FERTINET

CASE STUDY

Fortinet Security Fabric Protecting Critical Public Services and Complying with Utility Industry Standards

Nestled in the heart of Missouri, the City of Columbia supports a population of approximately 150,000 residents. Nicknamed the "Athens of Missouri" for its stunning neoclassical architecture, the city is home to the University of Missouri and its popular Missouri Tigers football and basketball teams.

Securing the City Administration

The city administration is responsible for various services to manage the city and support its residents. These include public safety, public works, urban planning, parks and recreation, and public transportation services. The administration also provides essential utilities, including water supply, sewage treatment, and electricity.

As John Maier, senior network engineer at the City of Columbia, explains, its role as a utility has a major impact on the city's cybersecurity posture: "We must ensure our cybersecurity controls are sufficient to meet a wide range of guidelines and regulations, not least the NERC standards, which in part mandates stringent cybersecurity standards for utility companies. NERC audits us regularly, and a significant portion of my job is ensuring that our networking and security infrastructure makes the grade."

Protecting the Public

Beyond compliance, robust cybersecurity controls are also critical to ensuring public safety. For instance, as a water utility, the city is responsible for providing a safe, uninterrupted supply of potable water to Columbia's residents. The city uses advanced supervisory control and data acquisition (SCADA) systems to monitor and control water treatment and distribution. Protecting these systems from threat actors is an essential part of ensuring resiliency.

Across all its utility operations, a complicating factor is that the city works with a wide range of vendors. It therefore needs a networking model that ensures resources and data can only be accessed by authorized people. As Maier puts it: "We need visibility into who is accessing our network, what they are accessing, and how they have gained entry. We cannot afford any unauthorized access to systems that support critical services."

Another major consideration from a cybersecurity perspective is the city's responsibility to secure its citizens' sensitive data. "We have internal databases and servers containing information that is highly tempting to criminals, such as residents' financial information," says Maier. "We need to ensure that this data is protected and that it is not easily accessible to unauthorized parties."

city of Columbia

"There is nothing worse than having a one-off solution that you have to shoehorn into your system to make it work. Fortinet products integrate seamlessly with other Fortinet devices and with security tools from other vendors. This is a clear differentiator for Fortinet—it has only been concerned about one thing: creating a solution that meets our needs and is easy to use."

John Maier
Senior Network Engineer
City of Columbia

Details

Customer: City of Columbia
Industry: Government
Location: Missouri, United States

Business Impact

- Ability to comply with North American Electric Reliability Corporation (NERC) electricity industry standards

- Enhanced protection of residents' data

A Growing Fortinet Security Fabric

The City of Columbia has partnered with Fortinet for over a decade to meet its security needs. The relationship started when the city replaced its legacy firewall solution, which was no longer fit for purpose, with FortiGate Next-Generation Firewalls (NGFWs). "The relationship with Fortinet has advanced greatly under my watch," says Maier. "Over the past six years, we have steadily ramped up our security controls, focusing on enhancing remote access, endpoint security, and network visibility. Fortinet has been front and center on this journey."

Today, the City of Columbia uses FortiGate NGFWs to provide edge security across a citywide dark fiber network. The FortiGate devices are also used for failover in high-availability pairs and for network segmentation to separate the networks that serve its various city functions. Network segmentation through the FortiGate NGFWs enables the city to control who has access to which areas of the network.

The city benefits from further security controls through a FortiWeb web application firewall, which defends its website against common security threats, DDoS attacks, and malicious bot attacks.

Meanwhile, the city uses the FortiClient Endpoint Management Server (EMS) for the robust protection and streamlined management of endpoints. FortiClient EMS provides visibility across the network so the city can monitor unauthorized activity and potential threats. "We have fully implemented FortiClient EMS, and it is now integral to our process for network access," says Maier.

Finally, the city has deployed FortiAnalyzer for log management, analytics, and reporting, and is leveraging training services provided by the Fortinet Training Institute to ensure its security team can get the most out of its Fortinet Security Fabric deployment.

Automating for Better Defense

Before Fortinet, the City of Columbia used an unnecessarily complex system to block unauthorized access to network resources. The city can now rely on a 100% automated process with the Fortinet Security Fabric. "With Fortinet, we know that only people with the right authorization and legitimate needs can now access cyber assets. It is a smooth process that, thanks to FortiAnalyzer, is trackable as we check the logs to review who has been accessing the network," says Maier. The city can better protect its sensitive utility systems thanks to Fortinet, thereby increasing public safety and ensuring the resilience of critical services.

Automation has also proved beneficial from a compliance perspective. As Maier explains: "One of the regulations in our city states that all network users must be based in North America. In one case, a vendor was using subcontractors based abroad. The system blocked subcontractor access, and we were immediately alerted to the incident. We were then able to take this up with the vendor as it was a breach of their contract with us."

A Proactive Defense Posture

Meanwhile, FortiClient EMS assists Maier and his team with internal security audits. Every week, the security team pulls information from FortiClient EMS to see if any endpoints have updates or patches pending. Armed with this information, the team can proactively contact users to turn on their devices, enabling the updates to occur. "With FortiClient EMS, we can work with business stakeholders to ensure that their devices are ready for use the moment they are needed," adds Maier.

Business Impact (cont.)

- Increased resiliency of public services
- Increased uptime of endpoints and improved productivity

Solutions

- FortiGate Next-Generation Firewall
- FortiClient Endpoint Management Server
- FortiAnalyzer
- FortiWeb

Services

- Fortinet Training Institute

"FortiClient EMS was one of the best moves I ever made. Thanks to the solution, we can adapt quickly as regulations change by implementing new features and deploying them across all devices automatically. Meanwhile, the auto-connect feature has reduced our risk levels, as there is no way users can directly access the internet—they have to go through the VPN with our full suite of controls."

John Maier
Senior Network Engineer
City of Columbia

The range of Fortinet form factors is another key benefit for the City of Columbia. As Maier explains: "We fuel city vehicles such as buses and trash trucks with compressed natural gas. When drivers fill up their vehicles, they use keycards. However, the fuel station is the one facility we do not have a fiber connection to. Given that the location is out in the open and vulnerable to harsh weather conditions, we use a ruggedized FortiGate NGFW, which sits in front of a VPN back to the city. It is great that Fortinet has the flexibility to meet such specific needs."

Strengthening Remote Access

The FortiClient EMS has been a game-changing solution for the City of Columbia. Maier was already looking at how FortiClient EMS could help strengthen its VPN-based approach to remote working by making connecting easier for users when the COVID-19 pandemic arrived. The pandemic accelerated the city's plans, and FortiClient EMS was deployed across its operations. "Fortinet was a huge help during this period," says Maier, "helping us to deploy as quickly as possible during what was a highly turbulent time."

Now, every endpoint is protected and managed with FortiClient EMS, which automatically connects remote devices to the VPN, providing a user-friendly and secure approach to remote working that reduces the support burden on the security team.

"FortiClient EMS was one of the best moves I ever made," comments Maier. "Thanks to the solution, we can adapt quickly as regulations change by implementing new features and deploying them across all devices automatically. Meanwhile, the auto-connect feature has reduced our risk levels, as there is no way users can directly access the internet—they have to go through the VPN with our full suite of controls."

Protecting the City's Website

Another area that the city needs to protect is its website, which, among other things, is used by residents to pay their utility bills. While payment processing is conducted by a third party on a separate site, the processor needs access to information concerning the utility user. FortiWeb ensures that this process is secure and that no data is accessed or exfiltrated by unauthorized parties.

In addition, the city uses FortiWeb as a buffer between its servers and the internet, further increasing its defensive capability. "This is a big advantage," says Maier. "If you look at our logs with FortiAnalyzer, we are under a constant barrage of scanning and attempts at hacking the website. FortiWeb is a valuable tool in combating those threats."

The data provided by FortiAnalyzer enables the city to take mitigating actions in other ways. Recently, FortiAnalyzer revealed that the city was being targeted with a DDoS attack. It was therefore able to act before the attack affected its website.

Seamless Integration

More broadly, the City of Columbia appreciates the high level of integration that comes with the Fortinet Security Fabric. As Maier puts it: "There is nothing worse than having a one-off solution that you have to shoehorn into your system to make it work. Fortinet products integrate seamlessly with other Fortinet devices and security tools from other vendors. This is a clear differentiator for Fortinet—it has only been concerned about one thing: creating a solution that meets our needs and is easy to use."

Maier sees the city's relationship with Fortinet extending further, particularly with zero-trust network access, further leveraging FortiClient EMS, and potentially deploying FortiAuthenticator. "One thing is for certain," concludes Maier, "Fortinet will continue to provide the tools we need to protect our systems, meet our compliance obligations, and keep vital public services up and running for Columbia's residents."

F⊡RTINET

www.fortinet.com