CASE STUDY

Fortinet Managed Endpoint Protection Efficiently Safeguards School District Information

For the IT infrastructure team at the third-largest school district in Nebraska, staff resources are always tight. The 3,000 staff members of the Omaha-area Millard Public Schools serve 24,000 students across 35 schools. Every elementary student has access to an iOS tablet. Every middle school and high school student has an assigned PC laptop. Still, the district's entire back-end infrastructure—from switches to telecommunications to security—is managed by a team of six.

"Our biggest cybersecurity challenge is finding the hours in the day," says Joe Kuehl, district technology manager for Millard Public Schools. "We are a small team when you consider that we are supporting around 30,000 endpoints. We know we are not getting additional money to bring more staff on board. So, as cybersecurity has become increasingly important, we have had to reconsider how to effectively protect our systems without eliminating any other critical day-to-day responsibilities."

Learning the Threat Landscape

Cybersecurity is a topic that keeps Kuehl up at night. "School districts are appealing to a certain type of attacker because of all the personal information we have," he explains. "If they were able to compromise a kindergartner, no one would even realize it for years. And it's the responsibility of my infrastructure team to protect the children in the district."

Another issue that worries him is the potential impact a ransomware or similar attack might have on district operations. "Technology is central to our learning environments, and our classroom management solution is in the cloud," Kuehl says. "If network services were disrupted, we might see all education across the district grind to a halt. On top of that, we have a number of support functions—including bus transportation, HVAC [heating, ventilation, and air conditioning], and food service—that are necessary to keep the district functioning. If an attack took down our data center, all those services would be at risk."

Millard Public Schools currently protects its network edges by deploying FortiGate next-generation firewalls (NGFWs) in its primary and disaster recovery (DR) data centers. "We have been thrilled with how FortiGate firewalls work," Kuehl reports. That established relationship made Fortinet a leading contender when the district needed to boost its endpoint protection a couple of years ago.

> *"I personally sleep better at night knowing that we have the Fortinet endpoint solutions in place, and the managed service is an additional safety net. We know the Fortinet team will let us know if something is going on, so that we can move quickly to address it."*
>
> *– Joe Kuehl, District Technology Manager, Millard Public Schools*

Details

Customer: Millard Public Schools

Industry: Education

Location: Omaha, Nebraska

Business Impact

- Protection of student and staff information from cyber threats
- Improved management confidence in security approach
- Substantial cost avoidance, as security expertise achieved without expanding staff
- Significant staff time savings projected on third-party software patching

The Right Endpoint Protection

"Our contract for our legacy antivirus solution was ending," Kuehl says. "The infrastructure and desktop support teams evaluated three or four products, including the FortiClient EMS [Endpoint Management Server]. We ran demos of the different products and quickly determined that FortiClient was the best solution to protect our endpoints from the increasingly complex threat landscape."

At the same time, Kuehl says, the infrastructure team wanted similar protections for the 330 servers housed in their two data centers. The FortiEDR endpoint detection and response tool caught their eye. The solution's advanced protection capabilities detect potential threats in real time and can automate threat response procedures with customizable playbooks.

Fortinet helped Millard Public Schools set up a proof of concept for both solutions, and the testing went very well. "Our client and infrastructure teams tested the Fortinet solutions and found that they worked well on both Windows and Mac platforms," Kuehl says. "In addition to the threat detection, the team was very excited about FortiClient's patching capabilities. It can scan devices for third-party products that are out of date, then apply granular patching of those third-party applications using FortiClient as the delivery mechanism. That really separated the Fortinet solution from its competitors."

The district began rolling out the FortiClient EMS to about 20,000 client and staff devices, and deploying the FortiEDR solution on all servers in its primary and secondary data centers. "Our team worked with Fortinet on the initial setup and configuration of the EMS solution, and everything worked well," Kuehl says. "We currently have just under 13,000 clients onboarded, and we continue to move forward."

Deployment of FortiEDR went similarly well. "We deployed everything in silent monitoring mode initially," Kuehl reports, "then went in and set up the exceptions. We tested and were satisfied that nothing within our applications was being blocked if it did not need to be blocked. We are now comfortable going into FortiEDR and making exceptions when events require additional tweaks to the system."

Solutions

- FortiClient EMS
- FortiEDR
- FortiGate
- FortiMail
- FortiAnalyzer

Services

- FortiGuard Managed Detection and Response

"In addition to the threat detection, the team was very excited about FortiClient's patching capabilities. That really separated the Fortinet solution from its competitors."

– Joe Kuehl, District Technology Manager, Millard Public Schools

Fortinet Support Services Offer Security Expertise

The new endpoint protection solutions increased the confidence Kuehl and his team had in their security protections, but they were still stretched thin. No one on staff was able to devote as much attention to cybersecurity as Kuehl would have preferred. The ramifications of not having a security-dedicated resource soon became clear.

"When FortiEDR had been up and running for about a month," Kuehl explains, "someone on the Fortinet team was doing a behind-the-scenes quality-assurance audit and stumbled across information in our environment that was concerning. Although this was not the purpose of the audit, they reached out to us to point out the issue. We had several conversations, where they walked us through what they were looking at, step by step. As a result, we discovered that someone was attacking us. FortiEDR had picked it up, but we had not seen it."

Millard Public Schools was quickly able to shut down the attack, preventing any possible data exfiltration or ransomware activity thanks to the FortiGuard team's quick detection and response. Mitigating the damage required rebuilding 10 servers, which took about a week. The attack was annoying, but its impact was not catastrophic. Instead, Kuehl and his team saw it as a learning experience.

"That whole experience highlighted the benefits of having someone with specific cybersecurity expertise looking at the data coming out of your endpoint protection systems," Kuehl says. "In a quick review of the data, the patterns of the attack just jumped out at the Fortinet auditor, who could easily distinguish the actual incident from typical background clutter. No one on our team has the experience or training to do this as well as the folks at Fortinet. We saw the value and added the FortiGuard Managed Detection and Response [MDR] Service on top of the Fortinet products."

Although the district has not experienced another attack since the transition to FortiGuard MDR, Kuehl is very happy with the decision. “I personally sleep better at night knowing that we have the Fortinet endpoint solutions in place, and the managed service is an additional safety net,” he says. “The people running the MDR Service are focused on security. It is all they do, so they are really efficient at recognizing problems. We know the Fortinet team will let us know if something is going on, so that we can move quickly to address it.”

Extending the Relationship

Over the past summer, Millard Public Schools evaluated the FortiMail secure email gateway, to add another layer of security to staff and student communications. “We used a large cloud-based email solution, which does a good job at blocking spam, but we were not confident in the security the solution was providing,” Kuehl says. “We did a demo over the summer and deployed FortiMail before the school year started.”

Previously, he continues, “our email solution might alert us, after the fact, that someone had received a suspicious email attachment, but we might not intercept it until after they had clicked on it. FortiMail has been doing a great job of quarantining suspicious attachments for security reasons, which is crucial in blocking threats.”

The district is still in the process of rolling out the FortiAnalyzer analytics and reporting solution, but Kuehl anticipates that it will boost his security visibility. “We are not yet getting a lot of reporting or notifications out of FortiAnalyzer, but I am looking forward to having a global view of what is happening across our network from a security perspective,” he says. “Taking advantage of the Fortinet Security Fabric and seeing all the different security solutions talk to one another will be powerful.”

Efficiency Plus Expertise Equals Peace of Mind

Millard Public Schools is already benefiting from the consistency of using multiple Fortinet solutions. “The FortiGate firewalls and the FortiMail solution have similar interfaces, which has made them easier for my team to learn,” Kuehl says.

He also appreciates that the Millard Public Schools network is constantly monitored by security specialists. “We did not have to hire a dedicated security person,” Kuehl says. “We have the safety net, at a significantly lower cost than if we had added staff.” The client-and-server team is looking forward to additional efficiencies when they next need to roll out a third-party software patch to tens of thousands of endpoints.

Ultimately, the biggest benefits derive from the relationship that Millard Public Schools and Fortinet have forged. “It is helpful, when we need support, to have just one point of contact at one vendor,” Kuehl says. More than that, “Working with the Fortinet team has been an extremely positive experience for us,” he concludes. “We lean on them anytime security-related questions come up. We bounce ideas off of them, and we always get a straight answer, not a sales pitch. Knowing they are there if we need them truly brings me peace of mind.”

FORTINET®

www.fortinet.com

February 13, 2021 6:42 AM

D:\Fortinet\2020 Old templates\Case Study\Teal Case Study\Millard Public Schools\cs-FA-fortinet-managed-endpoint-protection-efficiently-282021\cs-FA-fortinet-managed-endpoint-protection-efficiently-282021