CASE STUDY

Law Enforcement Technology Provider Bolsters Security and Improves Productivity for Diverse Customer Base

This systems integrator company provides advanced technology solutions to law enforcement, criminal justice, and government organizations throughout the United States. These solutions not only enhance public safety but also promote operational efficiency. Ranging from facial recognition and biometrics to solutions for inmate tracking, mugshots, and bookings, the company offers their services on-premises or in the cloud. They also offer management of these services after they are set up.

The director of IT, who has been with the company for almost 20 years, recalls the early years. "At the time, I was a part of a two-person support team, and the whole company had around 30 employees." Today, the overall employee count and support team have grown considerably. The director of IT provides some supervision of that team, but now spends more time on building and maintaining the network and helping with strategic IT projects for major customers.

Providing Exactly What Customers Need

Far from doing cookie-cutter implementations, this company provides customized solutions for each of its customers. "We understand that law enforcement agencies have diverse and specific needs," the director of IT notes. "Our customers range from the smallest to the largest at all levels of government. Some customers request our employees as 'boots on the ground' to directly manage their infrastructure onsite; other customers are serviced by regional teams."

"I am now able to have a complete, holistic view of our security posture at a glance. Our security operations have moved from reactive to proactive."

– *Director of IT*

Details

Customer: Law enforcement technology provider

Industry: Technology

Location: USA

One difference between agencies is their attitude toward cloud-based services. "Most law enforcement agencies are still skeptical of them," the director of IT explains. "Much of this hesitancy is because of appearances—the potential for negative attention from constituents. But some agencies are discovering the benefits of the cloud by having us manage cloud-based solutions on their behalf. This indirect approach has a less complicated internal approval process and places the agency one step away from the cloud infrastructure."

Struggling with Security as a Small Business

When the director of IT began managing the IT network a decade and a half ago, one of their first projects was to update the company's firewall infrastructure using newer, supposedly more integrated devices from the incumbent vendor. Unfortunately, even with the upgrade, the team found that as additional layers of security were needed, new pieces of hardware were still required. Even when those hardware pieces were cards that could be inserted into existing boxes, the cost was comparable to buying a new machine. "Adding an intrusion prevention system [IPS] doubled our cost, for example, and setup was always a nightmare," they remember.

Over the next several years, licensing and hardware costs for the legacy solution accelerated, eventually placing it out of reach for the small business. They began looking for an alternative solution. "My research showed that FortiGate next-generation firewalls [NGFWs] provided one box that handled everything we needed and met all customer requirements—including those of the FBI," they relate. "And the cost was 50% to 60% less than for our legacy solution."

Moving to an Integrated Solution

The company installed its first FortiGate in 2012, and the director of IT was amazed at how easy it was to use—and the broad visibility it brought to the security infrastructure. "Employees at our customer sites were jealous of the infrastructure we had built at our headquarters," they recall. "So, it was easy to sell many of them on the idea of building a FortiGate infrastructure at their sites."

Since then, the company has deployed dozens of FortiGate NGFWs at its headquarters and at multiple customer sites, and began deploying instances of FortiGate VM earlier this year for customers using Amazon Web Services (AWS) cloud-based services. "We have been pleased with the performance of the virtual FortiGate; we cannot tell a difference from the physical boxes," the director of IT says.

Broadening the Security Architecture

Over time, the company has taken advantage of multiple features built into FortiGate, and has bolstered security by seamlessly integrating other solutions in the Fortinet Security Fabric. For instance, setting up virtual private networks (VPNs) is seamless with FortiGate. "We were amazed at how intuitive and effortless it is to set up a VPN tunnel," the director of IT says. The company also uses FortiGate to control access to the network from wired and wireless endpoints.

The director of IT is also now inspecting all encrypted traffic using the FortiGate secure sockets layer (SSL)/transport layer security (TLS) inspection capabilities. "Unlike other solutions I have tested, using SSL and TLS inspection does not degrade the performance with FortiGate," they report. The company also takes advantage of the intent-based segmentation capabilities built into FortiGate devices. "Dynamic segmentation is critical for our customers, as they must comply with the FBI's Criminal Justice Information Systems [CJIS] standards," they explain. "Those standards have strict requirements for access control and inspection of east-west traffic."

The company deployed FortiAnalyzer VM several years ago to collect and analyze log data from its own data center as well as all its FortiGate deployments at customer sites. The solution is deployed in the company's on-premises Microsoft Hyper-V environment. "We realized that having a central repository for the logs protects us in the event of hardware failure, and the advanced analytics gives us actionable insights into what is out there," they explain. "Being able to view all the logs on a single pane of glass is really nice, and having it as a virtual machine helps us be more efficient."

The director of IT is now in the process of deploying the FortiClient endpoint security solution across the environment, replacing a legacy solution. "We have started with edge clients and have 50 out of 300 endpoints deployed so far," they report. "Being able to monitor our endpoints from the same Fortinet console will be a big improvement over our prior setup."

The company subscribes to the FortiGate Unified Threat Protection (UTM) bundle and has been using its Advanced Malware Protection, IPS, and web filtering features for some time. The director of IT recently began testing the antispam and sandbox analysis features that are a part of the bundle. "We're especially excited about FortiSandbox Cloud's ability to give us another layer of protection against unknown threats," they say. "And we have not seen reductions in performance so far."

Business Impact

- 99% reduction in time required to set up a VPN tunnel
- 16 weeks of reduced customer waiting time for VPN tunnels annually
- 20 hours per month saved in reviewing log pulls, while achieving a more comprehensive view
- 30% cost savings for one customer by moving to the AWS cloud, enabled by FortiGate VM
- No performance degradation from SSL/TLS encryption
- Enables new product offerings for customers

Solutions

- FortiGate
- FortiGate VM on AWS
- FortiGate Unified Threat Protection (UTM) Bundle
- FortiAnalyzer VM
- FortiClient
- FortiSandbox Cloud
- FortiCare 24x7

"FortiGate NGFWs provided one box that handled everything we needed and met all customer requirements—including those of the FBI. And the cost was 50% to 60% less than for our legacy solution."

– *Director of IT*

The company was also able to integrate an existing security solution, a two-factor authentication tool from Fortinet Fabric Partner Duo Mobile, into the Security Fabric for seamless visibility and control. "The ability to integrate third-party tools is a big plus," the director of IT says.

> *"Dynamic segmentation is critical for our customers, as they must comply with the FBI's Criminal Justice Information Systems (CJIS) standards."*
>
> – *Director of IT*

Realizing Significant Benefits

After using Fortinet solutions for close to eight years, the company has accumulated a number of benefits. One of the biggest pain points in the company's prior infrastructure is completely alleviated with FortiGate. "Setting up VPN tunnels was a nightmare before," the director of IT contends. "To do the job, one practically had to have the highest certification with the vendor—something we as a small business could not afford," they remember. "And even the experts had trouble. I once had a person come out from the vendor to help with a tunnel. It took him two weeks, and that deployment never really worked right. We still have a couple of those devices at customer sites, and they have problems fairly frequently."

On the other hand, setting up VPN tunnels with FortiGate is easy. "It takes a half hour and is totally intuitive," they say enthusiastically. This translates to a 99% improvement in how long it takes to set up a tunnel for a customer. So far this year, they have gone through this process once every six weeks or so, meaning that they are on track to save their customers 16 weeks of waiting time for the year.

But the efficiency gains do not stop there for this company. Using FortiAnalyzer VM to correlate logs from all the customer sites that it supports, plus the headquarters, also saves the director of IT a lot of time and makes everyone more secure. "I did not have time to do anything more than spot checks before, and even that was taking me 20 hours per month more than I am spending today," they assert. "I am now able to have a complete, holistic view of our security posture at a glance. Our security operations have moved from reactive to proactive."

The flexibility of the Fortinet solution is another benefit that the company promotes to customers. "One client is saving 30% by moving from a co-located, on-premises network to a cloud-based deployment secured by FortiGate VM," the director of IT describes. "And customers get the same protection regardless of form factor."

To ensure optimal uptime and rapid support, this company has access to 24×7 FortiCare support through its UTM subscription—and the director of IT has seen good results. "They are really quick to help, and their expertise in troubleshooting allows us to focus on more strategic things," they relate.

A Strong Relationship

This company is in conversation with some of its clients about providing audit reporting services to help them demonstrate compliance with CJIS standards. This new service will rely on expanded use of FortiAnalyzer VM. "Since we have been aggregating log data for a while, it will be easy to create the reports," the director of IT says.

This is just one example of expanded services that this company can offer its customers because of the flexibility and scalability of the Fortinet Security Fabric. "It really gives us the ability to provide the customized services we are known for," the director of IT concludes. "I expect our partnership with Fortinet to only grow."

FORTINET

www.fortinet.com

March 10, 2020 6:00 AM

482611-0-0-EN

D:\Fortinet\Case Study\Law Enforcement Technology\cs-FA-law-enforcement-technology-provider-bolsters-security-342020-947AM\cs-FA-law-enforcement-technology-provider-bolsters-security-342020-947AM