CASE STUDY

County Government Agency Increases Visibility and Control of Entire Infrastructure

The Information Security (IS) team for Salt Lake County, Utah, supports up to 6,500 end-users across a variety of locations and business types. A team of only seven is responsible for maintaining security and managing user access for services and businesses across the entire county—including Salt Lake City.

Replacing End-of-Life Legacy Hardware

About ten years ago, Salt Lake County first started working with Fortinet after existing security appliances from another vendor started having problems toward their end of life. They opened a request for proposals (RFP) to evaluate competing solutions. While price was a factor, they wanted physical next-generation firewalls (NGFWs) that could deliver ample performance and features for their needs at the time—which included protecting two internet feeds and two extranet partner feeds. Additionally, they knew they would need to scale their capabilities for growth in the near future.

They initially chose FortiGate 600-series NGFWs for three different clusters to protect county networks. "Fortinet was miles ahead of everyone else in terms of ability and performance. That's what impressed us. And I think Fortinet still outdoes everybody else when it comes to performance," says Salt Lake County's director of information security. This included the ability to perform deep packet inspections for encrypted traffic. Before working with Fortinet, the Salt Lake County IS team had spent several years unsuccessfully trying to implement inspection without bottlenecking network traffic.

Changing Times and Growing Networks

Over the next decade, Salt Lake County would add more FortiGates to protect additional parts of the county's infrastructure. Their current firewall deployments have scaled to 55 FortiGate NGFWs. One key reason for that expansion had to do with the growing number of county employees that needed a secure connection to the official network from home or in remote locations.

During the initial RFP, Salt Lake County was using another vendor's solution for virtual private networking (VPN). When that vendor went out of business, they found themselves in need of a replacement. As Salt Lake County's director of information security explains, "Rather than buy somebody else's VPN, we just looked to our existing FortiGates. They

SALT LAKE COUNTY

"Fortinet was miles ahead of everyone else in terms of ability and performance. That's what impressed us. And I think Fortinet still outdoes everybody else when it comes to performance."

– *Salt Lake County's Director of Information Security*

Details

Customer: Salt Lake County

Industry: Government

Location: Utah

Business Impact

- Enables network segmentation for PCI compliance via high-performance NGFW protection across distributed county-owned locations
- Provides secure remote login for county employees via robust virtual private network (VPN) and multi-factor authentication (MFA) capabilities
- Enabled cost-effective endpoint protection across all laptops, desktops, and servers—including antivirus (AV) and off-network filtering
- Simplified operations by centralizing network management and compliance reporting

were already licensed for VPN, we just hadn't been using it. So really, it cost us nothing to change. And it saved us whatever the going rate would have been for a couple of VPN concentrators from someone else."

Beyond perimeter protection and VPN access for employees, Salt Lake County also uses their FortiGates for WAN connections at remote sites, isolation of networks, and segmentation of PCI devices (e.g., point-of-sale [POS] terminals). They have also added other Fortinet security solutions to help complement specific security use-case needs.

Multi-factor Authentication (MFA)

In addition to FortiGate's built-in VPN capabilities, the Salt Lake County IS team is also using FortiAuthenticator to add multi-factor authentication (MFA) capabilities to employee access for added security. One of the many things the county uses MFA for is timecard submissions across as many as 6,500 full- and part-time employees via their enterprise resource planning (ERP) system.

"Our biggest successes with Fortinet right now really includes two things. First, moving to Fortinet's VPN capabilities and being able to have multi-factor authentication has been awesome. And second, in the last couple of years, we wanted to add MFA to our applications. Previously, we were using a ridiculously expensive vendor for single-sign-on MFA. They had a whole year to prove themselves and they failed miserably," says Salt Lake County's director of information security.

Solutions

- FortiGate
- FortiManager
- FortiAnalyzer
- FortiAuthenticator
- FortiToken
- FortiClient

"The biggest difference, really—things just work better. We have less frustration from the people."

– *Salt Lake County's Director of Information Security*

As with their VPN problems, Salt Lake County looked to Fortinet to help serve their users without breaking their budget. They purchased an additional FortiAuthenticator appliance and FortiToken licenses to design their own solution—fulfilling their needs while dramatically reducing the total cost of ownership (TCO) for application MFA. "I'd say it's probably not even half of what we invested in that other solution. Our users like everything about using it and it has worked really well. We love it."

Network Segmentation and PCI Compliance

At the majority of the county's branch locations, FortiGate NGFWs apply Layer 3 policies to segment certain things from the main county network that vendors need to access. Because the IS team does not want to connect vendors to any internal resources, they ensure vendor devices and users can only access what they need for their specific job functions—which minimizes risk to the broader organization.

The county's IS team also uses segmentation to ensure compliance with Payment Card Industry (PCI) regulations—ensuring that private credit card information of citizens who engage with county-owned businesses and services is kept safe from cyber criminals. This includes everything from people paying their taxes, donations to the aging center, visiting the local planetarium, or even making purchases at county golf courses and recreation centers.

Endpoint Device Protection

After a frustratingly fruitless experience with another vendor's antivirus (AV) solution, Salt Lake County again looked to Fortinet for help. They needed to protect county-owned devices (e.g., laptops, desktops, servers) from malware and other endpoint-targeted attacks. They were already successfully using the Fortinet FortiClient solution to help manage IPsec VPN for county devices.

"We already had FortiClient. It works great on all our laptops. We thought, why don't we just use it everywhere? We already have the whole backend built. More licenses are all we have to buy. Fortinet has become kind of the Swiss Army knife when other people fail us," says Salt Lake County's director of information security.

They started using FortClient for AV as well as off-network web filtering, which was a new capability added to the organization—helping to protect mobile devices from web-based attacks when using non-county network connections. "We keep coming back to Fortinet because the products work well and their price/performance beats the competition."

Centralized Management

As their infrastructure expanded, Salt Lake County security leaders also needed help managing the different Fortinet solutions they had deployed across the region. Scaling from three clusters of four firewalls each up to 55 individual FortiGates increases the need for greater visibility and centralized control. FortiManager was a perfect solution for their need to simplify network operations across all 55 firewalls. Also, FortiAnalyzer provided real-time visibility into their FortiGate clusters while gaining insight into PCI compliance.

As Salt Lake County's information security analyst explains, "It definitely is a huge advantage being able to centrally manage the devices—it saves time to where you have redundancies. You only have to manage it once instead of 55 times. If I had to go change a policy stack on ten firewalls, that's an hour and a half instead of five minutes."

A Partnership Built on Solving Problems

The needs of any government organization are going to be unique to the place where network technologies are deployed. As demand for remote access grew over the last decade, Fortinet's proven NGFW capabilities helped pave the way for added support like VPN, MFA, and endpoint protection when other solutions could not achieve the same performance or cost benefits. Hopefully, Fortinet and Salt Lake County will continue to work together for another ten years—and beyond. "We've been a happy customer for a long time now," says Salt Lake County's director of information security.

April 4, 2020 6:51 AM

591276-0-0-EN

D:\Fortinet\Case Study\Salt Lake\cs-FA-county-government-agency-442020