CASE STUDY

Helping a School District Recover from a Ransomware Attack

The challenge: Urgent Recovery: Restoring a School District After a Devastating Cyberattack

A large school district in the Western region found itself in a dire situation when a massive ransomware attack crippled its network, taking down 75% of its virtual machines and core infrastructure. The impact was swift and devastating, leaving the district's IT team scrambling to find a way to restore operations in time for the upcoming school term – in two short weeks.

Prior to the attack, the district had been making strides toward improving its security and data protection posture, recognizing the growing threats that educational institutions face. However, when the breach occurred, the district quickly realized that its existing backups were insufficient. The most recent usable data was months old, forcing administrators to rely on outdated information and systems to piece together a recovery plan.

The solution: Rapid Recovery & Future-Ready Cybersecurity: C1 Delivers Resilient Solutions

C1 swiftly deployed its expert recovery team for an emergency response, ensuring comprehensive remediation and a full system rebuild for the customer. Understanding the urgency of the situation, C1 dedicated a team of engineers to work on the project full-time, meticulously restoring operations and strengthening the customer's infrastructure. Thanks to this focused effort, the customer was able to regain full functionality in less than four weeks—minimizing downtime and mitigating further risk.

Beyond recovery, C1 took proactive steps to enhance the customer's long-term cybersecurity posture. Recognizing the need for a more resilient solution, C1 introduced an advanced Cyber Recovery Solution designed to provide stronger protection while simplifying management for the customer's IT team. This new system ensures greater security against future threats, offering seamless recovery capabilities and making ongoing cybersecurity management more efficient and accessible.

The result: Turning Crisis into Resilience: Strengthening Cybersecurity After a Ransomware Attack

The ransomware attack served as a critical turning point for the school district, prompting them to take significant steps toward strengthening their cybersecurity posture. The experience underscored the urgent need for a more resilient security framework, leading the district to implement a comprehensive cyber recovery solution designed to safeguard its systems from future threats.

Recognizing the vulnerabilities that had previously left their infrastructure exposed, the district overhauled its security protocols and introduced stringent access control measures. Now, before any data access is granted, a rigorous validation process ensures that all requests meet strict security requirements, minimizing the risk of unauthorized entry or malicious activity. These proactive measures are designed to prevent a recurrence of the attack and to fortify the district's defenses against emerging cyber threats.

Powering student outcomes through technology

Confidently deliver instruction without disruption.

Contact an expert: https://www.onec1.com/contact-us