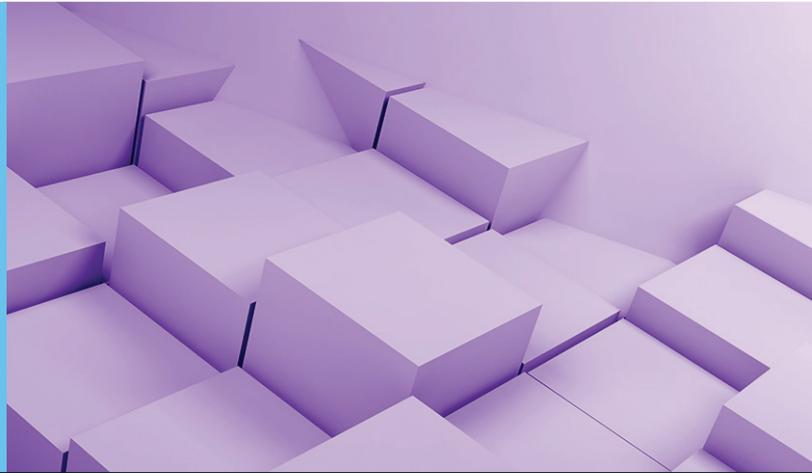# 10 REASONS
NetApp for Ransomware Protection

01 Tamperproof storage

NetApp® SnapLock® Compliance provides WORM capabilities that prevent data, including NetApp Snapshot™ copies, from being deleted before the retention period expires. This rule applies even to administrator accounts.

02 Rapid recovery

The most expensive aspect of a ransomware attack is the downtime experienced getting your data back online. NetApp immutable Snapshot copies restore terabytes of data in seconds, not hours.

03 Data monitoring

Rapid recovery capabilities are of the utmost importance. However, with NetApp FPolicy detection and prevention capabilities, ransomware is stopped from spreading in the first place.

04 Zero Trust compatible

NetApp embraces a Zero Trust approach to security with controls such as MFA, RBAC, comprehensive logging, and auditing to protect against ancillary attacks.

05 Layered security

NetApp features such as SnapMirror®, SnapVault®, and FabricPool® enable you to replicate your Snapshot backups and tiered data to multiple locations (DR site, cloud, secondary system) for enhanced resiliency.

06 Multicloud protection

NetApp Cloud Insights, using the Cloud Secure capability, can respond to ransomware incidents in real time. Combined with our Cloud Volumes ONTAP FPolicy feature, you get enterprise-grade protection and performance at cloud scale.

07 Application integrated

NetApp SnapCenter® software provides a unified, application-consistent data protection strategy for applications, VMs, and databases, ensuring that these data-critical systems are always recoverable at the application level.

08 Forensic analysis

With NetApp, you can do pre- and post-ransomware event forensics, giving you insights to understand, manage, and close attack pathways.

09 Risk mitigation

Services and tools give visibility into the security posture of your data and provide options for mitigating potential risks.

10 Proven

NetApp technologies have already enabled customers to prevent and recover from ransomware attacks and avoid paying the ransom.

■ NetApp