DELL Technologies

Lufkin ISD: Safeguarding student data from ransomware attacks

Customer profile

Education | USA

> “When you get into work and see the ransom notes and demands from threat actors, it drives home there’s 11,000 people counting on me and my department.”
>
> **Brad Stewart**
> CTO of Lufkin School District

Business needs

- Rapidly respond to a ransomware attack that threatened the security of 11,000 staff and students’ sensitive data
- Evaluate existing security strategy and undertake necessary upgrades
- Provide proactive education and training to staff

Business results

- Locked out ransomware attack and recovered staff and students’ data
- Evaluated environment and implemented security fixes
- 24x7 threat monitoring of environment
- Hired cybersecurity analyst
- Improved employee training

Solutions at a glance

- [Managed Detection and Response]
- [Incident Response and Recovery]

Acting decisively to retrieve sensitive data

Lufkin Independent School District (ISD) is a public school district based in Lufkin, Texas. It serves a range of primary, elementary and secondary schools, catering to students between 5-18 years of age throughout the community.

In 2021, Lufkin ISD was targeted by a major ransomware attack. Hackers based in the Netherlands gained control of four security camera servers, in turn accessing, moving and encrypting data from the district's virtual servers. Staff initially became aware of the issue on a Monday morning when they couldn't log into their systems, but the problem was already far more severe than that: sensitive data belonging to 11,000 of the district's staff and students had been stolen, while the district had also lost control of functions such as air conditioning, registration and grade administration. The hackers demanded $1.5 million dollars in bitcoin to restore access.

Lufkin ISD's CTO Brad Stewart faced some immediate challenges: he needed to recover the stolen data; he needed to discover the source of the breach; and he needed to ensure a ransomware attack like this couldn't happen again. He immediately called Dell Technologies to utilize their Incident Response and Recovery Services for recovery and Managed Detection and Response to improve the district's security posture.

> "Within two hours we had the first Dell boots on the ground in the office. We felt we could start leaning on someone to get us out of the mess we were in."
>
> **Brad Stewart**
> CTO of Lufkin School District

Protecting educational institutions with enterprise-class security

Restoring systems, security and trust

Following a review of Lufkin ISD's systems in the aftermath of the ransomware attack, Dell rebuilt the district's entire data center while implementing new security protocols. Dell also embarked on a series of educational measures to help ensure future business continuity. For example, Dell liaised with Lufkin ISD's technology department to upgrade its employee training procedures so they could understand how the ransomware attack occurred.

Meanwhile, as a result of Dell's 24/7 monitoring, the Lufkin ISD hired a cybersecurity analyst responsible for reviewing the Dell Managed Detection and Response dashboard each day.

A swift response delivered by cybersecurity specialists

A fast response to the ransomware attack was critical — and Dell delivered with its enterprise-grade response and recovery services. Within two hours of making the initial phone call, a member of its team arrived at the Lufkin ISD office to initiate the response to the ransomware attack. More Dell staff then continued to show up on site over the following 24 hours until a complete team of industry-certified cybersecurity professionals was present.

Following the ransomware attack, strengthening Lufkin ISD's security posture became an urgent priority. The Dell team completed an evaluation of the district's environment, from its IT infrastructure to its backups, identifying security concerns and implementing appropriate fixes. They also recommended a proactive solution in the form of 24/7 monitoring.

While the Lufkin ISD team had previously been unable to monitor its network due to a lack of personnel, Dell Managed Detection and Response powered by Secureworks® Taegis™ XDR provides this as part of an integrated service. By using Taegis XDR security analytics software with machine learning and curated threat intelligence — vital in today's rapidly changing security threat landscape — experienced and certified Dell analysts can monitor suspicious activity within Lufkin ISD's environment, alerting the Lufkin ISD team if a threat is malicious or requires their attention.

> "Dell's 24/7 monitoring gave us the opportunity to have monitoring full time when I didn't have the personnel to do it."
>
> **Brad Stewart**
> CTO of Lufkin School District

> “Dell really has come through for us. They have always been there. They’re always suggesting new products and different things that we can use.”
>
> **Brad Stewart**
> CTO of Lufkin School District

If any issues occur, the analyst can collaborate with Dell to remediate them. Following the vulnerability and uncertainty of the ransomware attack, Stewart added: “it really helps us sleep at night, knowing that we have Dell watching our back for us”.

Together, Lufkin ISD and Dell Technologies recovered the sensitive data of 11,000 staff and students, without caving into any ransomware demands. What started as a highly critical, time sensitive crisis management situation has now transitioned into a longer-term, holistic review of the district’s systems — but also a strong, lasting relationship. As someone who prefers cultivating a personal relationship with a vendor, Stewart said: “Dell really has come through for us. They have always been there. They’re always suggesting new products and different things that we can use.”

In a world where security threats are constantly evolving and becoming increasingly frequent, Lufkin ISD knows it can rely upon Dell Technologies and its Managed Detection and Response solution to stay secure.

Learn More About Dell Technologies Solutions.

Contact a Dell Technologies Solutions Expert.

DELL Technologies

Connect on social