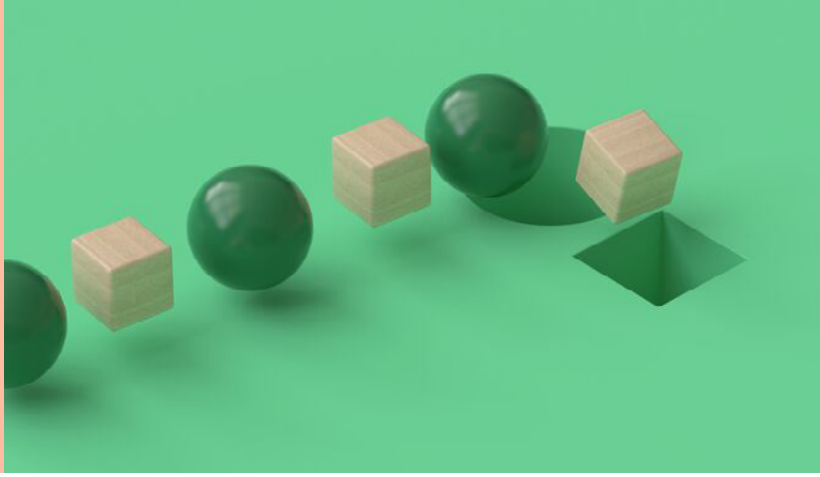
5 reasons – NetApp for ransomware protection



What if you could prevent cyberattacks before they happen, detect external and insider threats in real time, and accelerate data recovery to minimize downtime? With NetApp® technology, you can do all of this—no matter where your data lives.

1. Identify

If an attack occurs, you need to know immediately what's missing or compromised. Our solutions keep your data under close watch with automatic discovery and classification, easy inventory of the infrastructure system and resources, and optimized volume permissions—all while automatically applying system health recommendations.

2. Protect

An ounce of prevention is worth a pound of cure. Protect your data by blocking known malicious files, and prevent data destruction with copies that are efficient, immutable, and indelible. Encrypt data in flight and at rest, and block rogue actors with a Zero Trust architecture that uses multi-admin verification and multifactor authentication.

3. Detect

A ransomware attack is a race against the clock. With NetApp technology, you can identify threats in real time. Storage behavior monitoring can detect anomalies like slow-moving encryption. It can also detect user behavior anomalies that might indicate compromised user accounts or malicious insiders.

4. Respond

The faster you respond to an attack, the sooner you can recover and mitigate damage. Instantly block user storage access when an anomaly is detected, and automatically respond to detected threats with NetApp Snapshot™ recovery points.

5. Recover

Paying ransom isn't the most costly consequence of an attack; it's downtime. Recover terabytes of data in seconds to support rapid operational recovery, and conduct detailed forensic analysis and auditing so that lightning doesn't strike twice.

Explore ransomware protection

Connect with a cyber-resilience specialist

NetApp

+1 877 263 8277