CASE STUDY

Large School District Achieves Automated, Highly Effective Ransomware Protection

A large Texas school district faced an endpoint security crisis. Three employees were responsible for the district's entire network, supporting more than 20,000 students across 20-plus campuses and an assortment of support facilities, a data center, and a disaster recovery site. The small team managed security, as well as servers, storage, and internet connectivity, so they were spread thin.

Network security was working well overall, but endpoints represented a gap. All the teachers had Windows tablet computers that they used in the classroom and sometimes took off-site. Additionally, the district allowed teachers and staff to connect to the network using personal devices. The IT team developed tiered permissions to restrict which resources non-district machines could access.

Still, says the district's former CTO, "One of the greatest threats to any network is endpoints that are not within the control of the network. Teachers would take their mobile devices home, and they would bring external drives and personal devices onto our network. Anytime a device is connecting but is not securely and permanently attached to the network, there is a risk that the device might bring an attack into the network."

His small team worried about the potential ramifications of such an attack. "Protecting people's information and privacy, and the security of their data, is crucial," he says. "If information ever gets compromised, that could have an untold cost not only to the organization, but also to the individual." Pressure ramped up when the state legislature mandated greater security in K-12 schools. "They basically required us to adhere to the same standards that state universities and other large institutions do," the CTO says. "We needed to make sure we were doing all we could."

Two Attacks in One Week

The situation came to a head when the district experienced a pair of ransomware attacks. A science teacher doing research visited an infected website and unknowingly brought ransomware onto the network. By the time the district's security systems detected the malware, it was already spreading.

"When ransomware is moving through your network, you have to shut it down immediately," the former CTO says. "We locked down the servers, wiped them, reloaded the operating systems and applications, and then restored our data from backups. The attack started on Monday morning. We mitigated the threat and got all our systems back up by late on Tuesday. Then, Wednesday morning, our security systems detected the exact same ransomware. Another science teacher had visited the same site, and we had to start over with the mitigation work."

"FortiEDR can save districts a lot of embarrassment and unwanted press over a potential compromise. FortiEDR is a wonderful product. It does what it is supposed to do."

– Former CTO,
Large Texas School District

Details

Customer: Large Texas School District

Industry: Education

Location: Texas, USA

Business Impact

- Effective protection against ransomware, as demonstrated through thorough testing
- Avoidance of bad press, embarrassment, and district-wide downtime in the event of a successful ransomware attack
- More staff time for value-added activities

The staff of three lost almost an entire week of working on anything else, putting in 14- to 16-hour days focused exclusively on dealing with these attacks. "It was very time-consuming and disruptive, and it overloaded an already busy team," the former CTO recalls. "We needed to avoid such unnecessary mitigation work in the future by deploying a system that would do a better job of preventing these types of attacks from launching on the endpoints. Our goal was to protect teachers and staff from themselves, and to protect other network resources from not-well-informed decisions by people utilizing mobile devices."

Detecting Problematic User Actions—and Responding

The district began evaluating various endpoint detection and response (EDR) solutions. The selection criteria were simple, the former CTO says: "We needed a solution that could mitigate or stop ransomware.

"The problem," he continues, "is that some types of ransomware trigger a legitimate protocol within the Microsoft operating system that the attacker later uses to trigger the attack. The initial actions mirror legitimate admin activities, so some endpoint security tools fail to detect them. What we needed was a solution that would monitor—very closely and at the endpoint—how each end user's credentials are being utilized, and would respond anytime a user does something out of the ordinary."

For example, he says, most users do not need to be taking actions like encrypting data, so if their credentials are used to encrypt data, the endpoint solution should block that activity. Compared with the other EDR systems the district considered, FortiEDR has impressive response capabilities. "When it detects certain behaviors that a user does not have permission to execute, FortiEDR will prevent the user from taking that action," he says. "Then, it will notify the appropriate people to go investigate and clean up the problem before it becomes a networkwide issue."

Solutions

- FortiEDR
- FortiGate Network Firewall
- FortiMail
- FortiSandbox
- FortiAuthenticator
- FortiManager
- FortiAnalyzer

"In addition to substantial time savings on management, FortiEDR automated both detection and response. FortiEDR enabled my team to spend more time on the other things they needed to get done day to day."

– Former CTO,
Large Texas School District

The team also liked the tight integration of FortiEDR with Microsoft Active Directory and felt that Fortinet's pricing was fair. "My focus was to find the best product at the best price," the former CTO says.

His team worked with Fortinet to perform a proof of concept (POC). They tested FortiEDR against known threats, including the ransomware that had crippled its network for a week. FortiEDR thwarted all the attack attempts. Among other tests, "We ran ddr-attack on about 300 devices," the former CTO says. "We had an expectation of what we wanted the FortiEDR platform to do, and it always did what we expected. What we discovered through the POC is that FortiEDR works exactly as advertised."

Effective Security Leads to Fabric Deployment Districtwide

This experience was similar to the POC that first led the district to consider Fortinet solutions. Several years ago, the former CTO was shopping for firewalls. His team tested options from two other leading vendors but was not satisfied. "Those other firewalls did not perform like we needed them to," he explains. "We found we could defeat them using things like VPN platforms from within the network. When we were not happy with the other options, we tested FortiGates, and we were not able to breach them. They provided the level of security we needed."

FortiGate Network Firewalls have secured the district's network ever since. FortiMail protects the email system, which is crucial since more than one-third of ransomware attacks come via email. FortiSandbox integrates with both the FortiGate and FortiMail solutions, providing sandboxing when malware is detected.

FortiAuthenticator provides single sign-on user authentication throughout the network, providing the district with role-based access capabilities to ensure users have the right access. The IT team uses FortiManager and FortiAnalyzer (known collectively as the Fabric Management Center) to monitor and manage all the solutions in the district's Fortinet Security Fabric.

Also integrated with FortiSandbox, FortiEDR was a natural fit into this environment, and deployment went smoothly. "Anytime we had questions or issues, the team from Fortinet went the extra mile to make sure everything was working the way it was supposed to," the former CTO says. "I look at vendors as strategic partners. I needed Fortinet's help sometimes to get done what my team needed to do—and Fortinet was always there. I could not have asked for a better team in terms of support."

A Product That Does What It Is Supposed To Do

The former CTO sees great benefit in using multiple security solutions from the same vendor. "Deploying FortiEDR gave us a comprehensive solution," he says. "We already had FortiGates, and we had established firewall rules determining what we would allow and what we would not. FortiEDR added another layer of protection without much additional management burden once the initial setup and configuration was completed.

"In addition to substantial time savings on management," he adds, "the Security Fabric environment enabled my team to be proactive in utilization of our time. FortiEDR automated both detection and response, whereas more reactive solutions would have required us to go through logs to discover problems and then manually respond. FortiEDR enabled my team to spend more time on the other things they needed to get done day to day."

Most important, FortiEDR eased the team's worries about endpoint protection. The former CTO describes an attack on another large Texas school district: "Ransomware took that district's network offline for three full weeks. That is not just time-consuming for the security team. It disrupts the classroom; it disrupts logistics and business offices. Everything in a modern school district relies on technology. That is why I recommend FortiEDR so highly.

"FortiEDR can save districts a lot of embarrassment and unwanted press over a potential compromise," he concludes. "FortiEDR is a wonderful product. It does what it is supposed to do."

December 14, 2021 12:12 AM
123456-0-0-EN