CASE STUDY

Fortinet Gives Marketing Firm Maximum Protection While Requiring Minimum Staff Time

Sandy Alexander is ready to meet your needs when you need to communicate with customers or other stakeholders, whether one to one or one to millions. "We do conventional offset printing, web presses, direct mail, digital printing, building wraps, retail visual merchandising, annual reports, and much more," says Justin Fredericks, IT Manager for Sandy Alexander. "Basically, we print anything and everything."

The company supports clients' marketing communications through five locations across New Jersey, Florida, and California. Fredericks' lean IT team supports about 450 users in those three states. Prior to the onset of the COVID-19 pandemic, remote work was already beginning to create challenges for security management. The arrival of the pandemic, when many employees started working from home, rapidly exacerbated those challenges.

"At the time, we used the OPAQ Firewall-as-a-Service [FWaaS], Endpoint-as-a-Service, and Web Application Firewall-as-a-Service [WAFaaS]," Fredericks says. The company's primary security solutions were all cloud-based. To access the corporate network, endpoints connected to a small security appliance, which then tunneled to a local point of presence (POP) for connectivity to the cloud-based firewall and beyond.

"In that environment, we had a lot of visibility at our company sites but not so much for the remote users," Fredericks explains. "We would get information about remote users' traffic that traversed the firewall, but we could not see the other things they were doing. That was a blind spot for us."

One benefit of this approach was that the Software-as-a-Service (SaaS) solutions minimized the time Fredericks and his team needed to dedicate to security processes. "Years ago, we had hardware from multiple security vendors in all our sites," Fredericks says. "I wear a lot of hats, and managing that environment became too much."

When Sandy Alexander's systems were nearing end of life, Fredericks and his team began evaluating their options. Maintaining the SaaS ease of management was a key requirement. Gaining visibility into remote users' activities was another.

Integration and Automation Lead to Selecting Fortinet

The team evaluated several options, but Fredericks says none could compare to FortiSASE, the Fortinet secure access service edge (SASE) system. "FortiSASE even offered a fix to the blind spot we had with remote workers," he says. "It was clearly the right solution to meet our needs."

Further influencing his decision was that FortiSASE, FortiGate Next-Generation Firewalls (NGFWs), Fortinet Secure SD-WAN, FortiClient endpoint protection, and other Fortinet solutions all work together seamlessly. The enterprise-grade solutions

SANDY ALEXANDER

"Having one vendor that consolidates networking and security in a single product set is very beneficial, and Fortinet is a visionary in that regard. Fortinet saw where everything was headed and is now at the forefront of the technology. It is great to work with Fortinet and be at the forefront as well."

Justin Fredericks
IT Manager
Sandy Alexander

Details

Customer: Sandy Alexander

Industry: Business Services

Location: Clifton, NJ

Business Impact

- Enhanced sensitive corporate resources protection through granular user access management
- Significant reduction in IT staff time spent managing security environment
- Enterprise-grade security for a competitive advantage

converge networking and security capabilities, with single-pane-of-glass visibility into both. Rather than building a new security infrastructure piecemeal by adding components from a variety of vendors, the team decided to take advantage of the integration and automation available within the Fortinet Security Fabric.

"Having one vendor that consolidates networking and security in a single product set is very beneficial, and Fortinet is a visionary in that regard," Fredericks says. "Fortinet saw where everything was headed and is now at the forefront of the technology. It is great to work with Fortinet and be at the forefront as well."

Deploying a WAF and On-Premises Firewalls

At the same time they were considering SASE solutions, Fredericks' team also evaluated web application firewalls (WAFs) with the goal of adding protection for, and visibility into, public-facing web-based applications. They ran a proof of concept of the FortiWeb Cloud WAF and liked what they saw.

"Our previous WAF was managed, and we did not have any visibility into it," Fredericks says. "With FortiWeb Cloud, by contrast, we were in control. I set it up, working with the Fortinet team to understand how it worked and how to optimize the features. When we did the proof of concept, we realized this would be a great solution to protect our public-facing web-based applications, and Fortinet keeps adding more capabilities."

One potential sticking point was that Fredericks wanted the security infrastructure to be as easy to oversee as Sandy Alexander's legacy environment. Fortinet worked with a partner to develop a managed security service provider offering for all the solutions Sandy Alexander wanted to deploy. The partner purchases the Fortinet products and provides them to Sandy Alexander on a monthly subscription basis, with 24×7 support.

Sandy Alexander deployed the FortiWeb Cloud WAFaaS. Next, the company rolled out a FortiGate NGFW at each location. "Previously, the firewalls were in the cloud, but we went back to on-premises firewalls," Fredericks says. Sandy Alexander leveraged the NGFWs' built-in Fortinet Secure SD-WAN (software-defined wide area networking) capabilities to create efficient WAN connections between locations.

The company uses the FortiGuard Unified Threat Protection (UTP) Service Bundle from FortiGuard Labs to enhance the protections of the NGFWs. The bundle includes intrusion prevention service, web security, content security, and data loss prevention (DLP) functionality. "Having all those capabilities gives us the appropriate level of protection," Fredericks says. "We do not have to worry about our security posture.

"And then," Fredericks adds, "the last piece was getting all the remote workers connected through FortiSASE."

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSASE
- FortiWeb Cloud WAF
- FortiClient
- FortiAuthenticator

Services

- FortiSASE and FortiGuard UTP Bundle
- Security Operations Center (SOC)-as-a-Service

"The FortiGate firewalls make network segmentation for remote users much easier because user access policies are all in one place. Our users connect to the POP closest to them, and we manage their access through a single dashboard."

Justin Fredericks
IT Manager
Sandy Alexander

Sandy Alexander Gets SASE

One option Sandy Alexander considered for remote user connectivity was virtual private network (VPN) access. "Prior to the SASE platform, we had employees using VPN to connect directly to each site," Fredericks says. "Every employee [who] worked out of a site would get VPN access to it." The problem with that approach was users' broad access to corporate resources. Fredericks' team worked to provide some network segmentation, but the process was complex.

"The FortiGate firewalls make network segmentation for remote users much easier because user access policies are all in one place," Fredericks says. "Our users in the Northeast connect to the POP closest to them; people in Florida or on the West Coast do the same thing, and we can manage their access through the SASE single dashboard."

Many of the endpoints are now protected by the FortiClient endpoint protection solution for their remote security. The company has also purchased the FortiAuthenticator user authentication tool.

While on-premises user traffic moves through the local FortiGate NGFW, all remote user traffic is now tunneled through FortiSASE. "Everything is protected, and FortiSASE gives us a lot of visibility into remote users' actions," Fredericks says. "We like being able to keep our remote workers safe while they are doing what they need to do."

Sandy Alexander is saving a lot of time with the Fortinet platform. "Having firewalls, SASE, and endpoint protection from the same vendor is saving us time," he says. For one thing, the integration between the solutions means a single partner can manage the entire environment. That might not have been the case if Sandy Alexander was using solutions from different providers. "I am very happy we can do it all with Fortinet," Fredericks adds.

In addition, the portions of the security workflow that require his attention are quick to implement. "For example," he says, "over the past year and a half, we have added a lot of controls, and that has taken very little of my time. I have been able to tune the Fortinet tools to block out all the noise so that I get only actionable intelligence out of them. And I do not spend much time responding to security events because many of them get automatically cut off by the Fortinet solutions. Unless an alert comes through for a real incident, security management now takes very little attention."

Fortinet Brings a Competitive Advantage

Sandy Alexander recently began using FortiGuard SOC-as-a-Service to ensure that outside experts are monitoring its security environment 24×7×365. "The logs from our FortiSASE and FortiGate firewalls go into a SIEM [security information and event management] solution, and the service looks at the data there," Fredericks says.

A separate external security operations center (SOC) team also monitors the SIEM. "I meet with the SOC team monthly for updates on what they are seeing," Fredericks reports. "We try to aggregate and correlate all the data in one place. Putting together all the log data from FortiSASE and the firewalls enables us to look at the big picture of what is happening in our sites, as well as with our remote users.

"Plus, Fortinet is looking at our logs as well," he continues. "If something comes up, we are going to know right away because we have two sets of experts looking at everything from all these different angles. That greatly enhances the strength of our security posture."

Fredericks appreciates that Fortinet was able to accommodate the operational expenditures cost model that Sandy Alexander was accustomed to with its legacy solution. "The Fortinet hardware and licensing are rolled into an agreement where we make monthly payments," he says. "The payments are predictable, and everything is included. We are definitely getting more for our money than previously because the platform has grown with a lot of new features."

He adds that Sandy Alexander considers the relationship with Fortinet to be "a great partnership." As an example, he cites a recent situation in which Fortinet suggested Sandy Alexander's improved security posture might reduce its cyber-insurance premiums, something the marketing company had not previously considered.

All in all, it is a relationship that makes Sandy Alexander more effective at protecting against the cyberthreats that plague every modern company. "Not only are we concerned with security, but our customers are as well," he concludes. "Often, our customers demand security capabilities that they would like us to use to protect their data. For example, they want to know we have DLP before they will share data with us. Using Fortinet's leading-edge security solutions gives Sandy Alexander a competitive advantage."

October 9, 2023 11:58 PM

2357851-0-0-EN