Ransomware Unlocked

Attackers typically gain unauthorized access to networks 6 months or more before they are detected.

Cybereason Ransomware Often Goes Undetected

Ransomware attacks are persistent, pervasive, and have a track record of success. That means it's essential for critical business data to be immutable to threats. Read on to learn about the latest ransomware trends powering the shift from prevention tactics to a data-resilient approach.

Paying the Ransom

The cost of downtime can be 50 times greater than the ransom demand.

44:01.70

96.88 percent of all ransomware infections take under 4 hours to infiltrate their target.

It could take a ransomware attack as little as 45 minutes to compromise a target.

AvePoint Companies that pay the ransom typically only get about 60% of their data back. Only 4% receive all of their data.

80% of organizations who paid a ransom demand were hit by ransomware a second time.

The Cost of Ransomware Is Rising

Cybersecurity Ventures predicts that by 2031, ransomware will cost victims $265 billion annually.

The Frequency of Ransomware Attacks

Attacks are becoming increasingly frequent, making it crucial to assume that your organization will be targeted at some point.

Resilience in the Face of Ransomware

Panzura protects companies from being8 validable data.

Ransomware Entry Points

Compromised Credentials
Phishing Emails
Cloud Misconfiguration
Accidental Data Loss/Lost Device
Malicious Insider
Physical Security Compromise
Vulnerability in Third-Party Software

Ransomware Often Goes Undetected

97% of organizations are aware of ransomware entry points. Still, only 72% of companies have detect-and-eradicate technologies in place to identify and remediate ransomware.

Back-Up Beware

95% of companies now backup their data, but only 21% of these backups are truly validable.

Learn more at Panzura.com