

Case Study

[SECURITY](#) > [NETWORK SECURITY](#)

How Wisconsin Center Took Control of Wi-Fi Network Security

The Wisconsin Center faced a mammoth Wi-Fi network security challenge for its three event locations. Learn how the organization's IT pros overhauled the network.

[Karen D. Schwartz](#) | Jul 14, 2022



Within two weeks of starting his job as the Wisconsin Center vice president of IT, Steve Totzke got a taste of what would become his biggest challenge. A few observant members of the IT staff's security team noticed that some systems weren't operating properly and correctly suspected a [ransomware attack](#). It was a lucky break, giving time for Totzke to respond. The team severed the infected system from the rest of the network before the ransomware had a chance to spread.

That experience quickly drove home the importance of hardening the organization's network -- a mammoth undertaking given that the organization manages three event locations: the Miller High Life Theater, which has a capacity of 4,100 people; the 10,000-seat UW-Milwaukee Panther Arena; and the Wisconsin Center itself, which houses a grand ballroom and convention center.

related: [How Kroger Consolidated Its ITM Tools](#)

Together with newly hired network operations manager Sean Colburn, Totzke examined the organization's [network security](#) from top to bottom. Totzke and Colburn found plenty of areas that needed improvement, especially for its public and private Wi-Fi networks. It was an important job, since the Wisconsin Center ultimately aimed to provide full Wi-Fi access and functionality for employees, customers, and vendors in its three venues.

“We encountered a situation where we needed to pretty much hit the reset button,” Colburn said. “It was a very immature network setup that had been developed years before and hadn't really been upgraded. For example, even though the network was segmented into vLANs, it didn't have the proper network security to block traffic from being able to see ... across those vLANs.”



Wisconsin Center, Convention and Exhibition Center, in Downtown Milwaukee

Connectivity is extremely important for event management. For example, employees benefit from the ability to connect wirelessly on one floor and print documents on another floor. But the most critical wireless connections were for customers attending events and for point-of-sale (POS) systems. While the venues had public and private Wi-Fi at the time, Colburn said the Wi-Fi networks lacked proper management and strong security features.

In fact, the situation was so tenuous that POS systems, designed to be connected via Wi-Fi, were still

It was also challenging to meet the wireless security needs in multiple facilities. For instance, supporting a large company's week-long annual meeting with concurrent theater and [sporting events](#) could be a "network security nightmare," Colburn noted. "Both Wi-Fi and wired security have to be solid for our clients to avoid the pain of an unsecured, unstable network," he added.

And it wasn't just customers who were feeling the pain. Event production staff needed to connect to the Wi-Fi to use communication systems. For example, the Ticketmaster system that allows attendees to enter a venue requires secure connectivity to the Wi-Fi network, as do vendors selling merchandise.

Improving Wi-Fi Network Security

The project's first step was to identify how connections were developed, maintained, and secured in the current system. The team would then determine the available security protocols and Payment Card Industry compliance requirements.

Slowly, Totzke and Colburn combed through every area of network security, established what needed to be upgraded, and then replaced and added technology. They made an early decision to bring security in house. Before they joined Wisconsin Center, the original IT team relied on external professional services.

Next, Totzke and Colburn upgraded an aging Palo Alto firewall and added Palo Alto's WildFire malware analysis engine. They then reworked the switching network's Layer 3 routing and added the Paessler PRTG network monitoring tool to screen end-user devices connected to access points. With the Paessler tool, an access point could continue functioning even if network visibility to the access point was lost but still had a path to the internet.

The most significant decision the team made was to make better use of ExtremeCloud IQ, a cloud-based network management tool it inherited when [Extreme Networks](#) acquired Aerohive's technology. The original Aerohive product, as well as ExtremeCloud IQ, is controller-less, which means that the brains are in the access points instead of a controller.

While the Wisconsin Center had already purchased Aerohive technology, it wasn't being used effectively. For example, Aerohive's HiveManager provided location-based analytics -- the ability to map access points to end-user devices. Colburn wanted to take advantage of these types of capabilities already available to them.

More effective [security analytics](#) also helped the IT team keep things under control. The analytics functions that Aerohive, and now ExtremeCloud IP, provide has allowed the IT team to dramatically step up its game. The analytics function can provide a 90-day snapshot into a specific device's activity, which access points it used, and more.

And because ExtremeCloud IQ makes it easy to program service set identifiers (SSIDs), it was also a good time for the Wisconsin Center to move toward [6G](#). "If you're going to buy an access point that can do 4G, 5G, and 6G, why wouldn't you do that?" Colburn said. "We probably won't be using 6G for two or three years, but this allows us to move forward and start segregating technology based on radio frequency, which is something the cellphone and PCS industry has been doing since the early '80s." Until that time comes, the IT team can use ExtremeCloud IQ to program SSIDs in whatever frequency is required.

Wi-Fi Network Security Today

Wi-Fi throughout the three facilities now runs smoothly, and security is no longer as much of a concern. The Wi-Fi network currently accommodates multiple SSIDs with different authentication mechanisms across different buildings. For example, the IT staff provides each merchandise vendor in a venue with a password unique to just that device. The device then connects to a VLAN configured for that type of transaction. All network facilities are controlled through the same platform, optimizing efficiency and allowing each venue to tailor its network to meet the specific needs of customers.

The IT team has some major successes to show for its work. For example, during Michelle Obama's tour of her memoir, the Miller High Life Theater provided attendees with free WiFi. In addition, attendees could post Tweets and Instagram posts live to a digital backboard. Merchandisers at the venue had no problems selling books.

In addition, the Wisconsin Center hosted events like the virtual 2020 Democratic National Convention without any security issues.

But the team isn't finished yet. Next up is the installation of Ekahau technology for developing Wi-Fi designs and optimizing Wi-Fi networks. The team also plans to invite [ethical hackers](#) to try to infiltrate their networks. "We're going to build a network that's not only secure but will be one of the best Wi-Fi experiences an eventgoer can have outside of their home," Colburn said.



Karen D. Schwartz is a technology and business writer with more than 20 years of experience. She has written on a broad range of technology topics for publications including CIO, InformationWeek, GCN, FCW, FedTech, BizTech, eWeek and Government Executive.

TAGS: [SECURITY ANALYTICS](#)

0 COMMENTS

RECOMMENDED READING

Metaverse Jobs Are Disappearing as Hiring Slows at Google, Facebook

AWS Reinforces Cloud Security Efforts at re:Inforce 2022

Cloud Computing Sustainability: How Green Is the Cloud?

US Investigating ‘Significant’ Breach of American Court System



Follow us:



© 2022 Informa USA, Inc., All rights reserved

[Privacy Policy](#) | [Cookie Policy](#) | [Terms of Use](#)