datto | EDR

How Datto EDR With Ransomware Rollback Helps You Recover Fast From a Ransomware Attack

Every organization is at risk of a ransomware attack. By 2025, 75% of businesses will have been infected with ransomware at least once. If your organization falls victim to a ransomware attack, getting your data back could be one of the most challenging parts of your recovery. However, with Ransomware Rollback, it's easy to recover all of your data and get back to work quickly. Here's how it works:

1 Cybercriminals identify a vulnerability in your network

The most likely way for ransomware to enter your environment is through a phishing email that employs social engineering to trick users into clicking links or opening files. Organizations that have a weak point in their networks, such as a lack of training or a weak security posture, make cybercriminals' jobs easier.

2 Ransomware infects a device and begins spreading

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 company data. 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.

3 Data and systems are locked down by encryption

Ransomware starts its dirty work by encrypting systems and data. Once the ransomware infection is triggered, the malware encrypts data located on that system, making files inaccessible. However, paying off the extortionists is no guarantee you'll get your data back, as an estimated 40% of victims have discovered.

4 Ransomware Detection stops data encryption fast

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

5 Datto EDR isolates endpoints quickly to reduce the impact of a ransomware attack

Datto EDR enables you to quickly detect and respond to cyberthreats by isolating the affected endpoints to minimize damage and financial loss. This is important because a data breach caused by a ransomware attack is 12% more expensive than a data breach from another cause.

6 Get files back to their original state with Ransomware Rollback

If your data is encrypted in a ransomware attack, you face an expensive nightmare of recovery costs and lost productivity. Plus, bad actors can delete your files, making recovery impossible. However, the Ransomware Rollback feature eliminates that problem. With Ransomware Rollback, you can simply go back in time to before the attack and recover those files. By tracking changes to users' files in real-time, Ransomware Rollback allows you to restore files to their original state so you can get back to work faster.

Although ransomware recovery is expensive and challenging, the Ransomware Rollback feature in Datto EDR eliminates one of those problems immediately. Instead of worrying about how you can unlock your data or get it back from the bad guys, you can simply rollback your files to the state they were in before the attack, saving your company money and yourself stress.

Want to learn more about Datto EDR and Ransomware Rollback?
REQUEST A DEMO

datto
A Kaseya COMPANY