CASE STUDY

U.S. City Secures and Segments Departments and IT-OT Environments with Fortinet

One small, yet fast-growing Southeastern U.S. city is best known for its thriving university. But what makes the city unique from other municipalities and local governments is that, in addition to public services including police, fire, animal control, transport, and parks management, the city council also operates the town's utilities. This includes electricity and wastewater services. “The approach works well for our citizens,” explains the city’s IT Director, “as they only need to go to one place to set up and manage all their utilities.”

Securing Local Government

When it comes to cybersecurity, many of the challenges faced by the city are familiar to other city councils and municipalities across the U.S. These include protecting the personal data of citizens and putting in place mitigations to counter ransomware attacks.

However, as the city is also a utility operator, it has a higher risk profile than other municipalities. “As a utility provider, we need to be ready for threat actors linked to nation-states looking to take down the power supply,” says the IT Director. “Our security system needs to be able to protect operational technology every bit as well as our enterprise IT infrastructure. We are also alert to threats that come with IT-OT convergence, where poorly secured OT devices become a gateway into the corporate network for criminals.”

In the past, the city’s fragmented approach to networking, whereby every department operated its own systems, held back the effectiveness of security efforts. “The approach was costly, as it led to unnecessary duplication,” adds the IT Director, “and it also meant we could not achieve complete visibility right across the city’s network.”

Leveraging the Fortinet Security Fabric

Today, the city secures its systems using FortiGate Next-Generation Firewalls (NGFWs) to protect the network edge. In addition, the city has deployed FortiGates for internal segmentation to operate a unified network architecture that is securely partitioned for each department or site. The IT Director says: “We run virtual servers with those servicing the needs of one department sharing a hypervisor with those servicing another. The FortiGates allow us to logically separate these out with ease.”

The city also uses the FortiGate devices to create a security barrier between the city’s OT and IT systems environments. “In the digital age, air gapping OT is no longer an option but protecting them with a robust NGFW gives us the security we need,” says the IT Director.
Also, the city is starting to leverage other elements of the Fortinet Security Fabric, including FortiAPs for secure wireless access, FortiSwitch secure Ethernet switches, FortiNAC for network access control, and FortiAnalyzer for analytics-driven security management. The city also uses FortiAuthenticator for user identity management and remote sign-on and the FortiMail secure email gateway for email protection.

**Cost-Effective Segmentation**

The key benefit of the Fortinet Security Fabric is that it enables the city's network team to segment and secure the network cost effectively. The IT Specialist comments: "If we were to use completely air-gapped local area networks for our departments and facilities, we would need to deploy a set of servers for every department. Thanks to the FortiGate NGFWs, we can ensure that all traffic is logically separated, and we can save money by not having to buy multiple hardware sets."

**Protecting City Systems**

The Fortinet Security Fabric is also helping the city keep on top of emerging threats. As an operator of critical infrastructure, the IT Director and his team receive alerts and updates from the FBI and the Department of Homeland Security around threats to OT. The city’s IT Specialist comments: “Using the intrusion prevention capabilities of the FortiGates, we can quickly add policies based on new intelligence to ensure that any new attacks can be picked up and blocked by the system.”

The city’s IT Specialist is particularly appreciative of the broad range of features that come standard with Fortinet solutions. “Take the FortiGates,” he says, “a lot of important features are built into the solution, such as secure sockets layer virtual private network capabilities, so we do not need to pay for additional devices or licensing, and that allows us to provide city employees remote working options.”

**Enhancing Visibility and Control**

Both the IT Director and IT Specialist were keen to point out the increased visibility of its network, users, and devices it has achieved through the Fortinet solutions. “Just seeing one report from the IPS makes the whole system worth it,” says the IT Specialist. “We get complete insight into what is hitting our ports and web servers, which provides us the information we need to secure our infrastructure.”

The deep packet inspection (DPI) provided by the FortiGate NGFWs also allows the IT Director and his team to review all traffic flowing from employee devices to the internet. This visibility enables the network team to better enforce security policies and ensure employees are only using applications that the team has approved for work use.

**Closing Down Threats**

“On the one hand, we are trying to be as secure as possible; on the other, we have to let people do their jobs. The FortiGates provide us with the granular control to do that,” says the IT Director. Using the FortiGate NGFWs, the Director and his team can create custom policies to manage traffic coming into the network, ensuring employees can access the information and applications they need to do their jobs without putting the city at risk.

With the FortiAnalyzer and FortiNAC, the city’s network team can also quickly identify the location of devices on its network in the event of possible security incidents. “If we receive a notification of a compromised workstation or other device, we can quickly find all the information we need on a single-pane-of-glass dashboard and see where the device is currently connected,” adds the IT Specialist. “When deployed in full, FortiNAC will augment this capability with automatic enforcement and dynamic policy control.”
Seamless Network Access

With the Fortinet Security Fabric in place, city workers can now access corporate resources remotely. The FortiAuthenticator allows users to log into their remote desktop using two-factor authentication. The process is seamless and has won over the workforce. “Before Fortinet, everyone had to remember a second set of credentials to log on remotely,” explains the IT Specialist. “Now they can get in using their Windows login credentials, which is a much preferable approach.”

The FortiAPs are also benefiting the city. While 17 access points have just been deployed, the IT Specialist says the city already has plans to order more: “They are honestly the most plug-and-play solutions I have ever used for an access point system,” he says.

Cost and Time Efficiencies

The centralized approach enabled by Fortinet is saving the city’s network team considerable amounts of time and money. The FortiGate platform means that the team need only manage one network infrastructure across the city’s 20 departments and 20 locations and across both IT and OT systems. “If each department ran on its own network, the management overheads would be significant,” says the IT Director. “And with only five of us on the team, we would not have time to manage all the components that would be required.”

Thanks to Fortinet, the city operates just one set of high-performance, resilient systems. “We never get help desk tickets,” explains the IT Specialist. “Fortinet’s technology just works for our users. And where we have come across issues during deployment, Fortinet has worked as a true partner to our city, helping us come up with solutions and working hard to ensure the best possible outcomes.”

Future Plans

Given its positive experience with the Fortinet Security Fabric, the city is planning to build on its existing investments. Plans include activating the Fortinet Secure SD-WAN capability and implementing FortiSIEM in its OT environment. The city is also considering deploying FortiMonitor to gain insights into the real-time status of network devices to help ensure the user experience is optimal.

“Fortinet brings us a huge degree of integration and usability,” concludes the city’s IT Director. “And for that reason alone, we will always consider it for our future needs.”