BULLWALL FOR EDUCATION

With over 600 successful attacks against the education sector in the last five years, exceeding $53 billion in ransom payments and cost of downtime, ransomware remains a major threat.

A SUCCESSFUL RANSOMWARE ATTACK CAN HAVE GRAVE CONSEQUENCES THAT REACH FAR BEYOND THE FINANCIAL IMPACT.

From disrupting access to critical educational resources, to stealing student identities and causing massive operational damage, these attacks have lasting impacts on both learning outcomes and institutional reputations. The need for rapid containment and response is more urgent than ever.

WHY BULLWALL?

BullWall provides a specialized ransomware containment solution that protects educational institutions by quickly detecting and halting ransomware attacks before attackers can encrypt or exfiltrate data.

By stopping attacks in their tracks, BullWall helps educational institutions avoid data breaches that could expose student, faculty, and administrative data, thereby reducing the risk of identity theft, financial fraud and regulatory issues.

39%

of educational establishments attacked **were offline for more than 2 weeks**

37%

of educational establishments **who paid the ransom didn't receive the encryption key**

State of Ransomware in Education, Sophos

> *I experienced an attack where a cybercriminal used a valid user account to get in remotely. You can't prevent that.* ***You need a ransomware containment solution like BullWall.***"

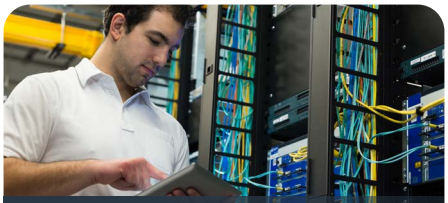
SHARN SOMERTON-DAVIES
IT Manager, Sir Roger Manwood's School

HOW EDUCATION BECOMES A RANSOMWARE TARGET

LEGACY SYSTEMS

40%

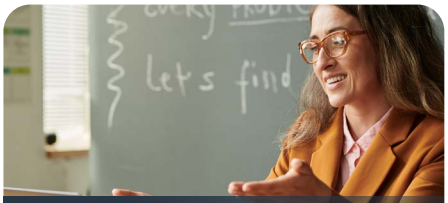
of ransomware attacks are a direct result of outdated legacy systems that are vulnerable to attack. Legacy systems are common in education due to budget limitations and the high costs of upgrading technology.



RESOURCE CONSTRAINTS

66%

of attacks against educational institutions exploited known but unpatched vulnerabilities, often due to resource constraints, limited cybersecurity staffing, and outdated infrastructure common in schools.



PHISHING EMAILS

30%

of ransomware attacks on educational establishments in 2024 were caused by phishing emails with harmful links or attachments, often impersonating trusted sources, such as colleagues or institutions.

THE IMPACT

The impact of an attack far outweighs the simple financial loss of paying the ransom. Many other factors must be considered, all of which have long-lasting implications for the future of the affected establishment.

STUDENT DATA PRIVACY

A ransomware attack that compromises student data can trigger violations of federal and state data protection laws, such as FERPA, HIPAA and UK GDPR.

STUDENT IDENTITY THEFT

When a system is compromised, attackers gain access to sensitive student data. Criminals can then use this data for identity theft, opening fraudulent credit accounts or applying for loans or benefits in a student's name.

PSYCHOLOGICAL IMPACT

Ransomware attacks create stress, anxiety and uncertainty for students and staff. Cancelled exams mean students might require more time to progress to higher education or employment, leading to claims for damages if students can demonstrate financial or career-related harm.

WHAT IS RANSOMWARE RESILIENCE?

Ransomware resilience is the ability to prevent, contain, and respond to ransomware attacks, minimizing damage and ensuring rapid recovery of data and operations to maintain business continuity.

PREVENTION

Reduce the risk of disruptions to operations, which can be costly and damaging to productivity.

CONTAINMENT

Minimize the impact to business operations when ransomware gets through, and significantly reduce recovery efforts.

RECOVERY

Resilient organizations recover quickly to limit operational downtime and return stronger.

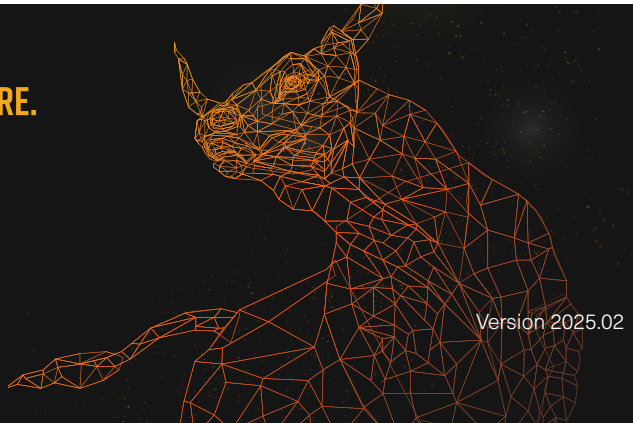
BE RANSOMWARE READY... WITH BULLWALL

BullWall's unique approach to ransomware provides server-based protection without an endpoint agent to secure critical IT infrastructure and maintain operational continuity across all stages of an attack—before, during, and after.

Legacy IT systems are easy targets for ransomware.	**BullWall is the only solution that immediately contains an active attack,** preventing spread, protecting staff and student data, and critical operations, even on legacy infrastructure.
Ransomware exploits weaknesses in critical academic systems such as student information databases and learning management platforms.	**BullWall addresses urgent gaps left by traditional security solutions,** containing attacks instantly without endpoint installations, ensuring these systems stay secure.
Cybercriminals use phishing emails to exploit the weakest link in the security chain – the human link.	When teachers, administrators or students click on something they shouldn't and trigger a payload, **BullWall instantly isolates and quarantines the user and stops the attack.**

THINK YOU'RE RANSOMWARE RESILIENT? FIND OUT FOR SURE.

BOOK ASSESSMENT



BULLWALL | RANSOMWARE RESILIENCE FOR CRITICAL IT INFRASTRUCTURE