FORTINET

CASE STUDY

Fortinet Helps a Florida School District Meet Its Insurer's Strict New Requirements

The Okeechobee County School District serves a rural area in Central Florida situated on the shores of the second-largest lake in the U.S. The district educates 6,000 students across 10 schools. Because there are no private secondary schools in the county and no sizable private elementary schools, the district serves almost every young person in Okeechobee County.

"This is an extremely tight community, where everyone pretty much knows everyone else and is willing to help out whenever they can," says Rashan Jones, the district's coordinator of network systems and de facto manager of cybersecurity. "In Okeechobee County School District, like for many other districts across the country, we are very concerned about ransomware and cyberattacks. We will do anything we can do to protect ourselves, our students and staff, and our community."

Mr. Jones is constantly pulled in many directions. Nevertheless, he served as the point person when the district decided to roll out a new endpoint protection system to solidify security for students, faculty, and staff.

The move was driven in part by a change in the district's insurance requirements. "Our insurance company let us know that they were tightening their requirements," Mr. Jones explains. "We needed to better secure email, and improve the endpoint solution on each workstation that has access to the internet." The district was at risk of losing insurance coverage at the time of its annual renewal if it did not bring endpoint and email security solutions up to the latest standards.

Inefficiencies in Endpoint and Mail Security District-wide

The Okeechobee County School District uses Gmail for faculty, staff, and student accounts, and it was relying on Google's anti-spam features to fend off attacks. That approach did not meet the insurance company's requirements. Meanwhile, the district was using a third-party point solution to protect its 1,000 endpoints.

"Our previous endpoint security product made it difficult to manage and enforce policies, or to see how the policies that we deployed were affecting users," Mr. Jones says. "I would make a policy expecting it to do one thing, but once we deployed it, it would not do what I wanted. And updating the policies was very manual."

The solution did include a web console designed to centralize management of endpoint security. However, Mr. Jones says, because the system was very complex, "it was not clear whether policies were being sent out, so I would have to drive around the district and check to make sure the product was doing what it was supposed to be doing."

When the insurer raised its expectations for endpoint and enhanced mail security protections, Mr. Jones and his colleagues knew that it was time to increase the efficiency of security district wide.

OKEECHOBEE COUNTY SCHOOLS
ACHIEVING EXCELLENCE

"Deploying FortiEDR was a real eye-opener. It caught some malware lurking on workstations that our previous endpoint security system had not detected."

– Rashan Jones, Coordinator, Network Systems, Okeechobee County School District

Details

Customer: Okeechobee County School District

Industry: Education

Location: Okeechobee, Florida

Endpoints Managed: 1,000

Business Impact

- Fortinet's endpoint and email security solutions met insurer's requirements
- Approximately one hour-per-day reclaimed for district cybersecurity professional
- Improved ability to detect and respond to ransomware or other attempted attacks

Fortinet Solutions That Have "Always Been Rock-solid"

As they began evaluating their options, Mr. Jones and his colleagues reached out to Fortinet. "We have been using FortiGate Next-Generation Firewalls for more than a decade, and FortiGates have always been rock-solid," Mr. Jones says. "It is the backbone of our network—serving not only as our firewall, but also as a router, a VPN (virtual private network) solution, and providing application control and web filtering for our workstations."

In addition, the district has long used FortiAnalyzer, which "gives me insights into what blocked sites our users are still trying to get to," Mr. Jones says. "FortiAnalyzer works hand-in-hand with the application control and web filtering capabilities of the FortiGate."

When the district decided to tighten endpoint and mail security, Mr. Jones contacted his Fortinet representative to see what solutions were available. FortiEDR endpoint detection and response and FortiMail were soon top contenders for the district's business because of their ease of deployment, configuration, and management. "We were impressed with the fact that these products are so easy to administer, yet do not get in the way of the user experience," Mr. Jones explains. "We decided to deploy FortiEDR on all the district's workstations."

Visibility into Application and Data Usage Throughout the District

Okeechobee County School District rolled out FortiEDR on every faculty and staff endpoint, as well as all the servers. Mr. Jones says the FortiEDR server was functional within the first day, and rollout to all the district's workstations took a few additional weeks.

During deployment, Mr. Jones particularly liked that FortiEDR enabled him to test policies before committing to them. "You can put policies in place but not enforce them," he says. "Then you can see what is going on and how your policies would affect that. In some cases, I would roll out a policy, then realize it was stricter than I wanted. This visibility in FortiEDR enabled me to adjust the policy before forcing users to follow it."

These insights continue to be valuable to the district's security posture. "The users do not even know FortiEDR is there—they have not noticed it," Mr. Jones says. "But I can see through the console that it is blocking threats."

In fact, he adds, "deploying FortiEDR was a real eye-opener. It caught some malware lurking on workstations that our previous endpoint security system had not detected. We also discovered quite a few games and other applications on teachers' and staff members' district-owned computers. In some cases, these applications had been there for years, even though they are not allowed by our security policy. The visibility provided by FortiEDR has really helped me crack down on that."

Today, FortiEDR is part of Mr. Jones' day-to-day security management, "On a daily basis, I go into FortiEDR and take a quick look to see what activities it has flagged," he explains. He spends a few minutes a day making sure no pressing endpoint security issues require his attention, then he can move on to his myriad other responsibilities. Before, with the district's legacy endpoint security solution, that daily monitoring took up to an hour and a half. Thus, FortiEDR has given him at least an extra hour per day to support student learning and district administration needs.

Business Impact (contd.)

- Streamlined rollout of new security policies, and quick modification of policies when needed
- Simplified enforcement of district-wide policies around application usage and detection of noncompliance

Solutions

- FortiGate Next-Generation Firewall
- FortiEDR
- FortiAnalyzer
- FortiMail

"Because the solutions are all tight-knit and woven into the Fortinet Security Fabric, I can see everything that is going on in the network within a single pane of glass. Our security environment is so much easier to manage when I do not have to log into four separate systems to see what is happening."

– Rashan Jones, Coordinator, Network Systems, Okeechobee County School District

He is saving time on rolling out updates to endpoint security policies, as well. "The endpoints are separated into groups, by school, and when I roll out a policy change, it can either go to all systems across the district or to specific schools. Either way, it takes one click and the policy is distributed to everyone who needs it," Mr. Jones says. Then, "if FortiEDR is blocking a certain application, activity or website, I can investigate it and determine whether we should allow it. One of the best features of FortiEDR is the great visibility it provides into the individual files and programs that are being used throughout our district."

Security Environment: Safer and Easier to Manage

The district is still finishing up the rollout of FortiMail, but Mr. Jones is looking forward to fully integrating that solution into the district's security landscape. In fact, he says, combining several Fortinet security solutions in his infrastructure has significantly streamlined its management.

"Because the solutions are all tight-knit and woven into the Fortinet Security Fabric, I can see everything that is going on in the network within a single pane of glass," Mr. Jones says. "Our entire security environment is so much easier to manage when I do not have to log into four separate systems to see what is happening."

Even more important, district administrators have more confidence that Mr. Jones is keeping the network secure, and the district's insurance company is satisfied with its endpoint and email security measures. "Attacks can always happen, but our IT infrastructure is much safer today than it was before we worked with Fortinet," Mr. Jones says. "I could not do what I do without the Fortinet community of products."

October 11, 2022 2:18 AM
1666551-0-0-EN