FORTINET

CASE STUDY

Fortinet Makes Security Best Practices a Reality for a City

Centerville, Ohio, combines the ethos of small-town Americana with proximity to larger cities. A suburb of Dayton, Centerville is situated right off of two major highways, with quick access to the Wright-Patterson Air Force Base. The community of nearly 25,000 prides itself on its parks and schools.

For Ryan Collins, IT Director for the City of Centerville, one key to maintaining the community's idyllic image is to shield it from cyberthreats, which are an ever-present fact of life for municipal governments, as for most other types of organizations. "As a city, we maintain records, and we need to hold some of those records for several years," Collins says. "Our biggest security concerns involve protecting all that data and preventing cyberattacks that would cause downtime of city systems."

Collins' team is responsible for the networking and IT infrastructure of every city function, including the municipal police department and the police dispatch team, which handles emergency calls for both Centerville and a neighboring community. "Our dispatch center must be available 24×7×365," Collins says. The city has a process for transferring duties to another organization in the event of a prolonged outage, but "if the systems supporting dispatch went down, even briefly, that would make it very tricky for police officers to do traffic stops. Background checks and other activities could not happen if the systems were down, which could create risk for officers and the community. That is why we follow best practices in everything we do."

Looking to Secure the City's Cyber Defenses

A few years ago, before Collins joined the team, the city was using what he calls a "hodgepodge" of networking and security equipment. "They had devices from several different vendors, some of which were 20 years old," he says. "There was no redundancy in place, and city leaders had little confidence in the stability or resilience of the network.

"A lot of nearby communities had been hit with cyberattacks, and the city did not want to face that situation," he continues. "Centerville wants to be in the forefront of innovation, not a follower." When Centerville hired a new city manager, "everyone took a good, hard look at our cybersecurity posture and said, 'This is not where we should be.'"

City leaders wanted to make a dramatic change and to do so quickly. "They also wanted to do things the right way," Collins explains, "so they reached out to Secure Cyber Defense and brought in Fortinet products."

Secure Cyber Defense is a Dayton-based managed security service provider (MSSP) that provides consulting, design, build, and implementation for clients' security environments. The City of Centerville engaged the firm to perform a holistic

"Having different solutions that do not communicate reduces your ability to automate and to gain single-pane-of-glass management. But with a single company solution, everything works together seamlessly."

Ryan Collins
IT Director
City of Centerville

Details

Customer: City of Centerville

Industry: Government

Location: Centerville, Ohio

Business Impact

- Fewer security issues than comparable neighboring municipalities
- Lower total cost of ownership (TCO) for security infrastructure
- Almost 100% uptime for municipal network, with no reduction in performance
- City positioned as a model city in cybersecurity

assessment of its network and security environment, identifying issues that could lead to vulnerabilities and establishing a plan to resolve those problems. Central to that plan were FortiGate Next-Generation Firewalls (NGFWs) and FortiSwitch secure enterprise switches, which integrate into the Fortinet Security Fabric as an extension of the FortiGate NGFWs.

"We re-architected the City of Centerville's technology infrastructure to build a 21st-century network that is able to defend itself," says Shawn Waldman, CEO and founder of Secure Cyber Defense. "Our MSSP service weaves together Fortinet solutions so the customer does not have to think about the Fortinet Security Fabric. We roll out predesigned integrations and capabilities, all of which rely on Fortinet."

Collins agrees that Centerville particularly likes a single-pane-of-glass visibility like what the Fortinet architecture offers with FortiManager and the reliability of Fortinet solutions.

Redundant Network Security, Monitored 24×7×365

Secure Cyber Defense implemented a high-availability pair of FortiGate NGFWs and a high-availability pair of core FortiSwitch switches in the city's data center. Centerville also deployed the FortiEDR endpoint detection and response solution on every city endpoint and integrated it with its NGFWs to automatically block IP addresses found in malicious events without ever having to file a ticket to do so. Now, the MSSP is also rolling out pairs of FortiSwitches in the city's other five locations.

"By the end of the year, all the city's switches will be Fortinet," Collins explains.

"Our municipal buildings are connected by a fiber ring, and we have built around 20 different VLANs [virtual local area networks]. We have segmented out the wireless network, wired phones, and all the different departments and locations, and enabling security down to the port level. This helps ensure that any threat that might get into our network will stay isolated."

Secure Cyber Defense manages the environment day to day using the FortiManager platform. The City of Centerville also uses Secure Cyber Defense's Managed SOC (security operations center) service for response to security alerts and extended threat detection and response (XDR). Secure Cyber Defense leverages the FortiSOAR security orchestration, automation, and response solution to automate the monitoring and investigation of workloads within its managed SOC.

Solutions

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiEDR
- FortiManager
- FortiSOAR
- FortiClient
- FortiToken

Services

- FortiGuard Enterprise Protection Bundle

"We rely heavily on our partners to alert us when something needs our attention. We can spend less time chasing our tails on things that are not actually threats because we know that our partners are going to do what they need to do to secure our network."

Ryan Collins
IT Director
City of Centerville

"We manage endpoints 24×7, and we also do predictive and proactive threat detection and response," Waldman reports. "FortiSOAR is our core case management system and our automation platform. The City of Centerville has access to more than 250 preconfigured playbooks and other proprietary automation scripts we have written to detect and respond to threats in real time."

The FortiSOAR platform and Secure Cyber Defense's Managed XDR service tie into the FortiGuard Enterprise Protection Bundle, which the City of Centerville added to each of its NGFWs. "We use all the features of the FortiGuard Enterprise Protection Bundle," Waldman says. "They integrate into our SOAR and XDR platforms. For example, the IPS [intrusion prevention system] capabilities provide a trigger point for our automation scripts. If an inbound or outbound threat trips an IPS signature, the city's XDR system automatically blocks that IP address, and the SOAR adds it to the block list for our entire customer base."

Introducing a VPN with MFA

The City of Centerville deployed the FortiClient solution on remote endpoints with the FortiToken platform for multi-factor authentication (MFA) to facilitate secure remote connectivity. "At one point in the not-too-distant past, the city did not have any VPN [virtual private network] access," Collins says. "One of the biggest concerns for city leaders was the possibility of VPN compromise."

By contrast, he adds, “the team wanted to use products with the MFA ability. We have not encountered any difficulties from end users regarding multifactor authentication being cumbersome or confusing. The experience has made it easier for us to implement the Microsoft MFA for our Office environment.”

Partners That Do What They Need to Do

For Collins, the best indicator of security efficacy for the new architecture is that the City of Centerville experiences security issues much less frequently than the surrounding communities. Although he relies on Secure Cyber Defense for hands-on security management, Collins remains engaged with what is happening in the environment.

“I review the reports from Secure Cyber to see whether there is anything we need to address, and I look at the firewalls and switches often,” he explains. “Sometimes I may log in to the firewalls just to find a device that I need to troubleshoot.”

Through all his workloads, Collins is more efficient because he can access network and security information in one place. “I do not have to log in to multiple solutions, in different locations, to troubleshoot or solve problems.”

In the past, Collins has worked with products that were not tightly integrated. “A vendor providing different solutions that work well together is, hands down, preferable to having switches from one vendor, firewalls from another vendor, and other security systems from still others,” he says.“Having different solutions that do not communicate reduces your ability to automate and to gain single-pane-of-glass management. Everything works together seamlessly. You can create rules to automatically quarantine devices or ports, and they carry from one solution to another.”

This type of efficiency is crucial for every organization that runs a lean security team, including many municipal governments. “As a fairly small city, we do not have a huge IT staff,” Collins says. “That means we have to be efficient. We rely on our partners to alert us when something needs our attention. That frees up our time to respond to help desk tickets or do strategic planning or project management. We can spend less time chasing our tails on things that are not actually threats because we know that our partners are going to do what they need to do to secure our network.”

Best Practices Recommended by Industry Experts

Even better, the Fortinet infrastructure has reduced the cost of security management for Collins and his team. “In my experience, anytime I can create a single pane of glass using products from the same vendor, that becomes not only a better solution but also a lower-cost solution,” he says. “If nothing else, trying to piece together a hodgepodge of products from different vendors to do the same things requires more effort, and time is money.

“Not only will a diverse infrastructure require you to hire people with expertise in each of the different systems, but managing an assortment of solutions will take more time for the staff you have,” he adds. “If you look at how much an hour of my day is worth, and you consider that I am not having to log in to four or five different systems on a daily basis, it is clear that a one company solution lowers the total cost of ownership of our network and security infrastructure.”

The Fortinet solutions have proven highly reliable, as well. “Our switches and firewalls are stacked for redundancy,” Collins relays. “As a result, we have had almost 100% uptime.” Performance has also been solid. “I have not seen or heard about any slowness or degradation of services on the network. The performance is as reliable as the security.”

He adds, “As IT director, I look for peace of mind knowing that a product is going to work. I look for companies that are able to help resolve an issue. We would not have to deal with finger-pointing; the issue would be taken care of quickly.”

Working with Fortinet and Secure Cyber Defense, the City of Centerville continues to improve its security environment. The city is looking to add FortiAP access points throughout its municipal buildings and several parks.

“We are always evolving our infrastructure,” Collins says. “We want to be a model city, and by using industry proven solutions, we know we are doing things the way we should. We are not just going through the motions to say we have cybersecurity; we are implementing best practices recommended to us by experts in the industry.”

FORTINET

www.fortinet.com

December 9, 2023 12:53 AM

2405406-0-0-EN