CASE STUDY

How a Lean Team Is Keeping K-12 Students and Staff Secure

The Spring Branch Independent School District (ISD) is a large K–12 public school district in the Houston area. About 6,000 faculty and staff educate 35,000 students on 47 campuses and in 52 buildings. This dispersed IT infrastructure supports students' learning in a wide range of subjects and prepares them for life beyond high school. Keeping students, staff, and all district data safe is the responsibility of a remarkably tight staff.

"Our security team consists of about one and a half FTEs [full-time equivalent employees]," says Troy Neal, executive director for cybersecurity and technology operations for Spring Branch ISD. "I used to handle all the cybersecurity myself, but I was able to hire an engineer last year to focus on security, as well as other duties as assigned." Neal and his colleague make this work by leveraging efficiencies everywhere they can.

First, Secure the Perimeter

Several years ago, before Neal was on staff, the district decided to upgrade to enterprise-grade firewalls to protect the network perimeter. "If you look at our size, we have around 40,000 end-users, which is bigger than most companies," Neal says. "At the same time, Spring Branch is a typical school district. We really emphasize optimization of every CapEx [capital expenditures] dollar spent."

After a "journey of lessons learned" with other firewalls, Spring Branch ISD deployed a pair of FortiGate next-generation firewalls (NGFWs). Over the next couple of years, the district started to explore additional components from the Fortinet Security Fabric portfolio and added the FortiMail secure email gateway, FortiAuthenticator user authentication, and FortiSIEM security information and event management (SIEM) to its security toolkit. The goal was to protect the district's entire attack surface.

Around the time Neal joined Spring Branch ISD, the district was looking to increase network throughput and upgrade the firewalls. "I was tasked with building and supporting a 100-Gig network," he says. All network traffic funnels through the firewalls in the district's colocation center. One of Neal's primary concerns was to find secure networking solutions that could scale with the district.

"The FortiGates are a phenomenal product," Neal says, "but we considered other options because I wanted to make sure to select a solution that would future-proof us for the next 5 to 10 years. We quickly saw that in the Fortinet Security Fabric. We upgraded our FortiGate infrastructure to a larger HA [high-availability] pair and started augmenting it with the rest of the Fortinet Security Fabric to better protect us." Neal's team also plans to set up virtual clustering on the HA pair to enable failover between the virtual domains (VDOMs) on each of the firewalls.

"The advantage of the Fortinet Security Fabric is the single pane of glass. I do not want to have to go to five different interfaces to figure out a problem. We use FortiManager for monitoring traffic, watching every event that might require response."

– Troy Neal, Executive Director, Cybersecurity and Technology Operations, Spring Branch Independent School District (ISD)

Details

Customer: Spring Branch ISD

Industry: Education

Location: Spring Branch, Texas

Business Impact

- Manage external risks by protecting students and staff from a wide range of security threats
- Efficient operations by freeing up hours that small security team would otherwise spend on manual activities

Better Visibility, More Efficient Control

Neal's next steps in optimizing the security infrastructure were to tune FortiSIEM and better leverage the FortiManager centralized management console and the FortiAnalyzer security analytics solution (together known as the Fortinet Fabric Management Center). "Our SIEM was ingesting a huge amount of log data," he says. "We stepped back to figure out where our pain points were, what information we needed to focus on, and how to use it." Some organizations fail to take this perspective, he says, and that is a mistake.

"We developed a central repository, we made sure it was collecting all the right information, and we developed a dashboard-level view of what is going on inside the Security Fabric," Neal says. The centralized dashboard is available to district administrators. "My boss can log into a GUI [graphical user interface] and see what is going on. If he has questions, I can then drill down to investigate what is truly happening: What is the risk? What actions need to be taken? With FortiSIEM, we know all our high-impact risks are being captured, and it is easy to drill into the details to measure risk."

In fact, Neal adds, FortiSIEM's insights are not exclusive to security questions. "We are ingesting all kinds of logs," he says. "The SIEM can help us troubleshoot an application that is not working right or network performance issues. Instead of engineers having to go to server logs and poke around, we can go to FortiSIEM, get the same relevant information more quickly, and make better decisions."

Moreover, he says, the ability to manage the firewalls, FortiMail, and FortiAuthenticator through a centralized console further enhances the district's visibility into incidents networkwide. "The advantage of the Fortinet Security Fabric is the single pane of glass," Neal says. "I do not want to have to go to five different interfaces to figure out a problem. With a team as lean as ours, we cannot be there in person every time someone has a security question. We use FortiManager for monitoring traffic, watching every event that might require response."

As an example of the ways in which the Fortinet solutions have enhanced district efficiency, Neal points to the ease with which he can change firewall settings around acceptable traffic patterns. "In education, the landscape is constantly evolving," he says. "One particular class, or even one student, may need access to a certain application or a particular resource. In 2020, for obvious reasons, our teachers and students started using web conferencing extensively. We set up a specific firewall rule that prioritizes Zoom traffic and created a very specific set of public IP addresses to maximize our performance. Being able to make these changes within FortiManager enables us to make adjustments quickly based on user needs and demands, while still protecting district security."

All told, Neal says, "The Fortinet management tools are saving around four hours a day for my team of two. We still have a lot of alerts coming through in FortiSIEM, but it is all valid. Now that we have the SIEM tuned, the security team has four additional hours each day for other activities."

Ready To SOAR

Now, Spring Branch ISD is taking the next step forward in increasing the efficiency of the district's Fortinet security infrastructure: Neal and his colleague have installed, and are in the process of configuring, the FortiSOAR adaptive security orchestration, automation, and response (SOAR) platform. "The exciting part

Business Impact (contd.)

- Ease of use with a single view providing district administrators confidence in security visibility, by providing a user-friendly incident dashboard
- Security Fabric protecting the entire attack surface through actionable threat intelligence sharing, automated protection, and efficient operations

Solutions

- FortiGate
- FortiManager
- FortiAnalyzer
- FortiSIEM
- FortiSOAR
- FortiMail
- FortiAuthenticator

Services

- FortiGuard UTP Bundle

"What makes Fortinet the right partner for Spring Branch ISD: The solutions are enterprise-class, they protect us from all angles—from perimeter to internal threats to email to authentication—and they provide 24×7 protection while effectively taking the human factor out of many of our processes."

– Troy Neal, Executive Director, Cybersecurity and Technology Operations, Spring Branch ISD

of FortiSOAR is the ability to start automating," Neal says. "The SIEM contains great information, but digging through it can require a lot of processing power and manpower. With the SOAR, we will be able to take the people portion out of immediate, reactive security response so that our team can focus on higher-priority and bigger-picture concerns."

One of the key drivers of the SOAR implementation was phishing emails. "The number-one problem in organizations across the United States, no matter what industry, is that staff love clicking on things they should not," Neal says. "We needed to figure out how to eliminate that problem. FortiMail removes probably 90 percent of the malicious emails before people have an opportunity to click them. But no product is perfect. And for phishing messages that are missed, we have a spam reporting mailbox.

"What FortiSOAR will do is pull in the emails from that mailbox and take automated actions, such as checking whether the email address is valid and detonating attachments," Neal continues. "It does all the cleanup for us, versus two engineers going in and writing scripts to pull emails from mailboxes. This will eliminate a lot of manual work for the security team in an area that is always a pressing concern."

"In addition to the automation and orchestration, FortiSOAR will enable us to see the path, the trajectories, the events leading up to a security incident. We are looking forward to using that information to learn and grow as a security team."

– Troy Neal, Executive Director, Cybersecurity and Technology Operations, Spring Branch ISD

Neal is now working with Fortinet to build playbooks that provide a description of the response to specific security incidents. He points out that, as a school district, Spring Branch ISD cannot afford to hire a team of specialized cybersecurity investigators. "Automation is the obvious answer," he says. "The playbooks will be vital in our ability to optimize use of the SOAR. And it has been critical to have access to Fortinet expertise in building them; it would have been very difficult to do it ourselves."

One additional goal of the FortiSOAR deployment is for the solution to pull in information from Spring Branch ISD's third-party vendor of wireless access points, switching, and user access control. "We want to ingest information from all those tools into the Fortinet Security Fabric," Neal says. The third-party tools could fit into FortiSOAR playbooks, which orchestrate the multiple vendors' solutions in automated threat mitigation processes.

"In addition to the automation and orchestration, FortiSOAR will enable us to see the path, the trajectories, the events leading up to a security incident," Neal says. "We are looking forward to using that information to learn and grow as a security team. We want to translate that knowledge into training for junior staff, and we want to leverage our time savings to focus on better supporting instructional value throughout the district."

A Future-ready Partnership

Spring Branch ISD has purchased FortiClient endpoint protection as well and intends to deploy the solution to 6,000 systems during schools' next summer break. From here, Neal sees the relationship with Fortinet continuing to grow. "I do not do business with vendors," he says. "I do business with partners. I see Fortinet as an extension of our IT team. We have a lean staff who can reach out to Fortinet, as necessary, to escalate issues." FortiGuard Unified Threat Protection (UTP) services are core to this approach. FortiGuard UTP includes, among other security capabilities, market-leading intrusion prevention system (IPS), content protection, and URL filtering.

"I am not going to get a bigger security team," he says, "and frankly I do not even want a bigger team. School districts have to maximize the dollars that are available to us, and to my mind, the best way to do that is through automation and streamlining management processes as much as possible. That is what makes Fortinet the right partner for Spring Branch ISD: The solutions are enterprise-class, and they protect us from all angles—from perimeter to internal threats to email to authentication. They are integrated so we have centralized visibility to it all. And the FortiGuard UTP services provide 24×7 protection while effectively taking the human factor out of many of our processes."

FORTINET

www.fortinet.com

July 2, 2021 5:08 AM
1077528-0-0-EN