NetApp

Reboot2025
Anticipez l'avenir de la cyber et de l'infra

16 septembre, 2025
Crissier, Suisse

S'inscrire dès maintenant

La sécurité de vos données vous préoccupe-t-elle ?

Breakout

Christophe Danjou
Systems Engineer / Channel support

NetApp™

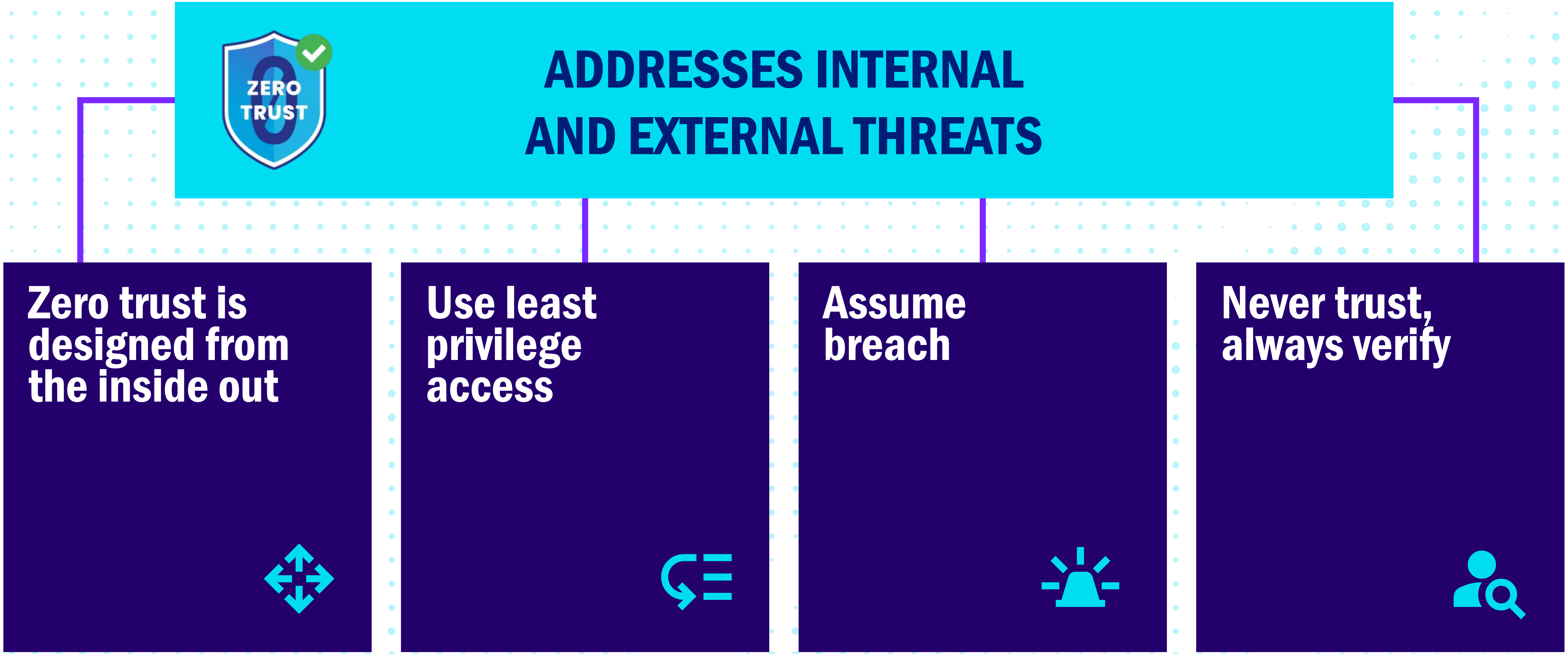
Cyberdefense

2024 SAW A 68% INCREASE IN DATA BREACHES

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

NetApp Supports Zero Trust Architectures

In line with NIST Special Publication SP 800-207, Zero Trust architecture (ZTA)



ADDRESSES INTERNAL AND EXTERNAL THREATS

Zero trust is designed from the inside out

Use least privilege access

Assume breach

Never trust, always verify

NetApp

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

The only enterprise storage vendor validated to store top-secret data everywhere

Commercial Solutions for Classified (CSfC) Component List

FIPS 140-3™

Department of Defense Approved Product List (DoDIN APL)

Common Criteria

Visit security.netapp.com/certs/ for the latest lists of all certifications, and for a list of Common Criteria certified products, visit netapp.com/esg/trust-center/compliance/common-criteria/

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

RANSOMWARE

Detect, Prevent, and Recovery Quickly

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

⚠

89%

Ransomware is considered a top business risk

It’s still top of mind

89% of IT and cybersecurity professional rank ransomware as a top-five threat to the overall viability of their organization.

ESG Ransomware Preparedness Lighting the Way to Readiness and Mitigation

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

How NetApp helps against ransomware

Detection and prevention

Remediation and restoration

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

NetApp solution for ransomware

Taking a layered defense approach

Detection and prevention

NetApp FPolicy

- Common ransomware file extension blocking in native mode
- File and user behavioral analytics in external mode

NetApp® ONTAP® autonomous ransomware protection (ARP)

- Automatic detection of ransomware in 9.10.1 and later

NetApp Cloud Insights

- Monitors files that access NetApp file systems
- Storage Workload Security leverages UEBA to detect and stop attacks

NetApp Cloud Backup DataLock

- Ransomware encrypted backup detection with auto rollback

Anomalous and intuitive indicators

- NetApp Active IQ® Unified Manager alerting
  - NetApp Snapshot™ copy rate of change and decrease in storage efficiency loss alert
- NetApp Active IQ® and System Manager insights
  - ”Ransomware defense” best practices

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Detection and prevention

NetApp FPolicy

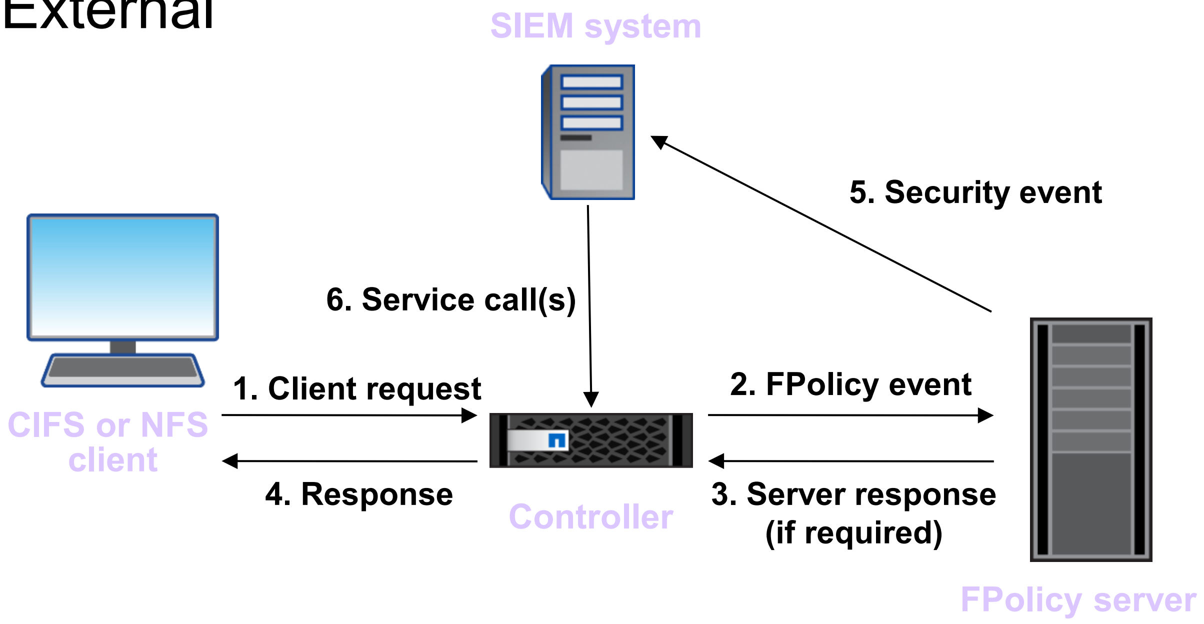
Modes

- **Native** and/or **External**

Native

- **Block and Deny list** (file extension blocking)
- **Allow or Permit list** (only allow certain extensions)

External



PARTNERS

NetApp CLOUD INSIGHTS

VERITAS

VARONIS

CLEONDRIS

STEALTHbits TECHNOLOGIES

ProLion

Brainwave GRC

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

CYBER RESILIENCY

NetApp

AUTONOMOUS RANSOMWARE PROTECTION

Detection and response embedded in the storage layer.

REAL-TIME DETECTION AND RESPONSE

AI-powered ransomware detection and response for file

Real-time file anomaly detection - respond with automatic snapshots

AI-powered ransomware detection and response for block

Real-time vm anomaly detection - respond with automatic snapshots

Ransomware detection and response for native cloud

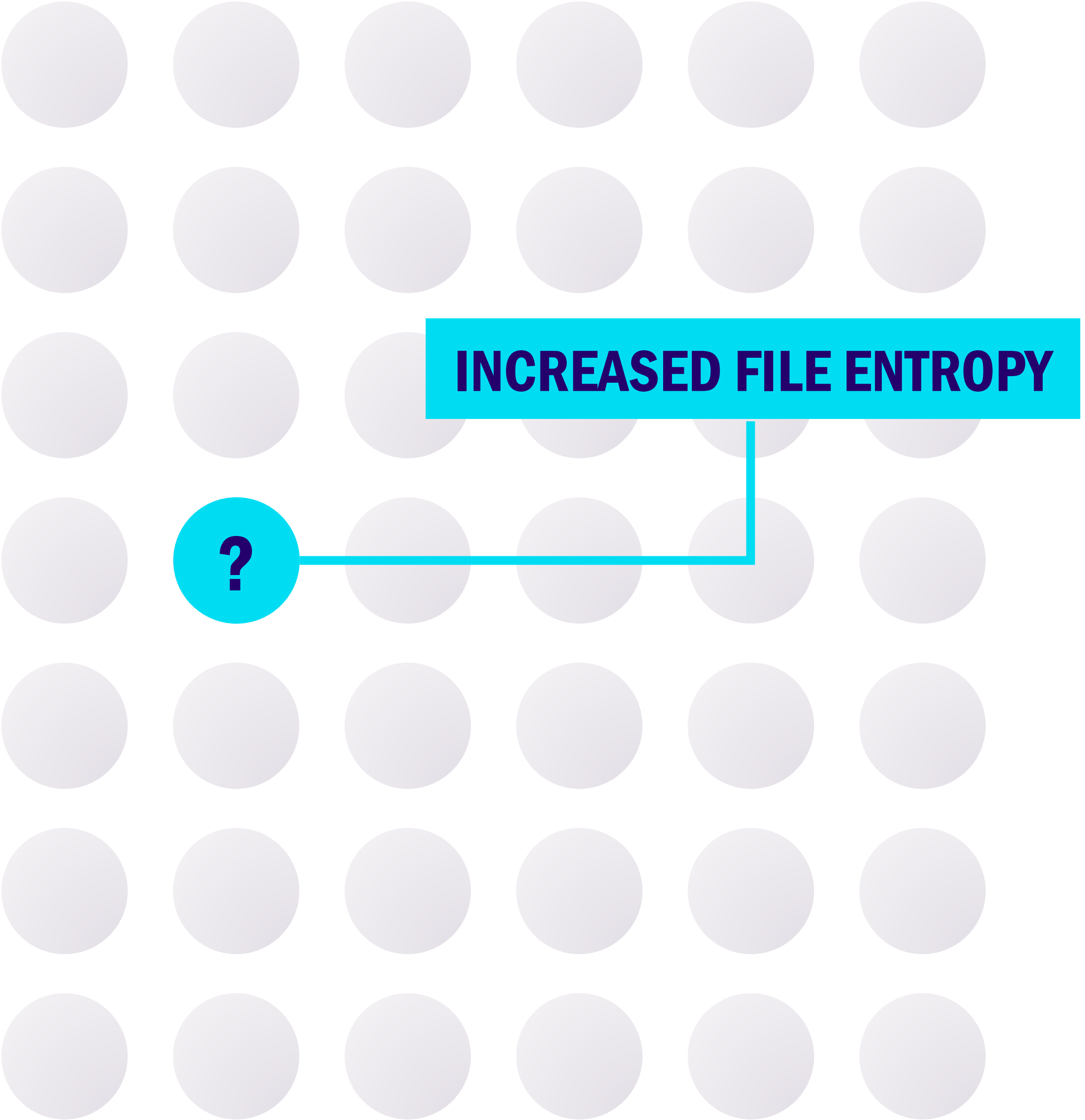
Real-time file anomaly detection for FSx - respond with automatic snapshots

AI-powered detection for user behaviour

Real-time user behaviour anomaly detection with automatic snapshots

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Available in 9.16.1



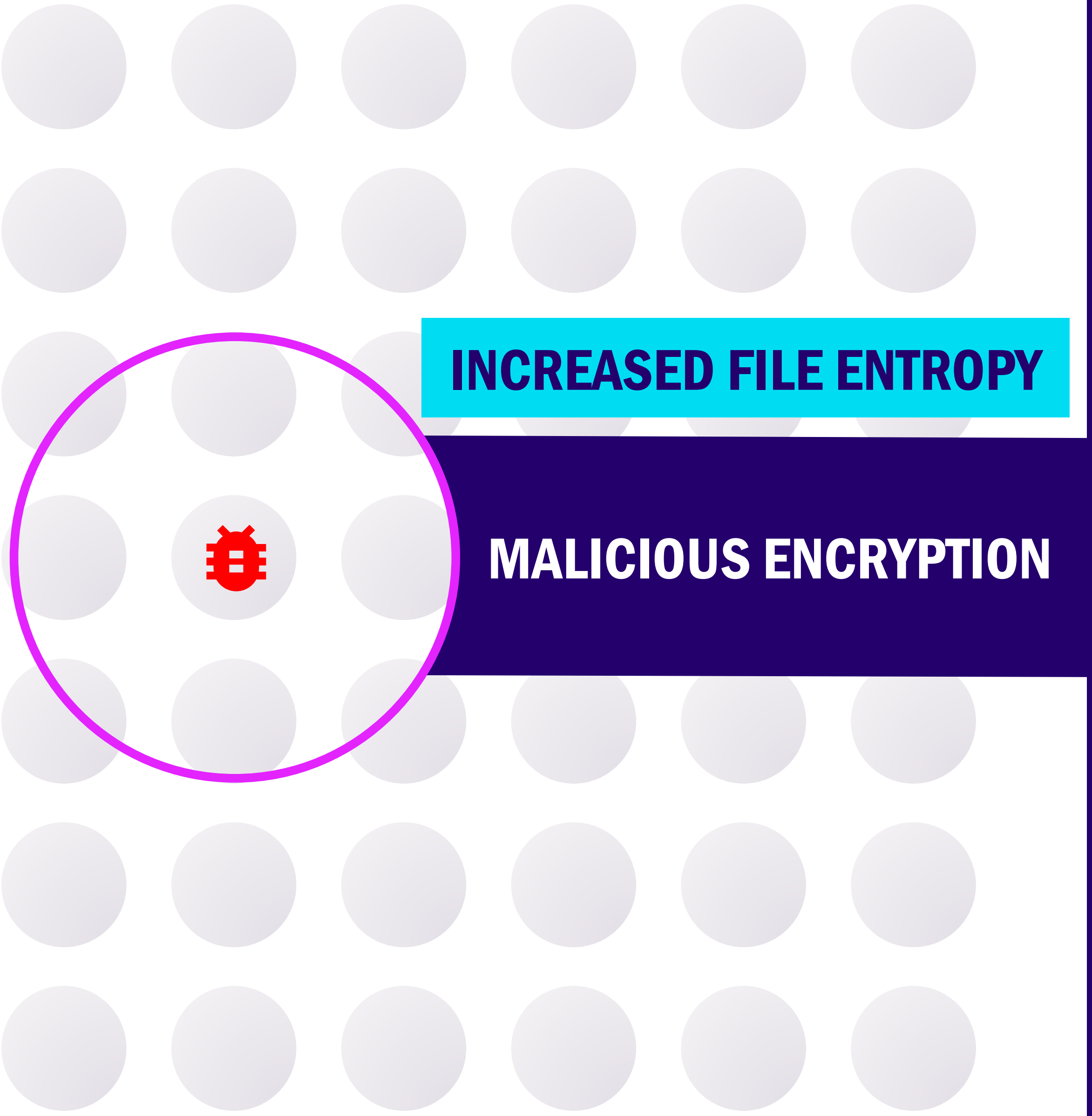
On-Device Anomaly Detection

World’s first on-box, AI-powered, real-time ransomware detection and response

1 **Real-time signal monitoring**

NetApp © 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Available in 9.16.1



On-Device Anomaly Detection

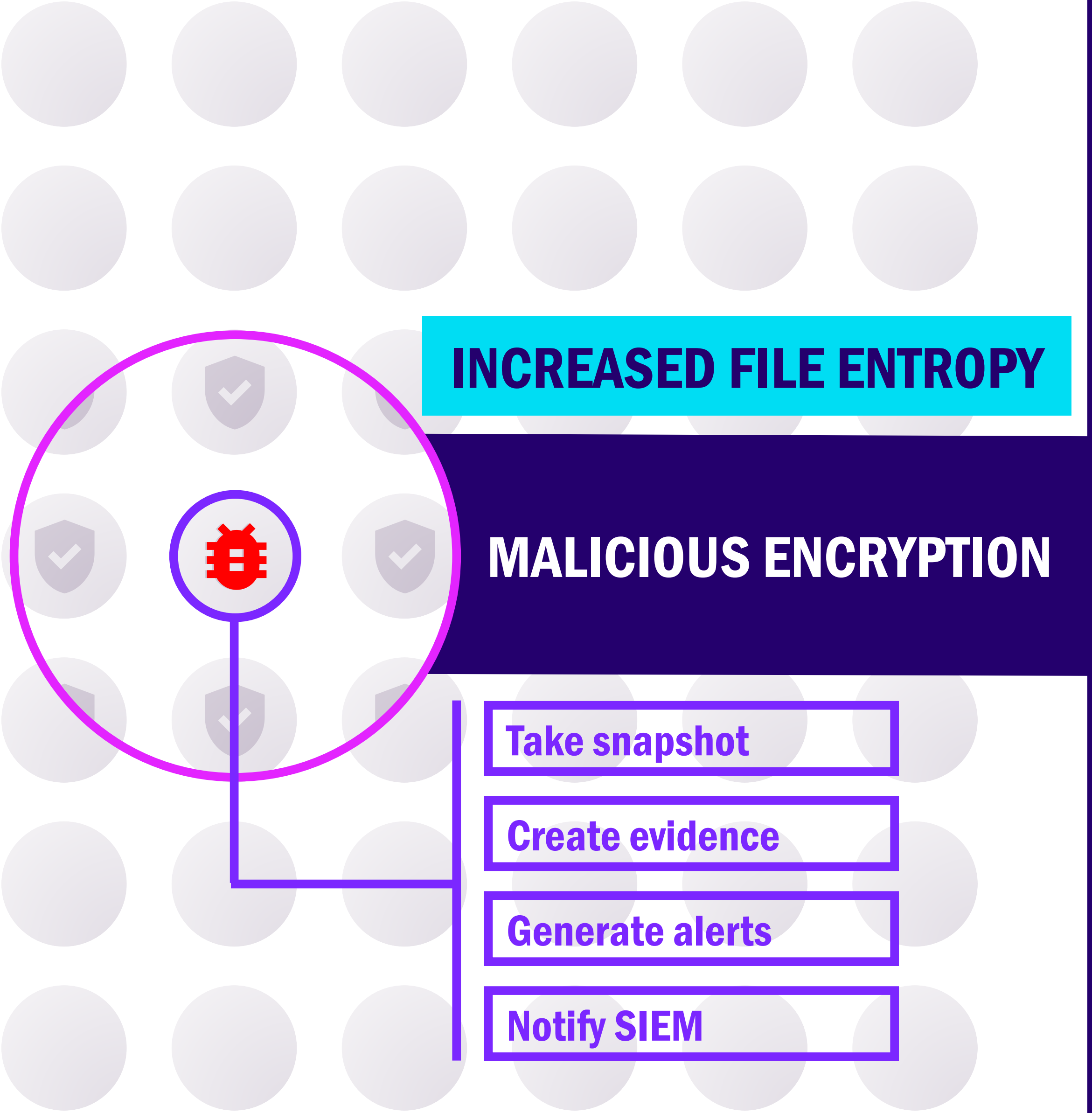
World’s first on-box, AI-powered, real-time ransomware detection and response

1 Real-time signal monitoring

2 Suspicious activity confirmed

NetApp © 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Available in 9.16.1



On-Device Anomaly Detection

World's first on-box, AI-powered, real-time ransomware detection and response

1 Real-time signal monitoring

2 Suspicious activity confirmed

3 Automated response

NetApp

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Detection Accuracy with built-in AI-Powered Ransomware Protection

SE Labs

World's first and only AI-driven on-box ransomware detection for NAS

Multiple signals: Entropy, file activity, and file headers

Next-generation AI ensure precise detection from day one

Auto-update for optimal, efficient, and accurate turn-key detection (GA)

Precision
(Alerts are accurate)

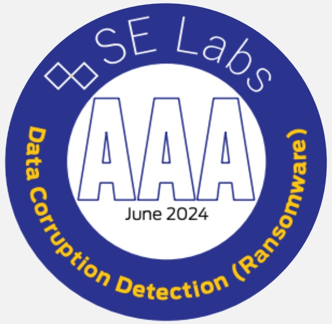
100%

Recall
(Detect every attack)

>99%

Data corruption detection (ransomware) award

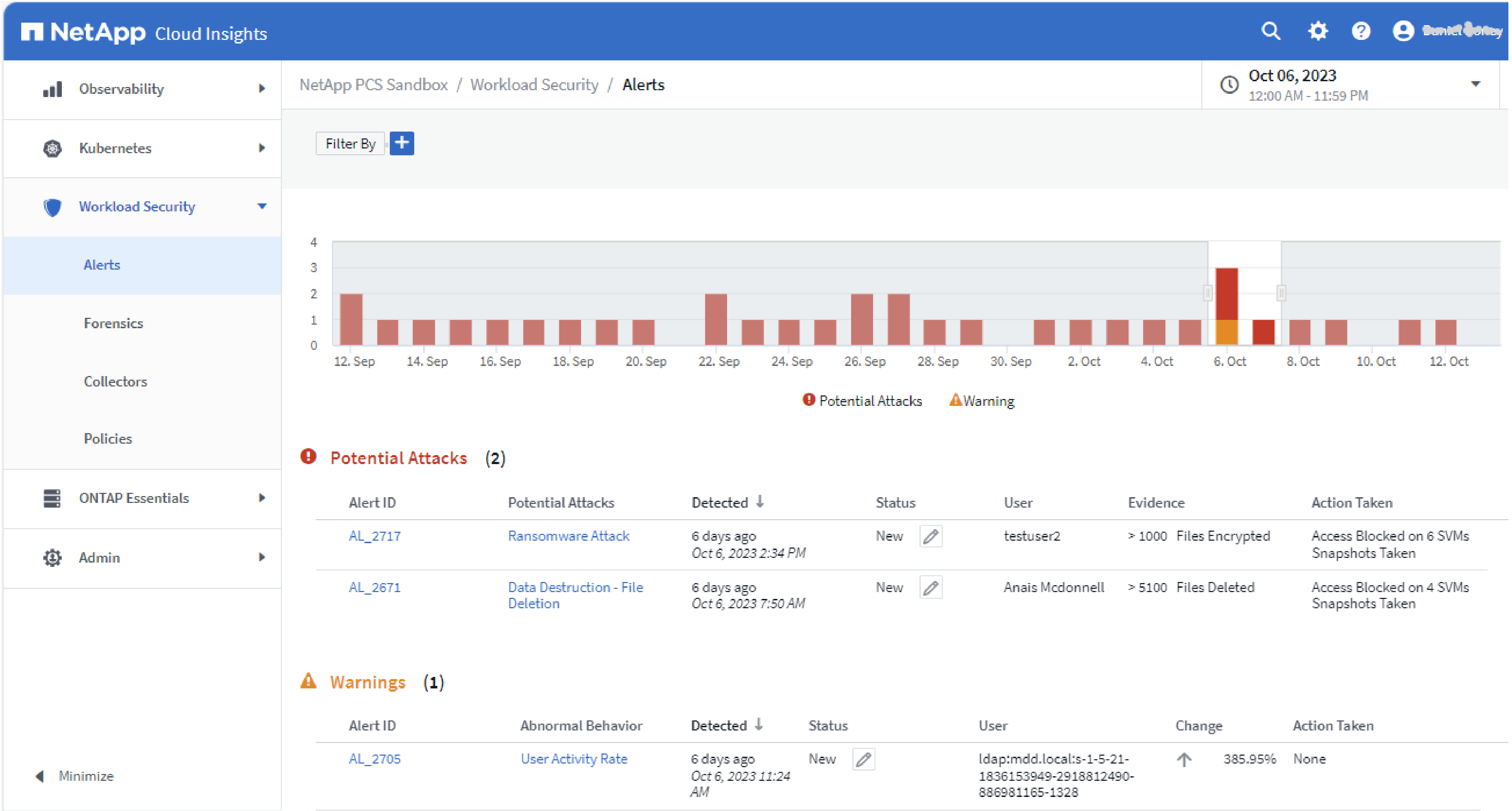
The following product wins the SE Labs award:



NetApp
ONTAP Autonomous Ransomware Protection with AI

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

NetApp Cloud Insights - Workload Security



Potential Attacks (2)

Alert ID	Potential Attacks	Detected ↓	Status	User	Evidence	Action Taken
AL_2717	Ransomware Attack	6 days ago *Oct 6, 2023 2:34 PM*	New	testuser2	> 1000 Files Encrypted	Access Blocked on 6 SVMs Snapshots Taken
AL_2671	Data Destruction - File Deletion	6 days ago *Oct 6, 2023 7:50 AM*	New	Anais Mcdonnell	> 5100 Files Deleted	Access Blocked on 4 SVMs Snapshots Taken

Warnings (1)

Alert ID	Abnormal Behavior	Detected ↓	Status	User	Change	Action Taken
AL_2705	User Activity Rate	6 days ago *Oct 6, 2023 11:24 AM*	New	ldap:mdd.local:s-1-5-21-1836153949-2918812490-886981165-1328	↑ 385.95%	None

How NetApp Cloud Insights detects anomalies in user behavior

Detection and prevention

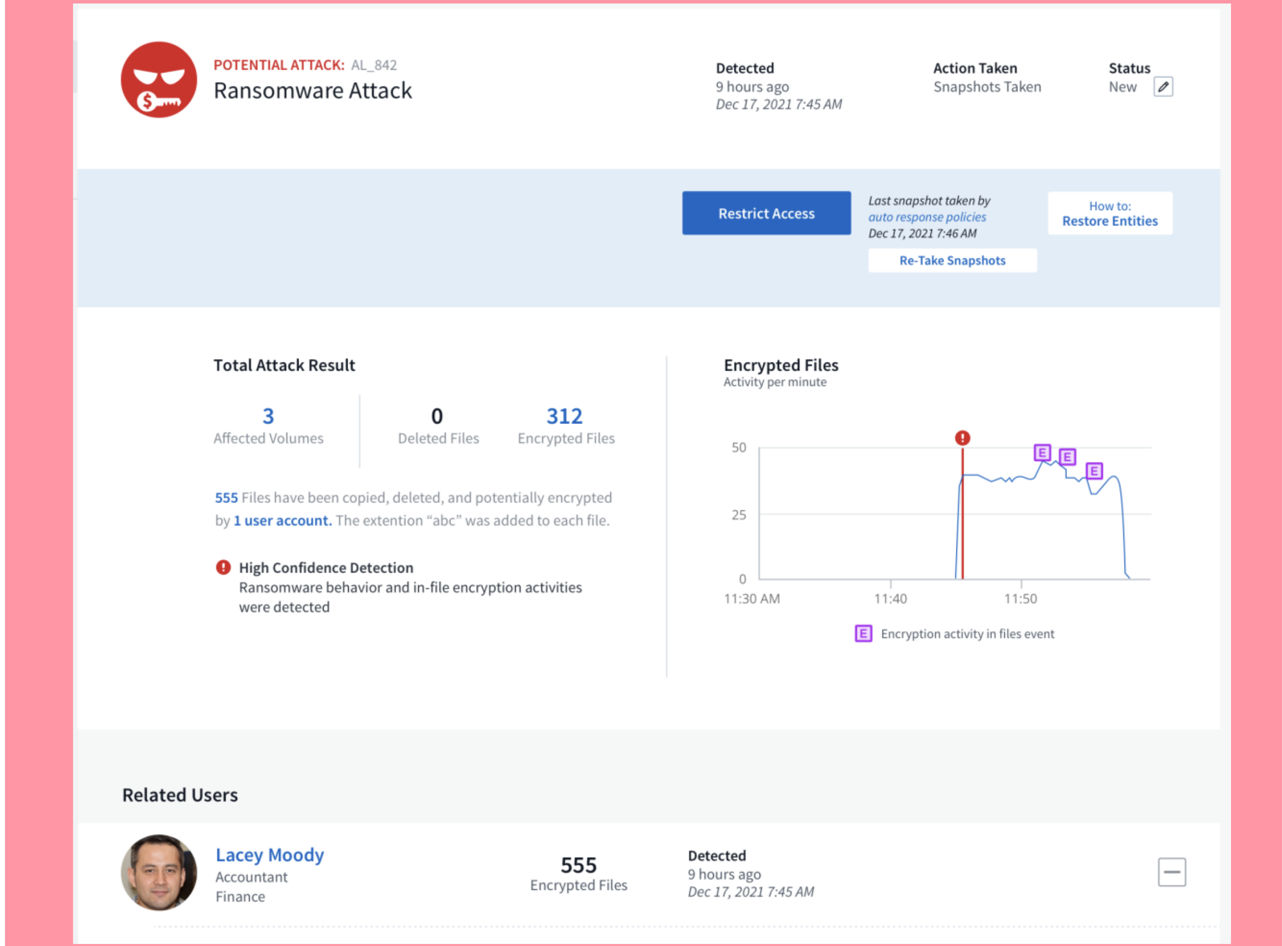
Detects abnormal change in user activity

Analyzes abnormal behavior patterns to determine type of threat

- Detects ransomware
  - **Now displays alerts for NetApp® ONTAP® ARP**
- Provides insights on potential attacks
- Takes automatic actions
  - NetApp Snapshot™ copies
  - **Blocks the user**

Identifies and reduces false-positive noise

Audit trail for data breach investigation and remediation



POTENTIAL ATTACK: AL_842

Ransomware Attack

Detected
9 hours ago
Dec 17, 2021 7:45 AM

Action Taken
Snapshots Taken

Status
New

Restrict Access

Last snapshot taken by auto response policies
Dec 17, 2021 7:46 AM

Re-Take Snapshots

How to:
Restore Entities

Total Attack Result

3	0	312
Affected Volumes	Deleted Files	Encrypted Files

555 Files have been copied, deleted, and potentially encrypted by 1 user account. The extention "abc" was added to each file.

High Confidence Detection
Ransomware behavior and in-file encryption activities were detected

Encrypted Files
Activity per minute

Related Users

Lacey Moody Accountant Finance	555 Encrypted Files	Detected 9 hours ago *Dec 17, 2021 7:45 AM*

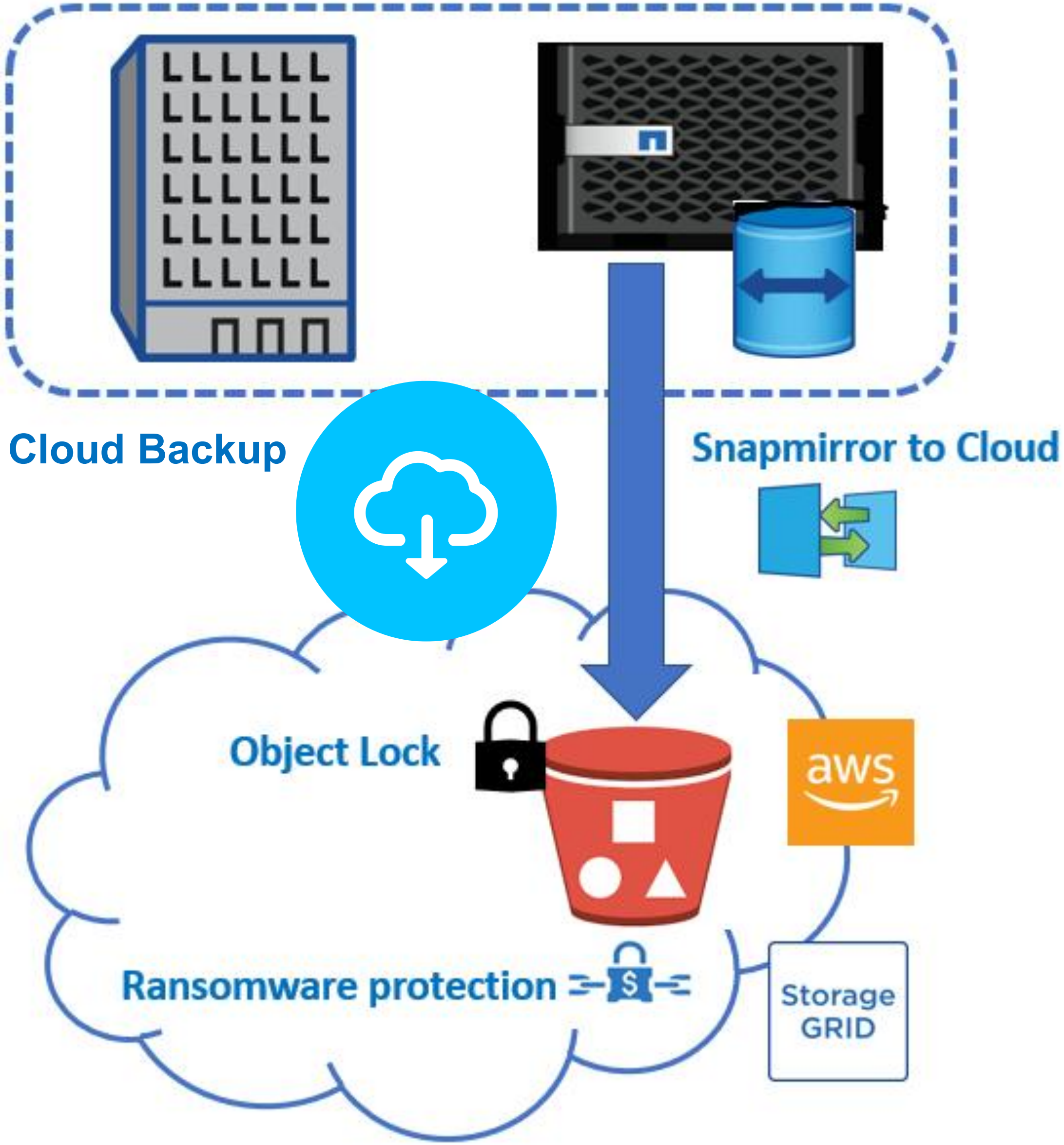
NetApp

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

NetApp Cloud Backup: DataLock and ransomware protection

What is DataLock and ransomware-protection feature?

- Protection against ransomware attacks and unauthorized deletions have become one of the high priority requirements among customers.
- NetApp® Cloud Backup now provides the option to set DataLock and ransomware scan feature on cloud backups.
- This feature provides:
  - A mechanism to lock the NetApp Snapshot™ copies replicated to cloud object-store
  - The ability to detect a ransomware attack and recover the consistent copy of the cloud Snapshot copy
- The solution uses both SM-C and ADC to achieve this functionality.
- Currently the feature is supported only for SGWS and AWS.



NetApp © 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

BlueXP Ransomware Protection

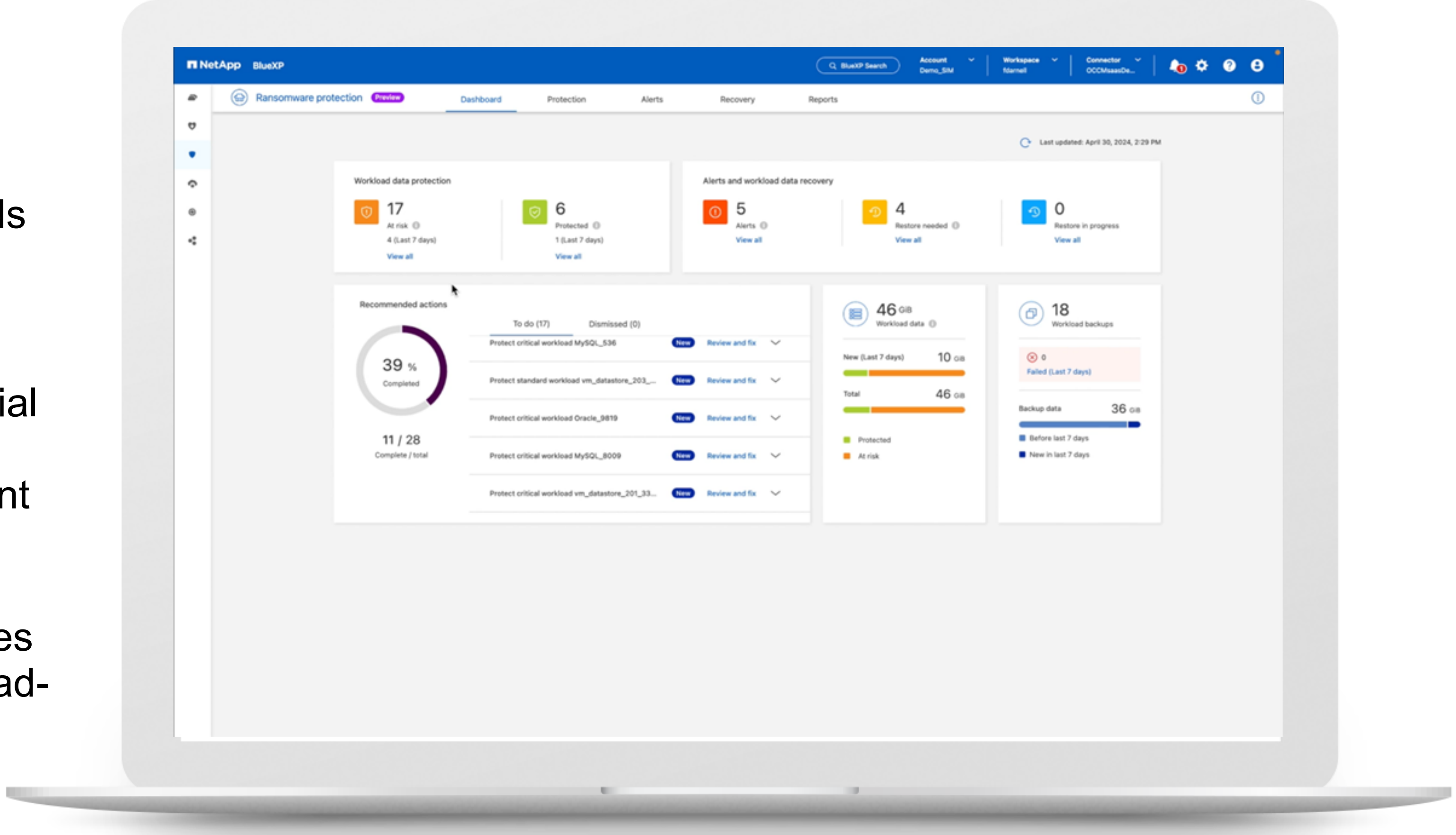
AI-driven defense beyond backup

Ransomware Protection

Identify and Protect: Automatically identifies workloads at risk, recommends fixes, and protects with one-click

Detect and Respond: Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point

Recover: Restores workloads in minutes through simplified, orchestrated workload-consistent recovery



Last updated: April 30, 2024, 2:29 PM

Workload data protection

17 At risk
4 (Last 7 days)
View all

6 Protected
1 (Last 7 days)
View all

Alerts and workload data recovery

5 Alerts
View all

4 Restore needed
View all

0 Restore in progress
View all

Recommended actions

39 % Completed

11 / 28 Complete / total

To do (17) Dismissed (0)

Protect critical workload MySQL_536 New Review and fix
Protect standard workload vm_datastore_203_... New Review and fix
Protect critical workload Oracle_9819 New Review and fix
Protect critical workload MySQL_8009 New Review and fix
Protect critical workload vm_datastore_201_33... New Review and fix

46 GiB Workload data

New (Last 7 days) 10 GiB

Total 46 GiB

🟩 Protected
🟧 At risk

18 Workload backups

0 Failed (Last 7 days)

Backup data 36 GiB

■ Before last 7 days
■ New in last 7 days

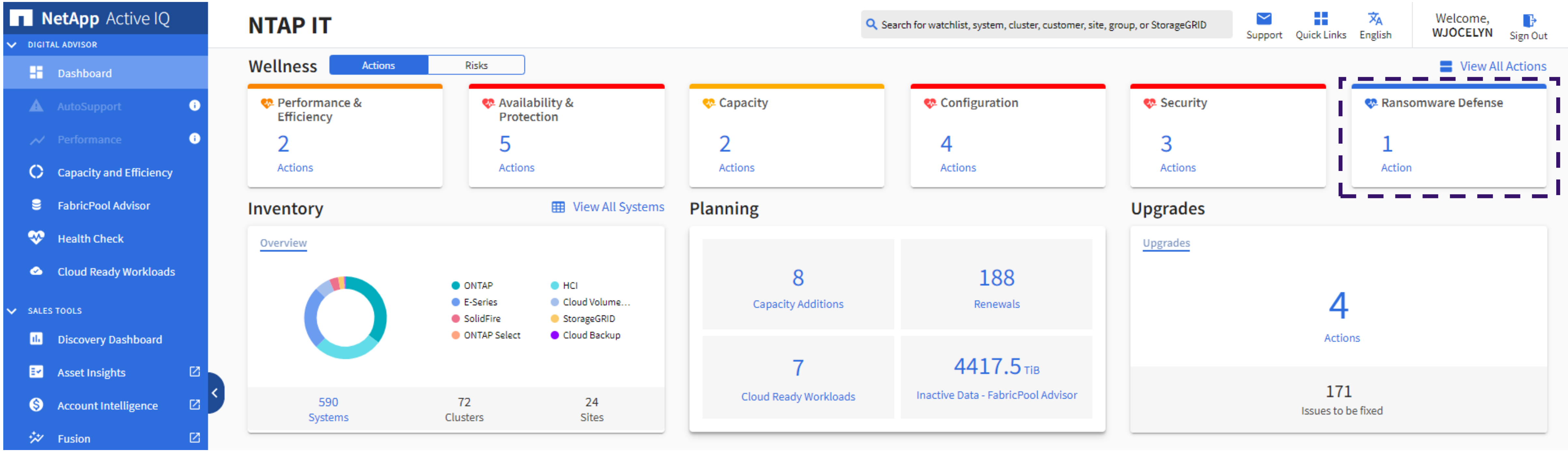
© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

NetApp Active IQ digital advisor

Ransomware defense

A set of prescriptive wellness checks to help protect customers against ransomware and recover quickly if they are impacted

- Checks cover NetApp® Snapshot™ count/retention/auto-delete settings, Fpolicy, and encryption



Performance & Efficiency	Availability & Protection	Capacity	Configuration	Security	Ransomware Defense
2 Actions	5 Actions	2 Actions	4 Actions	3 Actions	1 Action

590 Systems
72 Clusters
24 Sites

8 Capacity Additions
188 Renewals
7 Cloud Ready Workloads
4417.5 TiB Inactive Data - FabricPool Advisor

4 Actions
171 Issues to be fixed

NetApp
© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

NetApp Ransomware Protection and Recovery Service

Plan, implement, and manage a ransomware-ready solution to keep data secure, available, reliable, and recoverable

Assess + Configure and manage + Recover

Assesses current environment

- Determines whether you need NetApp® ONTAP® upgrades (9.10.1 or later required for ransomware protection software)
- Checks for gaps in NetApp native software solutions
- Determines potential data protection risks
- Evaluates your ability to recover
- Assesses policies and retention periods

Implements and configures NetApp ransomware tools/ARS

- NetApp Cloud Insights, Cloud Secure
- NetApp SnapMirror®, SnapVault®
- NetApp SnapLock® Compliance
- NetApp SnapCenter®
- Advanced data encryption
- NetApp Active IQ®, Active IQ Unified Manager
- NetApp FPolicy allow/deny lists

Delivers high-touch managed services

- Monitors and triages alerts 24/7/365
- Administers and upgrades software
- Creates and manages replication policies
- Modifies FPolicy configurations
- Performs ONTAP upgrades as required
- Sets service-level objectives for response
- Assists with scoring for cybersecurity insurance

Speeds ransomware data recovery

Maintains business continuity and speeds recovery times:

- Recovers data through SnapCenter
- Assists in confirming that data is in place to meet your recovery needs
- Assists in containing ransomware spread
- Rolls back NetApp Snapshot™ copies where necessary
- Helps you isolate, patch, and restore (customer responsibility)

Subscription-based service

© 2025 NetApp, Inc. All rights reserved.

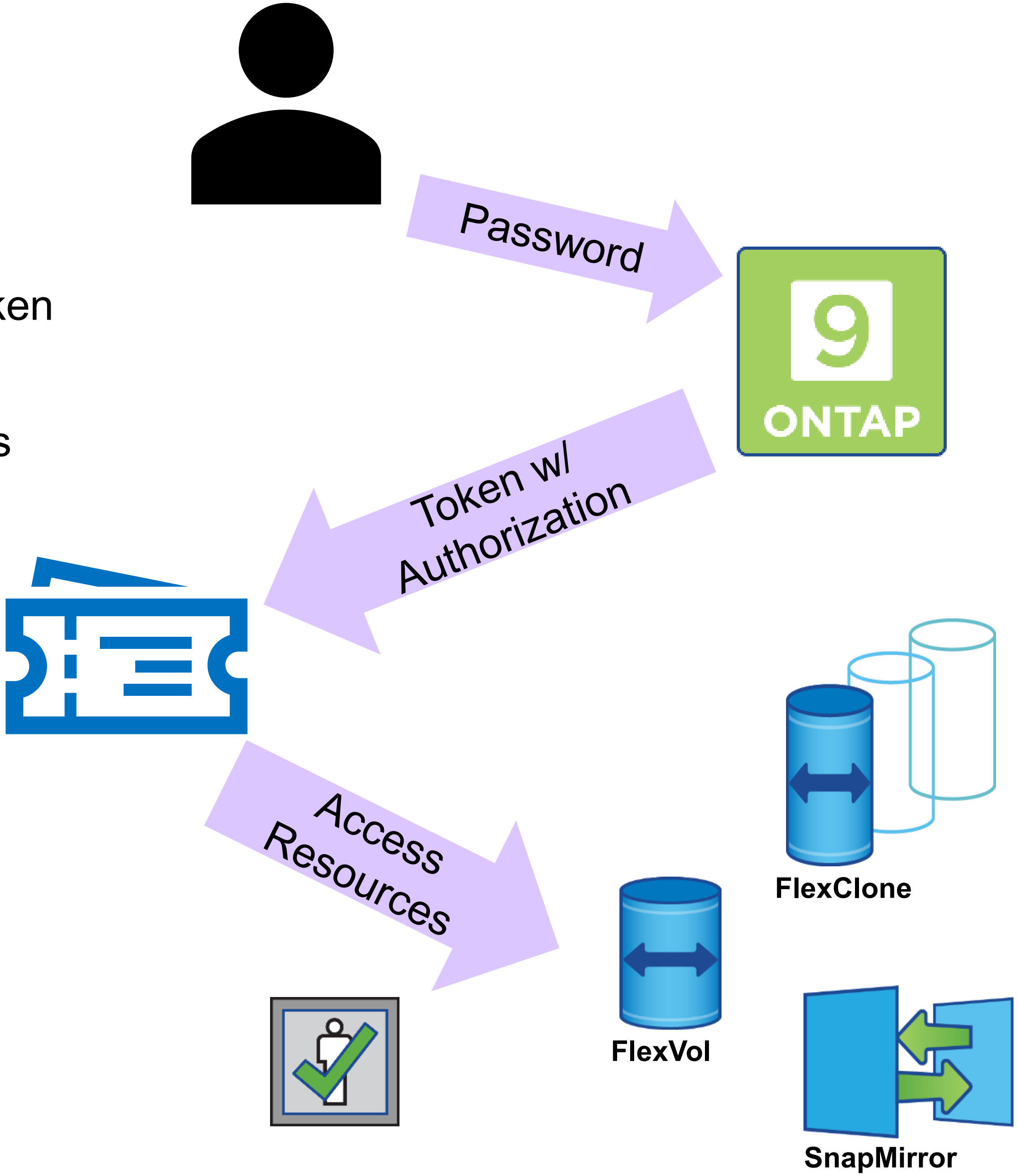
HARDENING THE PLATFORM

Control accesses and actions

Token Based Authentication

OpenID Connect (OIDC) and OAuth 2.0

- Tokens replace passwords for user account authentication
- ONTAP provides access to manage the cluster using a token instead of a password
- Token is like a ticket providing access and time capabilities
- Enhanced Security
  - Passwords are easy to steal
  - Tokens provide more granular control of user account actions
  - Tokens can have a time limit
  - Don’t have to leave passwords in files
- Primary use cases
  - Configuration and Management Automation
  - REST API’s
  - Ansible
  - All OFFTAP products (AIQUM, SysMgr, SnapCenter, etc.)



© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Monitoring and Logging Administrative Access

Monitoring can serve as a deterrent and can help refine security architectures

After (role-based access control) RBAC policies are in place, active monitoring, auditing, and alerting must be deployed

Syslogs can be shipped off box for preservation

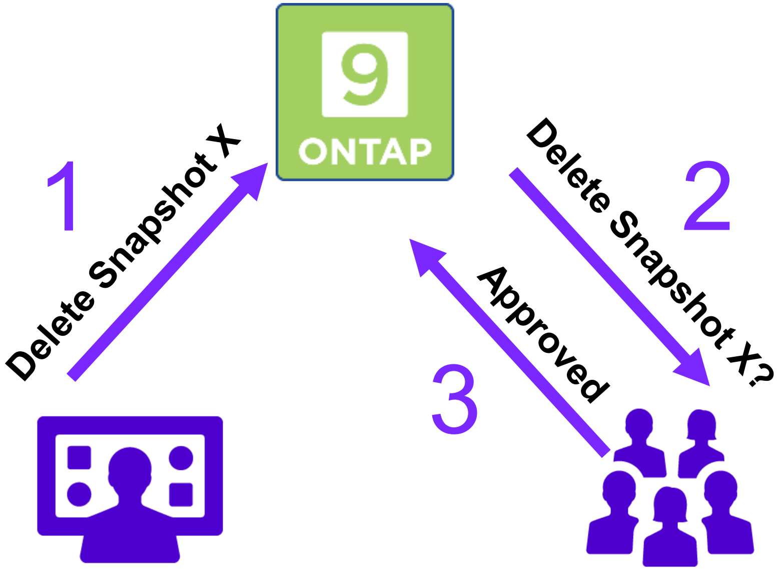
Integrations with Splunk can add an extra level of insight

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Multi Admin Verification commands

ONTAP 9.15.1 adds more than 100 commands to MAV framework

- **Cluster** level commands to prevent hijacking of cluster logs or tampering of NTP time service
- **Security** commands to prevent modifying security audits, IPSec and SAML

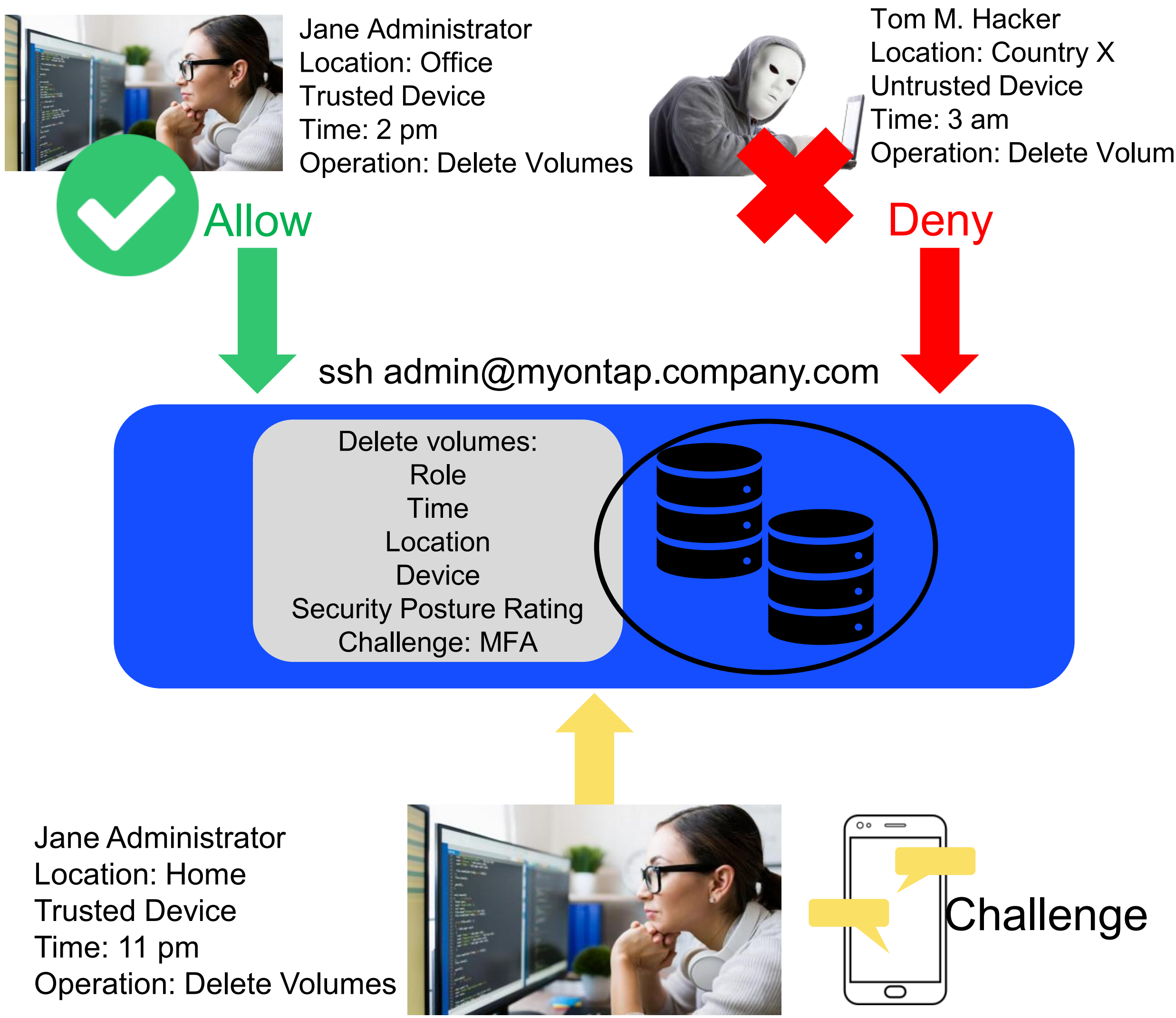


- **Storage** commands to prevent changes to disk encryption settings
- **System level** commands to prevent changes to system health status, alerting, auto-support policies and physical system changes
- Additional **volume** level commands to prevent tampering with volume recovery queue, volume encryption settings and additional volume snapshot controls
- **SVM** commands to prevent tampering with SVM level security settings, logs and auditing

© 2025 NetApp, Inc. All rights reserved.

Dynamic Authorization Framework

Real time security based on environment



Jane Administrator
Location: Office
Trusted Device
Time: 2 pm
Operation: Delete Volumes

Allow

Tom M. Hacker
Location: Country X
Untrusted Device
Time: 3 am
Operation: Delete Volumes

Deny

ssh admin@myontap.company.com

Delete volumes:
Role
Time
Location
Device
Security Posture Rating
Challenge: MFA

Jane Administrator
Location: Home
Trusted Device
Time: 11 pm
Operation: Delete Volumes

Challenge

- ONTAP Dynamic Authorization framework uses user attributes such as time of day, location, IP address, trusted device, user authentication and authorization history, and resource attributes such as commands and objects to determine if a request should be challenged by the system.
- Multi-release journey
- For ONTAP 9.15.1 release
  - SSH/CLI only
  - Initial Trust Score and framework
  - Custom component support
- Future
  - GUI and REST API support
  - Storage object support
  - Full MFA Support
  - Additional user assets

© 2025 NetApp, Inc. All rights reserved.

Tamperproof Snapshot copies using Snapshot copy locking

By leveraging NetApp® SnapLock® technology, NetApp Snapshot™ copies are now protected from deletion by compromised administrator credentials

Snapshot copies can’t be deleted or changed, even by NetApp support

NetApp® SnapLock® Compliance (SLC)

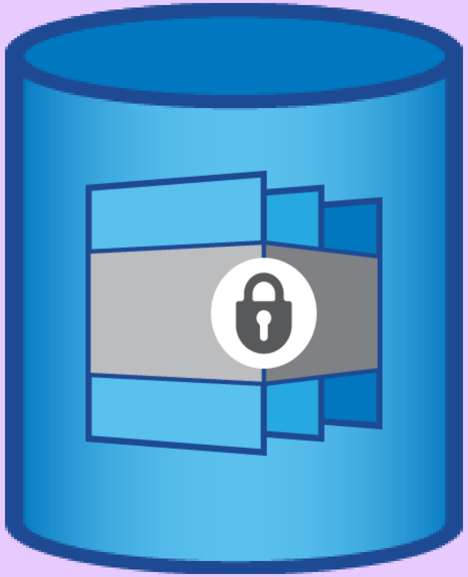
- Licensed feature of NetApp ONTAP®

Ransomware recovery use case

- SLC provides immutable NetApp Snapshot™ copies for NAS and SAN on SLC volumes
- Prevents rogue admins from deleting vaulted Snapshot copies to recover from ransomware

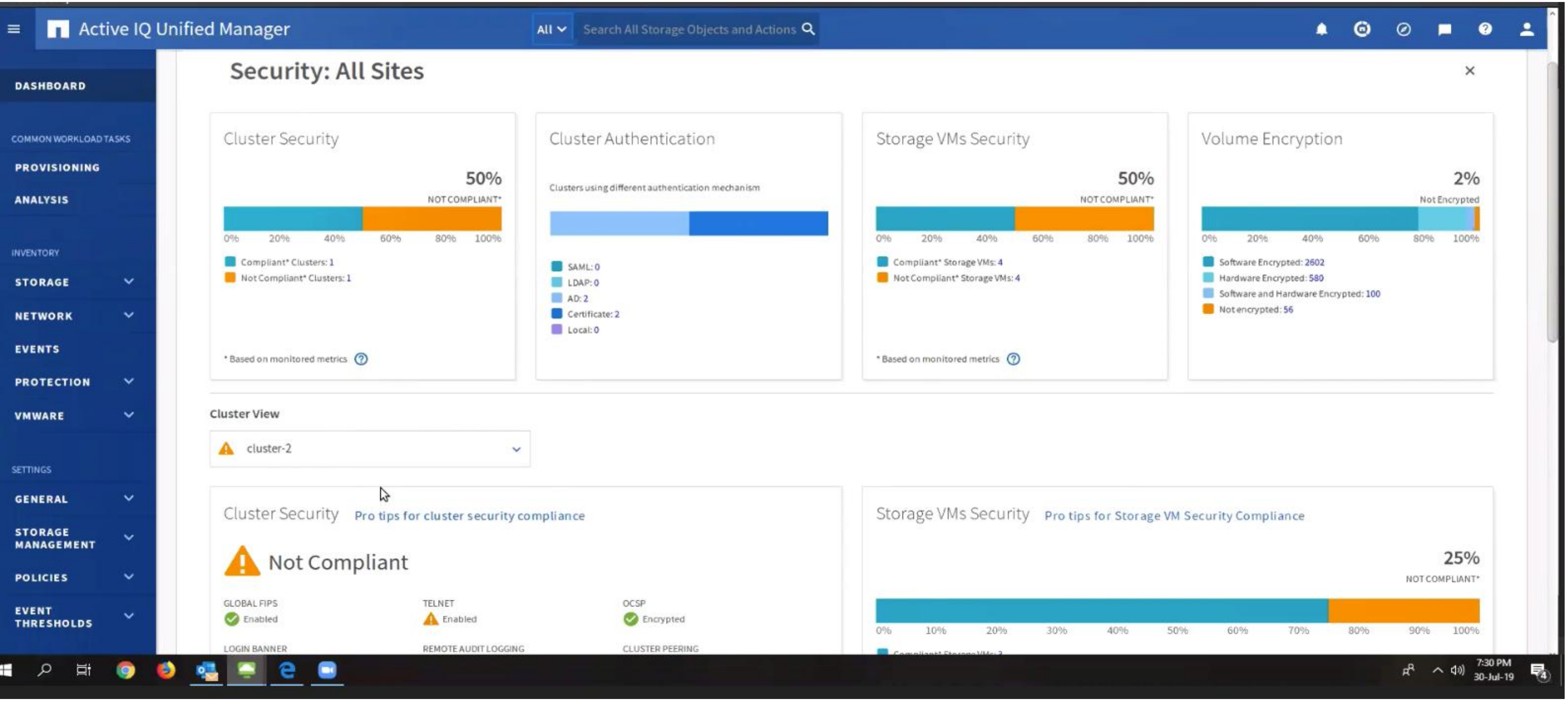
Tamper-proof Snapshot locking on primary storage

- **New In ONTAP 9.12.1, leveraging SLC**
- Works on any volume (not SLC volumes only)
- Manual Snapshot locking or automatic via schedule



Tamperproof Snapshot copies protect against cybersecurity threats

NetApp Active IQ Unified Manager Security Dashboard in 9.7 and later



Security: All Sites

Cluster Security

50%
NOT COMPLIANT*

- 🟦 Compliant* Clusters: 1
- 🟧 Not Compliant* Clusters: 1

* Based on monitored metrics

Cluster Authentication

Clusters using different authentication mechanism

- 🟦 SAML: 0
- 🟦 LDAP: 0
- 🟦 AD: 2
- 🟦 Certificate: 2
- 🟪 Local: 0

Storage VMs Security

50%
NOT COMPLIANT*

- 🟦 Compliant* Storage VMs: 4
- 🟧 Not Compliant* Storage VMs: 4

* Based on monitored metrics

Volume Encryption

2%
Not Encrypted

- 🟦 Software Encrypted: 2602
- 🟦 Hardware Encrypted: 580
- 🟦 Software and Hardware Encrypted: 100
- 🟧 Not encrypted: 56

Cluster View

cluster-2

Cluster Security

Pro tips for cluster security compliance

Not Compliant

GLOBAL FIPS	TELNET	OCSP
✓ Enabled	⚠ Enabled	✓ Encrypted
LOGIN BANNER	REMOTE AUDIT LOGGING	CLUSTER PEERING

Storage VMs Security

Pro tips for Storage VM Security Compliance

25%
NOT COMPLIANT*

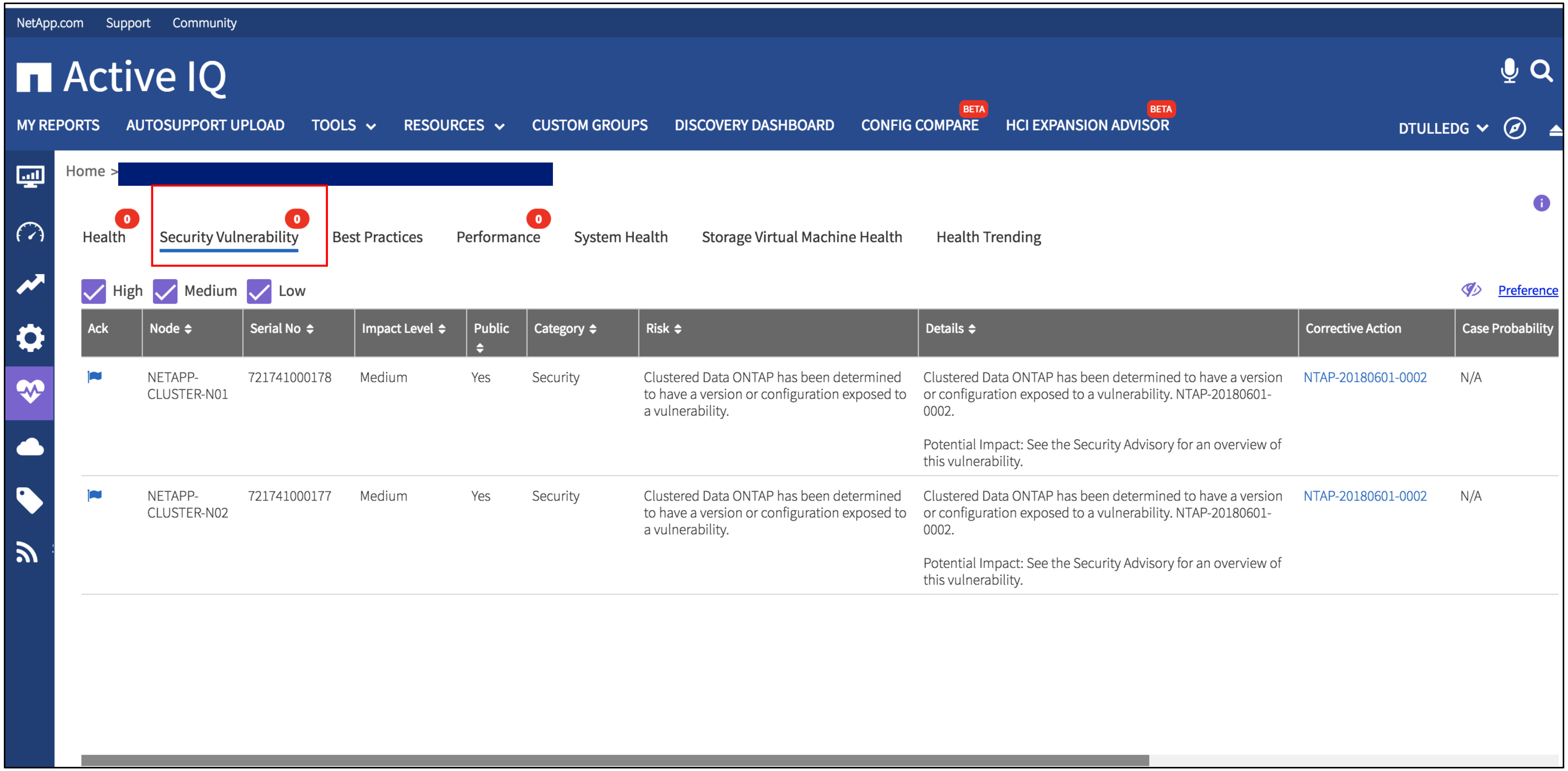
- 🟦 Compliant* Storage VMs: 3

NetApp

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

NetApp ActiveIQ

Security vulnerability health tab



Home > [redacted]

Health 0 | Security Vulnerability 0 | Best Practices | Performance 0 | System Health | Storage Virtual Machine Health | Health Trending

☑ High ☑ Medium ☑ Low

Preference

Ack	Node	Serial No	Impact Level	Public	Category	Risk	Details	Corrective Action	Case Probability
⚑	NETAPP-CLUSTER-N01	721741000178	Medium	Yes	Security	Clustered Data ONTAP has been determined to have a version or configuration exposed to a vulnerability.	Clustered Data ONTAP has been determined to have a version or configuration exposed to a vulnerability. NTAP-20180601-0002. Potential Impact: See the Security Advisory for an overview of this vulnerability.	NTAP-20180601-0002	N/A
⚑	NETAPP-CLUSTER-N02	721741000177	Medium	Yes	Security	Clustered Data ONTAP has been determined to have a version or configuration exposed to a vulnerability.	Clustered Data ONTAP has been determined to have a version or configuration exposed to a vulnerability. NTAP-20180601-0002. Potential Impact: See the Security Advisory for an overview of this vulnerability.	NTAP-20180601-0002	N/A

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

UEFI Secure Boot on Next Generation Platforms

On new platforms that have yet to be released, image validation will be done each time the system boots

Verifies that software is genuine ONTAP **software during boot**

Prevents hacked versions of ONTAP® any time the system boots

- Prevents customers from running images directly from engineering

Signed ONTAP images are **verified by the boot loader**

Only available with the next generation set of platforms

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

CYBER VAULT

Logical air gap

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

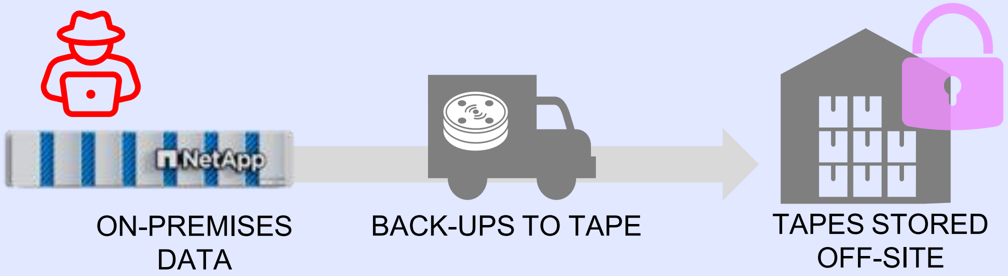
The evolution of data protection

Customers desire to protect their data against ransomware

Challenges:

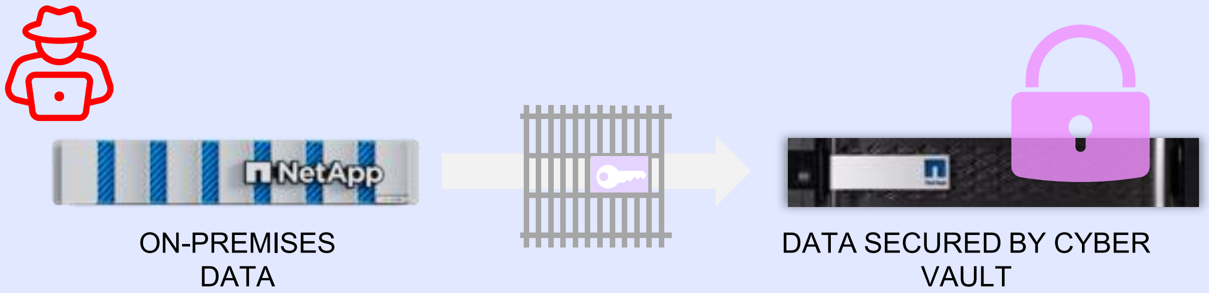
- Most cyber vault solutions create all-new **architecture silos**
- Without an integrated solution, orchestration of complete protect, detect, recovery methodology **is manual**.
- Cyber vaults **still require long restores**, so tamper-proof primary snapshots are still preferred.

PAST



Challenges: Infrequent backup, massively slow restore, and impossible to validate

FUTURE



Cyber vault solutions can offer a logical air-gap, protecting secondary data from attack

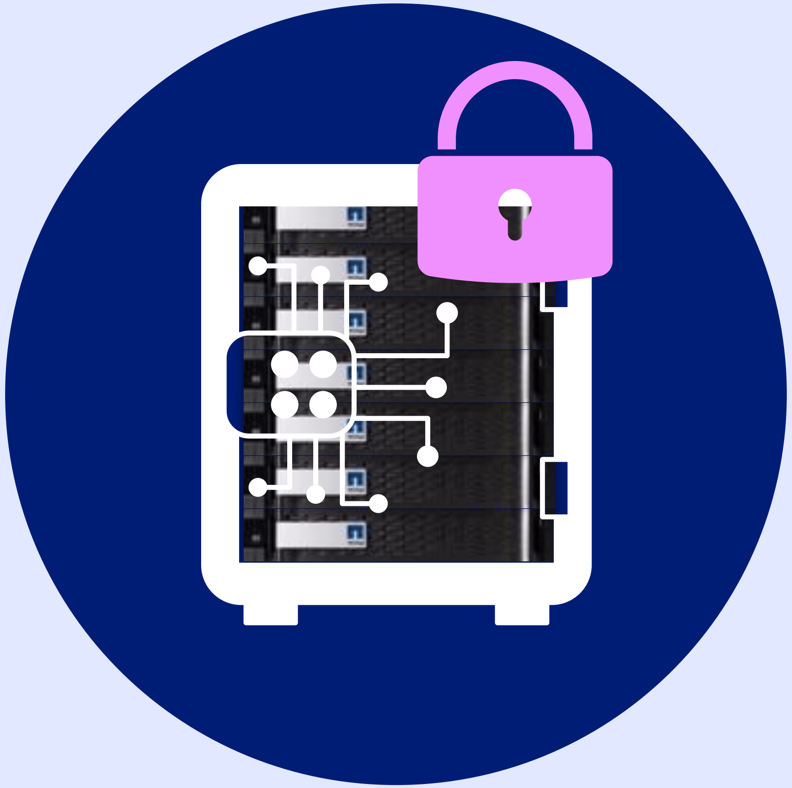
© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

NetApp cyber vaulting

Unified data storage with built-in layered ransomware protection

No silos. A purpose-built architecture for a logically air-gapped cyber vaulting, built-in to NetApp ONTAP.

- **Immutable, indelible snapshots** locked on the cyber vault, with strict access controls on a hardened configuration
- **Same API and orchestration suite support as all NetApp ONTAP systems**
- **Leverage the lowest cost storage possible, with capacity flash and hybrid flash options**



NETAPP CYBER VAULTING SOLUTION
LAST LINE OF DEFENSE

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

ENCRYPTION

At-rest and In-flight

NetApp Storage Encryption

Hardware-based data-at-rest encryption

Purpose-built, self-encrypting drives that encrypt all data

FIPS 140-2 level 2 validated drives

AES-256 bit encryption

Leverage NetApp® ONTAP® storage efficiency features

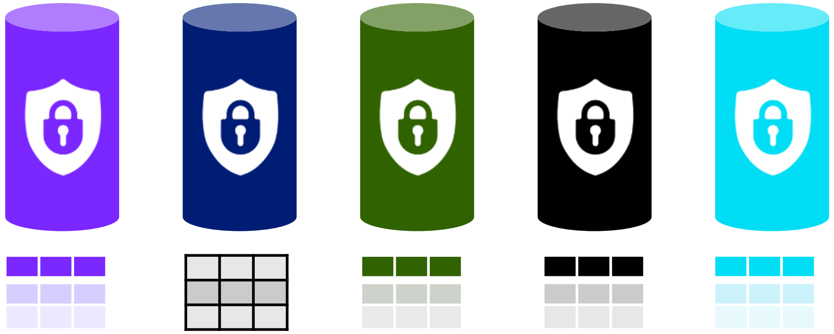
All drives in a high availability (HA) pair must be NSE drives

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

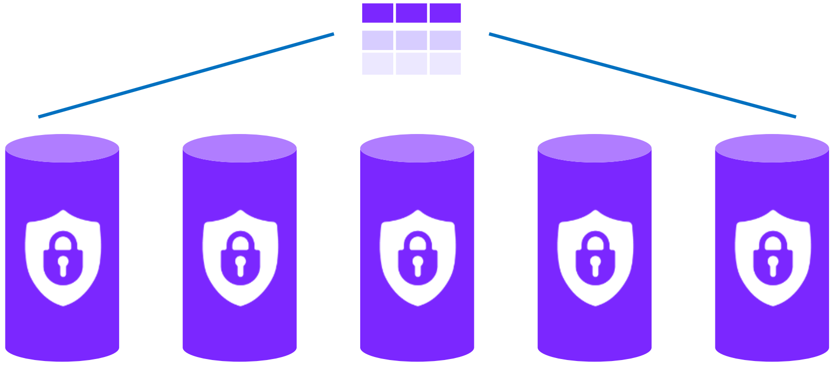
Software Encryption with All Storage Efficiencies

Leverage software-based encryption and aggregate deduplication

NetApp Volume Encryption (NVE)



NetApp Aggregate Encryption (NAE)



Encrypt new or existing data without specialized disks non-disruptively

- Non-disruptive enablement
- Zero-management encryption solution for data on disk
- Unique encryption per volume

FIPS 140-2 level 1 validated cryptographic module

AES-256 bit encryption

Leverage storage efficiency features

Onboard and external key management

Encryption key creation time in volume show starting in ONTAP® 9.11.1 for NVE and NAE

© 2025 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —

IPSec – Simplified Encryption Everywhere Client Data Goes

Securing data in-flight with Ipsec with ONTAP 9.8+

Data must be secured at all points in time, including in transit

Simple, intuitive, secure default configuration

- Powerful options for customer tweaking

Authentication

- Certificate
- Pre-shared/out-of-band secret

Support for NFS, iSCSI, and SMB

AES-256-bit Encryption

Available with ONTAP® 9.8 GA and later

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

TLS 1.3

A faster and more secure web “HTTPS” communication protocol

Removes insecure ciphers and only allows PFS-capable ciphers, improving security

Utilizes fewer ”round trips” vs TLS 1.2, improving speed

- Also removes renegotiation ability

Primary use in ONTAP is System Manager and Off Box connections such as AIQUM, Snap Center, and KMIP

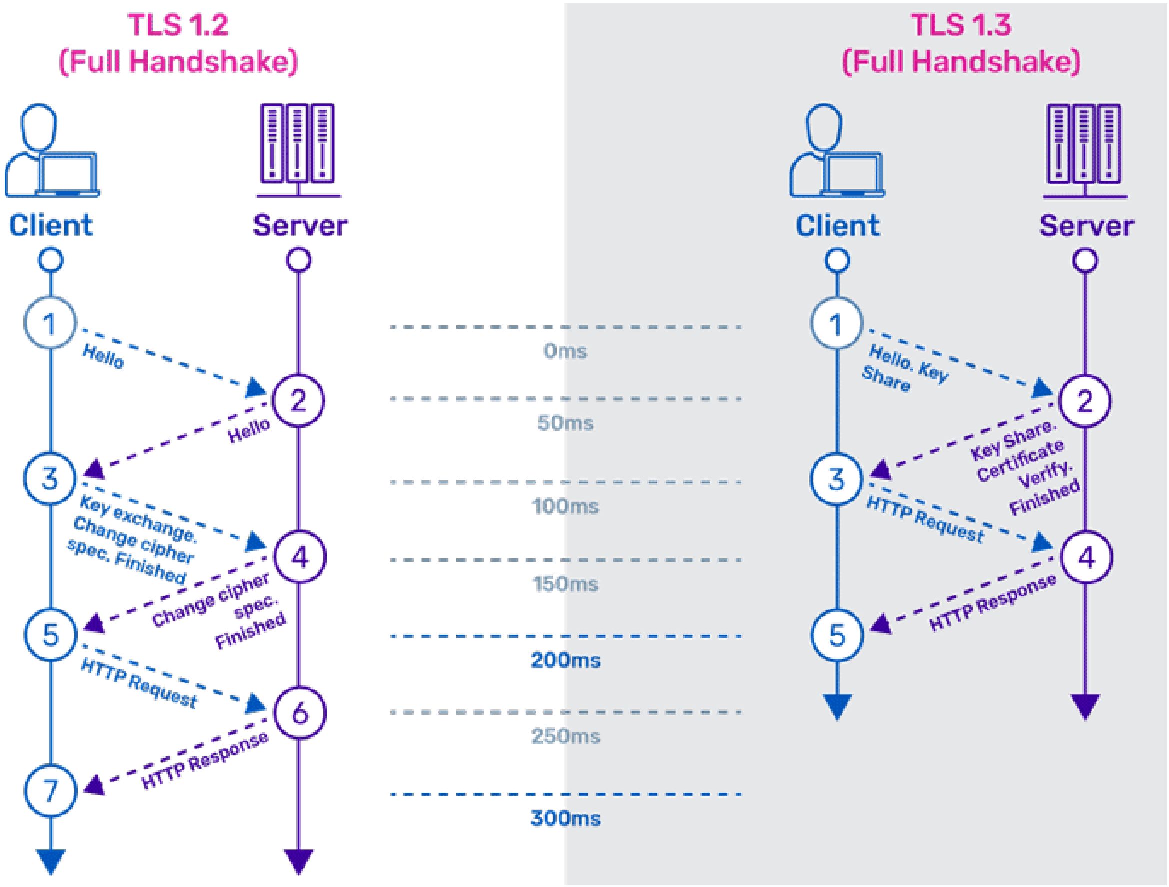
Requires ONTAP OpenSSL update to 3.0

- Current OpenSSL version is 1.0.2

FIPS 140-2 Compliance Mode validation (mgmt) is expected 6 months after TLS 1.3 in ONTAP is released

Some organizations phasing out TLS 1.2 connections

Cluster Peering Encryption (SnapMirror Encryption) will continue to use existing TLS 1.2



TLS 1.3 is faster than its predecessors

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Onboard Key Manager (OKM)

Integrated key management in NetApp ONTAP

Simplicity

Easy, quick setup

Provides all that is needed to protect against stolen, lost or repurposed disks

No external appliance to set up and manage

Integrated with NetApp® ONTAP® 9

No additional license

No additional costs

Available for any NetApp Storage Encryption (NSE) and NetApp Volume / Aggr Encryption (NVE / NAE) solution

- If using the Onboard Key Manager and the power goes off, a passphrase is required to decrypt data
- For NetApp Storage Encryption (NSE) and NetApp Volume Encryption (NVE), **protected reboot provides protection against the entire storage array being stolen**, not just the drives. All keys are stored encrypted in hierarchy on the system that is only unlocked with passphrase

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Onboard Key Manager on a USB Drive (PVR only)

Physically Destroy Data When Location is Compromised

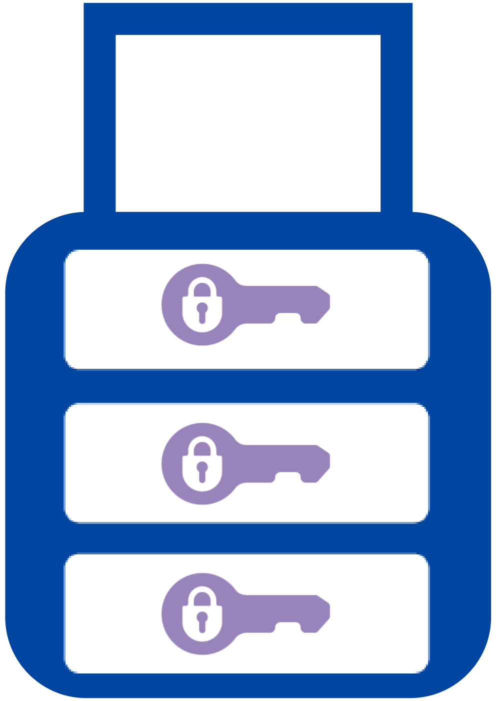
Onboard Key Manager (OKM) on a USB drive feature allows contents of OKM to be store on a USB drive that plugged into an ONTAP® system

- Optional feature – default off

Provide a **physical mechanism to crypto-shred** all data even in the event of power loss – **think Big Red button**

USB must be present for unlocking drives and decrypting volumes after a node is rebooted

- NetApp Storage Encryption (NSE) – system will not boot
- NetApp Volume Encryption (NVE) only – volumes will not come online



© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

External Key Managers

NetApp partners with several vendors to provide an added level of security

Centralized Key Management Infrastructure

Manage multiple clusters keys with a solution

Manage other KMIP-compatible encryption products with the same solution

Separation of Duties

Allows for separation of cryptographic material management and networked storage management

Higher FIPS 140-2 Compliance for Key Management

NetApp® offers FIPS 140-2 level 3 compliant key management solutions

HashiCorp

THALES

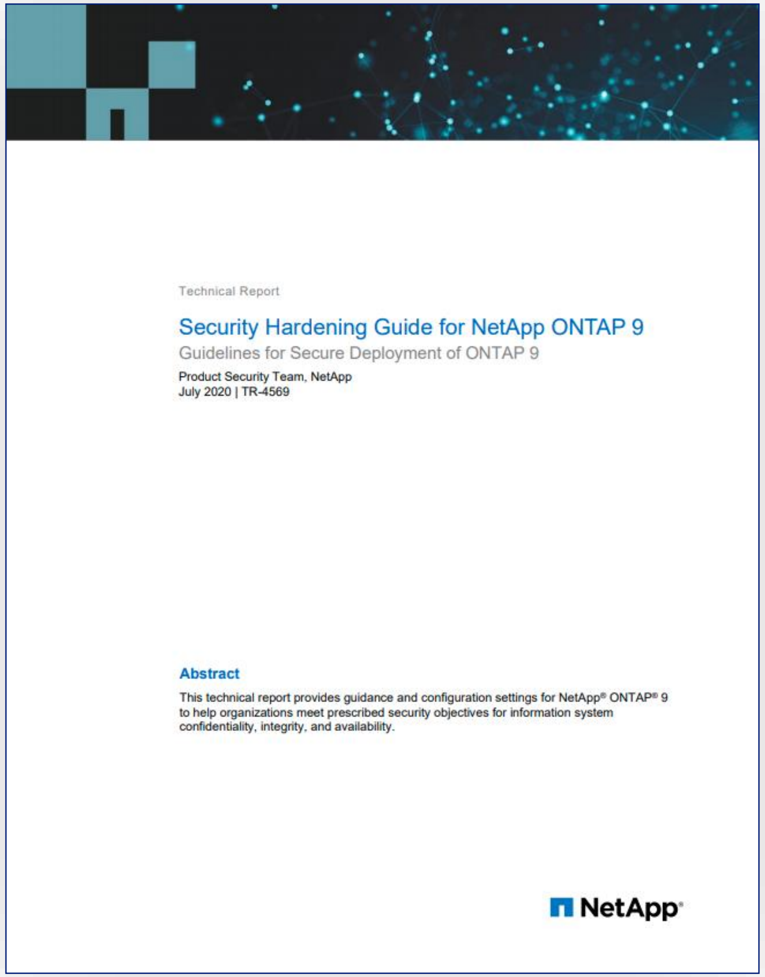
IBM

Can be configured in System Manager in 9.13.1

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

Security Hardening Guide for NetApp ONTAP 9

TR-4569



Technical Report

Security Hardening Guide for NetApp ONTAP 9

Guidelines for Secure Deployment of ONTAP 9

Product Security Team, NetApp
July 2020 | TR-4569

Abstract

This technical report provides guidance and configuration settings for NetApp® ONTAP® 9 to help organizations meet prescribed security objectives for information system confidentiality, integrity, and availability.

Best practices

RBAC

Auditing

Secure protocols

Fpolicy

Encryption at rest and in flight

Port usage

http://www.netapp.com/us/media/tr-4569.pdf

© 2025 NetApp, Inc. All rights reserved. NETAPP CONFIDENTIAL

MERCI DE VOTRE ATTENTION !

Sondage de satisfaction

Merci de votre feedback

Scannez-moi

Cyberdefense