# **Ransomware Protection Comprehensive Data-Centric Protection**

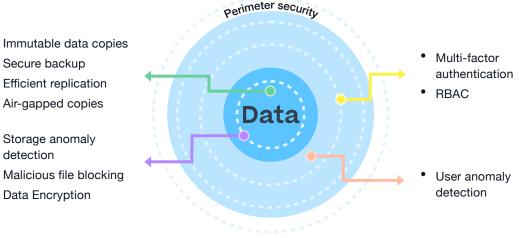
Datasheet



#### Protect What's Most Important–Your Data

Ransomware attacks target your data, not your network. Your protection should start where it counts the mostat the data level.

- Immutable data copies
- Secure backup
- Air-gapped copies
- Storage anomaly detection
- Malicious file blocking
- Data Encryption



#### Protect Your Data Estate With NetApp's Complete Set of Capabilities

## Protect

Assess and refine your data security posture to mitigate vulnerabilities in your data estate

- Analyze file access permissions
- Categorize and locate sensitive data
- Block malicious files
- Establish rapid, granular recovery ٠ points
- Replicate data efficiently for backup and disaster recovery in multiple accounts and regions
- Create a logical air gap and flexible, secure data retention
- Harden your environment and correct storage security lapses
- Learn normal user file access behavior patterns

## **Q** Detect

Quickly identify data usage anomalies to minimize the impact of ongoing malicious activity

- Discover data and storage anomalies
- Trigger alerts based on storage behavior
- Spot unusual user behavior
- ۲ Get visibility into unusual user directory performance metrics
- Detect changes in user file access patterns
- Identify attempted mass file encryption, deletions, and exfiltration
- Block malicious user accounts
- Initiate a NetApp Snapshot recovery point when abnormal activity takes place



Avoid costly downtime and recover rapidly

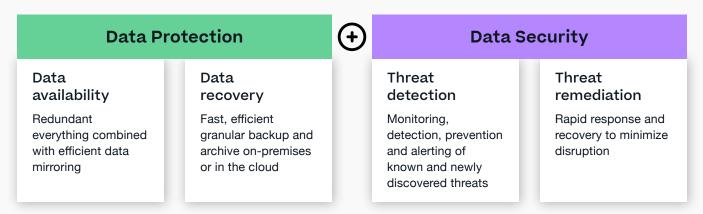
- Asses the damage with file-level forensics and identify which files to restore
- Restore data instantly from a specific point in time
- Place data directly in the location you specify on a block level
- Choose between restoring full volumes or individual files
- Locate last uncorrupted copy of the data with indexed catalog
- Analyze the impact of the attack with data mapping and classification

### A Single-Control Plane for Your Cyber Resiliency Posture

Cloud Manager's ransomware protection dashboard enables you to gain full visibility of your data security posture across a variety of working environments so you can better respond to threats as they occur.

ALERTS			Working environment name
Cloud BackUp Missing (3)			File Operations Auditing is Not
Mass encryption Detected (2)	-		Turned On
Highly sensitive files are open to public (1)	\$3, prod 3.3.3.3	Storage Grid 1.1.1	More details + 21/12/2021
DataSense is not scanning (2)	53,prod 13333		Sensitive Data with wide permissions     found
ONTAP version not updated (3)			Go to Investigation +
No Snapshots configured (2)		•	21/12/2021
No On-Box anti-ransomware configured (1)			<ul> <li>One or more volumes are not backed up by Cloud BackUp Service</li> </ul>
No auditing configured (2)	OneDrive 8.6.3.4	CV0 8.6.3.4	configure Backup 🔶
			DataSense is not scanning your
			working environmen Configure DataSense Scan. +
			Configure DataSense Scan 🔸
	DHL		
No WORM	EMC. Islien, pred 2.3.6.5	Sharepoint 15.5.5.5	
Default Admin Permissions			
Guest users allowed			
Default Passwords			
No Snapshots Configured			
	MySQL prod 3.2.2.3.	Windows_server_dev	

#### Cyber Resilience: Where Data Protection Meets Data Security



## Ransomware Protection Designed for IT Professionals

As the stewards of the data, it's up to IT to find solutions that can reduce the risks of ransomware attacks, respond when attacks occur, restore the data, and ensure cyber resilience. Any effort to reduce the threat of data corruption by IT improves the overall security posture of the organization.





## Data Is Our Business, We Protect It Best.

At NetApp, we have been providing industry-leading data management solutions for decades. That's why we understand data protection better than anyone and are perfectly positioned to offer the most comprehensive suite of tools to protect your data.