



CUSTOMER STORY

BULLWALL PROVIDES EDUCATORS WITH AFFORDABLE RANSOMWARE PROTECTION TO SAFEGUARD STUDENT DATA



Industry
Education



Location
United States



Users
10,000



Students
80,000

SECURITY STACK



Why are schools ideal targets for ransomware?

1 Limited funding and resources make schools easy targets

2 Virtual and hybrid learning increased attack surfaces

3 Increasingly sophisticated attacks are harder to combat

FILESHARE INFRASTRUCTURE



Cloud

OVERVIEW

A large school district in Texas serving 80,000 students needed a cybersecurity solution that offered the greatest protection within its limited budget and resources. Their highest priority was securing student data and critical IT systems. With a narrow security stack and a mix of on-premises and cloud systems, they knew they couldn't afford to safeguard all entry points against ransomware threats. So the district adopted BullWall to deliver 24/7 ransomware monitoring with automated containment at the point of attack. This enabled the district to protect its data and most valuable assets without breaking the bank, and gave them peace of mind that should an attack occur, they will be able to identify and mitigate the threat immediately.

SCHOOLS PROVIDE LOW-COST, HIGH-REWARD TARGETS FOR RANSOMWARE ATTACKS

Cyber threats against the education sector are on the rise. Schools store a goldmine of sensitive student and staff data, including personally identifiable information (PII). This makes them valuable targets for bad actors. Yet, nearly a fifth of K-12 schools invest less than 1% of their IT budget on cybersecurity—leaving them open to greater risk of cyber attack and unprepared to mitigate the damage when it occurs.¹

UNDERFUNDED, UNDER-PROTECTED

This reality has made life as a school IT administrator increasingly difficult. Not only do administrators need to upgrade their infrastructure to support emerging technologies and BYOD policies, but they have to find a way to do so securely. This is the challenge the Head of Information Security at a large school district in Texas was struggling to address since the COVID pandemic.

With limited funding, minimal staffing, and a narrow security stack that did not provide comprehensive visibility or endpoint protection, the school district was exposed.

"I knew it was if, not when we were going to have an ransomware attack. So we've done as much as we can with our limited resources to identify, detect, and protect," he shared.

¹Multi-State Information Sharing and Analysis Center, "K-12 Report: A Cybersecurity Assessment of the 2021-2022 School Year."

The administrator knew that as a small IT team, they couldn't be available to respond to threats at all hours. And with 90,000 staff and students to cover, he didn't have the manual resources to monitor the district's extensive environment.

He needed a security solution that could detect and automatically stop active ransomware attacks in their tracks. So when he discovered BullWall, the decision was an easy one.

PROTECTING THE MOST VALUABLE RESOURCES

When you have limited resources, you have to make tough decisions about where to focus your dollars and security efforts.

"We had to ask ourselves, 'What do we care about the most?' And what we care about is keeping student data and our critical systems safe," he explained. "We just are not in a position to be able to afford high-end tools with all the bells and whistles."

But with BullWall, limited resources don't have to mean limited protection. Instead of focusing on ransomware prevention through endpoint security, BullWall provides targeted detection and containment at the source of the attack.

"Having BullWall in place was really beneficial because we could use our very limited school district resources to invest in a solution we knew would return the most value."

BullWall provides IT personnel with comprehensive visibility into their networks while enhancing security at a fraction of the cost. And because it is fully automated, it doesn't require an expert or additional staff to manage the solution—freeing up IT admin to focus on other priorities while enjoying greater peace of mind that when something does go wrong, BullWall will jump into action.

“

BullWall is keeping an eye on the data we care about most.

”

ABOUT BULLWALL

BullWall is a cybersecurity solution provider with a dedicated focus on protecting data and critical IT infrastructure during active ransomware attacks. We are able to contain both known and zero-day ransomware variants in seconds, preventing both data encryption and exfiltration.

BullWall is your last line of defense for active attacks.

Learn more at www.bullwall.com.

