SecureWorks

K–12 DISTRICT SCORES TOP GRADES WITH ADDED SECURITY

Fort Mill Schools strengthened its IT security to better protect against threats and to safeguard student, teacher and staff data, using SecureWorks solutions

FORT MILL SCHOOLS "Children First"

Industry: K–12 Education | **Country:** United States | **Employees:** 1,419 | **Students:** 13,100

Website: www.fortmillschools.org

"To protect the data privacy of students, teachers and staff, we're confident we're doing all we can do and improving on that daily, with SecureWorks on call if needed."

Brian Spittle, Director of Technologies, Fort Mill School District

BUSINESS NEED

After a denial-of-service attack succeeded against already-strong defenses, the Fort Mill School District sought even more protection and improved incident response capabilities.

SOLUTION

The district conducted a thorough incident response logging and monitoring review and strengthened its defenses with 24x7 network scanning, all with assistance from SecureWorks solutions.

BENEFITS

- Strengthens existing defense-in-depth protection
- Enhances protection of student, teacher and staff data
- Improves security posture and visibility to threats

PRODUCTS | SecureWorks Incident Management Proactive Services | SecureWorks Managed Vulnerability Scanning

SOUTH CAROLINA'S FORT MILL SCHOOLS HAS HAD DEFENSE-IN-DEPTH SECURITY LAYERS SIMILAR TO SECURITY SYSTEMS OF FORTUNE 500 FIRMS FOR YEARS.

Updated 24x7 anti-virus software and firewalls. Intrusion detection and protection systems. Limited VPN access. A locked-down data center. Security awareness training for students, teachers and staff. Despite all this, hackers from Eastern Europe still penetrated the district's network.

Director of Technology Services Brian Spittle recalls the denial-of-service (DoS) attack started at the same time his team was modifying the district's data center. "At first we thought the changes had caused our loss of internet connectivity," he says. "But after an hour, we confirmed with our Internet Service Provider that we were under a DoS attack — one lasting four days as it turned out."

Despite the continuing attack, Spittle and his team worked with the district's ISP to restore service five hours after they realized what had happened to their internet connectivity. "We were able to use the traffic-logging capability of our firewall to determine the source countries, source IP addresses, and ports used for the attack," he says. "We then shared that with our ISP, who blocked that traffic upstream from our connection, which restored our connectivity."

DATA PROTECTION, PART OF K–12'S MISSION

Spittle takes cybersecurity seriously. As a former systems engineer, he has earned an incident-handling security certification from the Global Information Assurance Certification (GIAC) organization, a leading provider of infosec certifications.

He sees data protection as a vital part of his district's educational mission. "Protecting student and employee data is a critical piece to maintaining the support and trust of the community," he says. "Parents entrust schools to create and maintain a safe environment for their children. This extends beyond the physical security of the buildings and includes student data as well."

For many K–12 districts that can be a tall order, especially since most have so many competing priorities for limited budgets. Other issues adding to this are the spreading bring-your-own-device (BYOD) phenomenon among students, teachers and staff; a lack of security awareness across those groups; and the growth in the use of online technology for instruction and testing. Plus, districts have to comply with personal data privacy regulations such as HIPAA, PCI, FERPA and others.

According to Spittle, the Fort Mill District's security posture is subject to all those factors. In addition, the district has been one of the state's fastest-growing for 15 years. "Our student numbers have been growing between 5 and 8 percent each year, so building schools, equipping more classrooms, and training new staff have all been challenges, not to mention providing secure IT infrastructure to support it all," he says. "Fortunately, we've been able to meet those challenges because of the leadership of the school board and the support of the community."

TIME TO TAKE SECURITY TO A HIGHER LEVEL

Spittle saw the attack as a wake-up call to take the district's IT security to even higher levels. He sought outside expertise to review and enhance the district's incident response plan and also its logging, monitoring and auditing. "We wanted a partner with experience gained from responding to breaches and successfully completing forensic investigations," he says. "When SecureWorks rose to the top of our search process, our long-standing, successful experience with made it an easy choice."

The district started with SecureWorks Incident Management Proactive Services, a portfolio of security consulting services, to help with two related efforts. One was to complete an incident response logging and monitoring review; the other was to review and improve the district's incident response plan where possible.

> *"We needed a plan we could train with, so we could improve our ability to identify an attack and respond appropriately," Spittle says. "We also needed to know what our limitations are so we can know when to escalate an incident and seek assistance from SecureWorks."*

SOLID INCIDENT RESPONSE PLAN

Today Spittle and his team are confident the district has a solid incident response plan, no matter what threat actor might emerge. But it's not a plan they've put on a shelf. SecureWorks has advised them on scenarios for tabletop role-playing exercises, so everyone knows what to do should an incident occur.

"In reviewing our incident response plan as well as our logging and monitoring, most of our IT security approach was validated by SecureWorks experts," Spittle says. "To know we're well prepared for any incident has also helped to boost our IT staff morale."

Spittle also engaged SecureWorks Managed Vulnerability Scanning services to add another 24x7 protective layer to the district's defense-in-depth security architecture. "We found some hidden vulnerabilities we've fixed by patching or reconfiguring settings, thanks to SecureWorks scanning services," he says. "That'd be expensive expertise to have on staff."

READY FOR THREAT ACTORS FROM AROUND THE WORLD

Overall, Spittle considers the district's partnership with SecureWorks has improved its security posture and threat visibility. Based on logs of the 24x7 network scanning by SecureWorks, the district gets hit daily by threat actors located in such far-flung places as Brazil, Russia, and nations from Eastern Europe and Asia. It also gets weekly phishing attacks and has had several cases of ransomware.

Has Spittle gained peace of mind with SecureWorks? "Given our responsibilities for maintaining network security, with new threats each day, we can't let down our guard," he says. "But to protect the data privacy of students, teachers and staff, we're confident we're doing all we can do and improving on that daily, with SecureWorks on call if needed."