datto
A Kaseya COMPANY

How Datto EDR with Ransomware Rollback Helps Schools Recover Fast from a Ransomware Attack

Schools are the top target of ransomware attacks - 80% of schools in the U.S. and 14 other countries have been victims of ransomware attacks since 2022. Ransomware also enables bad actors to access, steal and/or delete sensitive student and administrative data. Datto EDR's Ransomware Rollback feature makes it simple to recover all your data and resume normal operations swiftly in the event of an attack. Here's how it works:

01

Cybercriminals exploit a vulnerability in your network

The most likely way for ransomware to enter your environment is through a phishing email, a malicious message that uses social engineering to trick the recipient into clicking links, providing their credentials or opening files. Schools or school districts that have a weak point in their networks, such as a lack of training or a substandard security posture, make cybercriminals' jobs easier.

02

Malicious code infects a device and installs ransomware

Ransomware is a type of malware that bad actors use to force a variety of negative outcomes on an organization, like encrypting, stealing and/or leaking data. Once the attack is initiated, the perpetrators will demand payment to prevent those negative outcomes for the victim. However, paying them doesn't always work — 80% of organizations that pay a ransom are attacked again.

03

Files and systems are locked down by encryption

Ransomware starts its dirty work by encrypting systems and files. Once the ransomware infection is triggered, the malware encrypts data located on that system, making files and folders inaccessible. Bad actors often copy and sell the data they access on the dark web. If a school or school district has its data stolen, that could include sensitive student data. Paying off the extortionists is no guarantee you'll get your data back, as an estimated 40% of victims have discovered.

04

Ransomware Detection stops data encryption fast

The Ransomware Detection feature of Datto EDR detects a ransomware attack immediately, stopping the encryption process from going any further. This helps minimize the spread of ransomware as well as data loss, helping schools and school systems limit expensive damage and recover faster.

05

Datto EDR isolates endpoints and eliminates the ability for the ransomware to spread

Datto EDR enables schools and school districts to quickly detect and respond to cyberthreats by isolating the affected endpoints to minimize damage and any disruption to learning. The loss of learning following a cyberattack ranges from three days to three weeks, and recovery time could take anywhere from two to nine months.

06

Get files back to their original state and save money with Ransomware Rollback

If your data is encrypted in a ransomware attack, you face an expensive nightmare of recovery costs. Schools report monetary losses between $50,000 to $1 million if they face a cybersecurity incident, not counting any ransom paid. Plus, bad actors can delete your files, making recovery impossible. However, the Ransomware Rollback feature in Datto EDR eliminates that problem. With Ransomware Rollback, you can simply go back in time to before the attack and restore your files to their original state.

Although ransomware recovery is challenging, the Ransomware Rollback feature in Datto EDR makes it easier, faster and less expensive. Instead of worrying about how to unlock their data or get it back from the bad guys, a school or school district can simply rollback those files to the state they were in before the attack, making it easy to get back to the important business of schools: educating students.

Want to learn more about Datto EDR and Ransomware Rollback?

Request a demo