NetApp

COMBAT RANSOMWARE
WITH NETAPP

Protect: Secure your environment
Detect: Anticipate threats
Recover: Bounce back quickly

The challenge

When you consider how cheap, easy, and high-paying cybercrime is, it's no wonder that many businesses are sitting ducks for costly attacks.

- Over the past year, <u>72% of organizations</u> saw an increase in the volume, complexity, or impact of cyberattacks

- Ransomware attacks happen <u>every 11 seconds</u>

- Recovering from a ransomware attack costs <u>$1.4 million</u> on average

- The average victim loses <u>39%</u> of their data

- The average time to recover from an attack is <u>one month</u>

NetApp cyber resilience: a data-centric approach to ransomware protection

Most technology vendors have traditionally focused on ransomware recovery: getting businesses back online after they've been attacked.

But that approach alone is like cleaning up the feathers after the fox has been through the henhouse. A necessary task, but it doesn't help the chickens much.

NetApp takes a comprehensive and preventative approach to ransomware protection. In addition to advanced technologies that deliver rapid recovery, initiating backups even before admin intervention is needed, our solutions have built-in features that protect and secure primary data, using AI and machine learning to proactively spot and counter malicious or irregular actions.

NetApp's robust cyber resilience portfolio ensures you have the right enterprise data protection and security in place before an attack happens. With NetApp, you'll outfox cybercrime.

NetApp cyber resilience: a data-centric approach to ransomware protection

Most technology vendors have traditionally focused on ransomware recovery: getting businesses back online after they've been attacked. But that approach alone is like cleaning up the feathers after the fox has been through the henhouse. A necessary task, but it doesn't help the chickens much.

NetApp takes a comprehensive and preventative approach to ransomware protection. In addition to advanced technologies that deliver rapid recovery, initiating backups even before admin intervention is needed, our solutions have built-in features that protect and secure primary data, using AI and machine learning to proactively spot and counter malicious or irregular actions.

NetApp's robust cyber resilience portfolio ensures you have the right enterprise data protection and security in place before an attack happens. With NetApp, you'll outfox cybercrime.

Intelligently protect against internal and external threats

Avoiding ransomware attacks starts with knowing what data you have, what's valuable, sensitive, and vulnerable, where it is stored, and who has access to it. Cloud Data Sense identifies, maps, and classifies all your data, on premises or in the cloud, to help you improve your security posture and comply with regulations. Active IQ Digital Advisor takes a closer look at your defenses by performing health checks and providing best practices so you can better reinforce your storage environment.

The NetApp portfolio provides rugged, multilayered defenses to intelligently and efficiently protect your data, including secure data access through end-to-end encryption, multifactor authentication, and role-based access. ONTAP can block known malicious file extensions before they can be written to disk while Snapshot provides a read-only unencryptable data copy. By applying WORM (write once, read many), SnapLock prevents encryption and deletion of data with indestructible and efficient data copies.

And by enacting multi-admin verification, you can ward off lone rogue administrators by requiring more than one admin to approve critical tasks. Finally, Cloud Backup securely and efficiently copies data to object storage to reduce cost and increase recovery. Yes, there's a lot to it. And we make it easy to manage through a single UI, Cloud Manager.

KEY BENEFITS

Intelligently protect against internal and external threats

- Automatically discover and classify data to identify what is vulnerable, sensitive, or critical to protect

- Enact strong security controls with multi-admin verification, multifactor authentication, and role-based access

- Efficiently and securely protect data with inline and at-rest encryption, secure data replication, and immutable and indelible data copies

Quickly detect threats before they impact operations

- Identify user behavior anomalies to spot compromised user accounts or insider threats

- Detect possible ransomware attacks through storage-based anomaly detection and machine-learning-based file system monitoring

- Prevent malware attacks through integration with leading virus-scanning software

Rapidly recover data and accelerate application uptime

- Respond to threats in real time by automatically creating immutable recovery points or blocking user access to storage

- Apply intelligent forensics to help identify the source of the threat and which files to recover

- Restore petabytes of data in minutes, locally or remotely, to accelerate operational recovery

Quickly detect threats before they impact operations

Fighting ransomware attacks is not just about whether or not you can take a punch. It's also about dodging the blow before it connects. Using AI and machine learning, NetApp helps you identify threats quickly before they impact operations.

NetApp's ONTAP capabilities prevent malware attacks by integrating with leading virus-scanning software and alerting when detecting storage anomalies. Our autonomous ransomware protection feature provides early detection of file system anomalies, alerting you if something suspicious is afoot and automatically triggering a recovery point.

Cloud Insights tackles the human factor: identifying user behavior anomalies. This automated feature learns which patterns are normal and which ones are not. Are files being accessed or changed at unusual times or by different pathways? Is an attempt at mass file deletion in progress? For most businesses, this is too much to verify manually, and by the time an admin detects it, the damage may already be done. Cloud Insights can identify anomalous user behavior in real time and provide automated responses such as creating a Snapshot recovery point or even blocking user access to the storage. With these measures, NetApp makes your company a more elusive target for cybercrime.

Rapidly recover data and accelerate application uptime

A ransomware attack can happen despite your best preventative efforts. So rapid recovery is critical to minimize the cost of downtime. When anomalous user behavior is identified, Cloud Insights immediately stops the bleeding by automatically creating recovery points and blocking compromised user accounts. Cloud Insights and Cloud Data Sense together offer capabilities to help you forensically identify the source of the threat and prioritize which data to restore. Within minutes, ONTAP SnapRestore can restore petabytes of data locally or remotely, mitigating the impact of the attack on your business.

Ransomware can debilitate enterprises that don't take it seriously. Only NetApp's cyber resilience approach provides comprehensive, integrated data security and protection for primary and secondary data to keep your business safe.

Learn more here
www.netapp.com/cyber-resilience/ransomware-protection/

"We recently experienced a ransomware event, and when we saw what Cloud Insights ransomware detection provides, we were sold."

Director of IT, transportation company

Contact Us

NetApp