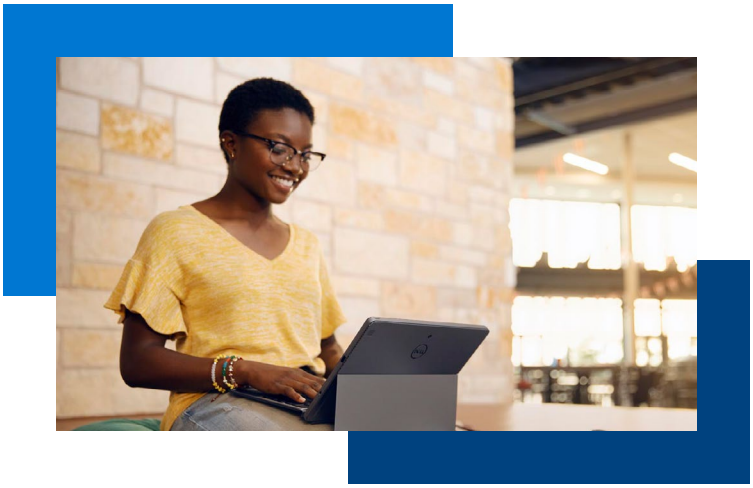
DELL Technologies

Hardening K–12 cybersecurity with expert managed services

Frenship ISD's cyber-aware culture strengthens its defense-in-depth security model, backed by 24/7 Secureworks vigilance.



Customer profile

K–12 Education | United States

"We wanted round-the-clock vigilance and response, simplified single-pane-of-glass management, prioritization of alerts and easy reporting, which is what we got with Secureworks."

Joe Barnett
Chief Technology Officer,
Frenship ISD

Organization needs

With cyberthreats growing in frequency and sophistication, Frenship Independent School District wanted to strengthen its layered, defense-in-depth cybersecurity model by raising awareness across the district, especially at the highest levels, and adding 24/7 proactive threat intelligence and reactive threat response.

Organization results

- Enhanced 24/7 threat protection and response.
- Improved visibility of threats and safeguards.
- Faster threat response, cutting reaction times by up to 85%.
- Simplified yet sophisticated threat reporting to save time keeping district leadership and staff well-informed.
- Prioritization of over 50 million threat alerts a year.
- A more informed and cyber-aware district culture supported by leadership.

Solutions at a glance

- Secureworks Threat Detection and Response
- Secureworks Managed Detection and Response

Cyberattacks are increasing in frequency and sophistication globally. But to think that Frenship Independent School District (ISD) in Lubbock County, Texas, might be targeted by nation-state threat actors located overseas may be hard to imagine for its 10,000-plus students and 1,200 faculty and administrators, not to mention students' parents.

Not so for Joe Barnett, the district's chief technology officer, who firmly believes each of those groups must be made aware of the many cyberthreats rocking the defenses he and his IT team have put in place. In fact, all would be shocked to learn these defenses issue more than 50 million threat alerts each year.

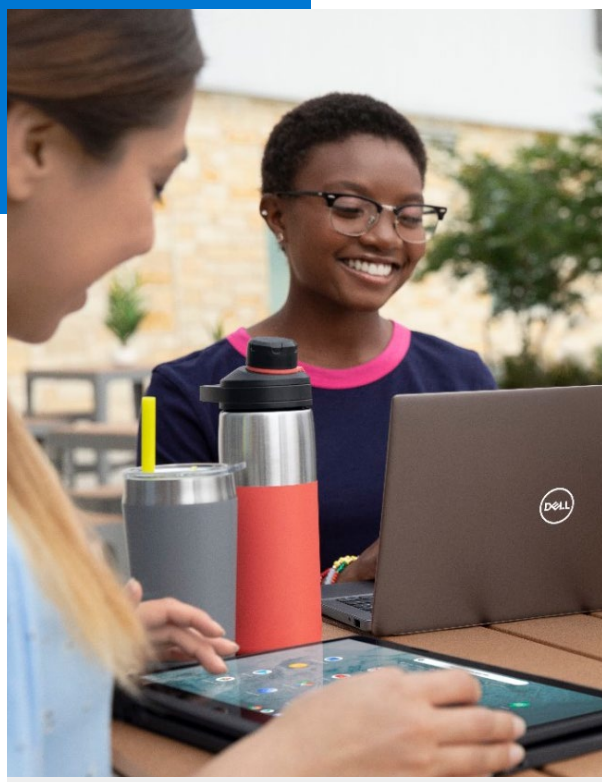
"We've seen a rise in nation-state activities in recent years, along with phishing and ransomware attacks," Barnett says. "K–12 can be as big a target as other institutions and businesses, so we have to keep our guard up like they do to protect our operations and data. The problem is that our job is education, and we need our limited IT resources focused on that mission."

Easy targets

One big concern is keeping student and teacher data private. Student data could be used to open credit card accounts long before the students reach adulthood and result in ruined credit ratings. A ransomware attack could also freeze a district's operations until its applications and data can be restored.

A 2020 U.S. Government Accountability Office report noted that breaches can go undetected for years. In one example, the data of hundreds of thousands of current and former students was compromised and exposed for two years before that district found the breach.

In Barnett's view, K–12 school districts can be easy targets because IT staff resources are limited, cybersecurity skills are expensive to hire and a district's attack surface can have countless vulnerabilities. "Of course, 2020's abrupt school closures and the launch of remote learning models for tens of millions of students sent those vulnerabilities soaring," Barnett says.



"Out of the 14 million alerts we got last quarter, Secureworks prioritized 4,000 of them, with 400 designated as being of medium importance and just one as critical."

Joe Barnett
Chief Technology Officer,
Frenship ISD

Staff time savings of 1,000 hours/year.

Adding safeguards

Fortunately, before all the schools closed, Frenship ISD had already taken a big step toward strengthening its layered, defense-in-depth model.

Barnett's IT team had the best available firewalls in place where needed, plus active antivirus endpoint defenses and strict identity and patch management protocols. It also had automated data protection and recovery in place. But after a prior ransomware scare, Barnett wanted the district to add protection — a 24/7 combination of proactive threat intelligence and reactive intrusion response.

After carefully evaluating all leading vendors, he chose Secureworks. "We wanted round-the-clock vigilance and response, simplified single-pane-of-glass management, prioritization of alerts and easy reporting, which is what we got with Secureworks," he says. "Others had some of what we were looking for, but only Secureworks offered it all."

Specifically, Barnett chose two Secureworks managed services:

- **Threat Detection and Response**, a proactive service delivered via a cloud-native platform that uses insights derived from artificial intelligence combined with threat intelligence from more than 300 security analysts about threats from around the world.
- **Managed Detection and Response**, a reactive service which is powered by sophisticated security analytics software that hunts for threats, prioritizes alerts and recommends appropriate actions, if needed.

The Secureworks engagement started with a discovery phase, conducted by cybersecurity experts, in which all the district's security assets and safeguards were identified and cataloged.

Simplified management, alert prioritization

"All our third-party defenses were being managed in silos," Barnett says. "But now we've simplified our security management with a single dashboard because our Secureworks services can ingest data from all our safeguards."

In addition to the 24/7 protection provided by Secureworks, Barnett appreciates the prioritization of threat alerts. "Out of the 14 million alerts we got last quarter, Secureworks prioritized 4,000 of them, with 400 designated as being of medium importance and just one as critical. Our system either automatically remediates critical incidents or isolates the infected device."

> "The level of specificity and actionable intelligence that accompanies Secureworks critical alerts helps us pinpoint and remediate a problem so much faster."
>
> **Joe Barnett**
> Chief Technology Officer,
> Frenship ISD

> “We’ve cut our incident response times by up to 85 percent with Secureworks threat detection alerts.”
>
> **Joe Barnett**
> Chief Technology Officer,
> Frenship ISD

Because the Secureworks services are cloud-based and its portal’s dashboard interface is coded in HTML5, Barnett and his team can get alerts on any preferred device. They can then immediately access the Secureworks portal to get further information, including an issue’s criticality, plus the tools and specific steps needed to remediate a problem.

According to Barnett, Secureworks managed services have reduced the district’s incident response times dramatically. “The level of specificity and actionable intelligence that accompanies Secureworks critical alerts helps us pinpoint and remediate a problem so much faster.”

Incident response times cut by 85%

“We’ve cut our incident response times by up to 85 percent with Secureworks threat detection alerts,” says Barnett. “Not only does that save us staff time, but it also means the threat has less time to spread and cause wider disruption.”

As for staff time savings, Barnett conservatively estimates those at about 1,000 hours per year. “That’s huge for my size staff,” he says. “It lets them focus more on driving the district’s educational mission.”

Each quarter, a Secureworks expert calls Barnett to review threat and incident activity. It’s intelligence he augments with reports drawn from the portal and then shares with his staff and the district’s cabinet, the superintendent and senior administrators. He makes sure that cybersecurity is also an agenda topic for teacher development meetings and speaks to computer science classes.

“Humans are often the weak link in the cyber-defenses most exploited by threat actors,” he says. “That’s why understanding and support from leadership and other district stakeholders — including teachers, staff and students — are so critical to building a cyber-aware culture that can serve as a human firewall to keep as many threats at bay as we can.”