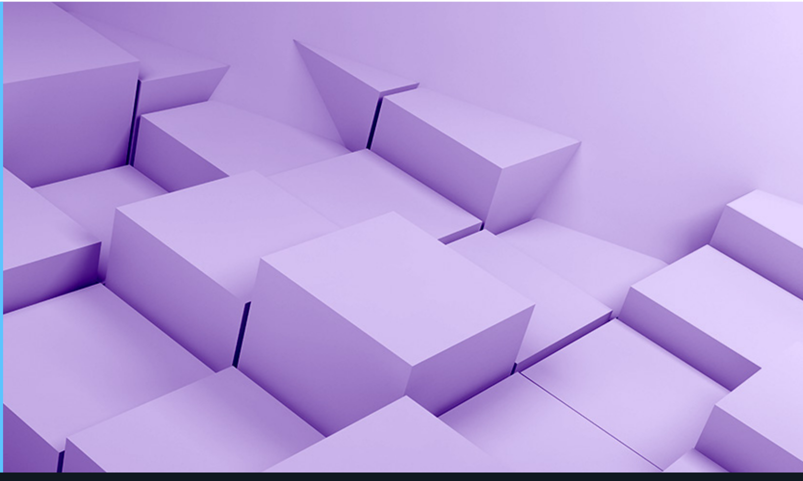
10 REASONS

NetApp for Ransomware Protection



01

Logical air gap

Create a logical air gap for secure file and object locking. NetApp® SnapLock® Compliance and NetApp StorageGRID® S3 Object Lock offer native WORM (write once, read many) capabilities to prevent data from being deleted during the retention period, even by compromised administrator accounts.

02

Rapid recovery

The highest cost of a ransomware attack is downtime. Quickly bring your data back online by using NetApp immutable Snapshot copies. And discover what it's like to restore terabytes of data in seconds, not hours.

03

Autonomous ransomware protection

Rapidly discover and remediate cyberthreats by using machine learning technology. Built into NetApp ONTAP® software, this technology monitors the file system for anomalies, which can indicate slow-moving malware. Use built-in anti-malware file-extension blocking to detect and prevent known malware from spreading in the first place.

04

User behavior anomaly detection

Detect anomalies in real time to identify compromised user accounts or possible rogue behavior by using the Cloud Secure feature of NetApp Cloud Insights. Combined with the NetApp FPolicy component of ONTAP, you can automatically create data recovery points and even block further account access to prevent data theft or mass deletion.

05

Zero Trust compatible

Embrace a Zero Trust approach to security with controls such as multifactor authentication, role-based access, comprehensive logging, and auditing to protect against ancillary attacks.

06

Rogue administrator prevention

Prevent damage from compromised administrator accounts by using native ONTAP multi-administrator verification. This feature requires more than one administrator to authorize critical storage actions such as the deletion of volumes and Snapshot copies.

07

Advanced copy management

Achieve enhanced backup and disaster recovery. Use NetApp SnapMirror® and the NetApp Cloud Backup service to replicate your Snapshot copies efficiently to another ONTAP system or object storage of your choice—on premises or in the cloud.

08

Risk mitigation

Gain visibility into the security posture of your data. Identify sensitive data and its location by using NetApp Cloud Data Sense. Track folder permissions and provide options for mitigating potential risks like data exfiltration.

09

Centralized monitoring

Monitor your hybrid cloud infrastructure through a simple UI. Identify threats and start remediation with the Ransomware Protection dashboard available in NetApp Cloud Manager.

10

Forensic analysis

Use NetApp proven solutions to do pre- and post-ransomware event forensics. Provide the insights you need to understand, manage, and close attack pathways.

NetApp