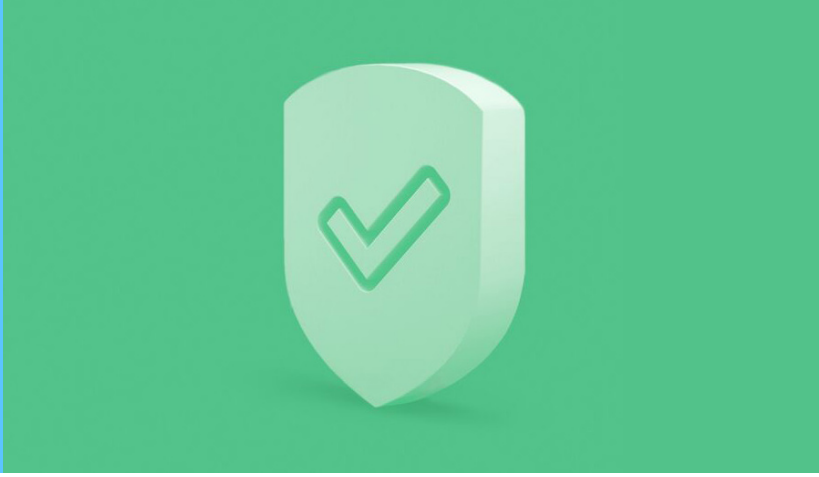
OVERVIEW

Protect your data from ransomware

Explore a datacentric approach to ransomware protection



Ransomware threats are dangerous and pervasive. They disrupt access to production data, and they may also destroy backup data to prevent quick recovery. For state and local governments, it's crucial to have the right data protection and security solutions as part of an overall cyber-resilience strategy.

NetApp is a leader in data management solutions and datacentric security. Protection and security aren't afterthoughts—they're built into our DNA. Our integrated solutions and services for ransomware align directly with the National Institute of Standards and Technology framework to help you protect and secure your data, with the ability to rapidly recover in the event of an attack.

Rise to the cybersecurity challenge with NetApp
The five pillars of the NIST Cybersecurity Framework:

Identify

How NetApp can help:

- Scan for vulnerabilities
- Assess data protection and security posture
- Classify data type, location, and permissions

Protect

How NetApp can help:

- Build a Zero Trust architecture with logical air gap; write once, read many (WORM) retention; and detailed logging
- Create indelible, immutable data copies
- Block malicious data from being written to disk

Detect

How NetApp can help:

- Monitor infrastructure for ransomware attacks
- Monitor user and storage behavior anomalies
- Generate regular reports
- Alert for suspicious activity

Respond

How NetApp can help:

- Block malicious accounts
- Advise on proper remediation approach
- Initiate NetApp® Snapshot™ copies if an attack is identified

Recover

How NetApp can help:

- Restore data in seconds and bring applications back online
- Apply intelligent forensics to identify the source of the threat

Don't wait until it's too late. Learn more about NetApp ransomware solutions and find out how you can improve your security posture.

NetApp

+1 877 263 8277