrated and open for simplicity, is unified in one location for visibility, and maximizes operational efficiency with automated workflows. **“The Cisco security platform will streamline the work for our small team and make security more efficient and effective—so we can actually focus on things that we may need to improve or keep an eye on,”** Vanderpool says. **“Moving toward an integrated, comprehensive platform with Cisco makes sure that we are truly secure, no matter if it’s at a local site or in the cloud.”**

Ultimately, the close partnership with Cisco helps Adventist Health carry out its mission to not only serve patients but also make sure they’re safe and their data is secure. Vanderpool concludes, **“The bottom line is, thus far we have not been hacked, so that’s probably the biggest indication that Cisco security is working.”**