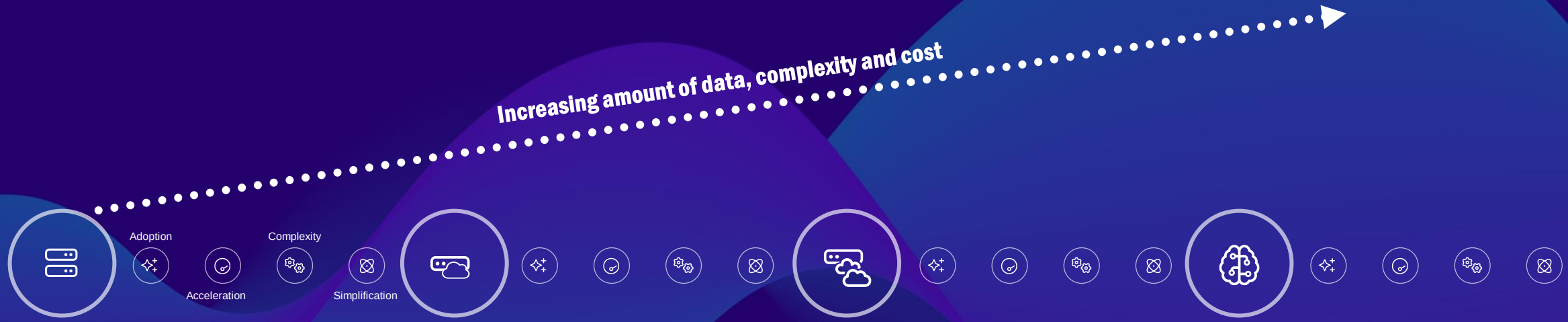
Data Community Conference Switzerland 2024

AI-powered built-in ransomware detection with NetApp storage

Christophe Danjou
NetApp – Partner Technical Lead

www.data-community.ch

Across several eras in the age of data, NetApp has led in data infrastructure innovation



2002

Data Silos & Unification

NetApp becomes the first vendor to **unify file & block workloads, and structured & unstructured data**

Hybrid Cloud

NetApp creates the first **data fabric strategy** that eliminates silos & provides unified control across any environment

Hybrid Multiclouds

NetApp becomes the ONLY vendor to introduce **cloud ops and data services** as key data infrastructure pillars in addition to being the **only vendor natively embedded in all major clouds**

Today

Intelligence

NetApp delivers **silo-free infrastructure,** then harnesses **observability and AI** to enable best data management everywhere

Data storage to meet every need – all powered by ONTAP

	For lowest cost, secondary use cases	For best price/ performance	For best performance On Tier1 workloads
	HYBRID FLASH	**CAPACITY FLASH**	**PERFORMANCE FLASH**
Unified	FAS 	AFF C-Series 	AFF A-Series 
Block Optimized		ASA C-Series 	ASA A-Series 

ONTAP Comprehensive data management software delivering automation, efficiency, data protection, and security capabilities for file, block, and object






Unified control across your hybrid multicloud

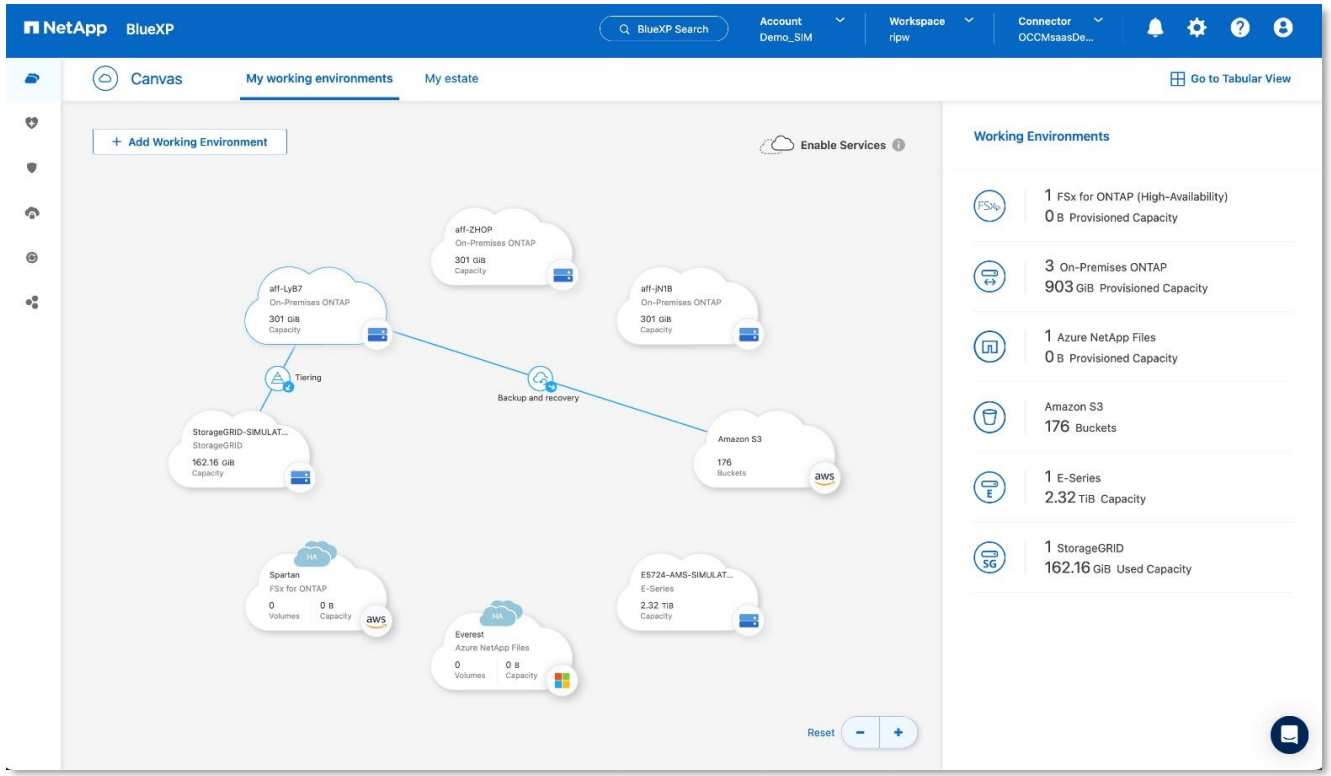
NetApp BlueXP

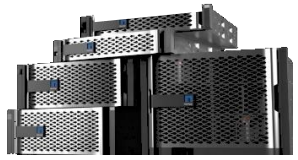
Unified control
of storage and services for
all your data wherever it lives

Powerful AIOps
drives operational simplicity

Flexible consumption of resources
unlocks control, investment protection,
and ROI

Integrated services
maximize data protection and cyber
resilience while minimizing costs





aws Microsoft Azure Google Cloud

Delivering the speed, simplicity, and security required in today's highly complex world

72%

In 2024, Ransomware affected 72% of organizations.
Source: Sophos "The State of Ransomware 2024"

It's not a matter of if but when you will experience a cyber-attack.

NetApp

Ransomware costs businesses millions annually

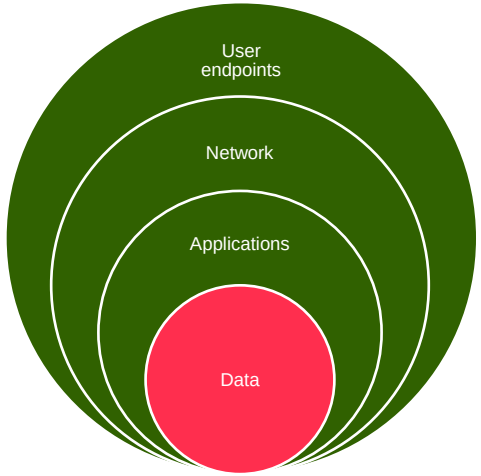
Sophos reports that 92% of companies that pay don’t get their data back

[1] Standard and Poor’s report https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-underwriters-premiums-surge-loss-ratios-improve-in-21-70247722

[2] Sophos report survey data of 5,600 IT manager on “The State Of Ransomware 2022” Average cost was for organizations. https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxqj9/sophos-state-of-ransomware-2022-wp.pdf

Zero trust

NetApp helps you design your protection and security solutions from the inside out. Verify, never trust.



NIST

Identify

Assess your data-protection and security posture

Classify type of data, location, and permissions

Protect

Block malicious data from being written to disk

Create granular, immutable copies to thwart infection

Prevent data deletion with indelible data copies

Detect

Monitor user behavior for suspicious activity

Detect storage behavior anomalies

Respond

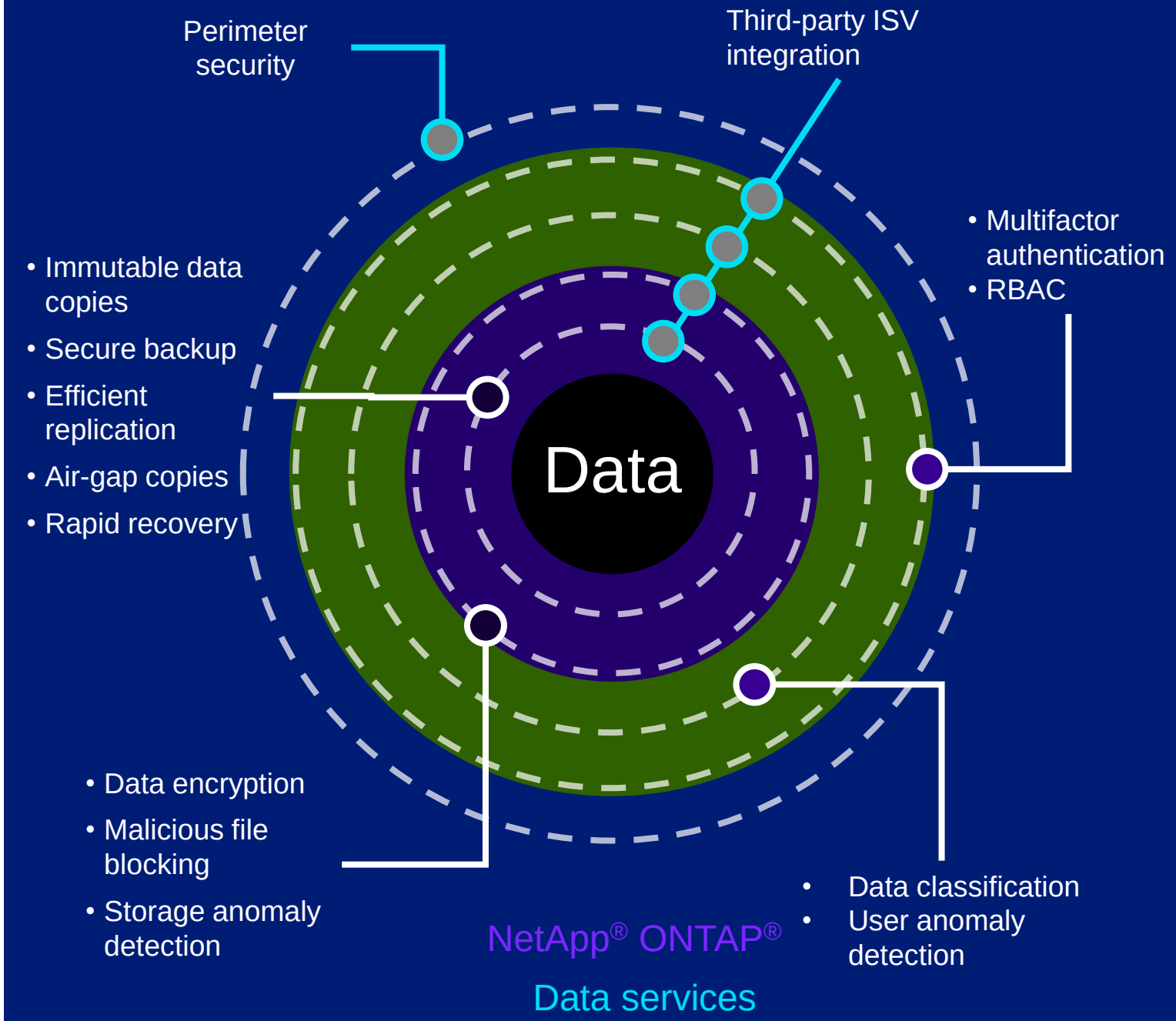
Initiate NetApp® Snapshot™ copies if an attack is identified

Block malicious user accounts

Recover

Restore data in minutes and bring applications back online

Apply intelligent forensics to identify the source of the threat



NetApp Ransomware Protection

1. Secure by design
2. Real-time detection & response
3. Single control plane to automate
4. Air-gapped cyber vaulting
5. Recovery guarantee


NetApp
The most secure storage on the planet

The only enterprise storage validated for top-secret data

NetApp®

Commercial Solutions for Classified (CSfC) Components List

FIPS 140-2

Department of Defense Information Network Approved Products 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/

BUILT-IN RANSOMWARE PROTECTION

AI-powered ransomware protection embedded in our storage.

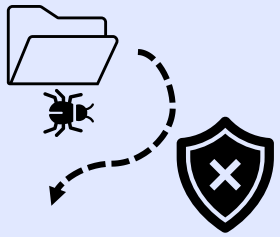
NetApp

Full-spectrum data protection built into ONTAP

Advanced data protection and security across your hybrid cloud

IDENTIFY & PROTECT

Policy Engine

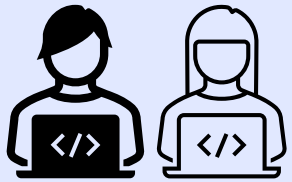


Automatically block known malicious file types

Immutable WORM Primary Data & Tamper-Proof Snapshots

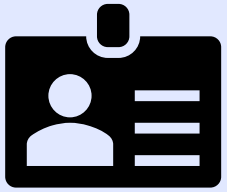
Prevent data destruction with immutable and indelible snapshots

Multi-Admin Verify



Block rogue admins and malicious users

End-to-End Encryption



Secure data access, end-to-end

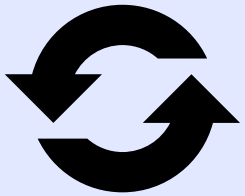
DETECT

Autonomous Ransomware Protection

Automatically detect and respond to file system anomalies **in real-time** – **built into ONTAP**

RESPOND & RECOVER

SnapRestore



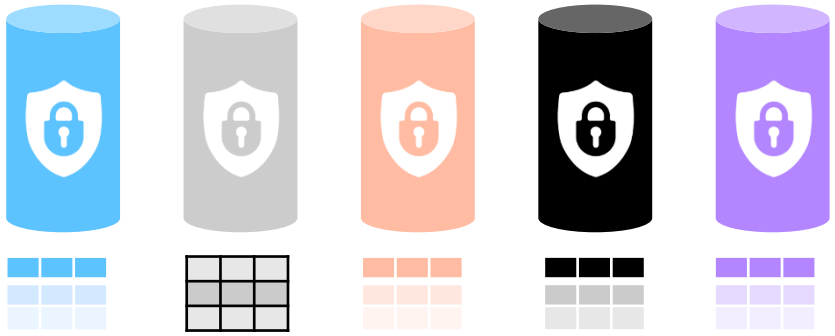
Restore data in minutes from secure snapshots

Some words from our lawyers… No ransomware detection or prevention system can completely guarantee safety from a ransomware attack. While it's possible an attack might go undetected, NetApp technology acts as an important additional layer of defense.

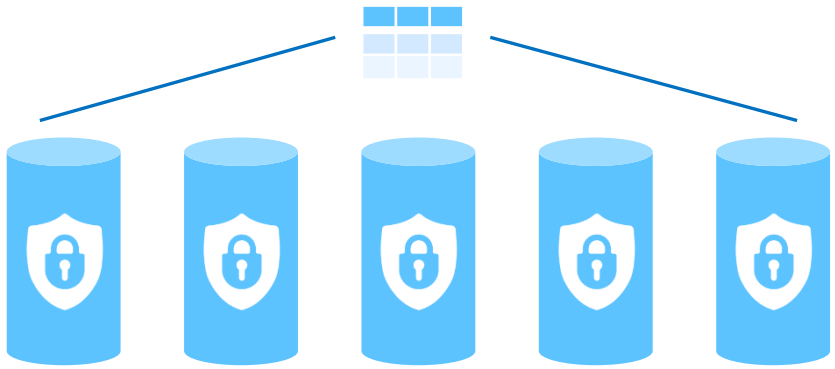
Software Encryption with All Storage Efficiencies

Leverage software-based encryption and aggregate deduplication

NetApp Volume Encryption (NVE)



NetApp Aggregate Encryption (NAE)



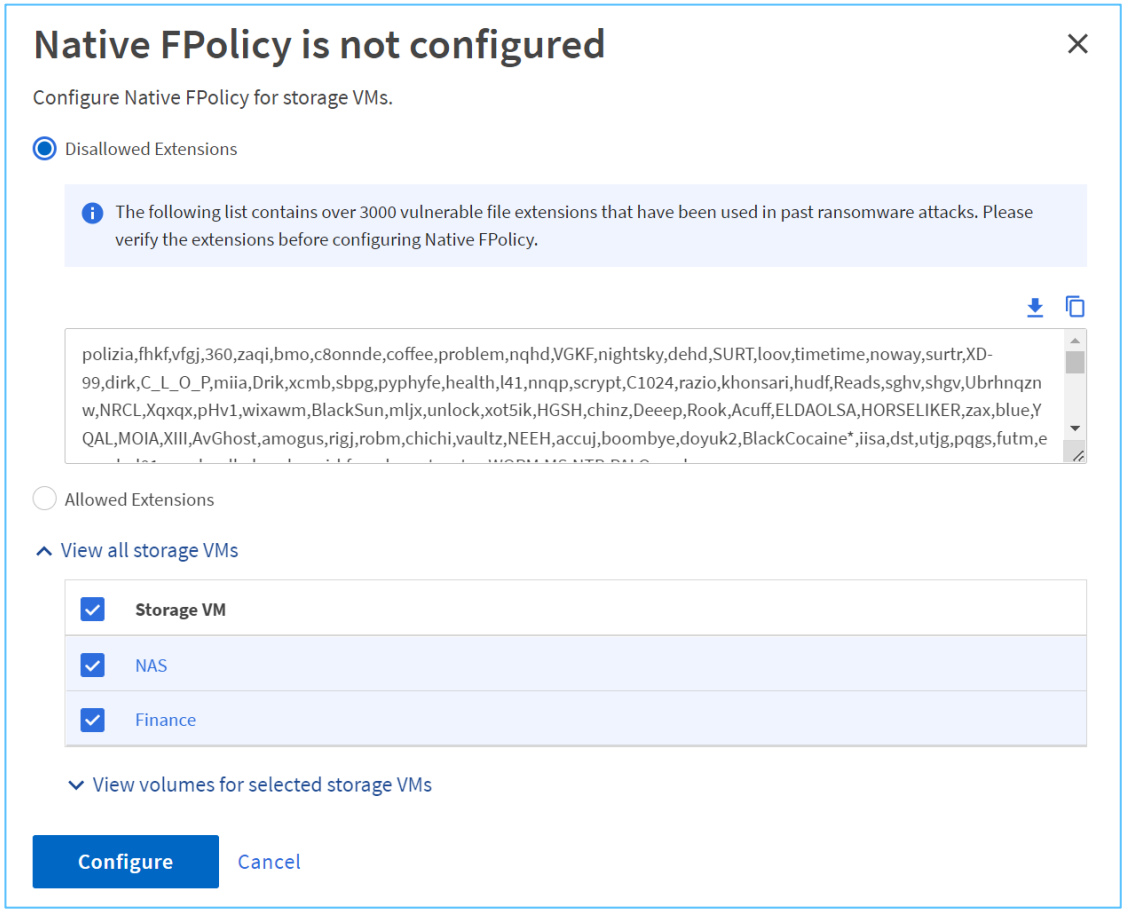
- Encrypt new or existing data without specialized disks non-disruptively
  - Non-disruptive enablement
  - Zero-management encryption solution for data on disk
  - Unique encryption per volume
- **FIPS 140-2 level 1 validated cryptographic module**
- AES-256 bit encryption
- Leverage storage efficiency features
- Onboard and external key management
- Encryption key creation time in volume show starting in ONTAP® 9.11.1 for NVE and NAE

Easy FPolicy configuration for ransomware defense

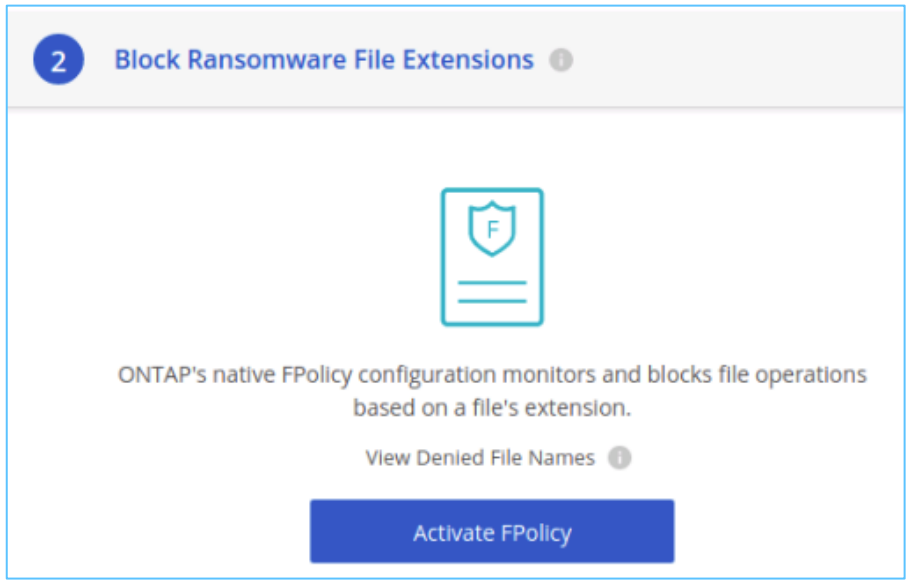
Block common ransomware file types with a simple wizard

- NetApp® FPolicy is included with every NetApp ONTAP® system and offers defense against common ransomware attacks
- Known malicious files can be blocked from ONTAP NAS exports
- ONTAP System Manager and NetApp BlueXP now offer simple enablement of this feature that blocks a predefined list of 3,000+ common ransomware file extensions

System Manager



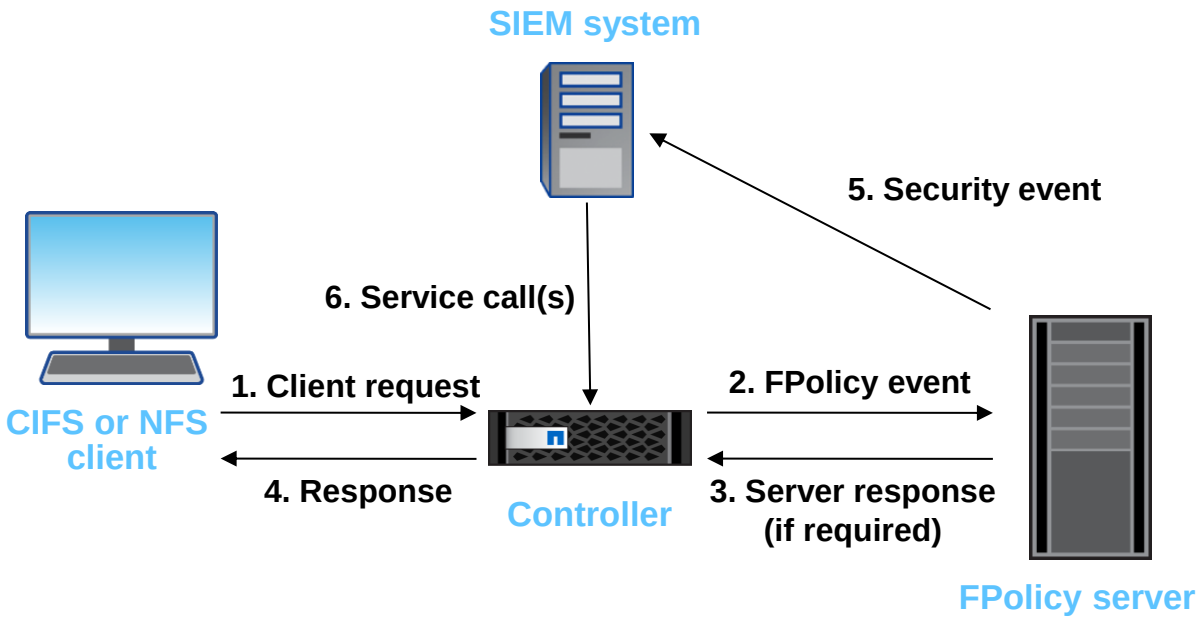
BlueXP



NetApp FPolicy

Detection and prevention

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



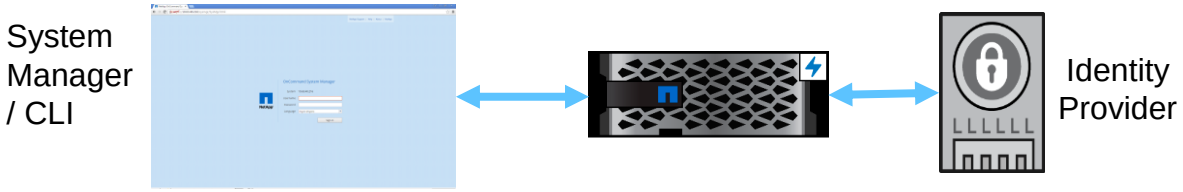
PARTNERS

NetApp CLOUD INSIGHTS
VERITAS
VARONIS
CLEONDRIS
STEALTHbits TECHNOLOGIES
ProLion
Brainwave GRC

Prevent unauthorized actions by compromised admins

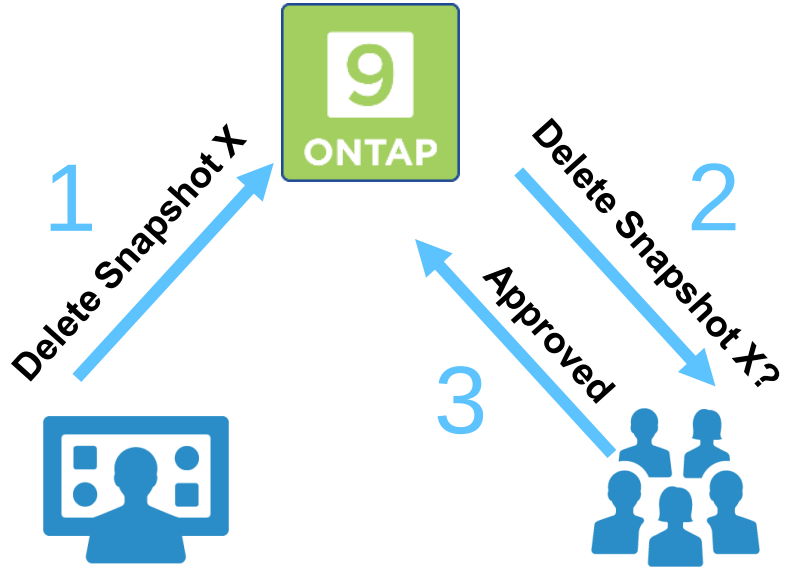
Multi-Factor authentication and / or multi-admin verify

- Secure Shell two-factor authentication (SSH 2FA) for administrative CLI access:
  - Administrative user SSH public key combined with username and password from either local ONTAP password or NIS/LDAP password.
- NetApp® OnCommand® System Manager and OnCommand Unified Manager 7.3 can leverage a third-party identity provider (IdP) for authentication to the web UI.
  - An IdP enables customers to define their own authentication factors and enables single sign-on (SSO) for System Manager, Unified Manager, and any other customer application that uses the IdP.



Multi-admin verification (MAV)

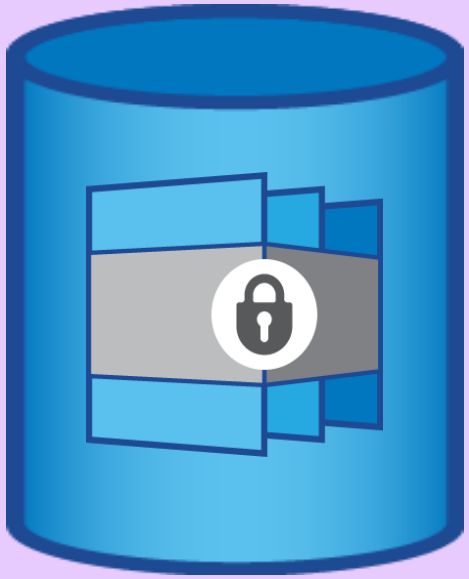
- Built-in feature of NetApp ONTAP® (no license required)
- Administrator accounts have the ability to run destructive commands like deleting Snapshot copies
- Requires N-number of approvals for all or a set of commands before allowing the command to take
- Snapshot deletion for unlocked Snapshot copies will require multiple admin approval



Tamperproof Snapshot copies using Snapshot copy locking

Rapidly create tamperproof recovery points

- By leveraging NetApp® SnapLock® technology, NetApp Snapshot™ copies are now protected from deletion by compromised administrator credentials or an internal rogue administrator attack
- Snapshot copies can’t be deleted or changed, even by NetApp support
- Enables rapid recovery in the event of data damage by providing an immutable recovery point on the primary data source
- Protection applies to Snapshot copies on both the primary and secondary systems
- Volumes or local tiers with tamperproof Snapshot copies can’t be deleted



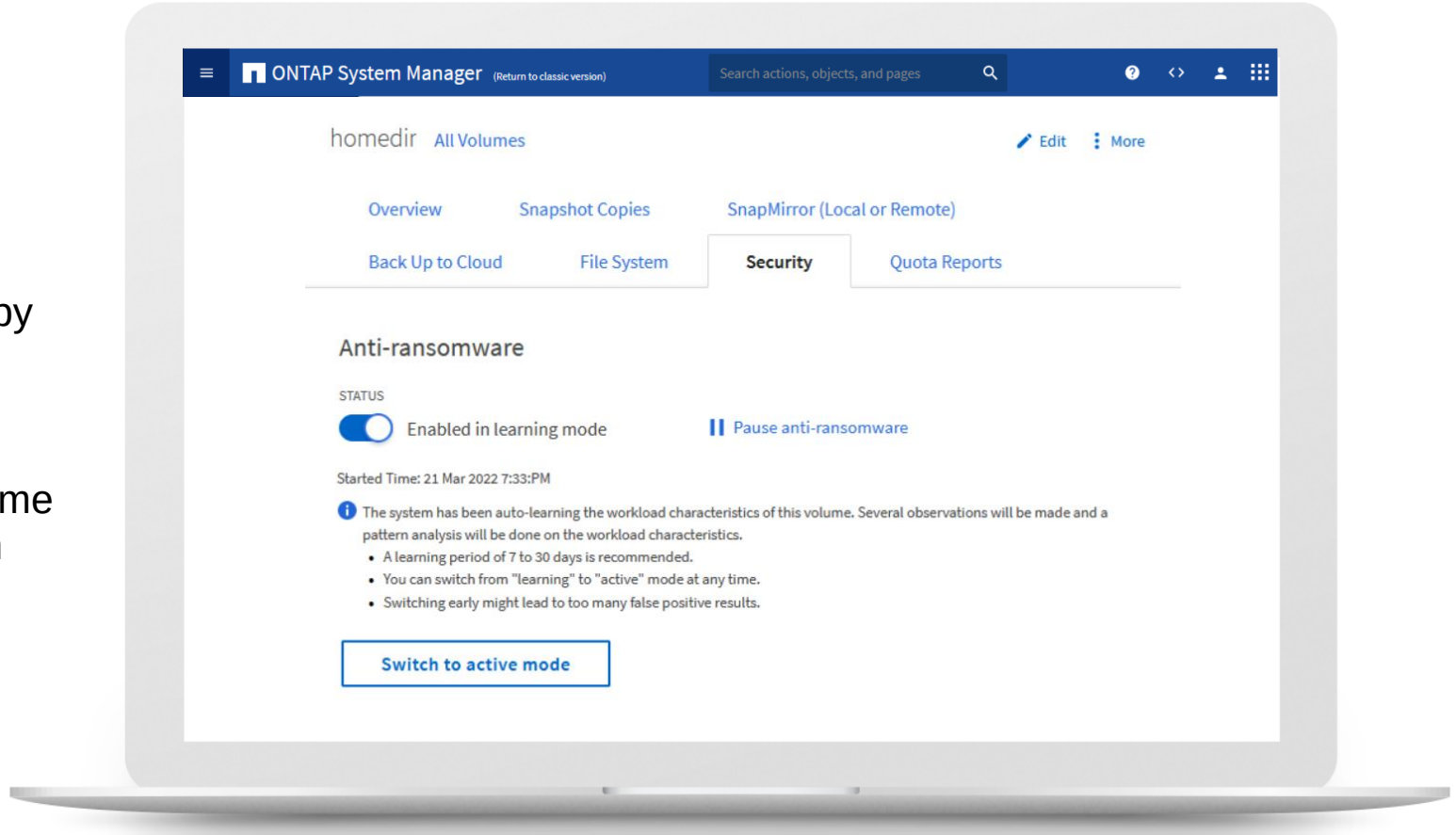
Tamperproof Snapshot copies protect against cybersecurity threats

NetApp ONTAP Autonomous Ransomware Protection

ONTAP Onbox Anti-Ransomware

- Proactively detect and warn about attack
- Learning Mode 7 days to 30 days.
- Automatically takes NetApp Snapshot™ copy during ransomware attack.
- Admin can determine if false positive.
- NetApp ML analytics engine based on volume file activity, data entropy and File extension types.

ONTAP Anti-Ransomware detection and protection with Snapshots



AI-Powered Ransomware Protection

Tech Preview

Next generation ransomware threat detection

- Industry-leading AI-powered ransomware detection for enterprise storage
- Next-gen AI/ML models deliver 100% precision and 99% recall, to detect more sophisticated and evolving cyber threats
- Automatically update model parameters regularly without a required ONTAP update or system reboot
- Seamless upgrade from current generation autonomous ransomware protection

Precision	**100%**
Recall	**99%**

TECH PREVIEW AVAILABLE NOW

Results are based on SE Labs Validation Testing.

Data Infrastructure Insights

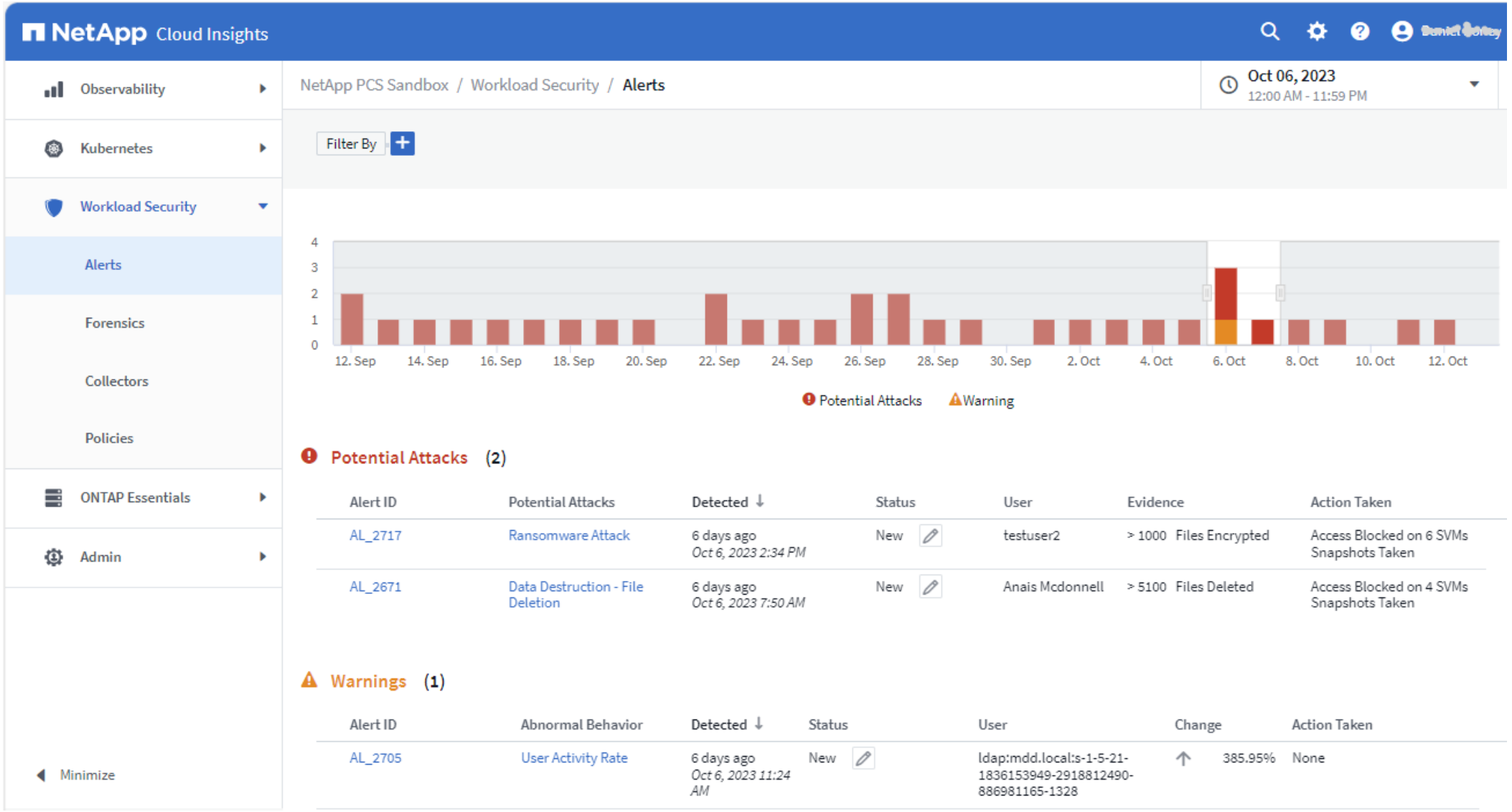
Workload Security

- NetApp's **observability service** provided as a Cloud offering
- Integrated to the unified BlueXP control plane
- Monitor, troubleshoot, optimize, and **secure** your hybrid cloud infrastructure
- Uses machine learning (ML) to analyze data access patterns
- Adopt trust no one approach. Inspects and analyze all data access activity in real time.
  - Monitor User Activity & File entropy
  - Detect Anomalies & Identify potential Attacks
  - Automated Response Policies
  - Forensics and User Audit Reporting

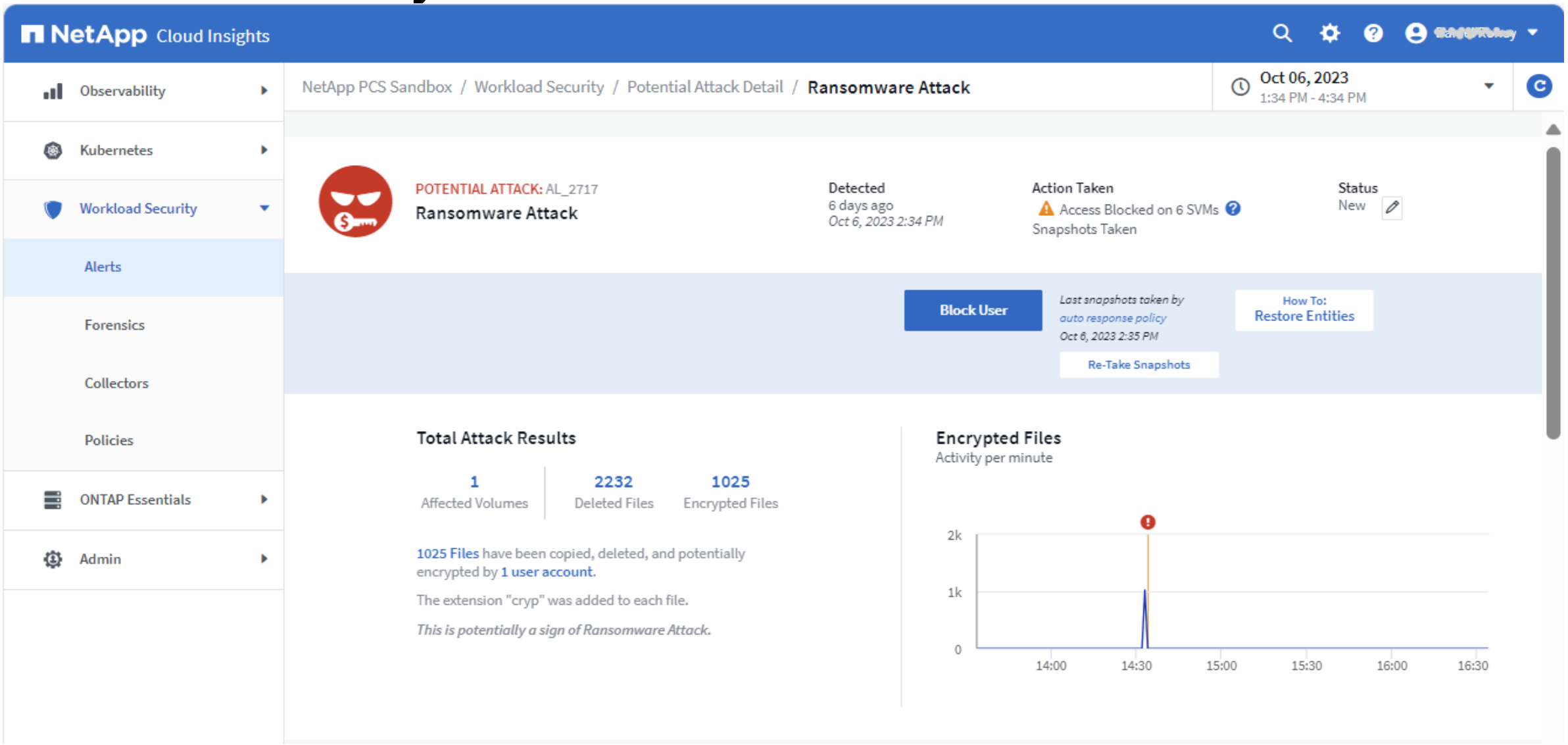
Workload Security - Data Collection

- Data is collected using a lightweight, stateless **Data collector agent** installed on a VM in the customer's environment
- Collects user data from active directory and LDAP servers
- Collects user file activity from ONTAP, Cloud Volume ONTAP (CVO) and Amazon FSx for NetApp ONTAP
- Scalability
- Supports multiple data collectors per agent
- Supports multiple agents

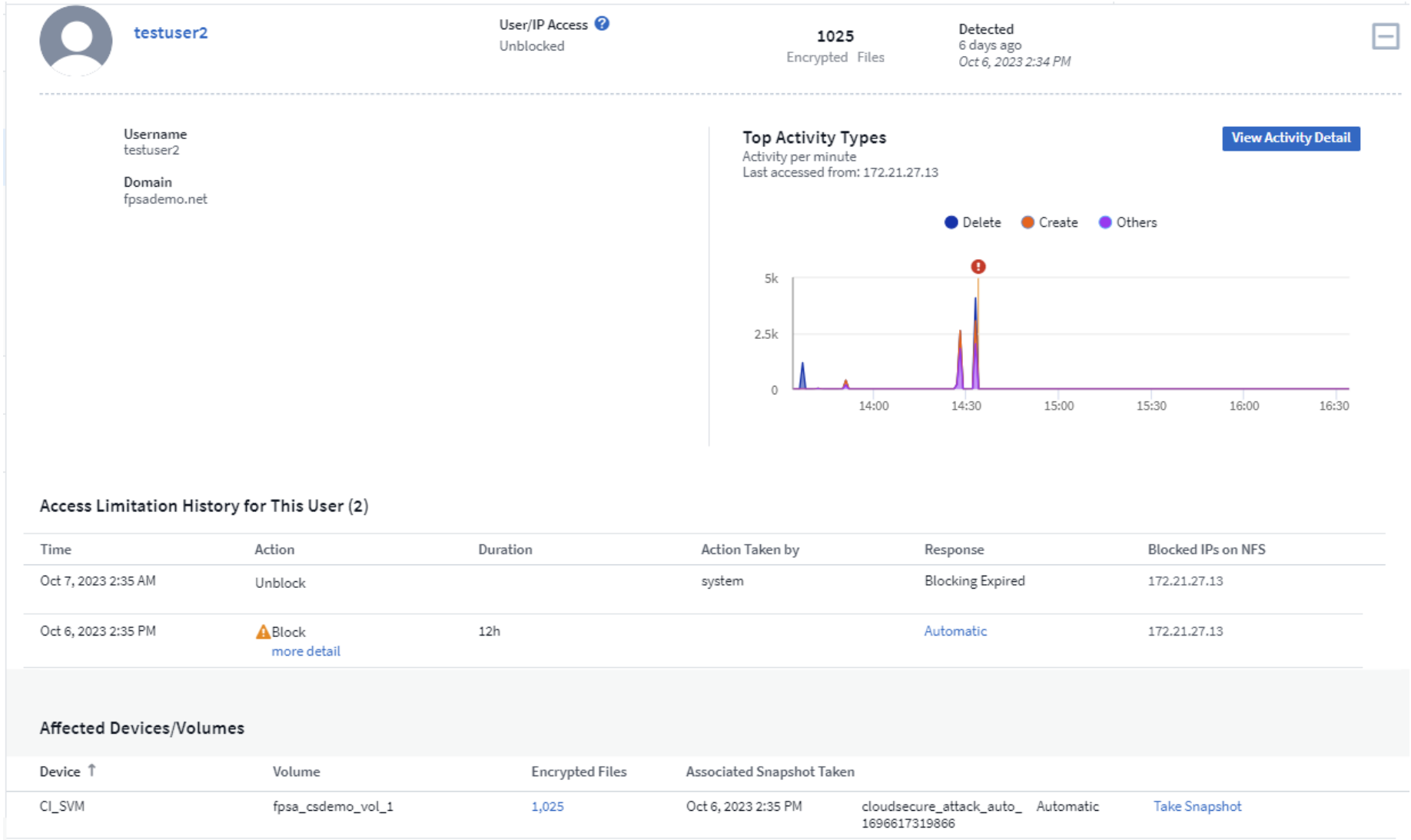
Workload Security – Alerts Page



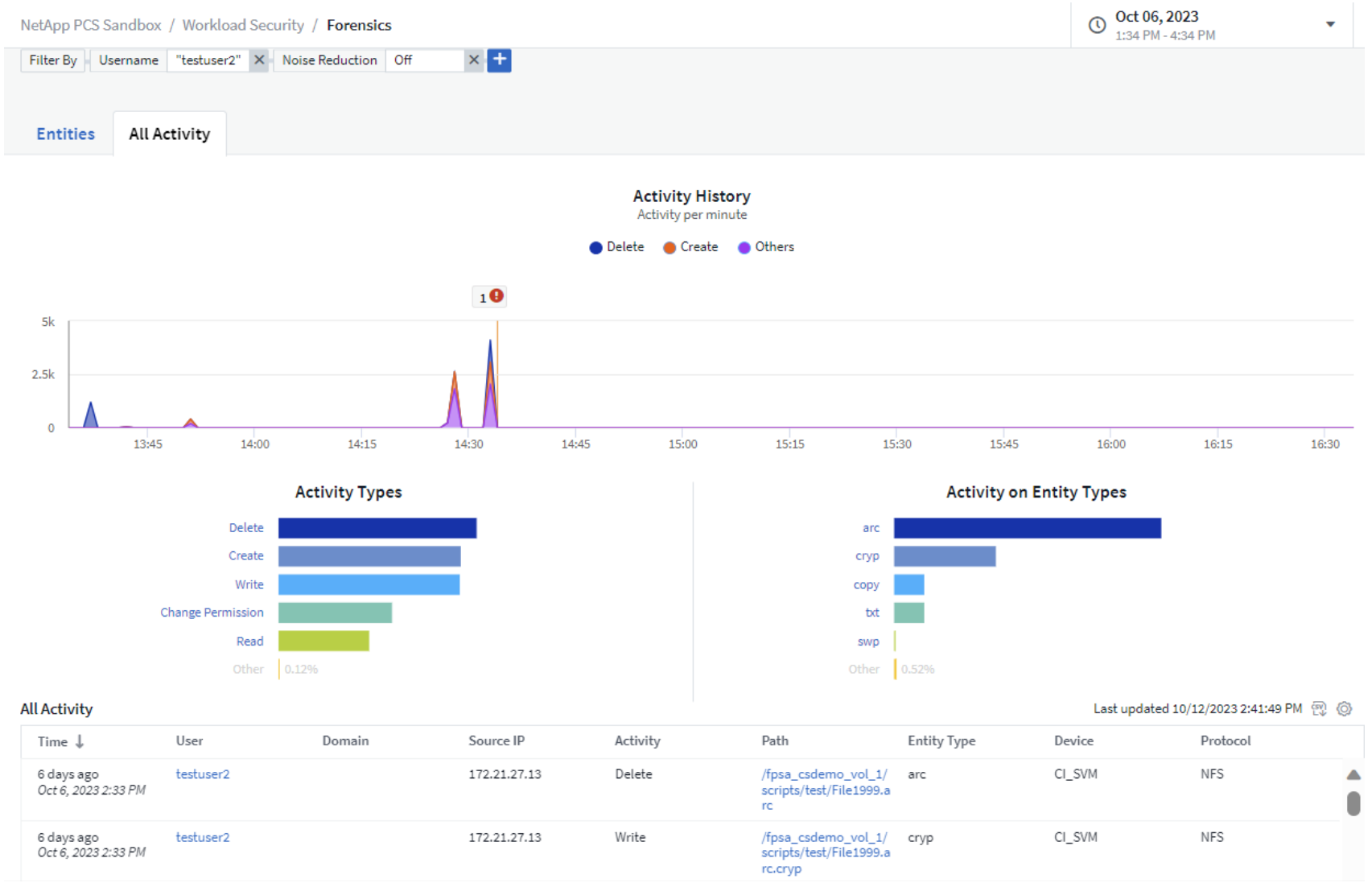
Workload Security – Alerts Details



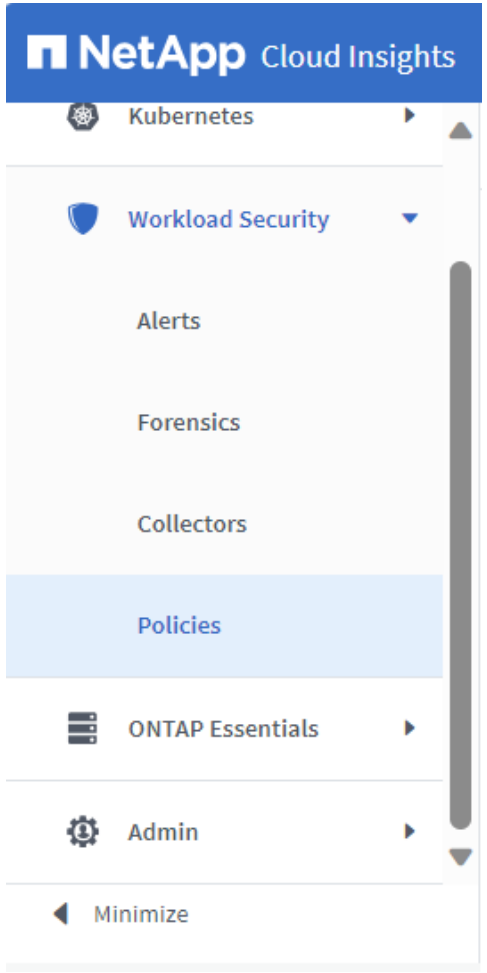
Workload Security Alerts - User Details

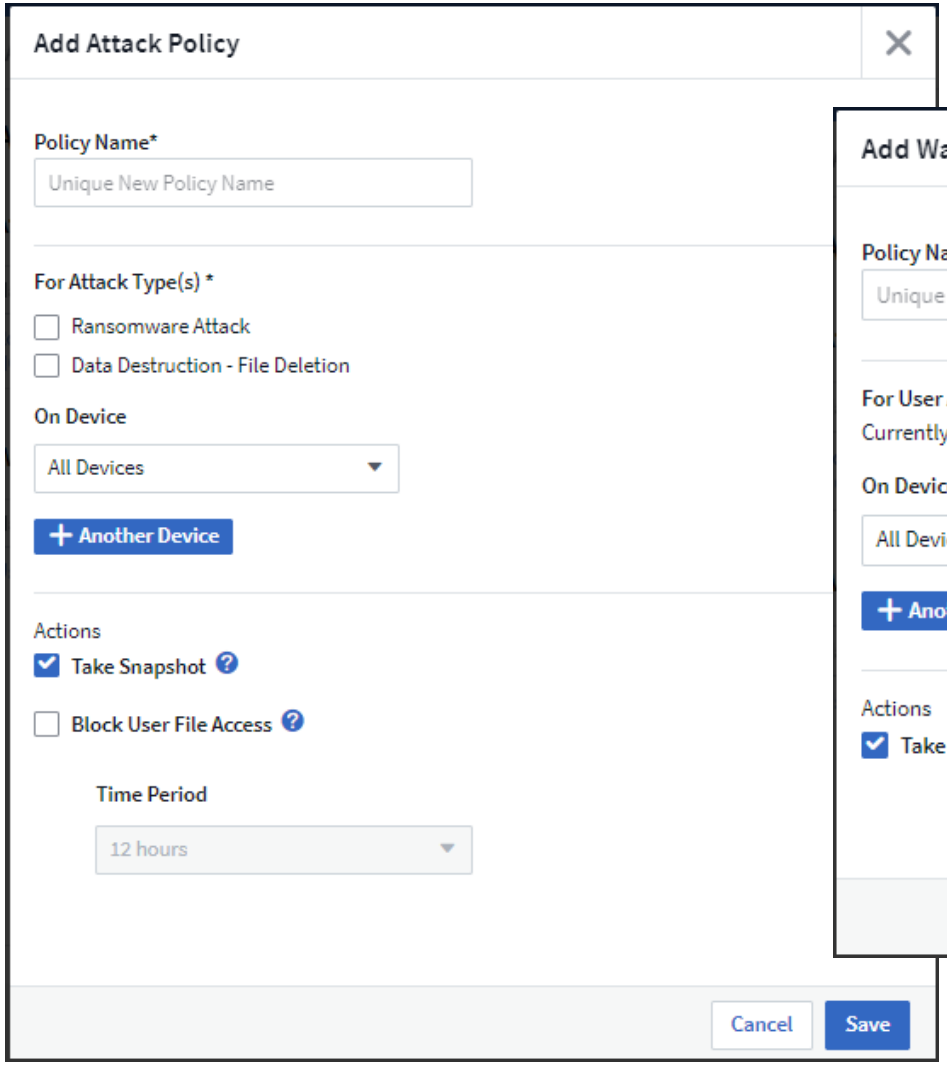


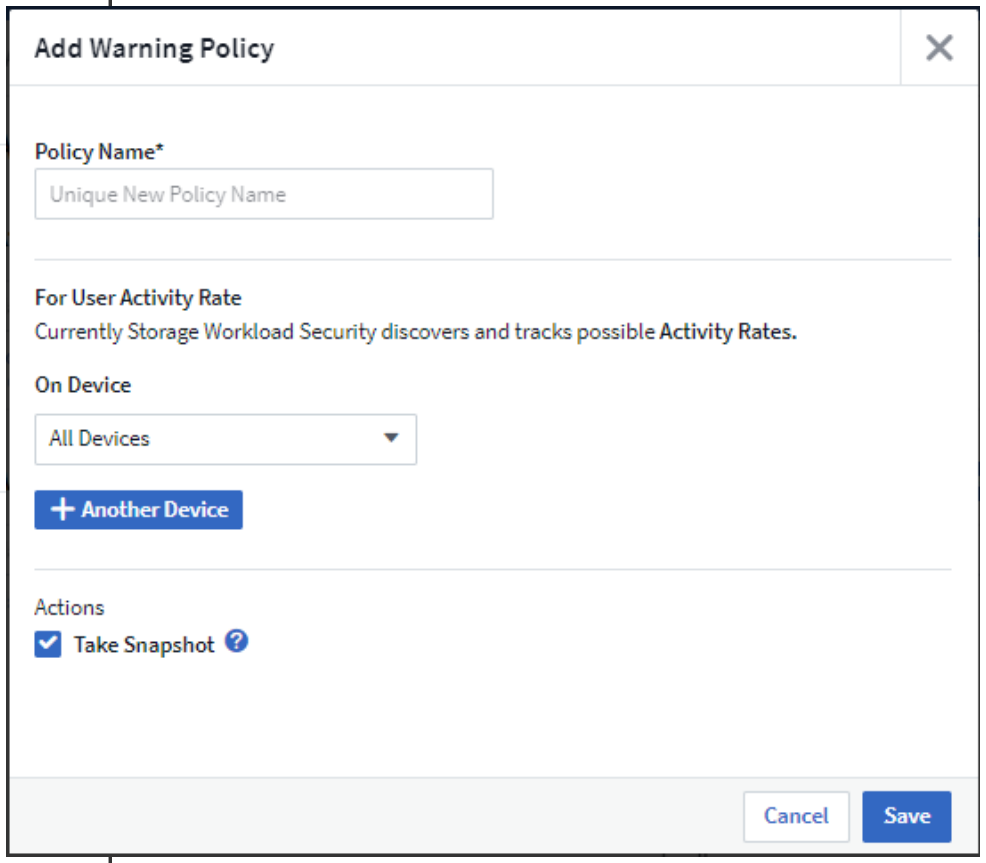
Workload Security Alerts – User Activity Details



Workload Security - Attack and Warning Policies

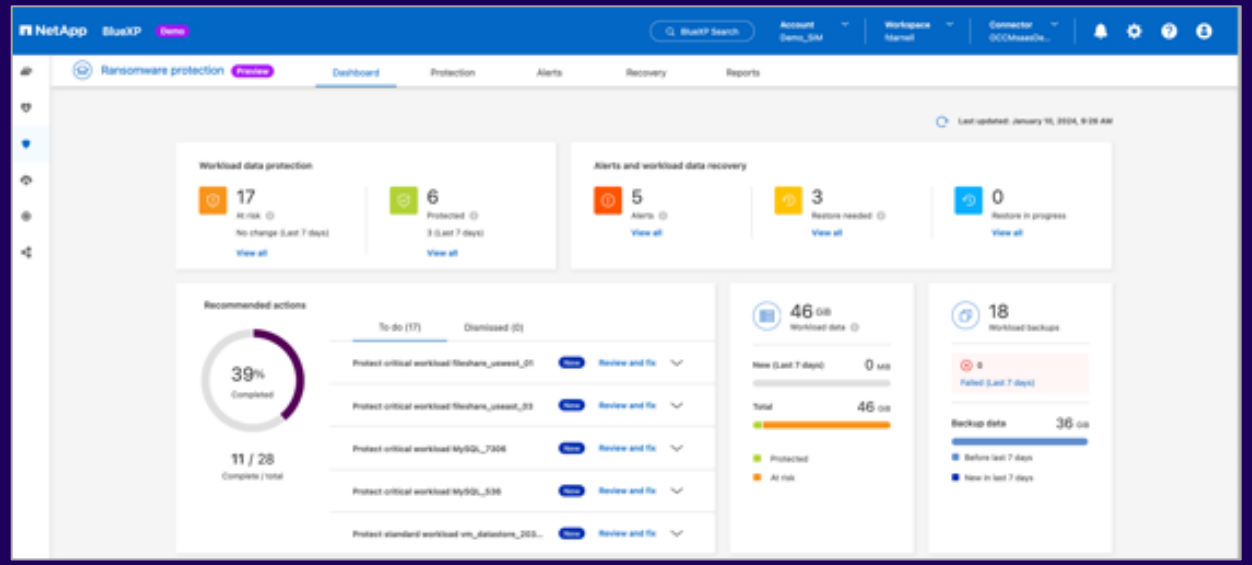






NetApp BlueXP ransomware protection

The AI-based intelligence and assistance needed to minimize workload data loss and bounce back quickly



IDENTIFY: Automatically identifies workloads (VMs, file shares, DBs) and their data in your NetApp storage, maps data to workload, determines workload importance, and analyzes workload risk.

PROTECT: Shows you what to protect. Recommends workload protection policies and applies them with one-click.

DETECT: Detects potential attacks on your workload data in near real-time using industry leading AI/ML.

RESPOND: Automatically responds in near-real time by taking immutable and indelible Snapshot copies when a potential attack is suspected. Integrates with popular SIEMs.

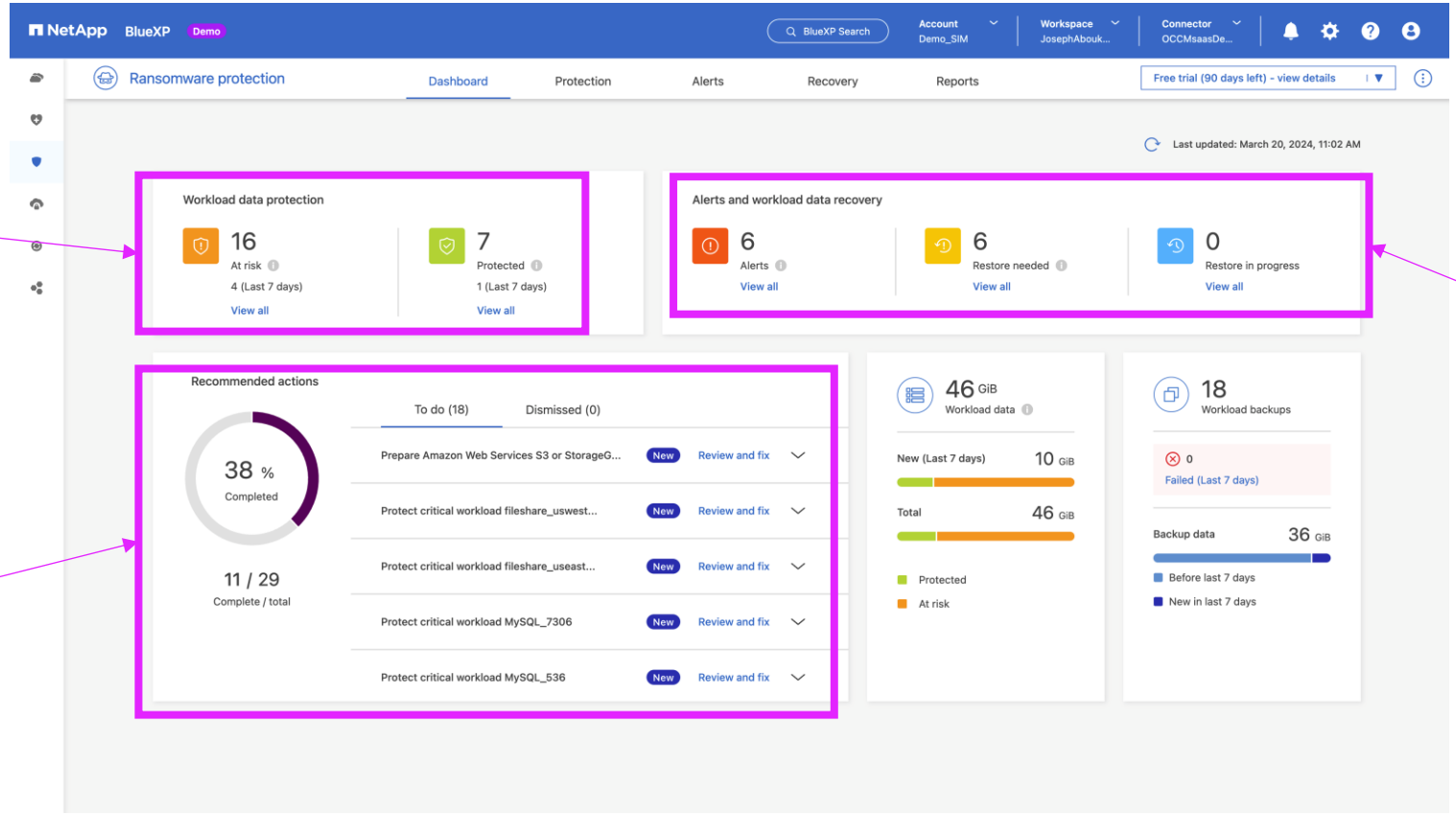
RECOVER: Rapidly restores workloads, with application consistency, through simplified orchestrated recovery.

GOVERN: Implements your ransomware protection strategy and policies, and monitors outcomes.

Dashboard – Posture assessment and recommendations

Workload protection posture assessment summary

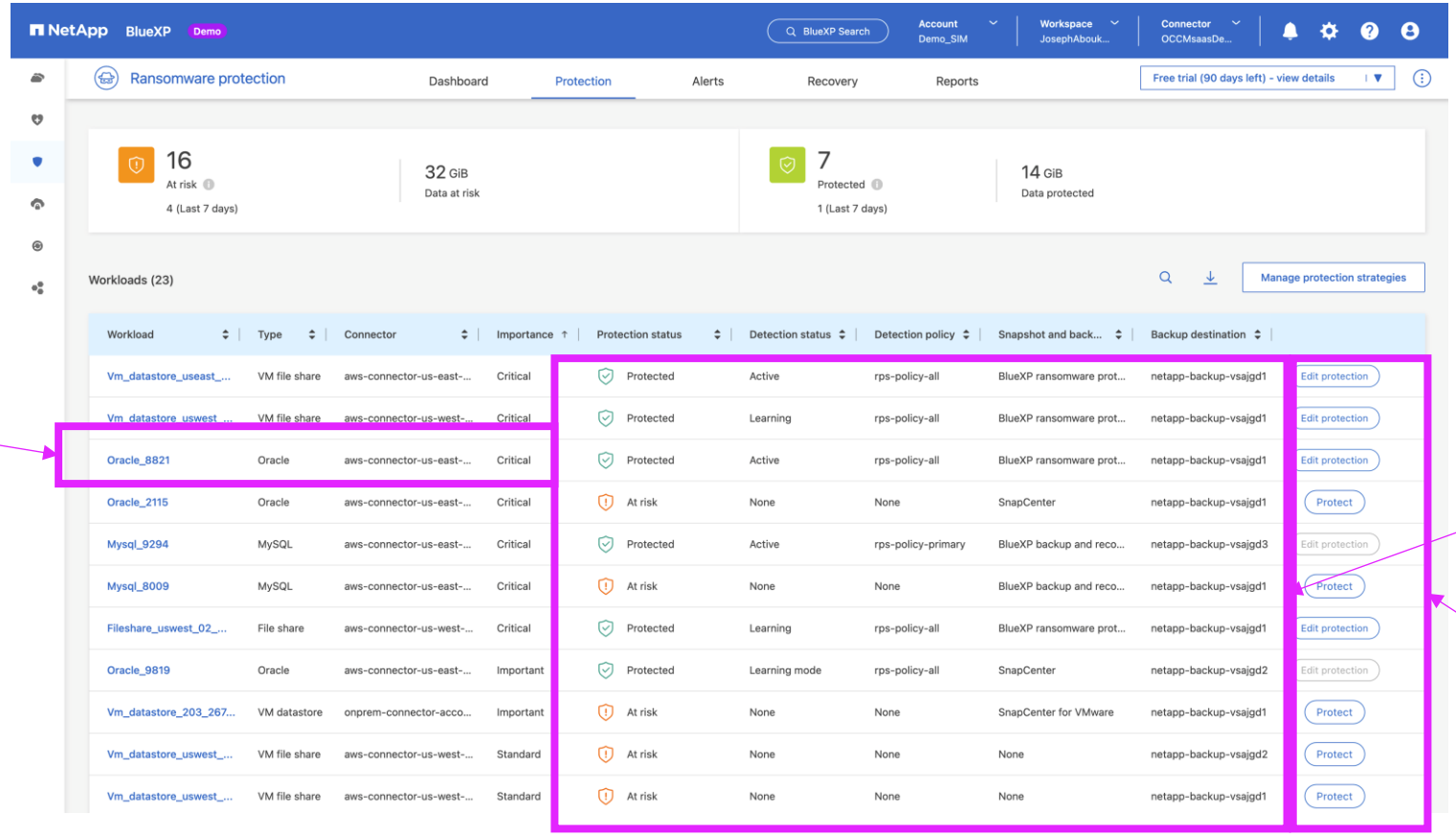
Recommendations to improve protection posture



Potential attack alerts and activities

Protection tab – Workload protection and configuration

Intelligently identify workloads and assign importance

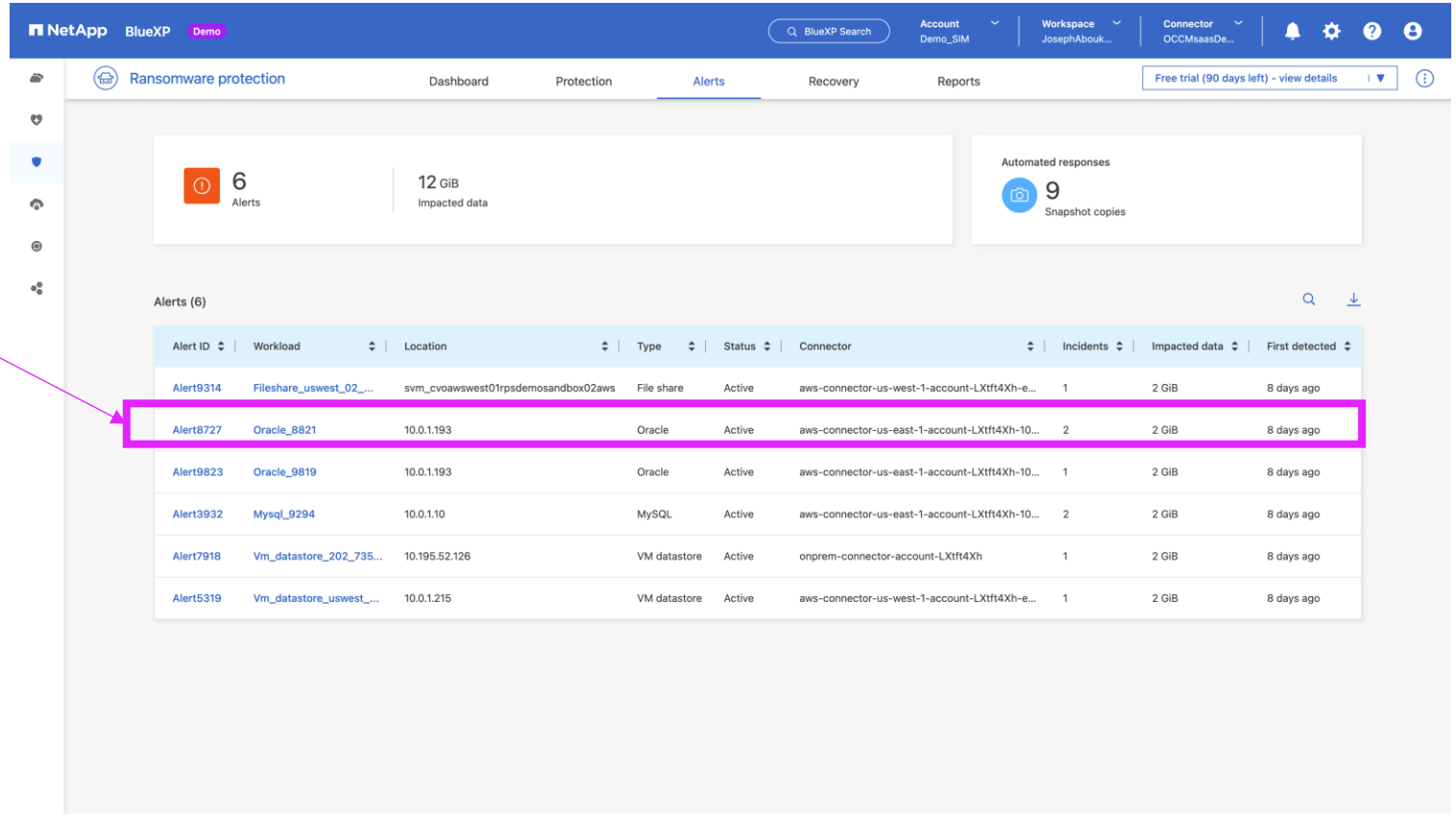


Discover existing protection posture

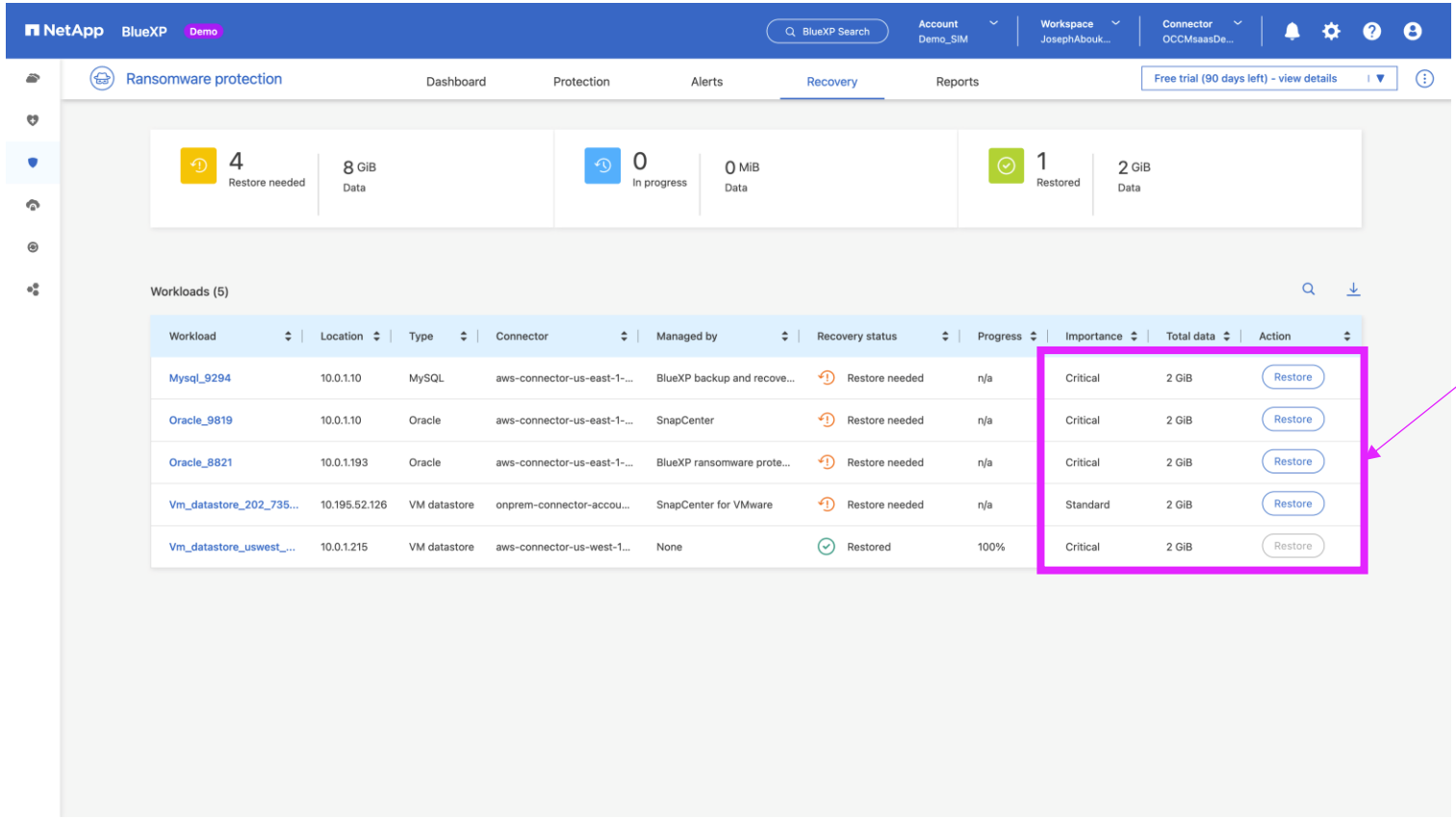
Improve protection posture

Alerts – View potential attacks

Alert details including number of incidents, impacted data, and timeframe



Recovery – View status and restore



Restore workloads in your preferred order: Priority, Type …

SIEM integration

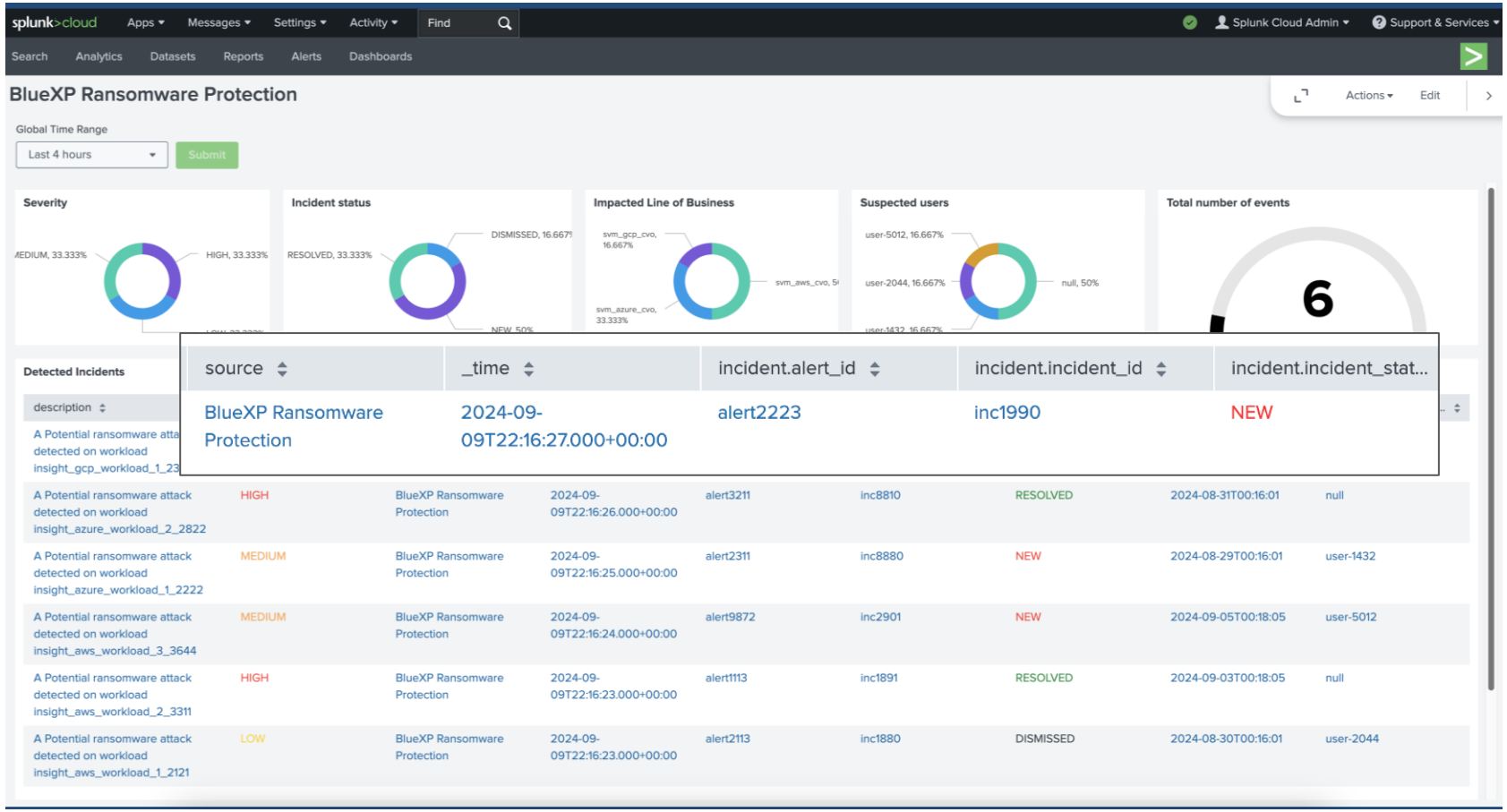
Streamlines threat detection and analysis across an organization's tools

- Sends logs from BlueXP to SIEM
- Shows incidents detected by SIEM (coming soon)
- Automated response and alerts on SIEM-detected incidents (coming soon)

splunk>cloud

AWS Security Hub

Microsoft Sentinel

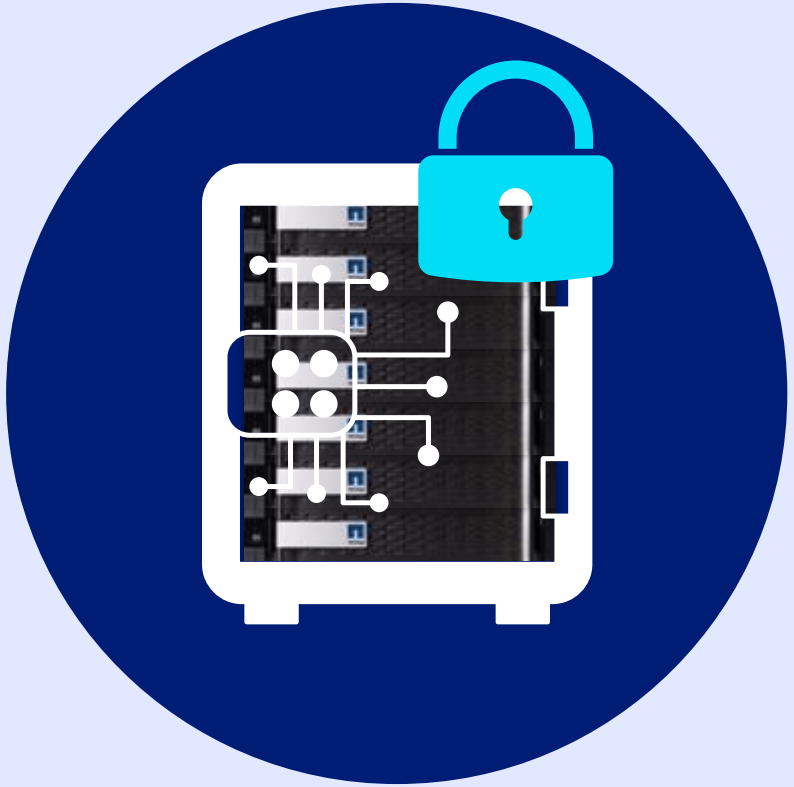


NetApp cyber vaulting

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**



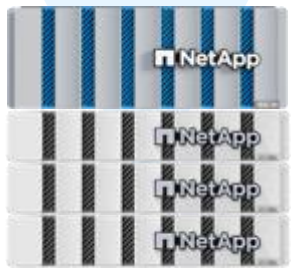
NETAPP CYBER VAULTING SOLUTION
LAST LINE OF DEFENSE

Cyber vaulting with NetApp ONTAP reference architecture benefits

Logical air gap: Isolated data plane without silos
A data pull operation copies from Primary to cyber vault

Cluster 1

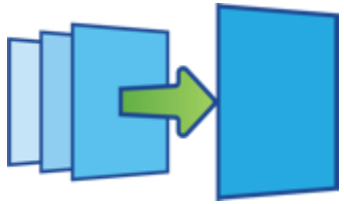
Source Volume



Primary

With SnapLock Compliance and protocols disabled:

- Attackers cannot reach the cyber vault from the primary storage
- No pierce through from the source possible
- Copies in vault cannot be read, modified or deleted by anyone (including NetApp)



On both primary and cyber vault

- Multi-Admin Verify
- Multi-Factor Authentication

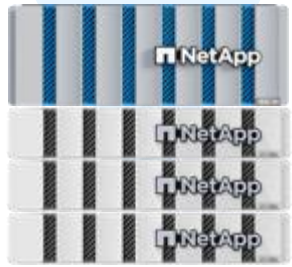
Between primary and secondary

- Isolate management networks
- Different credentials
- Separate administrators
- Dedicated replication network

Cluster 2

SnapMirror policy

Destination volume



Logical air-gap cyber vault

Ransomware Recovery Guarantee

NetApp can help. And now we guarantee it.

NetApp will warrant snapshot data recovery in the event of a ransomware attack

If you can't recover your data copies with help from NetApp assistance, NetApp will offer compensation*.

The NetApp Ransomware Recovery Guarantee

FOR ENTERPRISE PRIMARY STORAGE

*Guarantee includes both technology purchase and PS engagement. Terms and conditions apply.

Ransomware Recovery Guarantee

Program Details

SERVICE REQUIREMENTS

- Ransomware Professional Services engagement
- ActiveIQ remote monitoring (ASUP) enabled

GUARANTEE COVERAGE

- Based on tiered capacity deployed at the beginning of the term.
- Maximum payouts up to $5 million

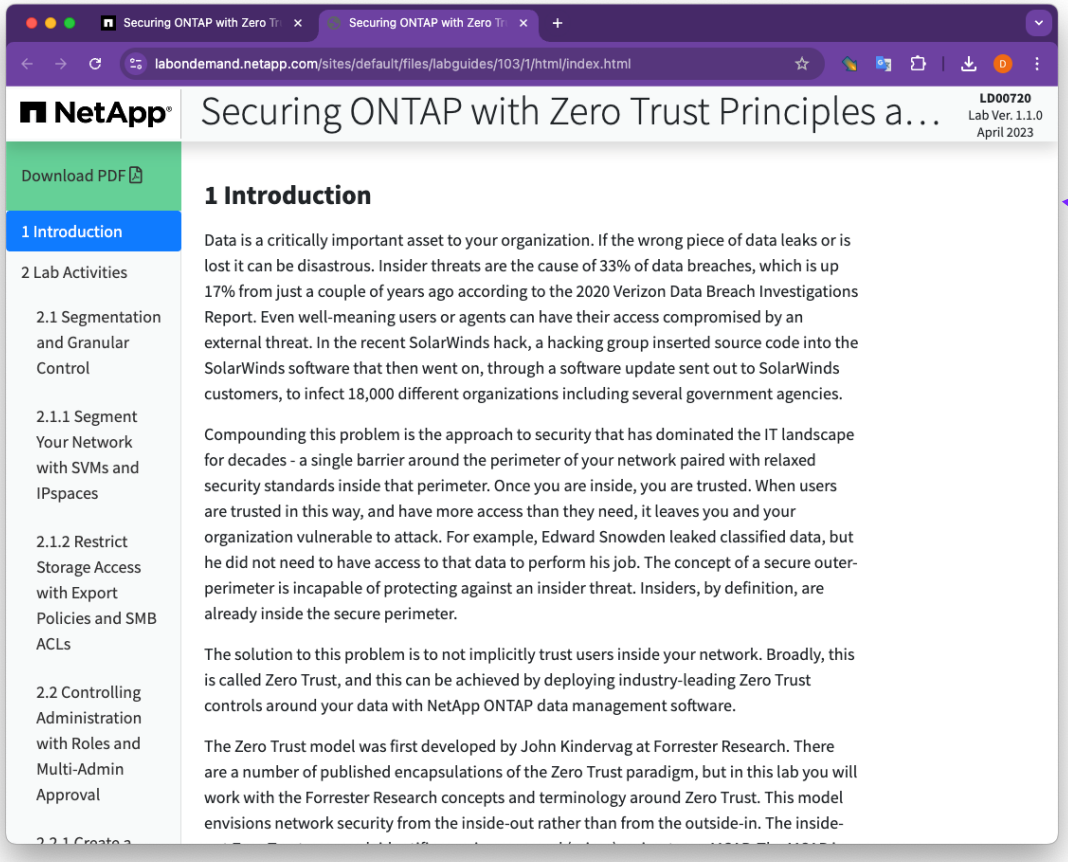
PROGRAM AVAILABILITY

- Storage purchased currently or within the past six months
- Guarantee period starts upon successful completion of services or up to 15 months after product ship date
- Multi-year terms & extensions are available

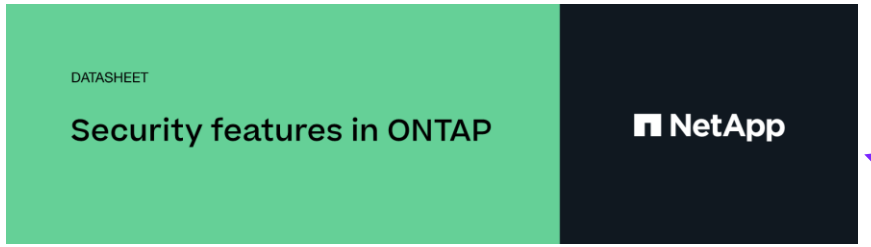
Where to go more information

Security hardening & Ontap features

https://labondemand.netapp.com/lab/securing-ontap-zero-trust

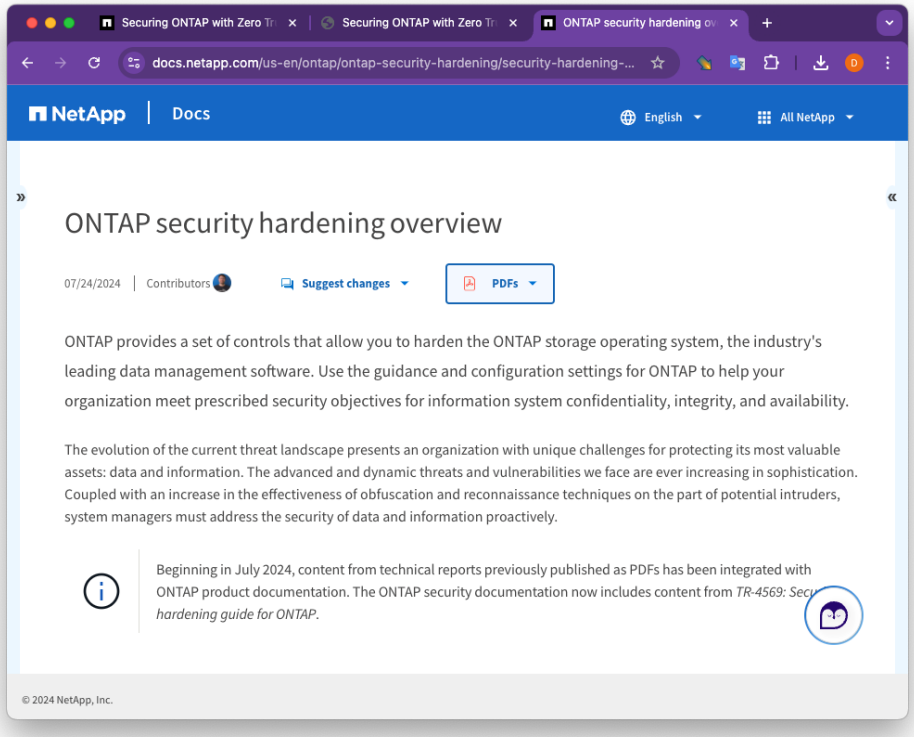


Hands-on labs for customers



Security features explained

https://www.netapp.com/pdf.html?item=/media/8128-ds-3846.pdf



Complete hardening guide for Ontap

https://docs.netapp.com/us-en/ontap/ontap-security-hardening/security-hardening-overview.html

ANY QUESTIONS ?

Learn more at:
https://www.netapp.com/cyber-resilience/ransomware-protection/

THANK YOU

NetApp

Learn more at:
https://www.netapp.com/cyber-resilience/ransomware-protection/