NetApp

connect

TECHNOLOGIE
FORUM

Sicher ist sicher: NetApp – The most secure storage on the planet

Filip Fickert

Account Technology Specialist

Klaus Wagner

Solution Architect

Felix Multhaup

Professional Services Consultant

Agenda

- Motivation
- NetApp Security Framework
- Protect
- Detect
- Recover
- Cloud Security

MOTIVATION

connect
TECHNOLOGIE FORUM

NetApp

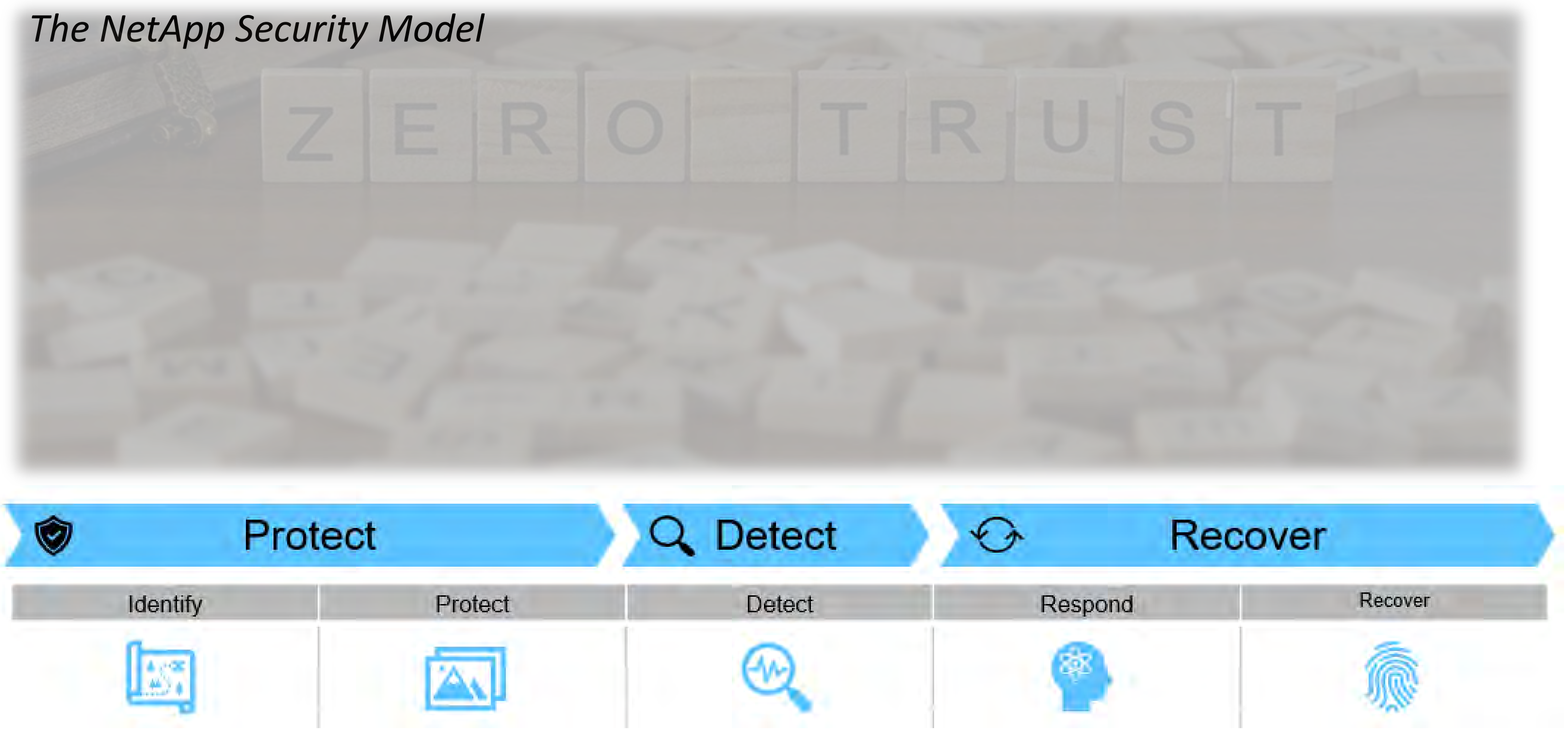
What keeps CISOs awake at night?

- Ransomware
- Zero Trust
- Hybrid threats
  -Espionage
  -Sabotage
- AI
- New Regulations
  -NIS 2
  -DORA
- Security Specialist Shortage

ISMS empfohlen: Frameworks für Information Security

Nicht warten, jetzt scannen

The NetApp Security Model



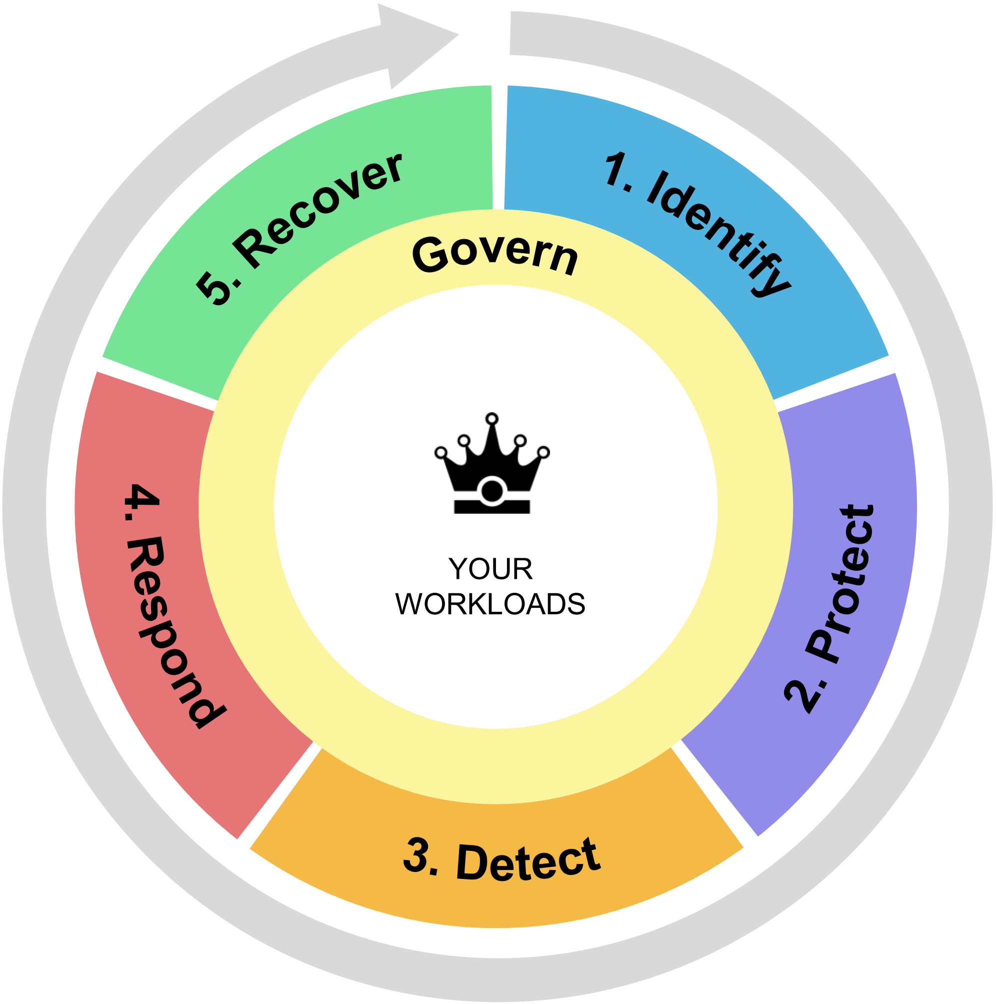
NEU!

NEU: NIST Releases Version 2.0 of Landmark Cybersecurity Framework | NIST

NIST vs IS027001 :   Whats the similarity, the difference, the co-exist?

NETAPP SECURITY FRAMEWORK

Covers the entire NIST cybersecurity framework in a few clicks and seconds



1. Automatically **discover** and prioritize data in NetApp storage **with a focus on top application-based workloads and sensitivity**

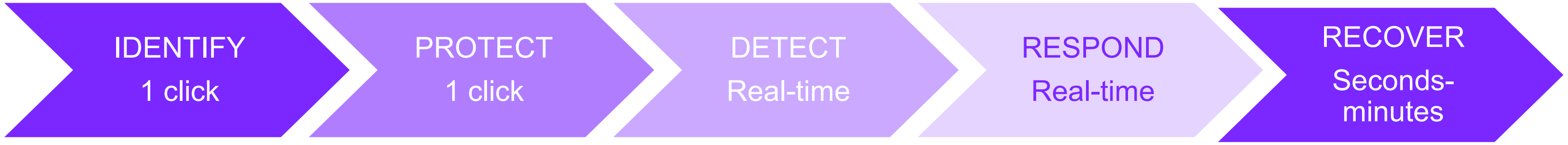
2. **One-click protection** of top workload data (backup, immutable/indelible snapshots, secure configuration, different security domain)

3. **Accurately detect** ransomware as **quickly** as possible using next-gen **AI-based** anomaly detection

4. Automated response to secure safe recovery point, attack alerting, and integration with top **SIEM solutions**

5. Rapidly restore data via simplified **orchestrated recovery** to accelerate application uptime

6. Implement your ransomware protection **strategy** and **policies**, and **monitor outcomes**



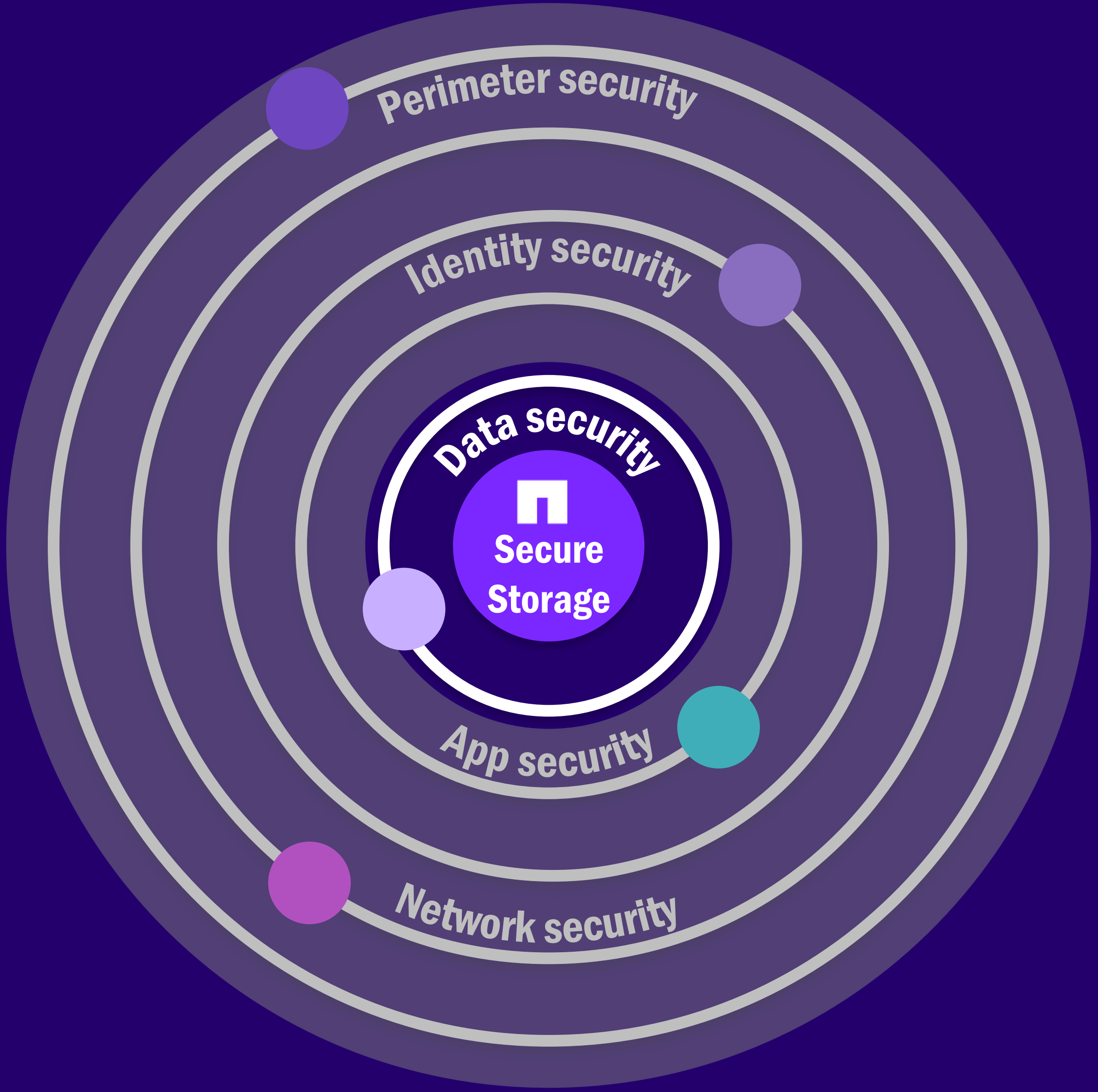
PROTECT

Zero Trust

Never Trust / Always verify

- The most secure by design / zero trust
- Detects and responds to attacks in real-time, to minimize business disruptions
- Provides the easiest and most-comprehensive recovery from disruptions

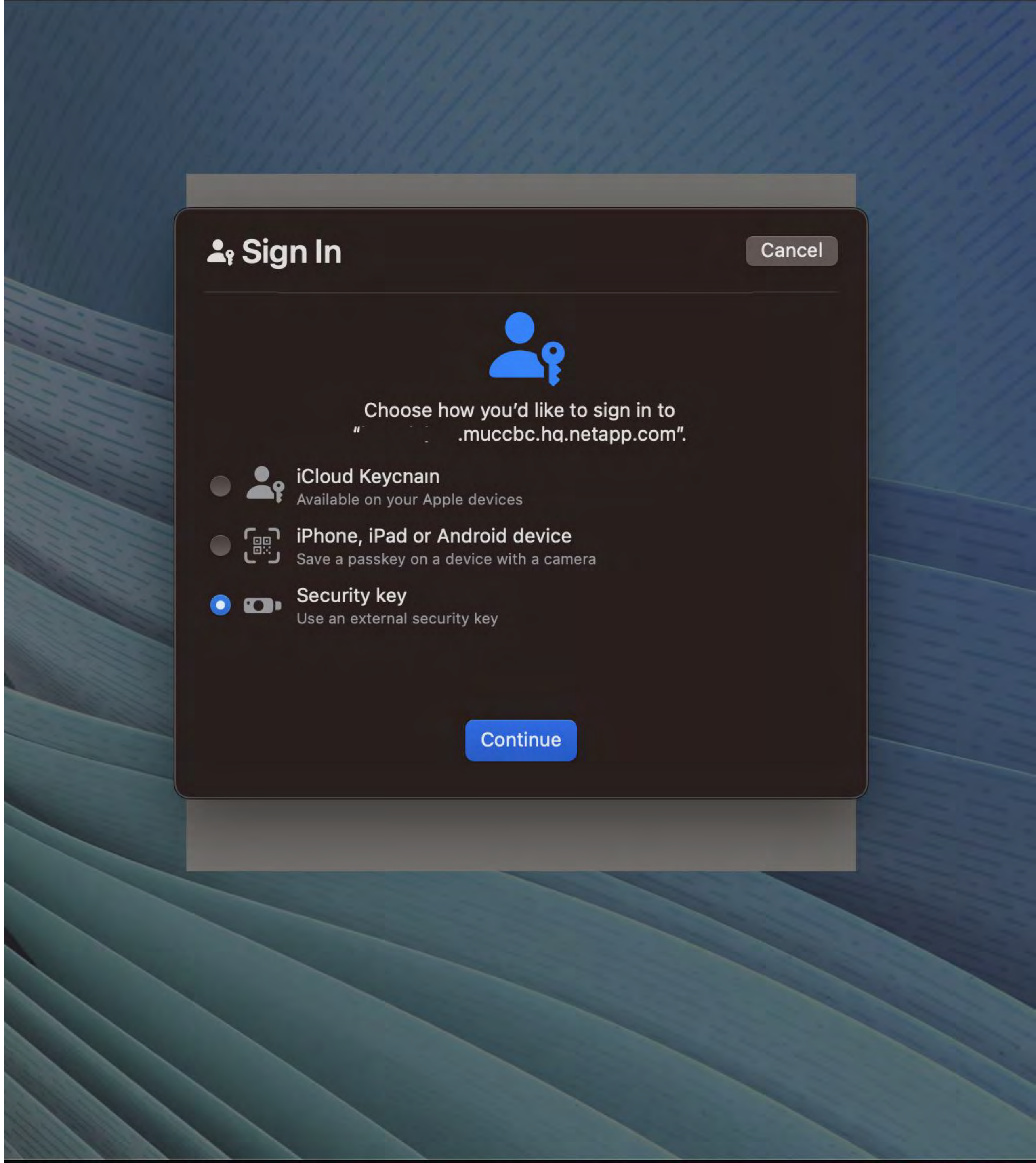
Defense in depth



System Manager: MFA

Phishing-resistant authentication

- Open standard: WebAuthn, Passkeys
- Enforced on first login
- Yubikey is supported
- Support for AD groups
- Requires valid SSL configuration
  - Names in certificates must match hostname
  - Chain of trust must be available on client
  - …
- Other FIDO2 compliant authenticators may work
  - Google Titan, iPhone (FaceID, TouchID), MacBook (TouchID), …



Sign In

Cancel

Choose how you'd like to sign in to
“[redacted].muccbc.hq.netapp.com”.

○ iCloud Keychain
Available on your Apple devices

○ iPhone, iPad or Android device
Save a passkey on a device with a camera

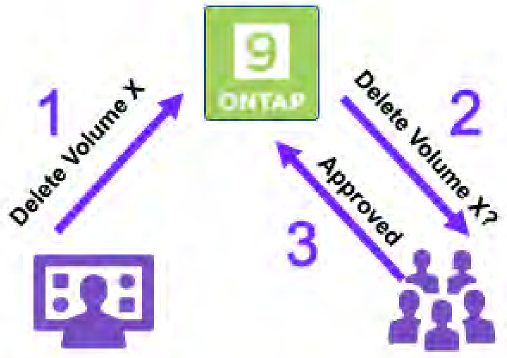
● Security key
Use an external security key

Continue

Multi-Admin Verification (MAV)

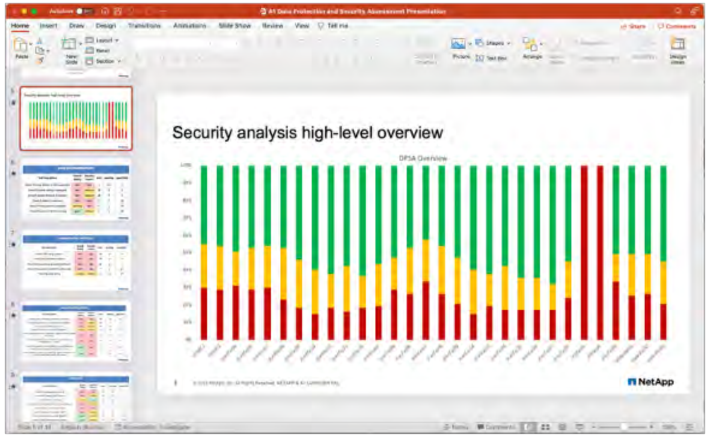
Enhanced dual-admin control

- Defend against a single compromised administrator account or a rogue administrator by requiring multiple approvals for commands that could result in data loss
- Approval groups where one or more additional approvals are required for a command to be executed
- With every ONTAP Release additional commands covered (e.g. Disabling vscan or ARP in 9.16)

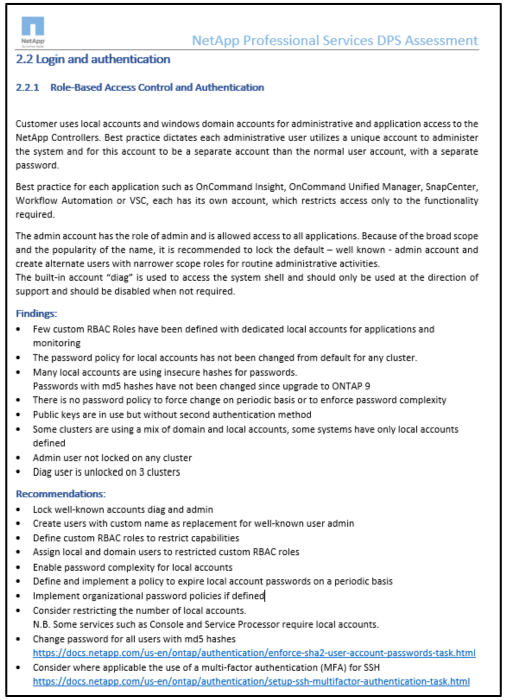


Data Protection & Security Assessment Service

NetApp DPSA Enhancement



Security analysis high-level overview



NetApp Professional Services DPS Assessment

2.2 Login and authentication

2.2.1 Role-Based Access Control and Authentication

Customer uses local accounts and windows domain accounts for administrative and application access to the NetApp Controllers. Best practice dictates each administrative user utilizes a unique account to administer the system and for this account to be a separate account than the normal user account, with a separate password.

Best practice for each application such as OnCommand Insight, OnCommand Unified Manager, SnapCenter, Workflow Automation or VSC, each has its own account, which restricts access only to the functionality required.

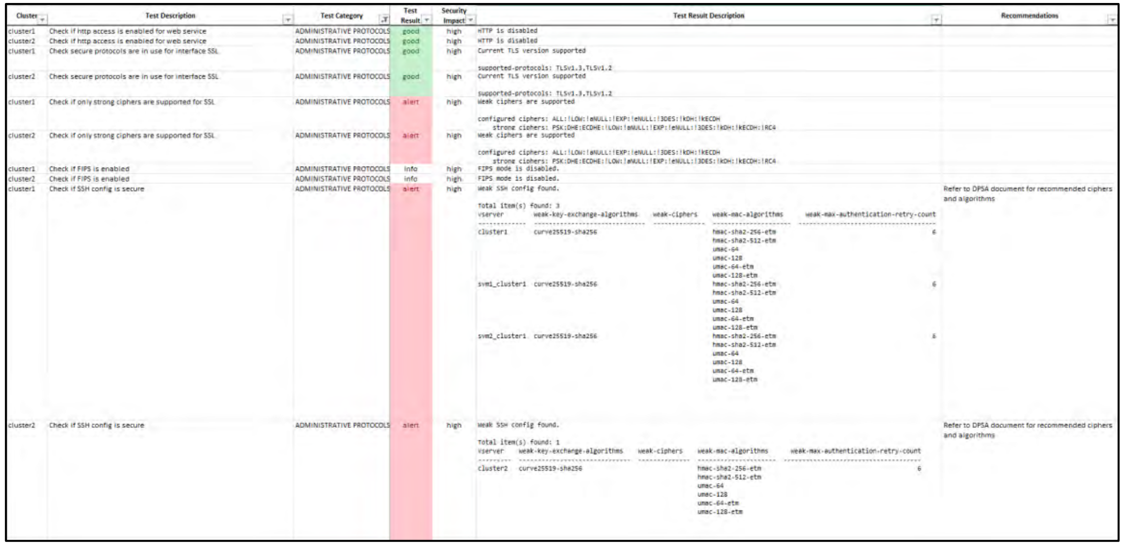
The admin account has the role of admin and is allowed access to all applications. Because of the broad scope and the popularity of the name, it is recommended to lock the default – well known - admin account and create alternate users with narrower scope roles for routine administrative activities.
The built-in account "diag" is used to access the system shell and should only be used at the direction of support and should be disabled when not required.

Findings:

- Few custom RBAC Roles have been defined with dedicated local accounts for applications and monitoring
- The password policy for local accounts has not been changed from default for any cluster.
- Many local accounts are using insecure hashes for passwords.
  Passwords with md5 hashes have not been changed since upgrade to ONTAP 9
- There is no password policy to force change on periodic basis or to enforce password complexity
- Public keys are in use but without second authentication method
- Some clusters are using a mix of domain and local accounts, some systems have only local accounts defined
- Admin user not locked on any cluster
- Diag user is unlocked on 3 clusters

Recommendations:

- Lock well-known accounts diag and admin
- Create users with custom name as replacement for well-known user admin
- Define custom RBAC roles to restrict capabilities
- Assign local and domain users to restricted custom RBAC roles
- Enable password complexity for local accounts
- Define and implement a policy to expire local account passwords on a periodic basis
- Implement organizational password policies if defined
- Consider restricting the number of local accounts.
  N.B. Some services such as Console and Service Processor require local accounts.
- Change password for all users with md5 hashes
  https://docs.netapp.com/us-en/ontap/authentication/enforce-sha2-user-account-passwords-task.html
- Consider where applicable the use of a multi-factor authentication (MFA) for SSH
  https://docs.netapp.com/us-en/ontap/authentication/setup-ssh-multifactor-authentication-task.html



Cluster	Test Description	Test Category	Test Result	Security Impact	Test Result Description	Recommendations
cluster1	Check if http access is enabled for web service	ADMINISTRATIVE PROTOCOLS	good	high	HTTP is disabled	
cluster2	Check if http access is enabled for web service	ADMINISTRATIVE PROTOCOLS	good	high	HTTP is disabled	
cluster1	Check secure protocols are in use for interface SSL	ADMINISTRATIVE PROTOCOLS	good	high	Current TLS version supported supported-protocols: TLSv1.3,TLSv1.2	
cluster2	Check secure protocols are in use for interface SSL	ADMINISTRATIVE PROTOCOLS	good	high	Current TLS version supported supported-protocols: TLSv1.3,TLSv1.2	
cluster1	Check if only strong ciphers are supported for SSL	ADMINISTRATIVE PROTOCOLS	alert	high	Weak ciphers are supported configured ciphers: ALL:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH strong ciphers: PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH:!RC4	
cluster2	Check if only strong ciphers are supported for SSL	ADMINISTRATIVE PROTOCOLS	alert	high	Weak ciphers are supported configured ciphers: ALL:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH strong ciphers: PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH:!RC4	
cluster1	Check if FIPS is enabled	ADMINISTRATIVE PROTOCOLS	info	high	FIPS mode is disabled.	
cluster2	Check if FIPS is enabled	ADMINISTRATIVE PROTOCOLS	info	high	FIPS mode is disabled.	
cluster1	Check if SSH config is secure	ADMINISTRATIVE PROTOCOLS	alert	high	Weak SSH config found. Total item(s) found: 3 vserver weak-key-exchange-algorithms weak-ciphers weak-mac-algorithms weak-max-authentication-retry-count ------------- ---------------------------- ------------- -------------------- ---------------------------------- cluster1 curve25519-sha256 hmac-sha2-256-etm 6 hmac-sha2-512-etm umac-64 umac-128 umac-64-etm umac-128-etm svm1_cluster1 curve25519-sha256 hmac-sha2-256-etm 6 hmac-sha2-512-etm umac-64 umac-128 umac-64-etm umac-128-etm svm2_cluster1 curve25519-sha256 hmac-sha2-256-etm 6 hmac-sha2-512-etm umac-64 umac-128 umac-64-etm umac-128-etm	Refer to DPSA document for recommended ciphers and algorithms
cluster2	Check if SSH config is secure	ADMINISTRATIVE PROTOCOLS	alert	high	Weak SSH config found. Total item(s) found: 1 vserver weak-key-exchange-algorithms weak-ciphers weak-mac-algorithms weak-max-authentication-retry-count --------- ---------------------------- ------------- -------------------- ---------------------------------- cluster2 curve25519-sha256 hmac-sha2-256-etm 6 hmac-sha2-512-etm umac-64 umac-128 umac-64-etm umac-128-etm	Refer to DPSA document for recommended ciphers and algorithms

Summary

- Zusammenfassung
- ScoreCard Präsentation

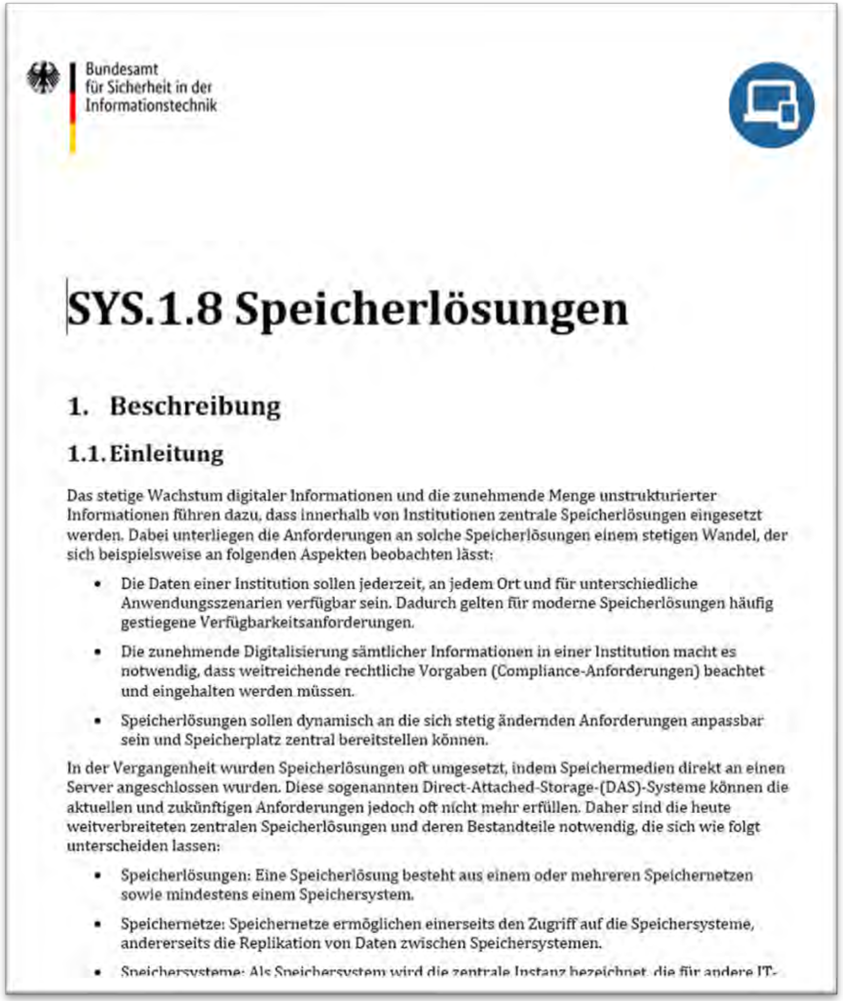
Handout

- Beschreibung der Analyse
- Erläuterung der Handlungsempfehlungen

Report

- Technische Details zu allen durchgeführten Tests
- Aufzeigen einzelner Handlungsempfehlungen

DPSA meets BSI Grundschutz



Bundesamt
für Sicherheit in der
Informationstechnik

SYS.1.8 Speicherlösungen

1. Beschreibung

1.1. Einleitung

Das stetige Wachstum digitaler Informationen und die zunehmende Menge unstrukturierter Informationen führen dazu, dass innerhalb von Institutionen zentrale Speicherlösungen eingesetzt werden. Dabei unterliegen die Anforderungen an solche Speicherlösungen einem stetigen Wandel, der sich beispielsweise an folgenden Aspekten beobachten lässt:

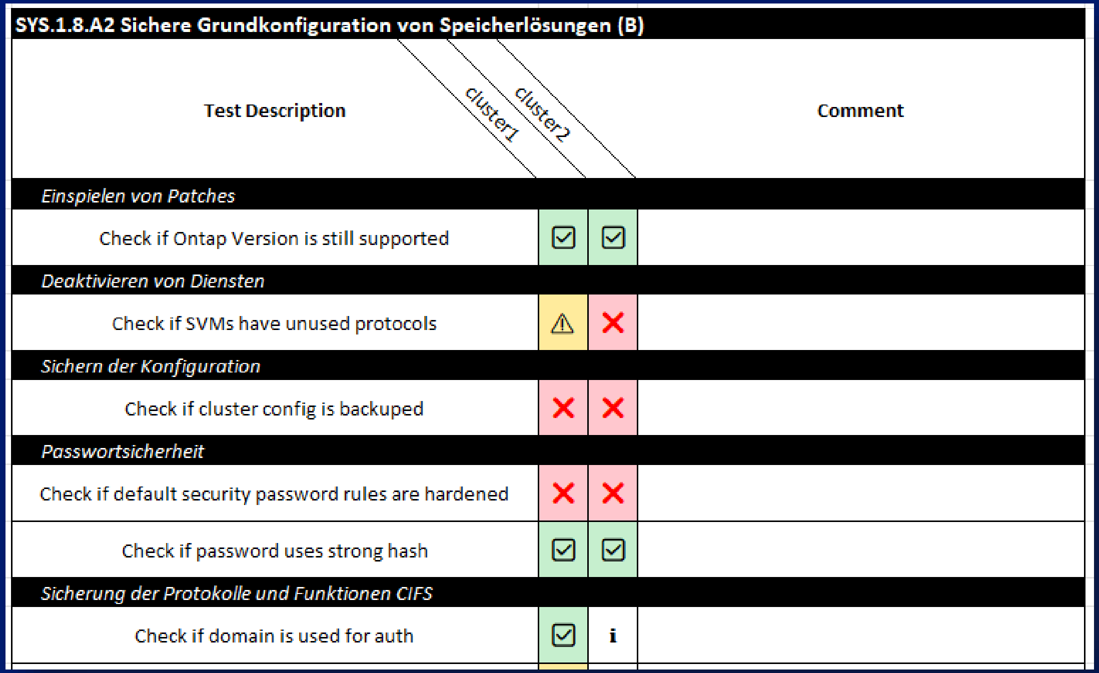
- Die Daten einer Institution sollen jederzeit, an jedem Ort und für unterschiedliche Anwendungsszenarien verfügbar sein. Dadurch gelten für moderne Speicherlösungen häufig gestiegene Verfügbarkeitsanforderungen.
- Die zunehmende Digitalisierung sämtlicher Informationen in einer Institution macht es notwendig, dass weitreichende rechtliche Vorgaben (Compliance-Anforderungen) beachtet und eingehalten werden müssen.
- Speicherlösungen sollen dynamisch an die sich stetig ändernden Anforderungen anpassbar sein und Speicherplatz zentral bereitstellen können.

In der Vergangenheit wurden Speicherlösungen oft umgesetzt, indem Speichermedien direkt an einen Server angeschlossen wurden. Diese sogenannten Direct-Attached-Storage-(DAS)-Systeme können die aktuellen und zukünftigen Anforderungen jedoch oft nicht mehr erfüllen. Daher sind die heute weitverbreiteten zentralen Speicherlösungen und deren Bestandteile notwendig, die sich wie folgt unterscheiden lassen:

- Speicherlösungen: Eine Speicherlösung besteht aus einem oder mehreren Speichernetzen sowie mindestens einem Speichersystem.
- Speichernetze: Speichernetze ermöglichen einerseits den Zugriff auf die Speichersysteme, andererseits die Replikation von Daten zwischen Speichersystemen.
- Speichersysteme: Als Speichersystem wird die zentrale Instanz bezeichnet, die für andere IT-

NetApp

ONTAP 9
Exemplarisches Sicherheitskonzept für BSI-Grundschutzanforderungen



SYS.1.8.A2 Sichere Grundkonfiguration von Speicherlösungen (B)

Test Description	cluster1	cluster2	Comment
Einspielen von Patches			
Check if Ontap Version is still supported	☑	☑	
Deaktivieren von Diensten			
Check if SVMs have unused protocols	⚠	✗	
Sichern der Konfiguration			
Check if cluster config is backuped	✗	✗	
Passwortsicherheit			
Check if default security password rules are hardened	✗	✗	
Check if password uses strong hash	☑	☑	
Sicherung der Protokolle und Funktionen CIFS			
Check if domain is used for auth	☑	i	

DPSA meets NIS2

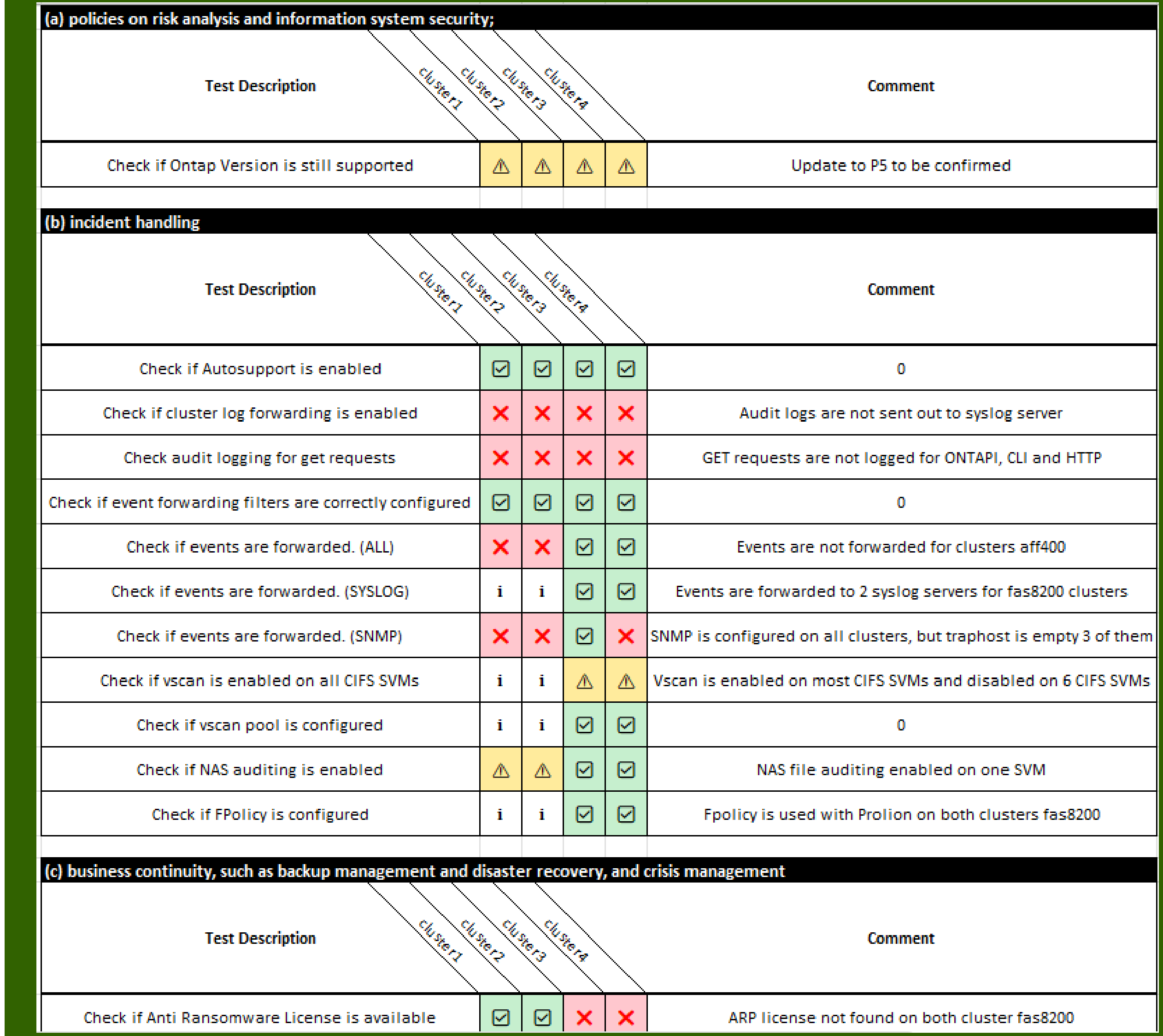
Policies on risk analysis and information system security

Incident handling

Business continuity: such as backup management, disaster recovery and crisis management

Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure

Policies and procedures to assess the effectiveness of cybersecurity **risk-management measures**



(a) policies on risk analysis and information system security;

Test Description	cluster1	cluster2	cluster3	cluster4	Comment
Check if Ontap Version is still supported	⚠	⚠	⚠	⚠	Update to P5 to be confirmed

(b) incident handling

Test Description	cluster1	cluster2	cluster3	cluster4	Comment
Check if Autosupport is enabled	☑	☑	☑	☑	0
Check if cluster log forwarding is enabled	✗	✗	✗	✗	Audit logs are not sent out to syslog server
Check audit logging for get requests	✗	✗	✗	✗	GET requests are not logged for ONTAPI, CLI and HTTP
Check if event forwarding filters are correctly configured	☑	☑	☑	☑	0
Check if events are forwarded. (ALL)	✗	✗	☑	☑	Events are not forwarded for clusters aff400
Check if events are forwarded. (SYSLOG)	i	i	☑	☑	Events are forwarded to 2 syslog servers for fas8200 clusters
Check if events are forwarded. (SNMP)	✗	✗	☑	✗	SNMP is configured on all clusters, but traphost is empty 3 of them
Check if vscan is enabled on all CIFS SVMs	i	i	⚠	⚠	Vscan is enabled on most CIFS SVMs and disabled on 6 CIFS SVMs
Check if vscan pool is configured	i	i	☑	☑	0
Check if NAS auditing is enabled	⚠	⚠	☑	☑	NAS file auditing enabled on one SVM
Check if FPolicy is configured	i	i	☑	☑	Fpolicy is used with Prolion on both clusters fas8200

(c) business continuity, such as backup management and disaster recovery, and crisis management

Test Description	cluster1	cluster2	cluster3	cluster4	Comment
Check if Anti Ransomware License is available	☑	☑	✗	✗	ARP license not found on both cluster fas8200

DPSA meets DORA

Technical requirements: DORA key articles

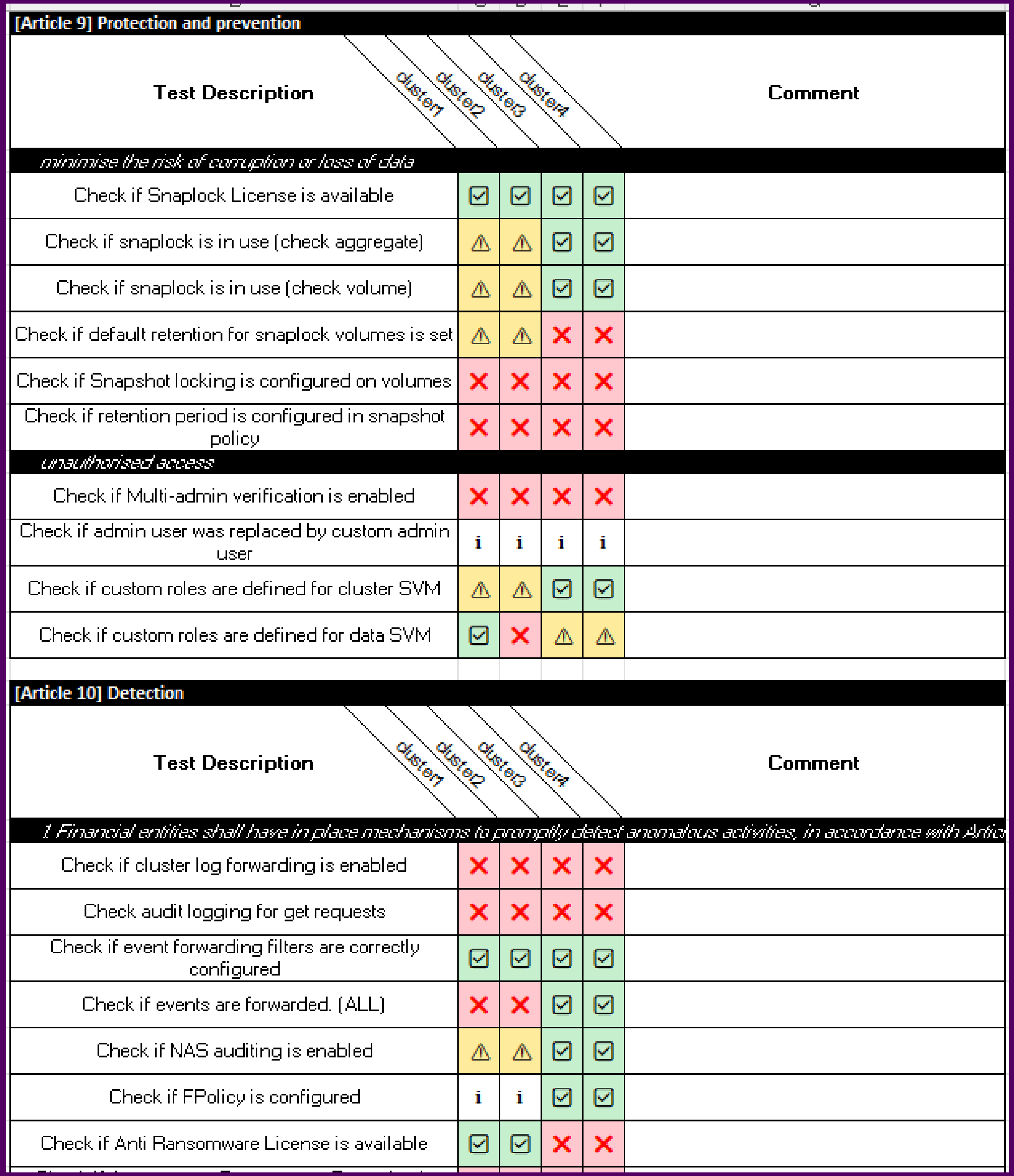
Article 25
General principles (cloud)

Article 8
Protection and prevention

Article 9
Detection

Article 10
Response and recovery

Article 11
Backup policies, recovery methods



[Article 9] Protection and prevention

Test Description	cluster1	cluster2	cluster3	cluster4	Comment
minimise the risk of corruption or loss of data					
Check if Snaplock License is available	☑	☑	☑	☑	
Check if snaplock is in use (check aggregate)	⚠	⚠	☑	☑	
Check if snaplock is in use (check volume)	⚠	⚠	☑	☑	
Check if default retention for snaplock volumes is set	⚠	⚠	✗	✗	
Check if Snapshot locking is configured on volumes	✗	✗	✗	✗	
Check if retention period is configured in snapshot policy	✗	✗	✗	✗	
unauthorised access					
Check if Multi-admin verification is enabled	✗	✗	✗	✗	
Check if admin user was replaced by custom admin user	i	i	i	i	
Check if custom roles are defined for cluster SVM	⚠	⚠	☑	☑	
Check if custom roles are defined for data SVM	☑	✗	⚠	⚠	

[Article 10] Detection

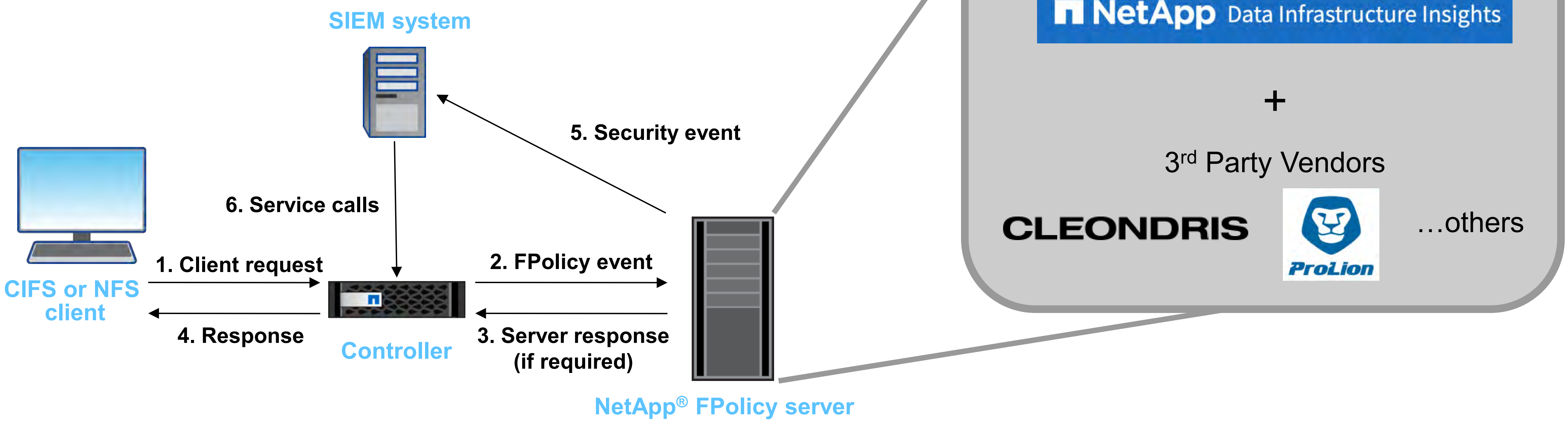
Test Description	cluster1	cluster2	cluster3	cluster4	Comment
1 Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Artic					
Check if cluster log forwarding is enabled	✗	✗	✗	✗	
Check audit logging for get requests	✗	✗	✗	✗	
Check if event forwarding filters are correctly configured	☑	☑	☑	☑	
Check if events are forwarded. (ALL)	✗	✗	☑	☑	
Check if NAS auditing is enabled	⚠	⚠	☑	☑	
Check if FPolicy is configured	i	i	☑	☑	
Check if Anti Ransomware License is available	☑	☑	✗	✗	

DETECT

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

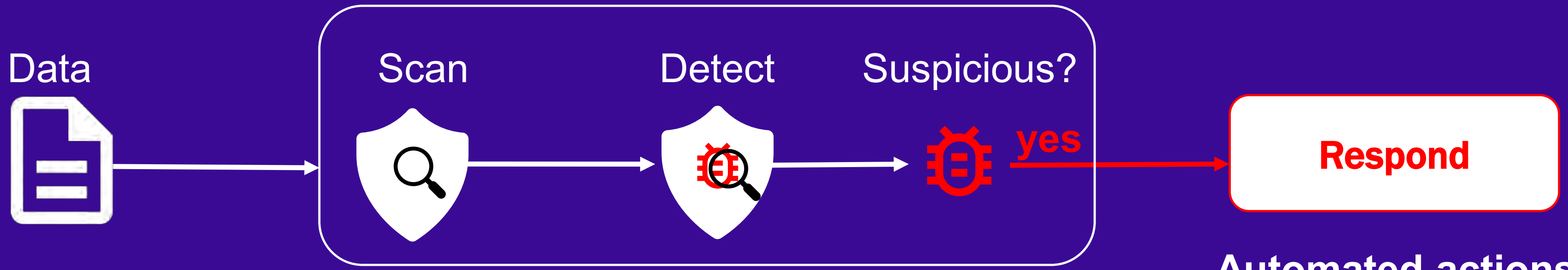


Available in 9.16.1

Detect

On-device anomaly detection (ARP/AI)

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



Scan for signals

- Encrypted file content
- Encrypted file headers
- File metadata signatures

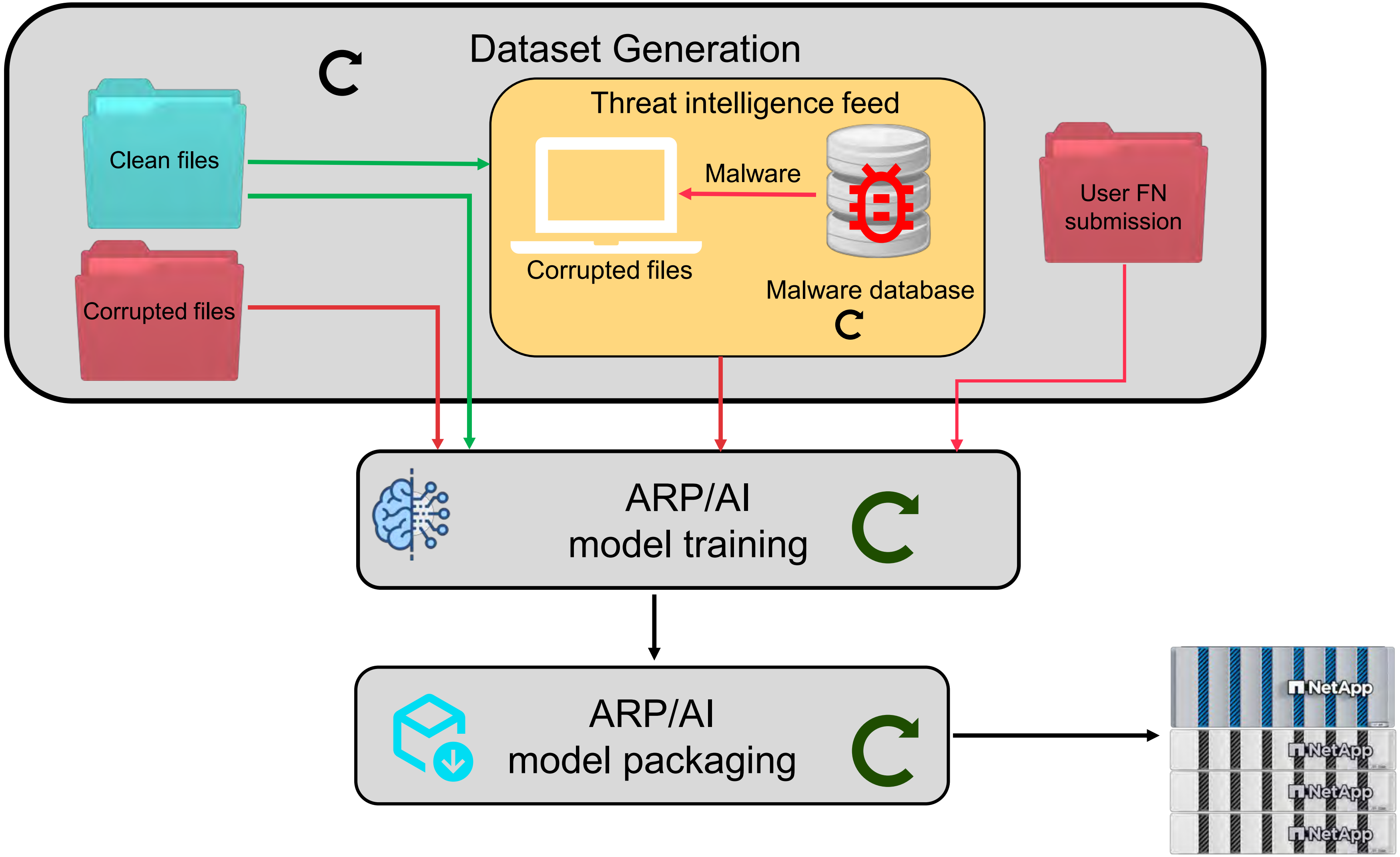
Automated actions

- Take snapshot
- Create evidence
- Generate Alerts
- Notify SIEM

Customer actions

- Investigate
- Block user
- Take system offline?

ARP/AI model training and deployment process



Protection against the latest types of ransomware

- Refreshes model parameters
- Refreshes file signatures
- **No full NetApp® ONTAP® upgrade needed**

Ransomware Protection Advantage with NetApp

How is the detection program different from the recovery guarantee?

Ransomware Detection Program is an opt in program for ARP/AI detection built-in to ONTAP with recovery assistance from PS if ARP/AI misses an attack.

Ransomware Recovery Guarantee is centered around NetApp's Snapshot technology. If you can't recover your data snapshot copies with help from NetApp assistance, NetApp will offer compensation.

The NetApp Ransomware Advantage

FOR ENTERPRISE
PRIMARY STORAGE

Ransomware Detection program

Confidence in ARP/AI backed by Professional Services

We have you covered: In the event that NetApp doesn’t detect certain attacks with ARP/AI, the **Ransomware Detection** program assists with recovery via NetApp Professional Services at no initial cost to the customer.

NetApp is the **first and only** storage vendor to offer ransomware detection with confidence in detecting attacks.

SE Labs
AAA
June 2024
Data Corruption Detection (Ransomware)

Ransomware attacks continue to pose one of the most significant threats to organizations worldwide in every industry.

Disclaimer: Terms and conditions apply. No ransomware detection or prevention system can completely guarantee safety from a ransomware attack. Although it’s possible that an attack might go undetected, NetApp technology acts as an important additional layer of defense.

ARP/AI SAN (Announcement)

Arrival expected this CY

AI-Powered Autonomous Ransomware Protection – for Block

- Next generation ransomware threat detection

- Industry-leading AI-powered ransomware detection for enterprise file storage… now will be extended to block storage
- Automatically update model parameters regularly without a required ONTAP update or system reboot
- Non-disruptive upgrade from current version of ONTAP to future version with ARP/AI for Block, at no additional charge via ONTAP One.

NetApp plans to release ARP/AI for Block later in CY25; Plans are subject to change.

Disclaimer: No ransomware detection or prevention system can completely guarantee safety from a ransomware attack. Although it's possible that an attack might go undetected, NetApp technology acts as an important additional layer of defense.

RECOVER

connect
TECHNOLOGIE FORUM

NetApp

Prevent Snapshot deletion by compromised admins

Tamper-proof Snapshot locking on any volume or multi-admin verify

NetApp® SnapLock®

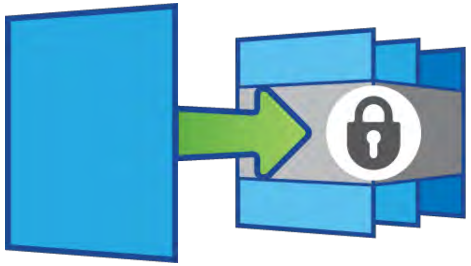
- Licensed feature of NetApp ONTAP® ONE
- Use SnapVault and SnapLock to create immutable AND indelible backups
- SnapVault backups to SnapLock Compliance volumes are virtually “air gapped”

Ransomware recovery use case

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

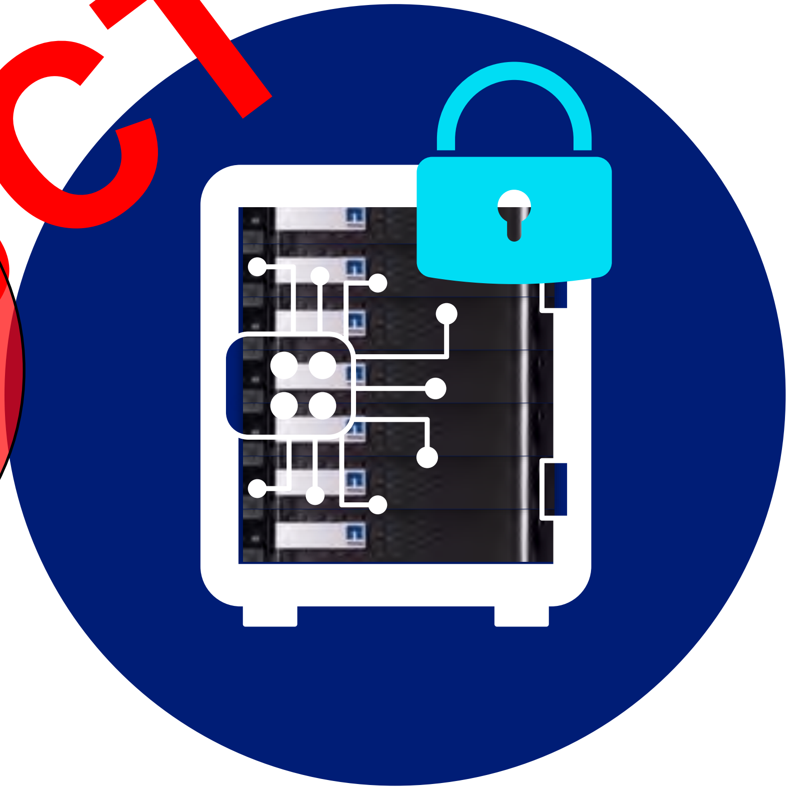
Tamper-proof Snapshot locking on primary storage

- **Since 9.12.1**
- Works on any volume (not SL volumes only)
- Manual Snapshot locking or automatic via schedule



NETAPP CYBER VAULT

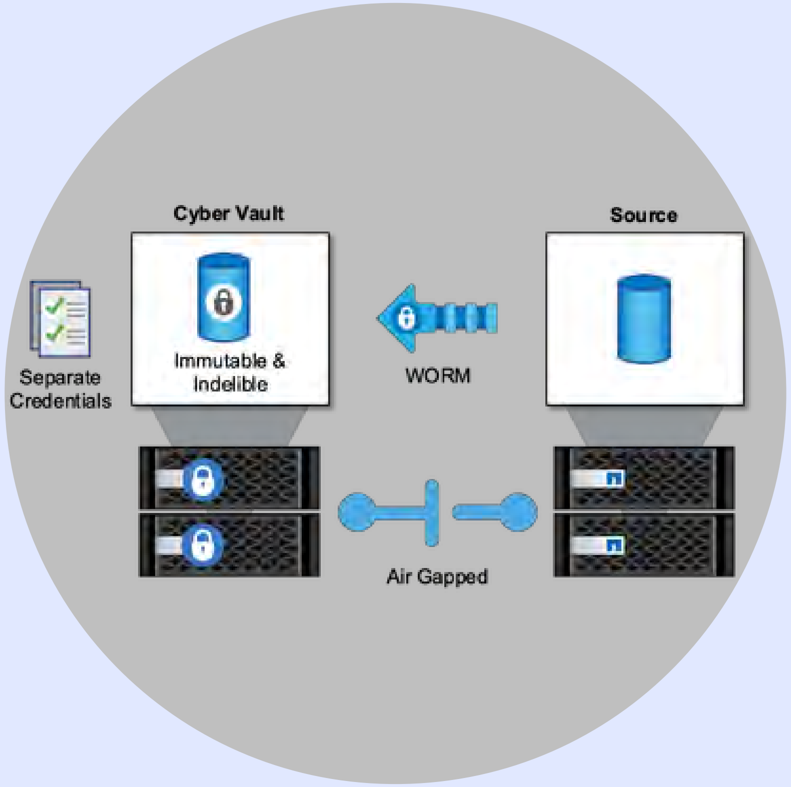
Multi-layered Ransomware Protectio
Reference Architecture



NetApp cyber vaulting

Multi-layered Ransomware Protection

- **Secure, isolated storage infrastructure (e.g., air gapped storage systems)**
- **Copies of the data must be both immutable and indelible without exception**
- **Strict access controls and multi-factor authentication**
- **Rapid data restoration capabilities**

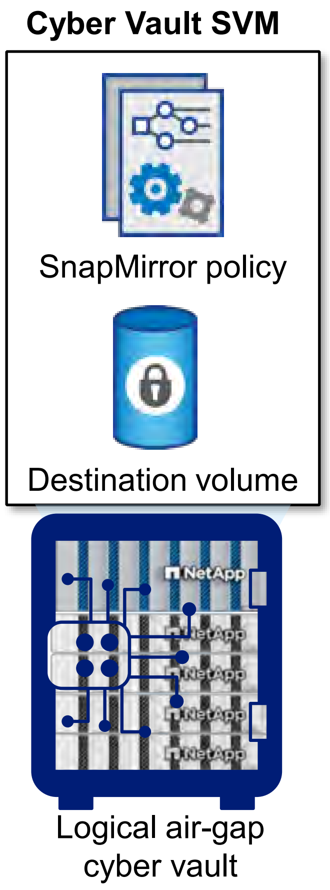


**NETAPP CYBER VAULTING SOLUTION
LAST LINE OF DEFENSE**

Cyber vaulting with NetApp ONTAP reference architecture benefits

Logical air gap

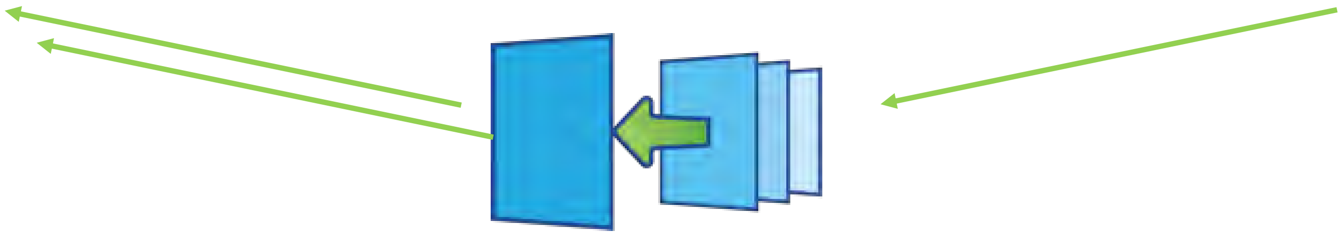
Isolated data plane without silos



A data pull operation copies from Primary to cyber vault

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)

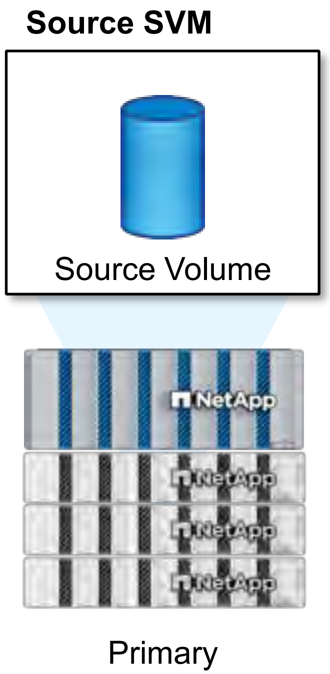


On both primary and cyber vault

- Multi-Admin Verify
- Multi-Factor Authentication

Between primary and secondary

- Isolate management networks
- Different credentials
- Separate administrators
- Dedicated replication network
- Separate data centers (optional)



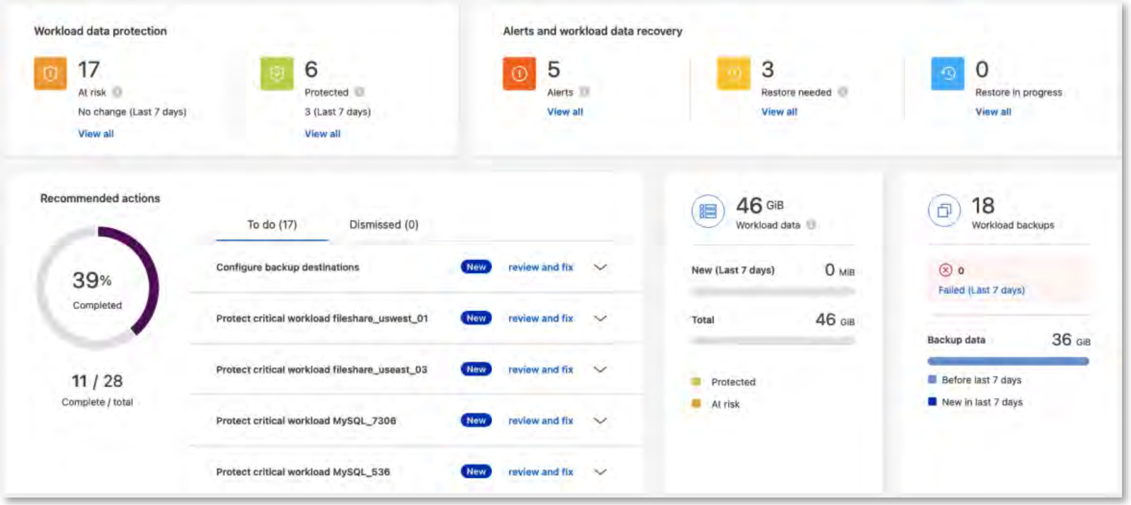
CLOUD SECURITY

connect
TECHNOLOGIE FORUM

NetApp

BlueXP ransomware protection

Intelligently orchestrate a comprehensive, workload-centric ransomware defense at the storage layer



Workload data protection

17 At risk
No change (Last 7 days)
View all

6 Protected
3 (Last 7 days)
View all

Alerts and workload data recovery

5 Alerts
View all

3 Restore needed
View all

0 Restore in progress
View all

Recommended actions

39% Completed

11 / 28 Complete / total

To do (17) | Dismissed (0)

Configure backup destinations	New	review and fix
Protect critical workload fileshare_uswest_01	New	review and fix
Protect critical workload fileshare_useast_03	New	review and fix
Protect critical workload MySQL_7306	New	review and fix
Protect critical workload MySQL_536	New	review and fix

46 GiB Workload data

New (Last 7 days) 0 MiB

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

NetApp is enabling the **entire NIST framework** for customers from
an **unified control plane (BlueXP)**

Automatically IDENTIFIES workloads & analyzes risks

Recommends & applies PROTECTION policies

Uses ML to DETECT potential attacks in near real-time

Automatically RESPONDS when attack suspected

Validates backup integrity and rapidly RECOVERS workload

NIST Framework

Protect | Detect | Recover

Identify

DPSA

Data Infrastructure Insights
(aka Cloud Insight)

Active IQ

SAM Report

BlueXP classification
(aka data sense)

Security.netapp.com
(product weakness)

Protect

RBAC

Fpolicy (nativ + Server)

Vscan (Antivirus Partner)

Tamperproof Snapshots

MAV

SnapLock

MFA

SnapMirror (Cloud)

BlueXP backup and recovery
(+Data Lock)

At Rest Encryption
In Transit Encryption

Multitenancy

Detect

Storage workload security
(Part of Data Infrastructure Insights)

AuditLog/Events/Syslog

NAS file auditing

ARP/AI

BlueXP ransomware protection

NABox (Harvest/Grafana)

Fpolicy (Cleondris, ProLion…

BlueXP backup and recovery
(Data Lock Scan)

Respond

Block user / IP

Create Snapshot

Fpolicy (Cleondris, ProLion…)

Storage workload security

ARP/AI

Recover

FlexClone

SnapRestore

SnapCenter

Backup applications

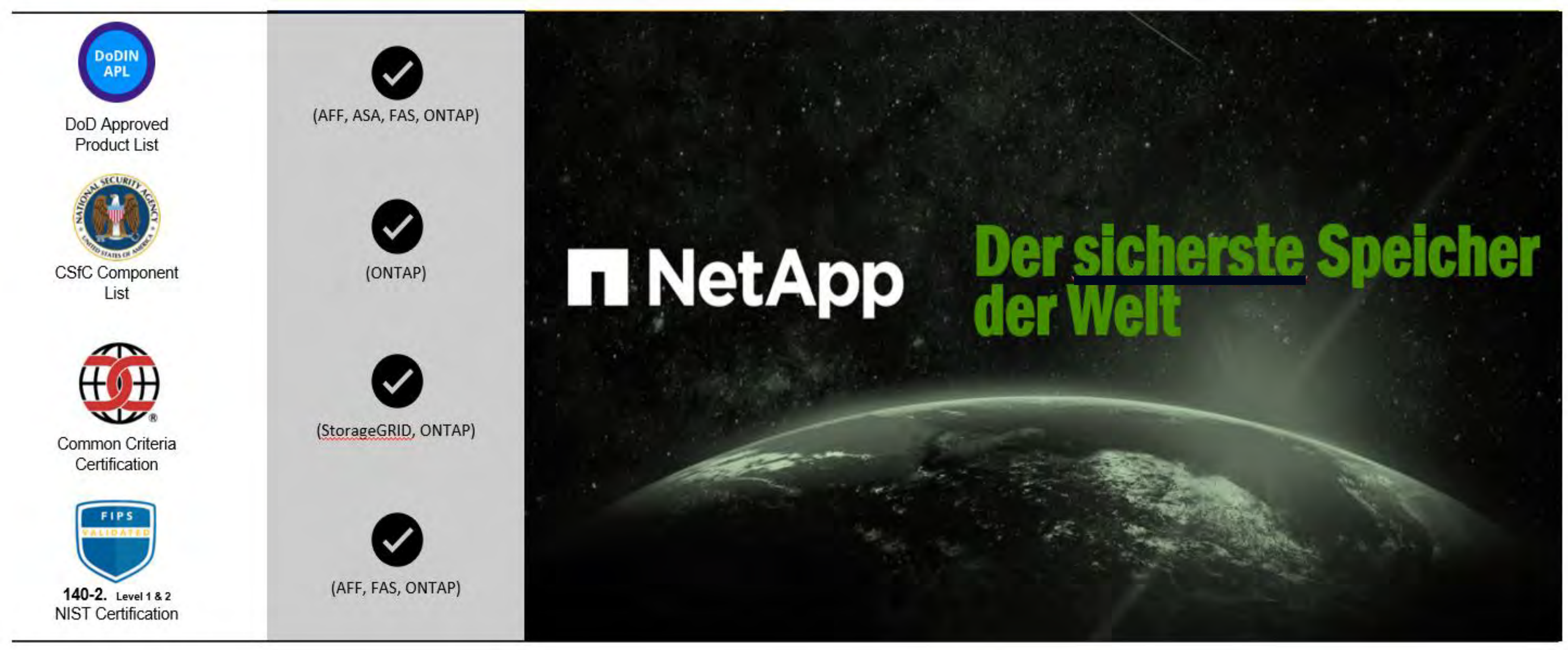
BlueXP Backup and Recovery

SIEM Integration

EURE FRAGEN, UNSERE ANTWORTEN

Handlung ist angesagt, gerne unterstützen wir seitens NetApp

KEY TAKEAWAYS



DoDIN APL DoD Approved Product List	✓ (AFF, ASA, FAS, ONTAP)
CSfC Component List	✓ (ONTAP)
Common Criteria Certification	✓ (StorageGRID, ONTAP)
FIPS VALIDATED 140-2. Level 1 & 2 NIST Certification	✓ (AFF, FAS, ONTAP)

NetApp
Der sicherste Speicher der Welt

Details, Infos & Updates unter: https://www.netapp.com/esg/trust-center/compliance

STAY CONNECTED

- 04.03.: KOMPAKT **Webcast**:
  „Frühlingsfrische Speicherlösungen “
- 20.03.: **Live-Lab Session** „Automatisierung“
- 25.03.: KOMPAKT **on-site** in Wallisellen
- 01.04.: KOMPAKT **Webcast**:
  BlueXP und die aktuellen Neuerungen
  (offizieller Name: tbd.)

KOMPAKT
Webcast

KOMPAKT
on-site

subscribe

Werde Teil der Community auf Discord

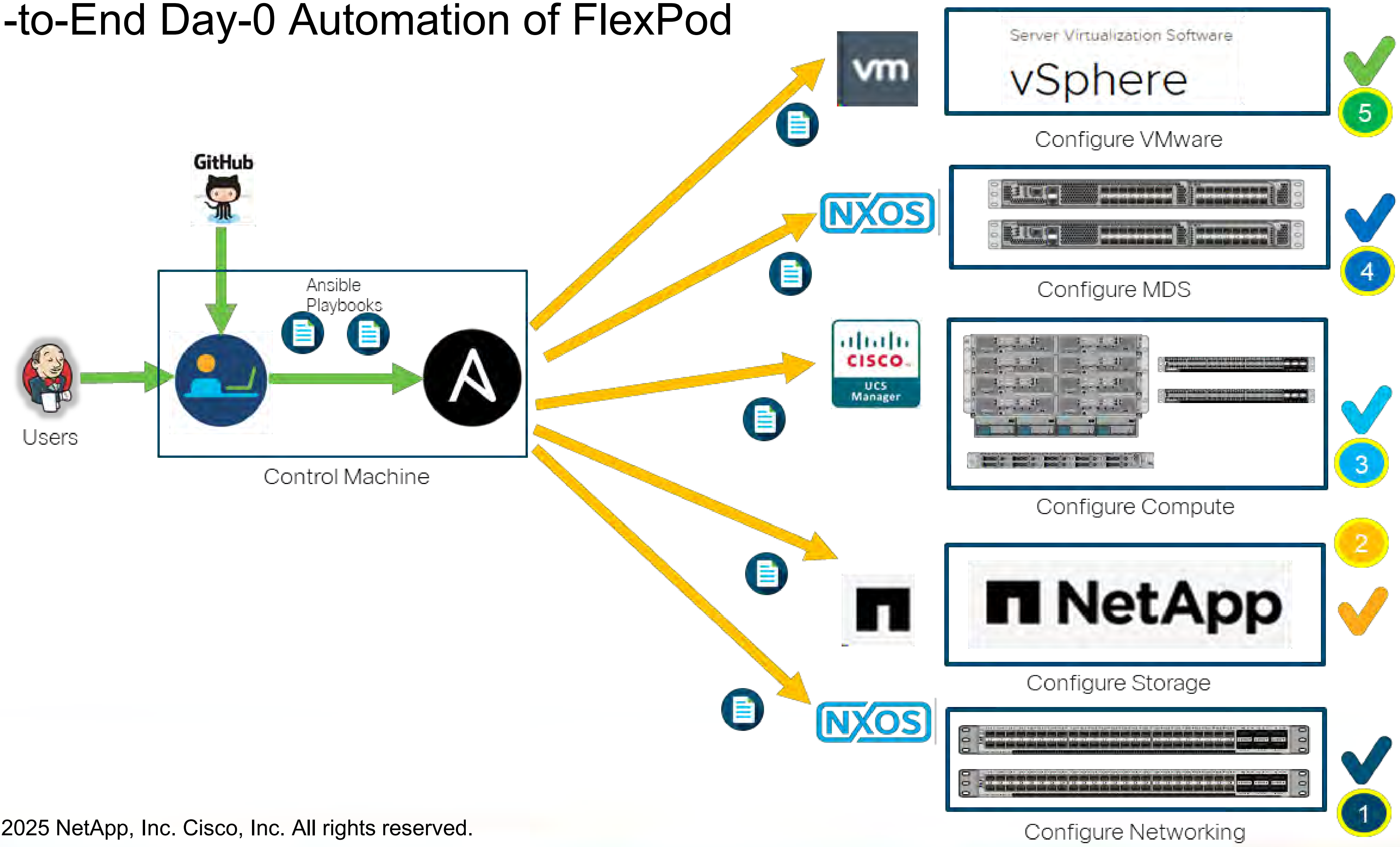
https://discord.gg/NetApp

Besuche unsere *NetApp Media Library*

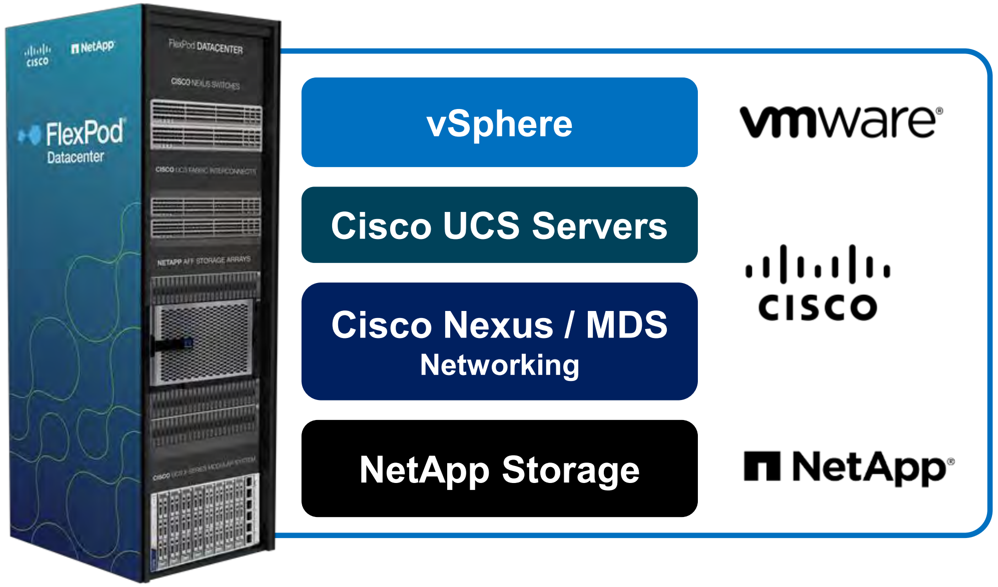
NetApp

Ansible Automation Workflows

End-to-End Day-0 Automation of FlexPod



How to Harden Your FlexPod Deployment



Hardened FlexPod

Leverage the Security Best Practices of FlexPod elements

Unified hardening guidance and security features for maximum protection

- Network traffic segmentation
- Disabling unused services
- Login authentication
- Role-based access control
- Login banners
- Session timeouts and limits
- Time synchronization
- Remote logging
- Configuration backup
- FIPS 140-2 compliance
- Secure boot
- Data in-flight and at-rest encryption
- (and many more…)

Security Automation

Ansible playbook to deploy security best practices in GitHub

Ansible Playbook for Security Hardening

ANSIBLE

- Selection of security features for Virtualization, Cisco UCS and Nexus, and NetApp ONTAP
- Hardening Automation Playbooks across the FlexPod Stack

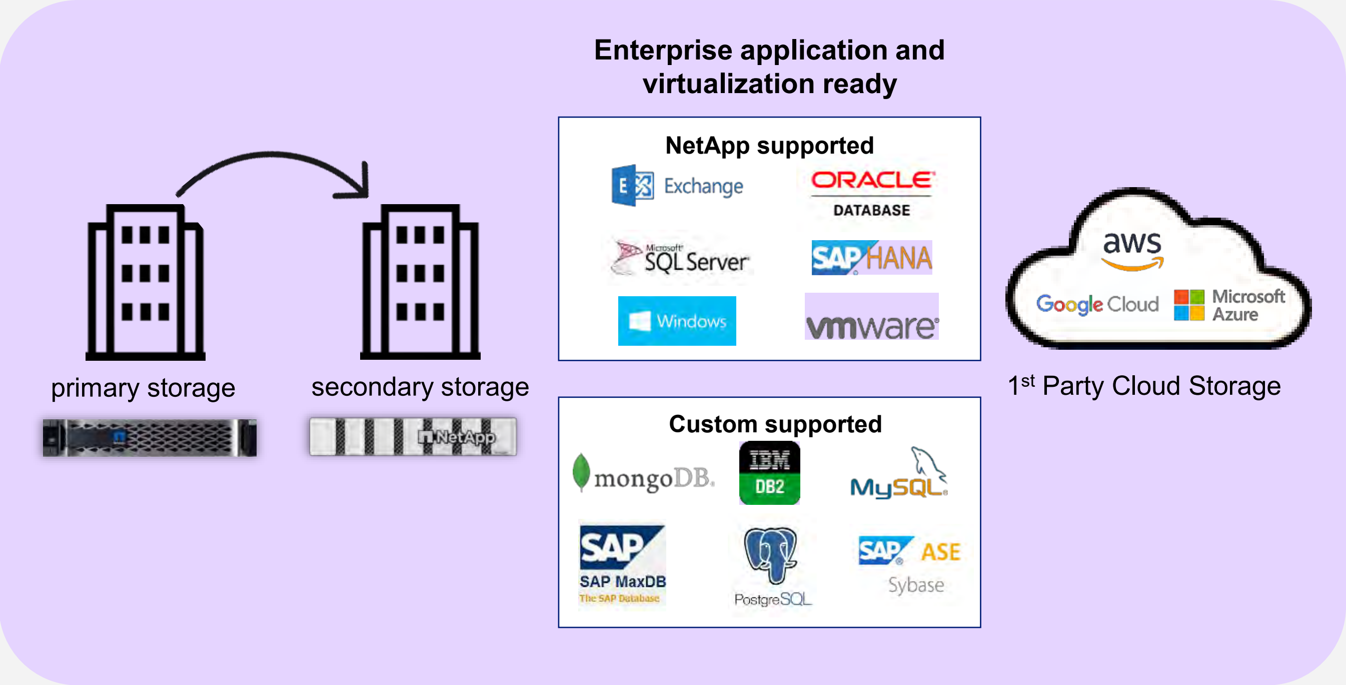
Bullet-proof continuity and recovery

Recover

Built-in application-consistent protection against ransomware, failure, disaster, error, and more

SnapCenter: Transparent Data Protection

- Single pane of glass to take snapshots of apps, databases, host file systems and VMs
- Efficient in-place copy data management
- Accelerated application development
- Snapshot copies secure from ransomware attacks



BlueXP Backup & Recovery: DataLock & ransomware protection

Recover

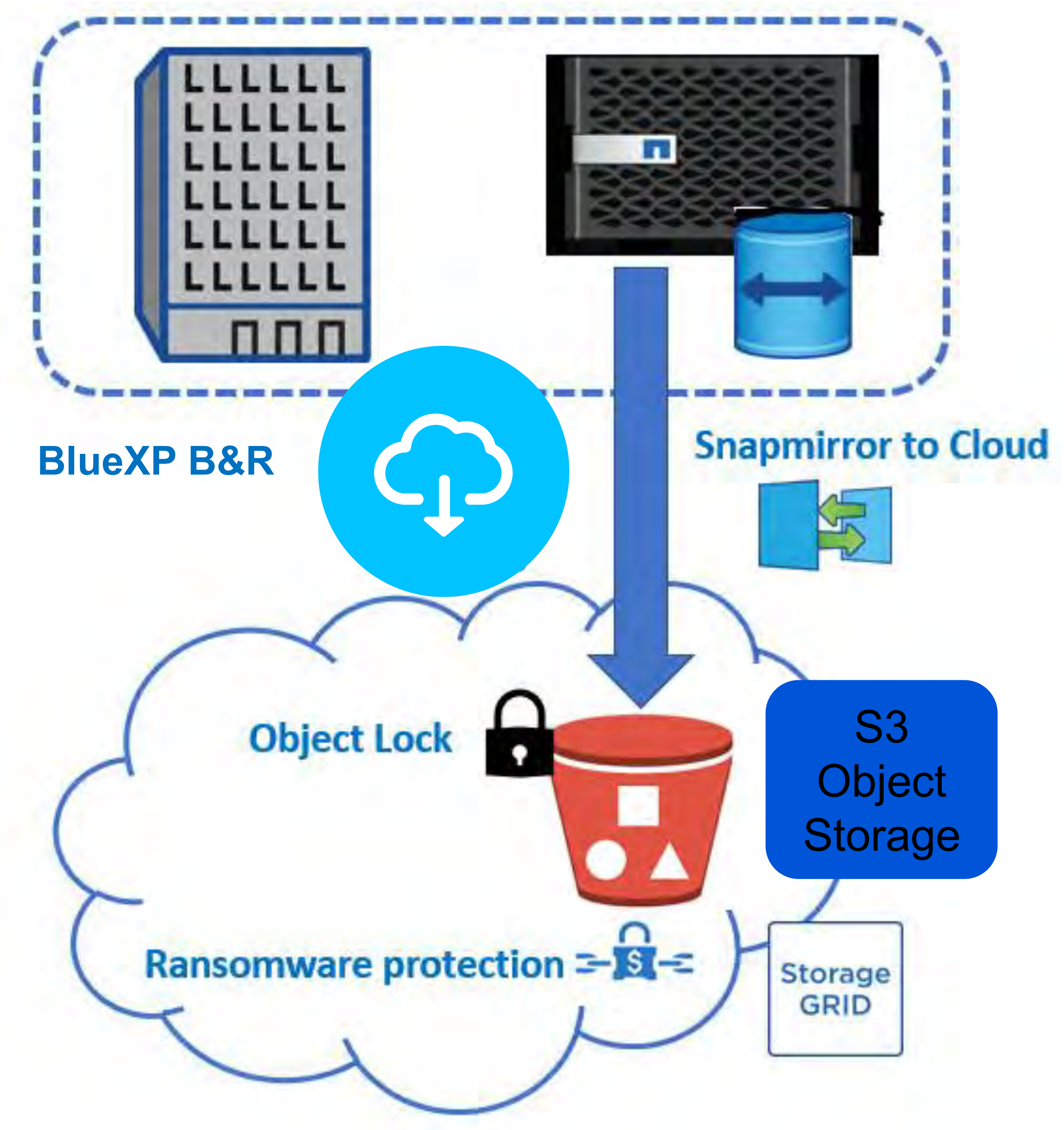
Protection against ransomware attacks & unauthorized deletions have become one of the high priority requirements among customers.

BlueXP Backup & Recovery provides the option to set ObjectLock & ransomware scan feature on backups.

This feature provides:

- Mechanism to lock the NetApp Snapshot™ copies replicated to cloud object-store
- Ability to detect ransomware attack & recover the consistent copy of the cloud Snapshot copy

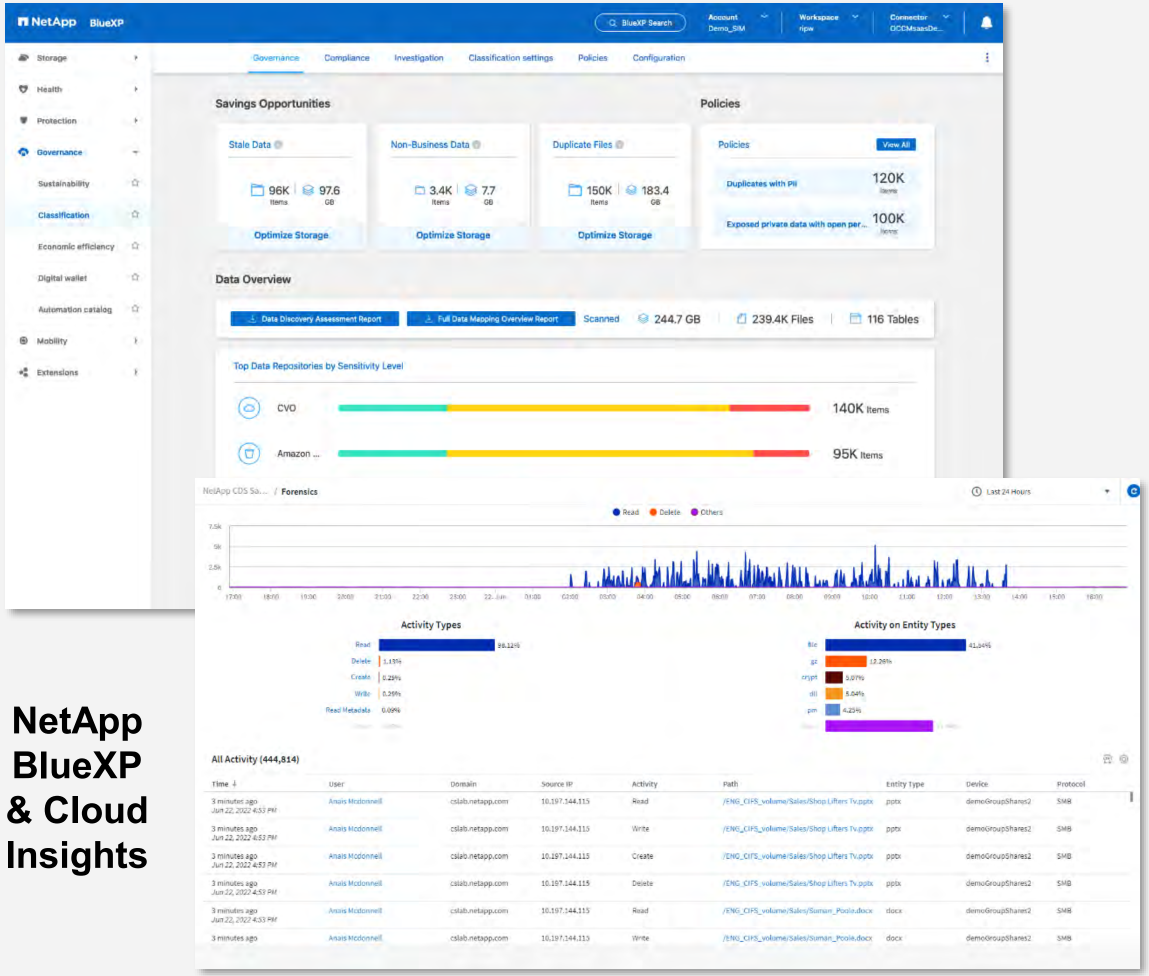
The solution uses both SM-C and ADC to achieve this functionality.



Detect

Deep dive into your data with ease

Additional hybrid multicloud services to give you control over your data



All Activity (444,814)

Time	User	Domain	Source IP	Activity	Path	Entity Type	Device	Protocol
3 minutes ago Jun 22, 2022 4:53 PM	Anais Mcdonnell	cslab.netapp.com	10.197.144.115	Read	/ENG_CIFS_volume/Sales/Shop Lifters Tv.pptx	pptx	demoGroupShares2	SMB
3 minutes ago Jun 22, 2022 4:53 PM	Anais Mcdonnell	cslab.netapp.com	10.197.144.115	Write	/ENG_CIFS_volume/Sales/Shop Lifters Tv.pptx	pptx	demoGroupShares2	SMB
3 minutes ago Jun 22, 2022 4:53 PM	Anais Mcdonnell	cslab.netapp.com	10.197.144.115	Create	/ENG_CIFS_volume/Sales/Shop Lifters Tv.pptx	pptx	demoGroupShares2	SMB
3 minutes ago Jun 22, 2022 4:53 PM	Anais Mcdonnell	cslab.netapp.com	10.197.144.115	Delete	/ENG_CIFS_volume/Sales/Shop Lifters Tv.pptx	pptx	demoGroupShares2	SMB
3 minutes ago Jun 22, 2022 4:53 PM	Anais Mcdonnell	cslab.netapp.com	10.197.144.115	Read	/ENG_CIFS_volume/Sales/Suman_Poole.docx	docx	demoGroupShares2	SMB
3 minutes ago	Anais Mcdonnell	cslab.netapp.com	10.197.144.115	Write	/ENG_CIFS_volume/Sales/Suman_Poole.docx	docx	demoGroupShares2	SMB

NetApp BlueXP & Cloud Insights

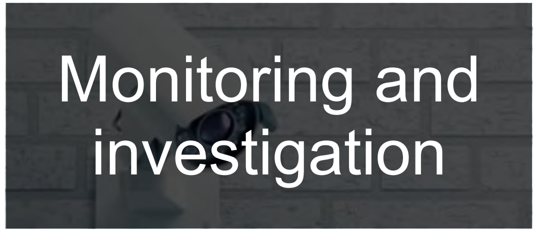
- Monitor for and alert on data access and **anomalous user behavior**
- Get **file-level forensics** and system auditing.
- **Discover, classify, and categorize** data across endpoints and clouds.
- Locate **personal, sensitive,** and **regulated** data, and identify permission issues
- Pull **compliance reports** in minutes.

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.

Detect

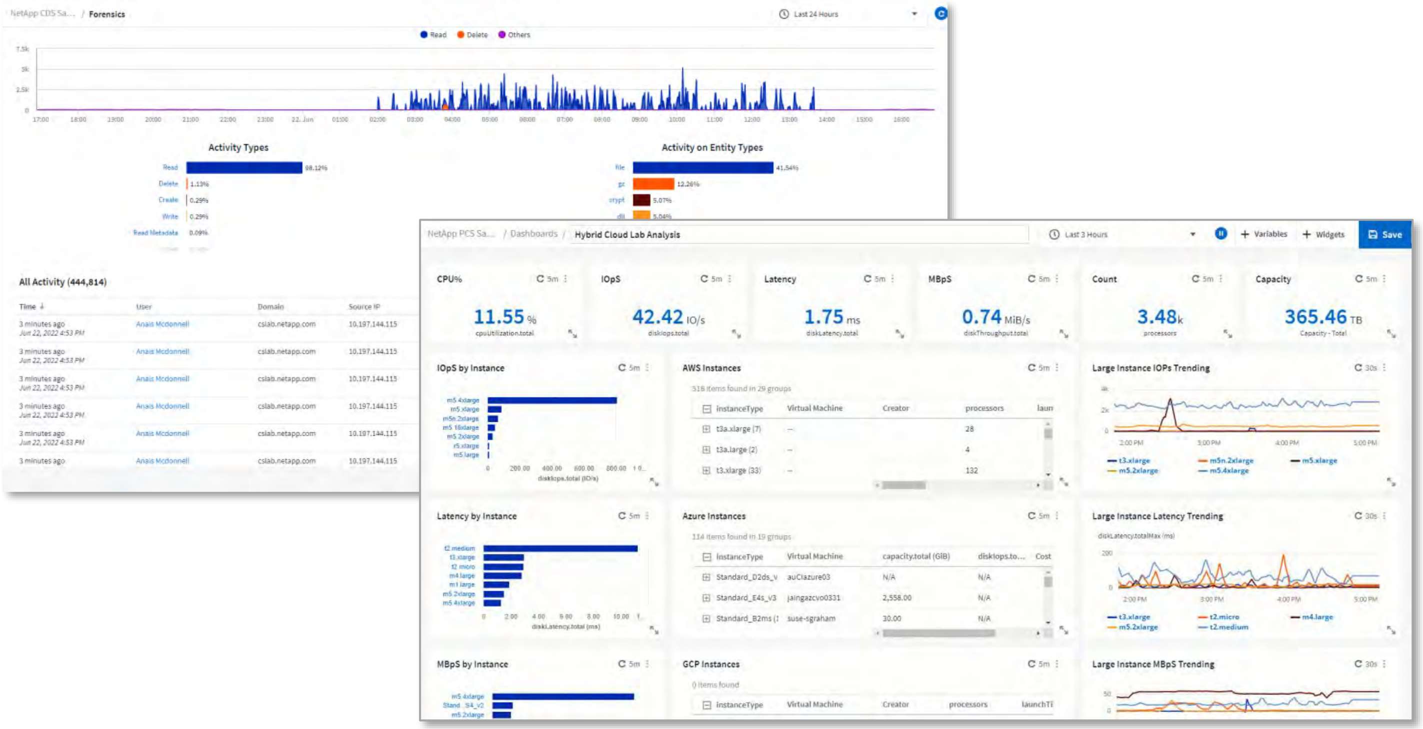
Keep NAS users in mind as well (DII & Storage Workload Security)

Discover anomalies & apply intelligent analysis



Monitoring and investigation

- Monitor for and report anomalous behavior.
- Receive alerts and identify suspicious activity.
- Get file-level forensics and system auditing.



All Activity (444,814)

Time	User	Domain	Source IP
3 minutes ago Jun 22, 2022 4:53 PM	Anais Mcdonnell	cslab.netapp.com	10.197.144.115
3 minutes ago Jun 22, 2022 4:53 PM	Anais Mcdonnell	cslab.netapp.com	10.197.144.115
3 minutes ago Jun 22, 2022 4:53 PM	Anais Mcdonnell	cslab.netapp.com	10.197.144.115
3 minutes ago Jun 22, 2022 4:53 PM	Anais Mcdonnell	cslab.netapp.com	10.197.144.115
3 minutes ago Jun 22, 2022 4:53 PM	Anais Mcdonnell	cslab.netapp.com	10.197.144.115
3 minutes ago	Anais Mcdonnell	cslab.netapp.com	10.197.144.115

CPU%	IOpS	Latency	MBpS	Count	Capacity
11.55 %	42.42 IO/s	1.75 ms	0.74 MiB/s	3.48k	365.46 TB
cpuUtilization.total	diskIops.total	diskLatency.total	diskThroughput.total	processors	Capacity - Total

AWS Instances

518 items found in 29 groups

instanceType	Virtual Machine	Creator	processors	laun
t3a.xlarge (7)	–		28	
t3a.large (2)	–		4	
t3.xlarge (33)	–		132	

Azure Instances

114 items found in 19 groups

instanceType	Virtual Machine	capacity.total (GiB)	diskIops.to...	Cost
Standard_D2ds_v	auClazure03	N/A	N/A	
Standard_E4s_v3	jaingazcvo0331	2,558.00	N/A	
Standard_B2ms (1	suse-sgraham	30.00	N/A	

GCP Instances

0 items found

instanceType	Virtual Machine	Creator	processors	launchTi

> “**NetApp Cloud Insights advanced analytics for pinpointing problem areas are outstanding.** It helps us to pinpoint where issues may be, whether they are with storage, the network, on the clients, or with the application itself.”
>
> **—Ed Alexander,** Senior Systems Administrator of a large software company

Single infrastructure observability tool for the hybrid multicloud

Detect

Data Infrastructure Insights Basics - AI/ML-powered Infrastructure Observability

AI/ML-Powered Optimization

for workload resource contention identification & resolution

Kubernetes Monitoring

for workload performance and troubleshooting

Storage Workload Security – ONTAP Only

for ransomware and threat prevention

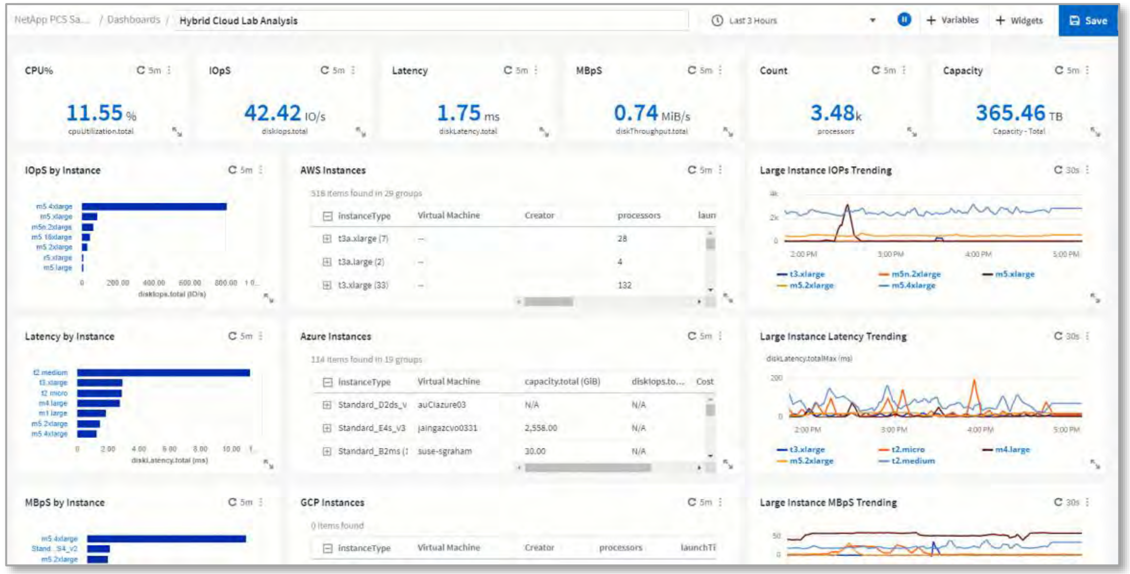
Workload Analysis and Placement

including resource baseline prior to cloud migration

Capacity Planning

for better infrastructure availability and optimization

Heterogeneous Hybrid Multicloud Observability



NetApp PCS Sa... / Dashboards / Hybrid Cloud Lab Analysis

Last 3 Hours

+ Variables + Widgets Save

CPU% 5m
11.55 %
cpuUtilization.total

IOpS 5m
42.42 IO/s
diskIops.total

Latency 5m
1.75 ms
diskLatency.total

MBpS 5m
0.74 MiB/s
diskThroughput.total

Count 5m
3.48k
processors

Capacity 5m
365.46 TB
Capacity - Total

IOpS by Instance 5m

AWS Instances 5m

518 items found in 29 groups

instanceType	Virtual Machine	Creator	processors	laun
⊞ t3a.xlarge (7)	–		28	
⊞ t3a.large (2)	–		4	
⊞ t3.xlarge (33)	–		132	

Large Instance IOPs Trending 30s

Latency by Instance 5m

Azure Instances 5m

114 items found in 19 groups

instanceType	Virtual Machine	capacity.total (GiB)	diskIops.to...	Cost
⊞ Standard_D2ds_v	auClazure03	N/A	N/A	
⊞ Standard_E4s_v3	jaingazcvo0331	2,558.00	N/A	
⊞ Standard_B2ms (1	suse-sgraham	30.00	N/A	

Large Instance Latency Trending 30s

MBpS by Instance 5m

GCP Instances 5m

0 items found

instanceType	Virtual Machine	Creator	processors	launchTi

Large Instance MBpS Trending 30s

Private

aws

Microsoft Azure

Google Cloud

How Data Infrastructure Insights Storage Workload Security Works

Cloud Insights Storage Workload Security does not assume trusted internal network, it takes ***trust no one*** approach. It inspects & analyzes all data access activity in real time to detect malicious behaviors.

1. **Monitor User Activity & File Entropy**

   Accurately identify breaches, every user activity across on-premises & hybrid cloud environments is captured and analyzed. To reduce false positives, ONTAP alerts are utilized to enrich detection abilities.

2. **Detect Anomalies & Identify Potential Attacks**

   Data Security uses advanced artificial intelligence & machine learning to uncover unusual data activity & detect potential attacks.

3. **Automated Response Policies**

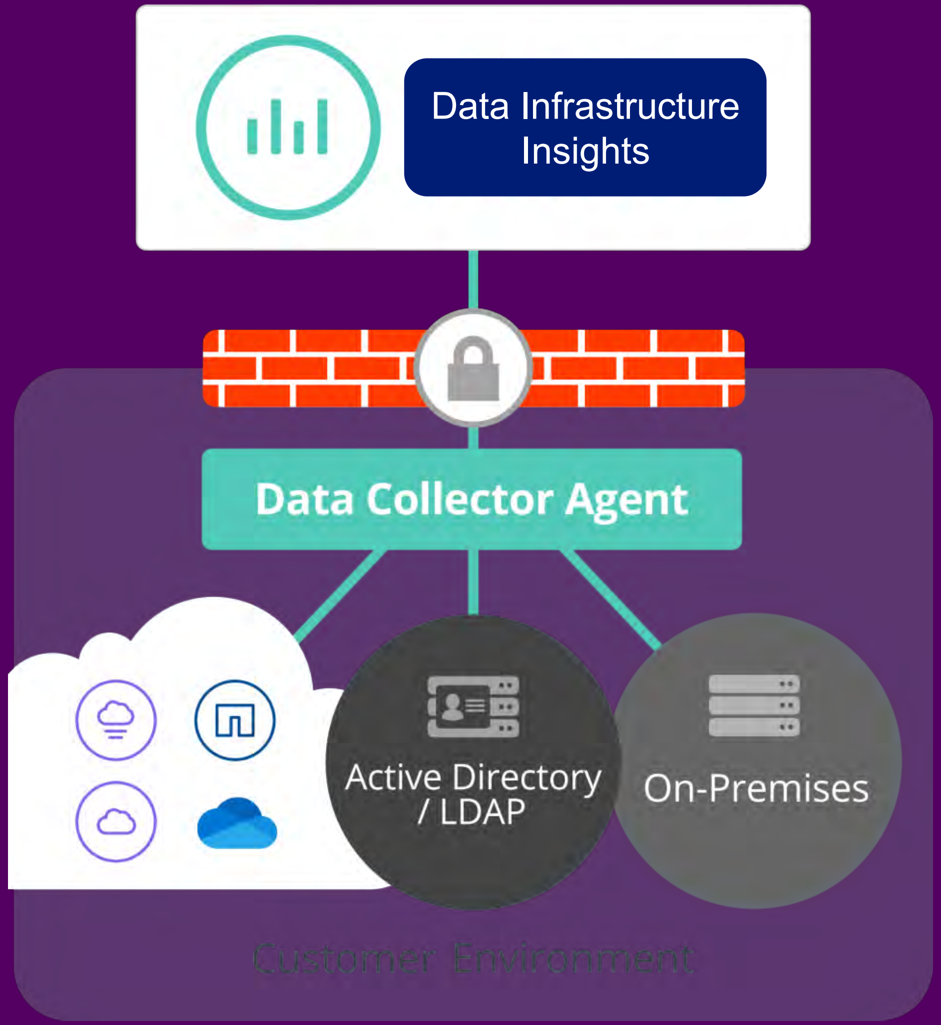
   Data Security alerts & automatically takes actions when detecting risky behavior, taking an immediate snapshot to protect data & blocking users to stop the attack

4. **Forensics & User Audit Reporting**

   Provides graphical interface to cut & slice activity data to perform data breach investigations & generate User Data Access Audit reporting.

How CI Storage Workload Security Monitors Activity

- Data is collected using a lightweight, stateless Data Collector Agent installed on a VM in the customer's environment
- Collects user data from AD & LDAP Servers
- Collects user file activity from ONTAP at any place
- Scalability
  - Supports multiple data collectors per single agent
  - Supports multiple agents



NetApp Cyber Resilience Partner Ecosystem

Virus detection

Industry-leading anti-malware and anti-virus solutions that build upon NetApp® ONTAP® Vscan technology

NetApp ONTAP integrations

symantec.
Trellix
TREND MICRO
SentinelOne
deep instinct

Data protection

Integration with NetApp ONTAP Snapshot™ and efficient replication with SnapMirror®

NetApp Snapshots, NetApp SnapMirror

COMMVAULT
rubrik
druva
veeAM
CLEONDRIS
VERITAS
ProLion
CATALOGIC SOFTWARE
IBM
COHESITY

User behavior

Integration with FPolicy to deliver an intelligent view of file and user behaviour

NetApp Cloud Insights and NetApp BlueXP™

Brainwave GRC
CLEONDRIS
STEALTHbits TECHNOLOGIES
VARONIS
VERITAS
ProLion

XDR and SIEM

Integration with forensic-analytic syslog or SIEM tools

NetApp Cloud Insights

splunk>
Brainwave GRC
CLEONDRIS
ProLion
VARONIS
VERITAS
STEALTHbits TECHNOLOGIES

Data protection is a multi-layered problem

NetApp storage systems offer additional cyber protection

Ransomware → Layered Protection ← Insider Threat Protection

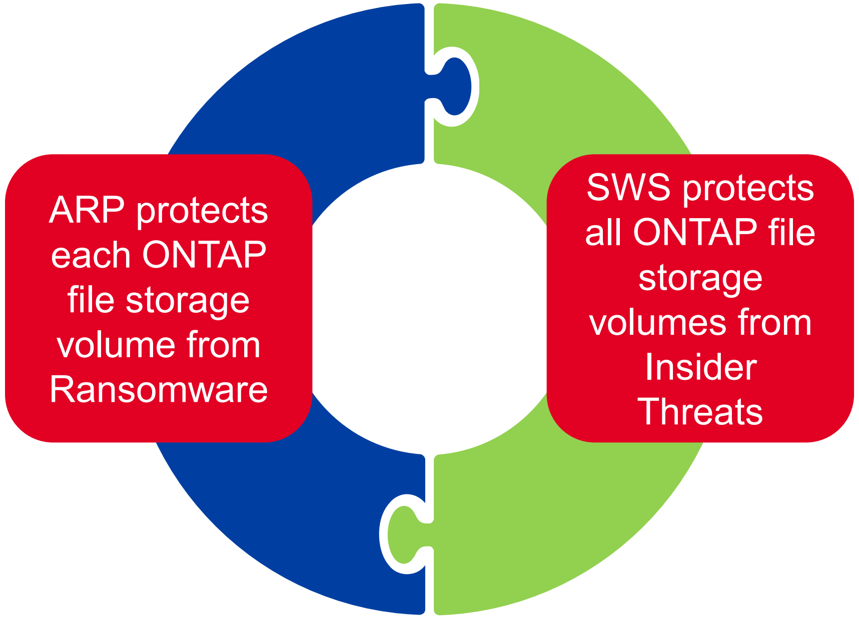
Ransomware

SWS adds
Offending user identification
Blocks user, includes full user file forensics across volumes

Other Storage Vendors Provide Some Protection

ONTAP ARP detection, criteria
Data Entropy
File Extension
Abnormal Surge in file activity
Snapshot & Alert

Layered Protection



ARP protects each ONTAP file storage volume from Ransomware

SWS protects all ONTAP file storage volumes from Insider Threats

Insider Threat Protection

Data Destruction
Massive Deletion action
Snapshot, Block User/Alert, includes full user file forensics across all ONTAP volumes

Data Exfiltration
Data Theft/Held for ransom
Snapshot, Abnormal user action detection alert, includes full user file forensics across all ONTAP volumes

Abnormal User Behavior
Abnormal file access patterns
Snapshot, Abnormal User action detection alert, includes full user file forensics across all ONTAP volumes

ONTAP Autonomous Ransomware Protection (ARP)

Cloud Insights Storage Workload Security (SWS)

Insider Threat Categories

Negligent user

Malicious insider

Credential Thief