COHESITY

Cyber Resiliency with Cohesity

IT’S TIME FOR

COHESITY & VERITAS

COHESITY

Cohesity + Veritas: The Leader in AI-powered Data Security

Our Mission:

To protect, secure & provide insights into the world's data.
The largest organizations in the world rely on us for their Resilience.

Our Focus:

Data Protection

- Broad Workloads
- Enterprise Scale
- Flexible Consumption

Data Security

- Threat Detection
- Posture Management
- Cyber Recovery

Data Insights

- GenAI Engine
- Search & Analytics
- Operational Insights

What We Bring:

$1.7B
Revenue[1]

100+ EBs
Data Protected

1600
Patents

2x
R&D of Nearest Competitor

19.4%
Market Share[2] (Leader)

140
Global Locations

12000
Customers

3000
Partners

Leader
Gartner MQ

Notes: *1. 2023 pro forma metrics after acquisition of Veritas data protection business*
2. Analyst and Company Research, Proforma 2023 Backup and Recovery Market Share

COHESITY

Our Commitment to Our Customers

> *Cohesity is committed to futureproofing our customers' investments … this means ongoing support for* ***all Veritas NetBackup, NetBackup Appliances*** *and* ***Alta Data Protection*** *… for many years to come".*

Sanjay Poonen, Cohesity CEO

Will Veritas data protection software, cloud, and appliance products continue to get roadmap investment?

YES!

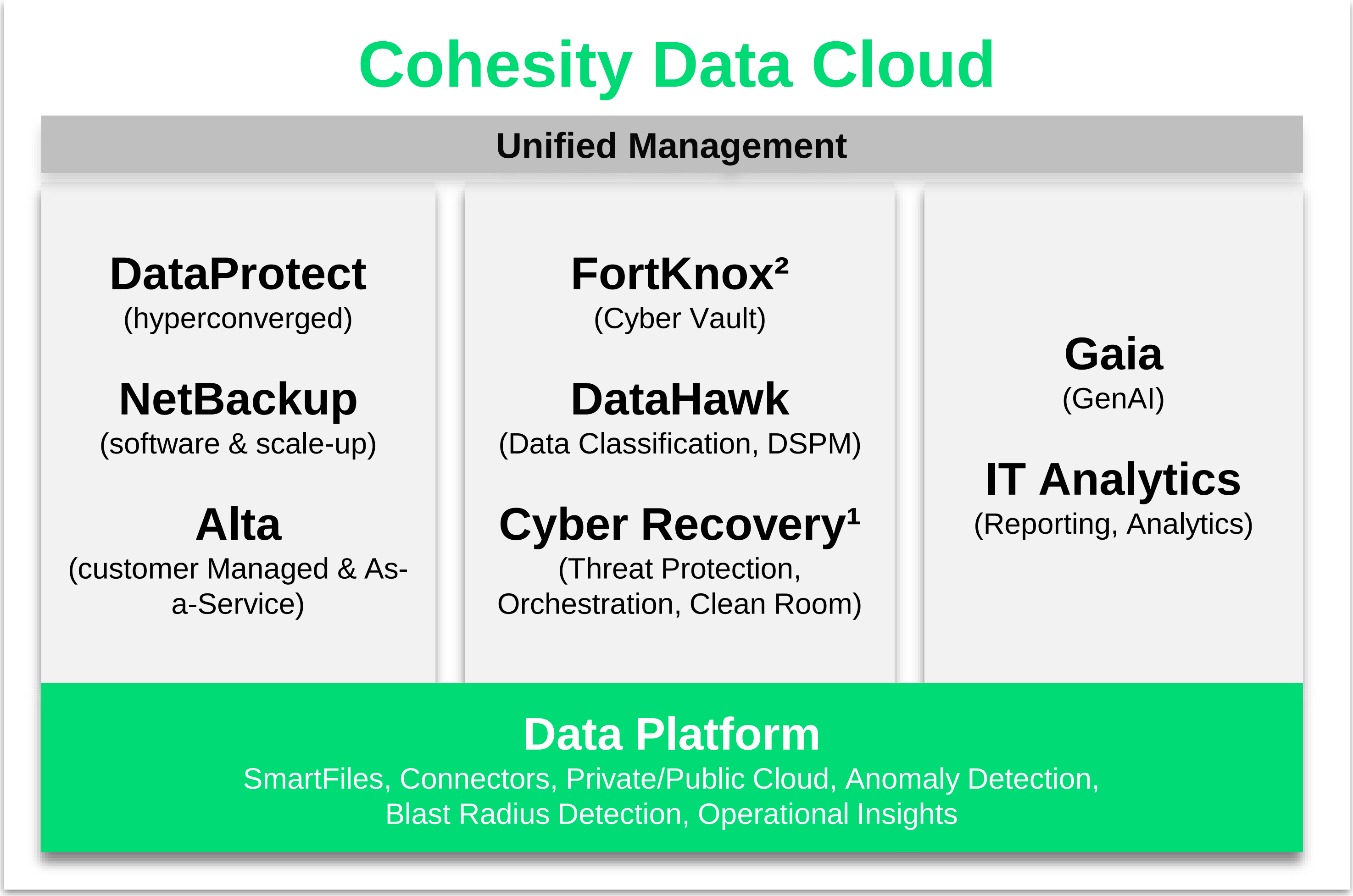
Will our customers be forced to migrate?

NO!

NEW!: Stay tuned for information regarding new commercial programs to further preserve your investment.

COHESITY

Cohesity + Veritas Product Roadmap



Cohesity Data Cloud

Unified Management

DataProtect
(hyperconverged)

NetBackup
(software & scale-up)

Alta
(customer Managed & As-a-Service)

FortKnox[2]
(Cyber Vault)

DataHawk
(Data Classification, DSPM)

Cyber Recovery[1]
(Threat Protection, Orchestration, Clean Room)

Gaia
(GenAI)

IT Analytics
(Reporting, Analytics)

Data Platform
SmartFiles, Connectors, Private/Public Cloud, Anomaly Detection, Blast Radius Detection, Operational Insights

1 – Official Name TBD
2 – Includes Recover Vault

COHESITY

Cyber Resiliency

Concept of Resilience

Data Resilience

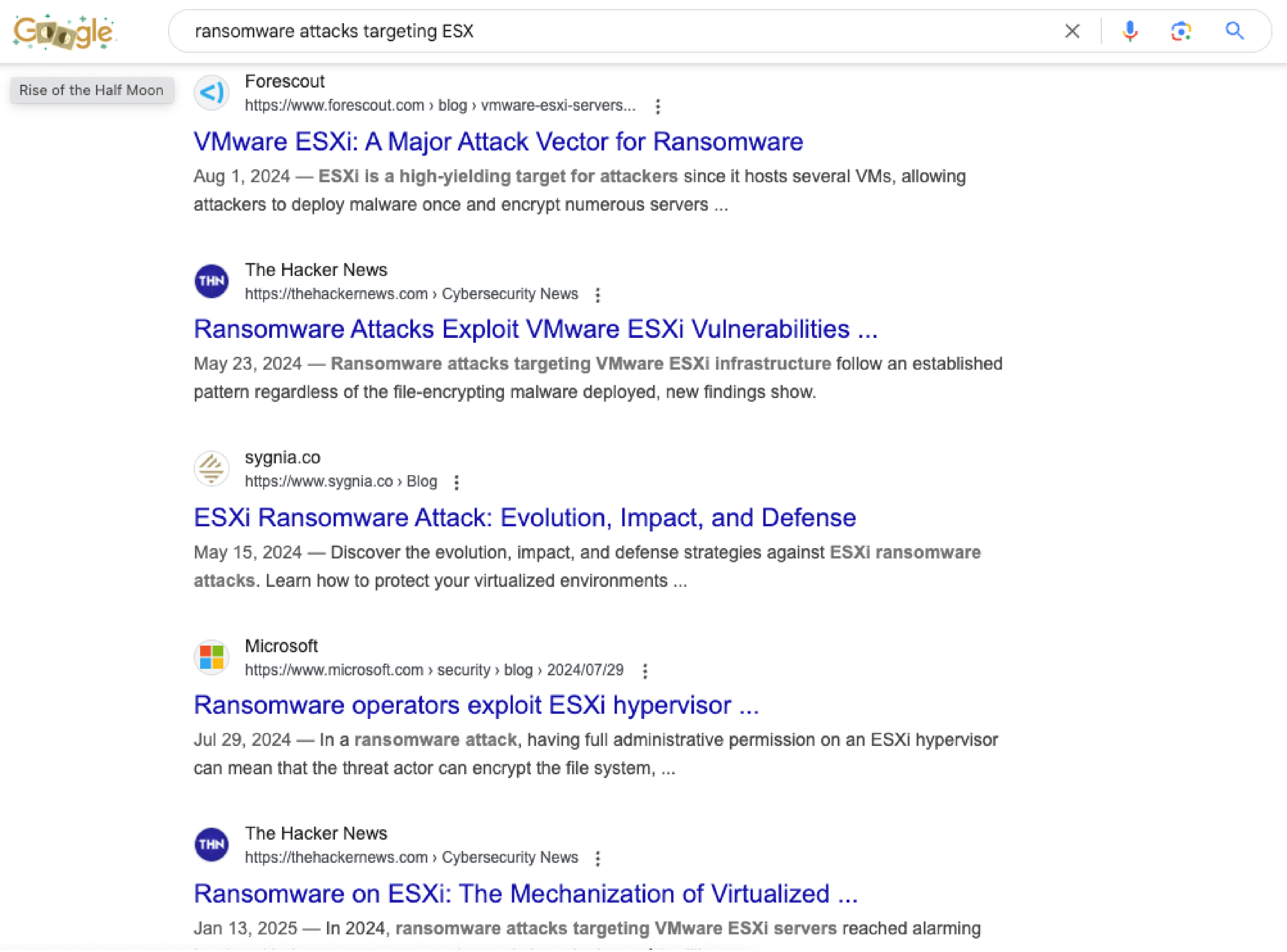
Continue business operations
& quickly recover

Cyber Resilience

Preparing, responding, & recovering
from Cyber attacks

Business Resilience

Adapt quickly to disruption



Forescout
https://www.forescout.com › blog › vmware-esxi-servers...

VMware ESXi: A Major Attack Vector for Ransomware

Aug 1, 2024 — **ESXi is a high-yielding target for attackers** since it hosts several VMs, allowing attackers to deploy malware once and encrypt numerous servers ...

The Hacker News
https://thehackernews.com › Cybersecurity News

Ransomware Attacks Exploit VMware ESXi Vulnerabilities ...

May 23, 2024 — **Ransomware attacks targeting VMware ESXi infrastructure** follow an established pattern regardless of the file-encrypting malware deployed, new findings show.

sygnia.co
https://www.sygnia.co › Blog

ESXi Ransomware Attack: Evolution, Impact, and Defense

May 15, 2024 — Discover the evolution, impact, and defense strategies against **ESXi ransomware attacks**. Learn how to protect your virtualized environments ...

Microsoft
https://www.microsoft.com › security › blog › 2024/07/29

Ransomware operators exploit ESXi hypervisor ...

Jul 29, 2024 — In a **ransomware attack**, having full administrative permission on an ESXi hypervisor can mean that the threat actor can encrypt the file system, ...

The Hacker News
https://thehackernews.com › Cybersecurity News

Ransomware on ESXi: The Mechanization of Virtualized ...

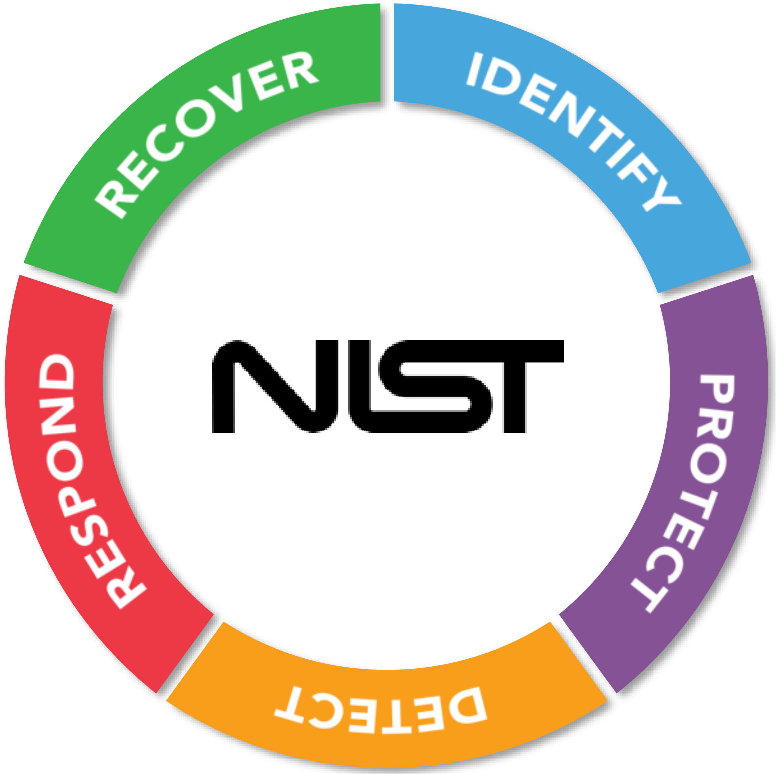
Jan 13, 2025 — In 2024, **ransomware attacks targeting VMware ESXi servers** reached alarming

NIST Cyber Security Framework and Best Practices

Protect all data from all sources

Detect threats as well as signs of threats

Recover to anywhere from anywhere



National Institute of Standards and Technology

INTERNATIONAL USE | Translations, Adaptations, and Other References Worldwide:

Netbackup

Pulai András

Pre-sales engineer

NetBackup

Unmatched Flexibility

Operating Systems

Windows
hp UX
AIX
SUSE

Virtual Systems

vmware
docker
Microsoft Hyper-V
Red Hat
NUTANIX

Databases and applications

Microsoft SharePoint
Microsoft Exchange
ORACLE
IBM Informix
SAP

Any Deployment

Cloud Platforms

Office 365
G Suite
salesforce
aws
Microsoft Azure
Google Cloud Platform
openstack

Next-Gen

MySQL
HORTONWORKS
mongoDB
PostgreSQL
MariaDB
SQLite
cassandra
hadoop
APACHE HBASE
cloudera

Storage Systems

PURE STORAGE
NetApp
Hewlett Packard Enterprise

Containers

kubernetes
VMware Tanzu
OPENSHIFT
Google Kubernetes Engine

Secure by Design

Turnkey Cyber Resilience

NetBackup Flex and Flex Scale

Prevent Unauthorized Access

- Network Access Control and MFA
- Root Access Removal
- Restricted Admin Access
- RBAC and Mandatory Access Control
- File System, Namespace and Network Isolation

Threat Monitoring, Scanning and Alerting

- Anomaly Detection, Threat Hunting, Malware Scanning
- Intrusion Detection System
- Audit Logging and Log Forwarding

Continuous Threat Mitigation

- Threat intelligence team provides expedited fixes to new vulnerabilities and threats as they emerge

Indestructible Data

- WORM with Indelible Compliance Clock Multi-Person Authorization
- Restricted IPMI

Unbreakable Data Isolation

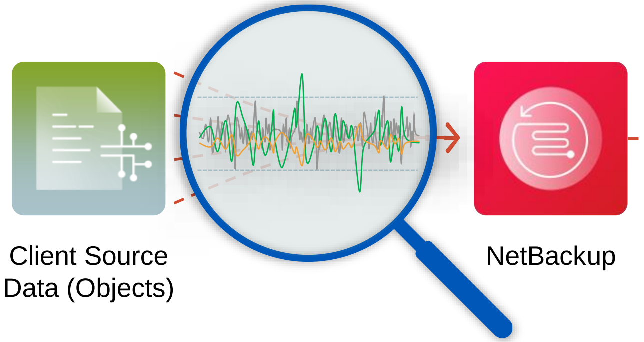
- Virtual AirGap (pull data model)

Independently pen-tested by 3rd party companies on behalf of two large financial institutions.

FOUND TO BE SECURE

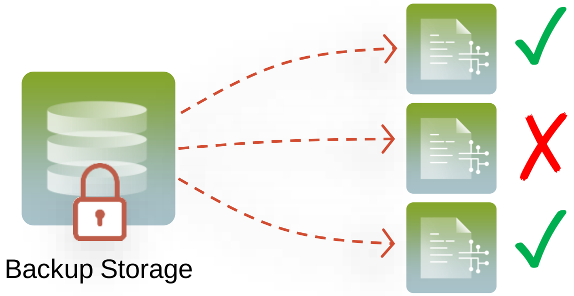
High-Level Overview of Malware Detection in NetBackup

During Backup



Anomaly detection in near real-time

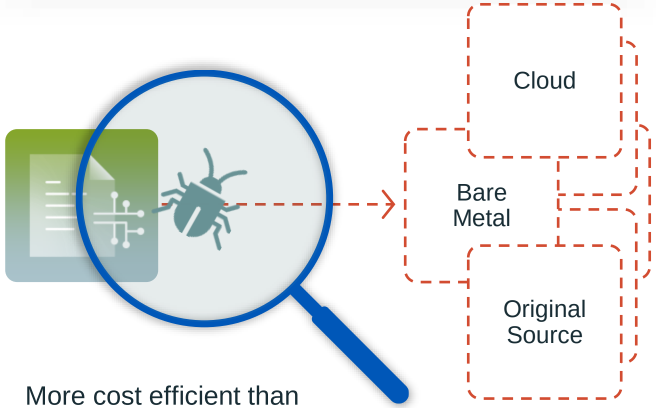
Post Backup



e.g., backups of internet-facing Windows clients

Spot-checking of known high-risk areas

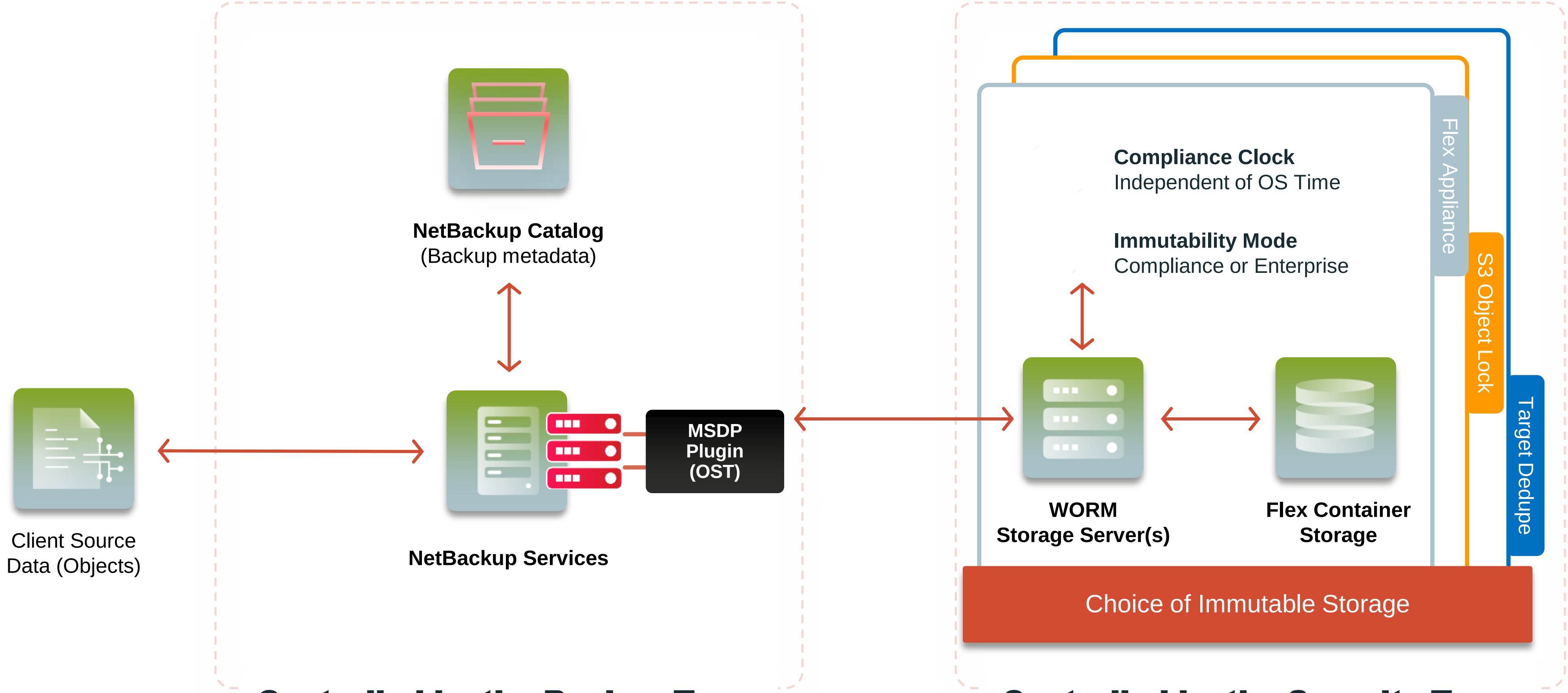
Before Restore



More cost efficient than storage scanning

Scanning before restore to ensure clean data

Immutable Storage



Controlled by the Backup Team

- Sets protection plans
- Defines policies

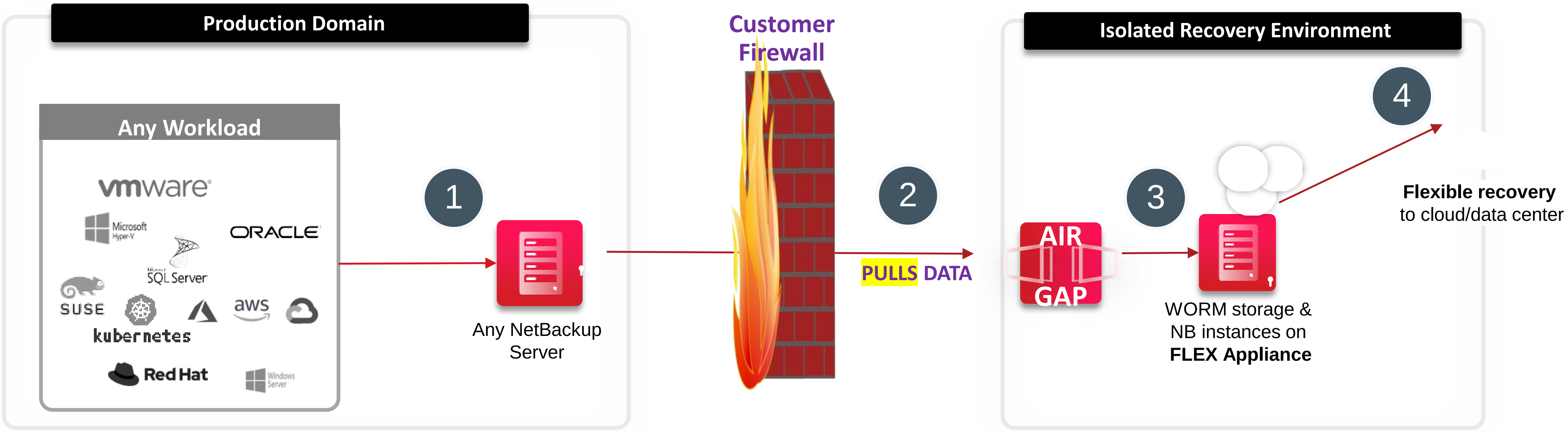
Controlled by the Security Team

- Decides when images can be deleted
- Data cannot be deleted by NetBackup

NetBackup Isolated Recovery Environment (IRE)

Eliminate need for Listening ports | Support 24 x 7 Data Replication | Pull Model

Powered by NetBackup



Real-time Anomaly Detection

Encrypted WORM storage

1 Real-time Anomaly Detection and On-Demand Malware Scan

2 OPTIONAL - Data Isolation using an operable air gap

3 Data Integrity with multi-tenant WORM storage

4 Recover at scale to "*Last Known Good State*"

Threat Hunting and Blast Radius Analysis

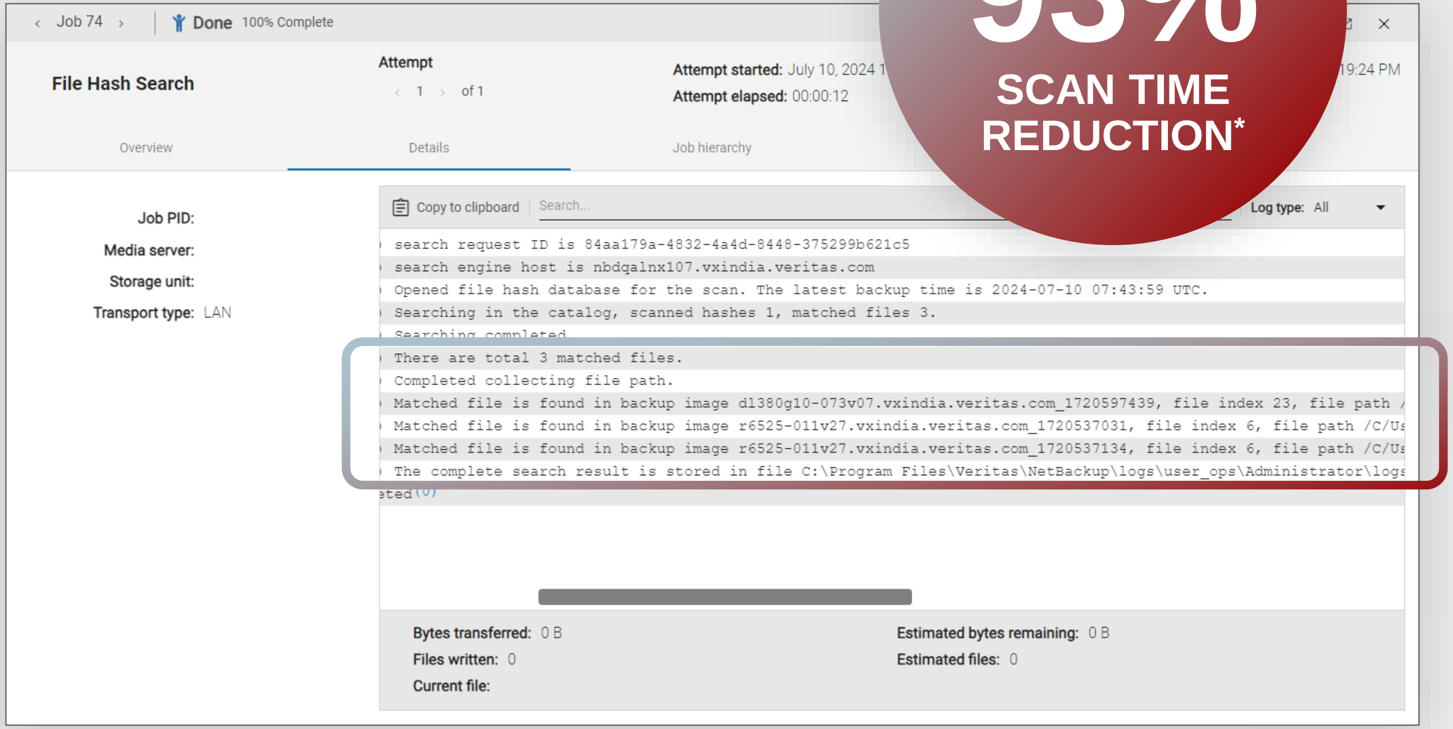
ABOUT THE FEATURE

- Search for potential Incidents of Compromise (IoCs)
- Searches index (vs. full scan) of hash-based signatures created from recent scans

BENEFITS

- Reduce search time from hours to minutes
- Identify all infected unstructured files across the entire NetBackup environment

UP TO **93%** SCAN TIME REDUCTION*



File Hash Search

Attempt ‹ 1 › of 1

Attempt started: July 10, 2024 1 … 19:24 PM

Attempt elapsed: 00:00:12

Job PID:

Media server:

Storage unit:

Transport type: LAN

Log type: All

```
search request ID is 84aa179a-4832-4a4d-8448-375299b621c5
search engine host is nbdqalnx107.vxindia.veritas.com
Opened file hash database for the scan. The latest backup time is 2024-07-10 07:43:59 UTC.
Searching in the catalog, scanned hashes 1, matched files 3.
Searching completed
There are total 3 matched files.
Completed collecting file path.
Matched file is found in backup image dl380g10-073v07.vxindia.veritas.com_1720597439, file index 23, file path /
Matched file is found in backup image r6525-011v27.vxindia.veritas.com_1720537031, file index 6, file path /C/Us
Matched file is found in backup image r6525-011v27.vxindia.veritas.com_1720537134, file index 6, file path /C/Us
The complete search result is stored in file C:\Program Files\Veritas\NetBackup\logs\user_ops\Administrator\logs
eted (0)
```

Bytes transferred: 0 B

Estimated bytes remaining: 0 B

Files written: 0

Estimated files: 0

Current file:

*Based on one TB of data, anticipate scan time reduction to increase as data volume increases

VERITAS ALTA™

Smarter

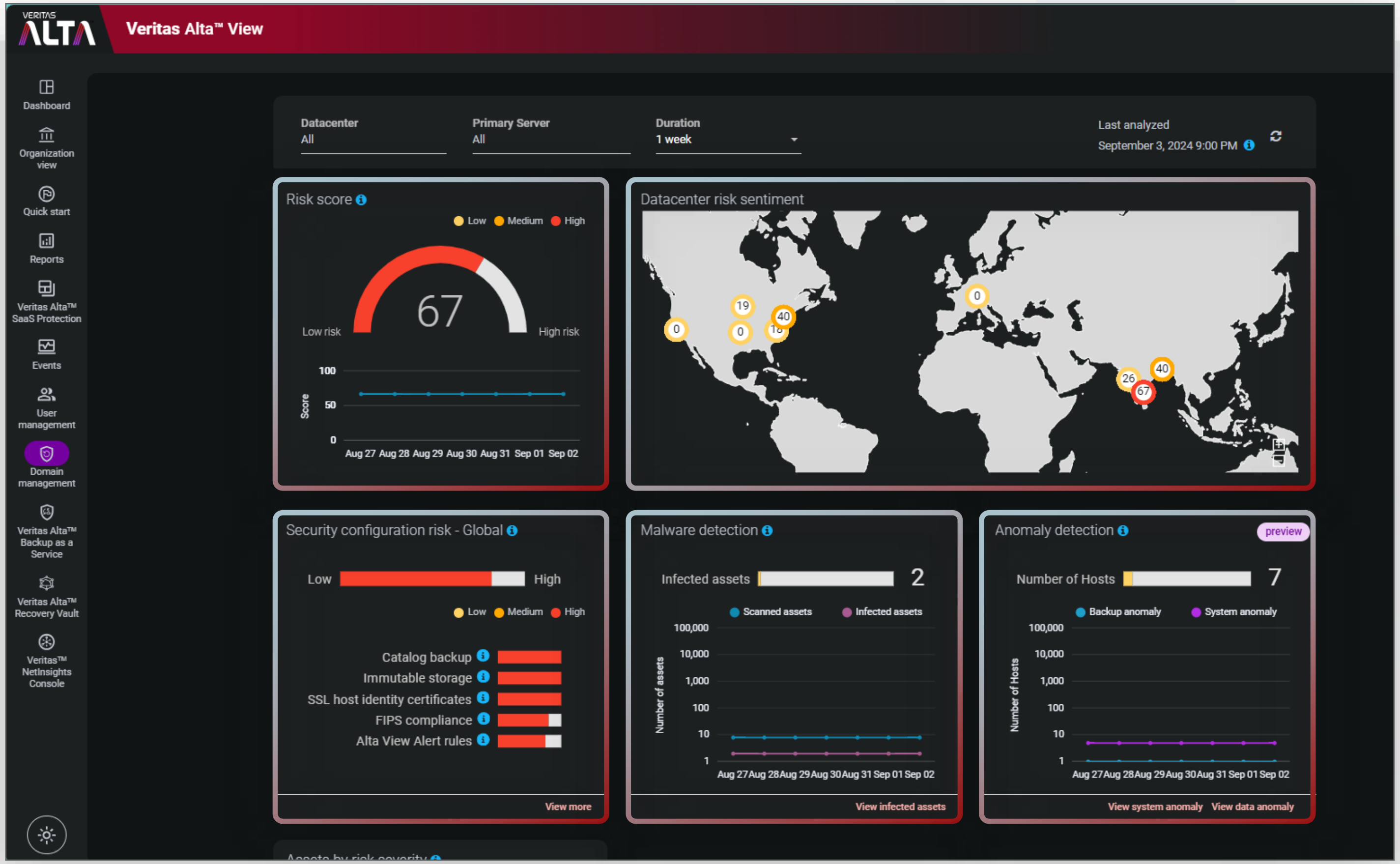
Automated Risk Assessment and Security Score

ABOUT THE FEATURE

- Visualize risk posture across entire data estate (datacenters, clouds, regions, etc.)
- Minimize duplicative alerts

BENEFITS

- Quickly ID and mitigate risks
- Reduced alert fatigue
- Evaluate and improve current risk mitigation measures



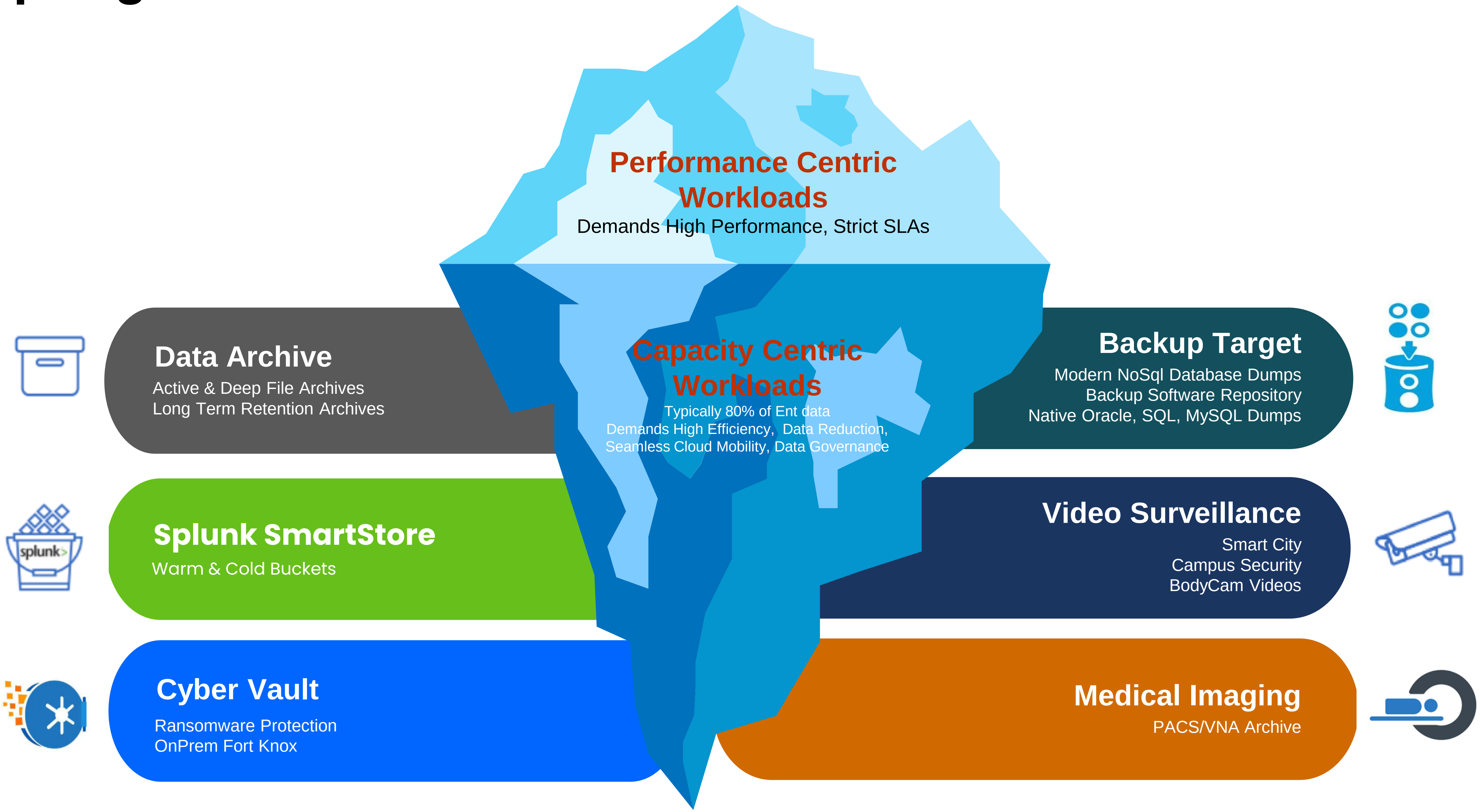
Veritas Alta™ View

Datacenter: All
Primary Server: All
Duration: 1 week
Last analyzed: September 3, 2024 9:00 PM

COHESITY

Cohesity Data Platform

Top High Level Use Cases



Performance Centric Workloads

Demands High Performance, Strict SLAs

Capacity Centric Workloads

Typically 80% of Ent data
Demands High Efficiency, Data Reduction,
Seamless Cloud Mobility, Data Governance

Data Archive

Active & Deep File Archives
Long Term Retention Archives

Splunk SmartStore

Warm & Cold Buckets

Cyber Vault

Ransomware Protection
OnPrem Fort Knox

Backup Target

Modern NoSql Database Dumps
Backup Software Repository
Native Oracle, SQL, MySQL Dumps

Video Surveillance

Smart City
Campus Security
BodyCam Videos

Medical Imaging

PACS/VNA Archive

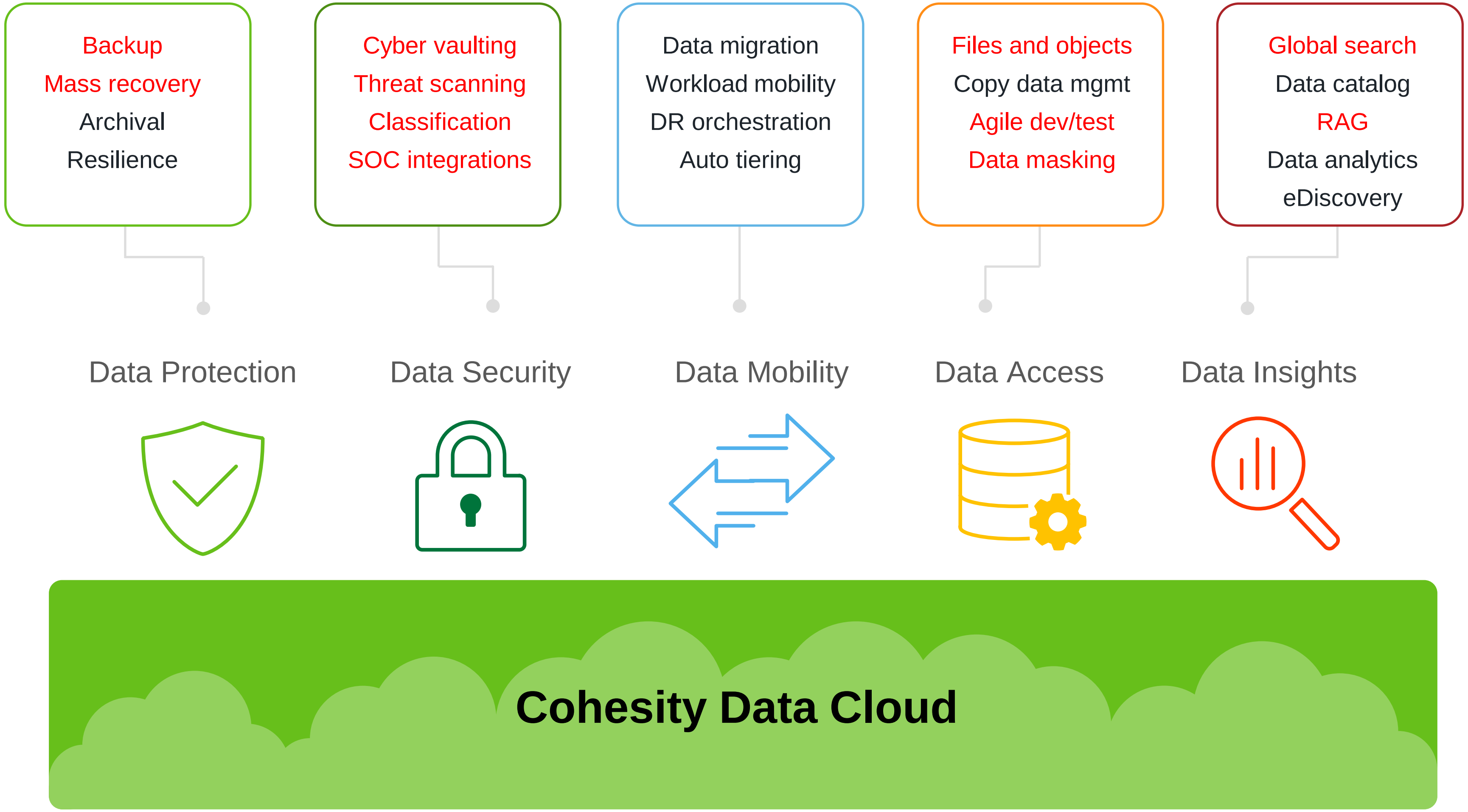
COHESITY

Unified, End-to-End Platform for AI-Powered Data Security & Management

MANAGE

SECURE

INSIGHTS



Backup
Mass recovery
Archival
Resilience

Cyber vaulting
Threat scanning
Classification
SOC integrations

Data migration
Workload mobility
DR orchestration
Auto tiering

Files and objects
Copy data mgmt
Agile dev/test
Data masking

Global search
Data catalog
RAG
Data analytics
eDiscovery

Data Protection

Data Security

Data Mobility

Data Access

Data Insights

Cohesity Data Cloud

Simple | Scalable | Secure | AI Ready | Extensible

Data Securtiy Alliance

Extensive Security Ecosystem

MANAGE

SECURE

INSIGHTS

LEADING DATA SECURITY ALLIANCE

paloalto NETWORKS
CISCO
CROWDSTRIKE
servicenow
splunk>
tenable
zscaler
CYBERARK
okta
Qualys.
MANDIANT
netskope
pwc
BigID
securonix

DATA SECURITY POSTURE MANAGEMENT PARTNERS

BigID
CYERA
CONCENTRIC
Dig Security
Normalyze data-first cloud security
Open Raven
securiti
sentra

SECURITY ADVISORY COUNCIL

Kevin Mandia
CEO Mandiant,
Google Cloud

Marianne Bailey
Former NSA
Exec and DOD CIO/CISO

Kelly Bissell
Corporate Vice President,
Microsoft Security Services

Alex Stamos
Former CSO,
Facebook and Yahoo

Sheila Jordan
Chief Digital
Technology Officer,
Honeywell

Jason Chan
Former VP of
Information Security,
Netflix

Laura Mather
Group COO
Societe Generale

World-Class AI/ML Capabilities

MANAGE

SECURE

INSIGHTS

AI

Ransomware Detection

Anomaly Detection

Capacity Prediction

Data Classification

Capacity Planning

Threat Intelligence

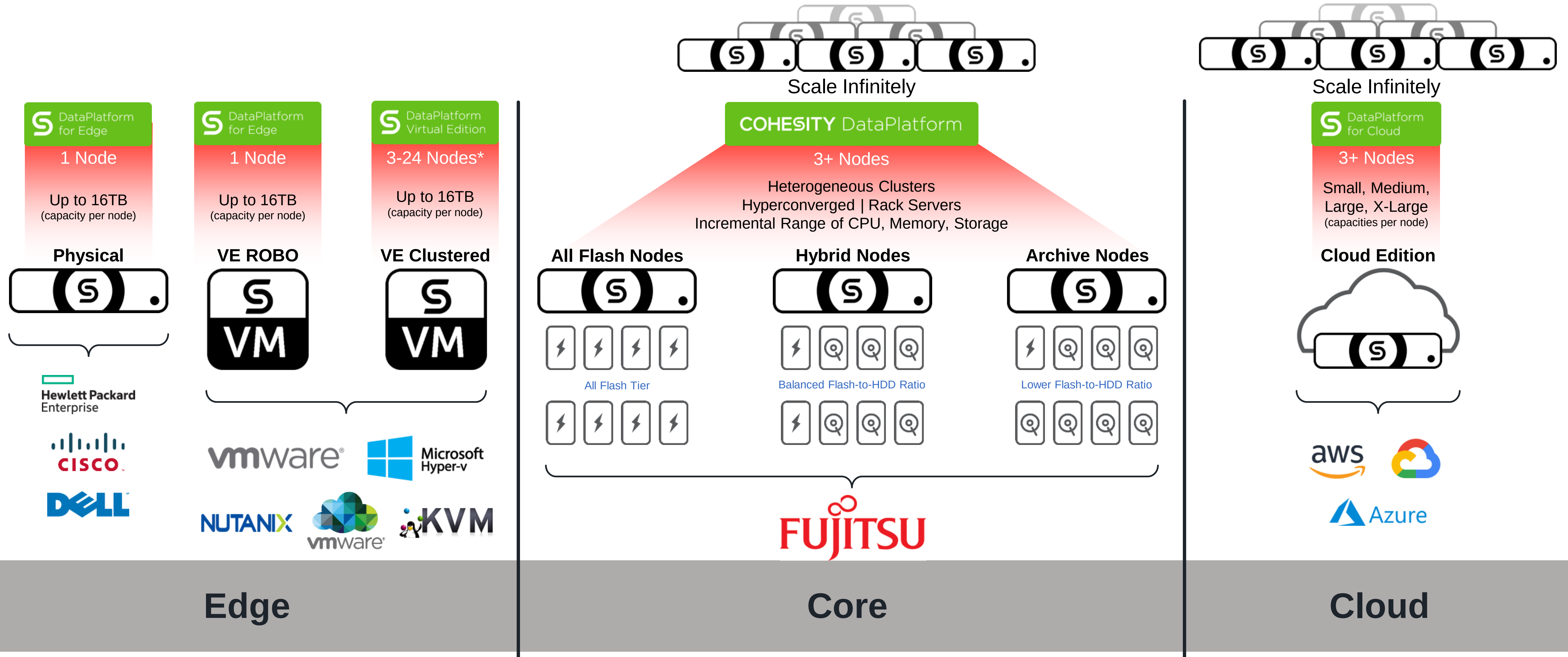
Data Entropy

GAIA LLM / RAG

COHESITY

Architecture and Services

Ultimate Scale & Flexibility



DataPlatform for Edge

1 Node

Up to 16TB
(capacity per node)

Physical

DataPlatform for Edge

1 Node

Up to 16TB
(capacity per node)

VE ROBO

DataPlatform Virtual Edition

3-24 Nodes*

Up to 16TB
(capacity per node)

VE Clustered

Scale Infinitely

COHESITY DataPlatform

3+ Nodes

Heterogeneous Clusters
Hyperconverged | Rack Servers
Incremental Range of CPU, Memory, Storage

All Flash Nodes

All Flash Tier

Hybrid Nodes

Balanced Flash-to-HDD Ratio

Archive Nodes

Lower Flash-to-HDD Ratio

Scale Infinitely

DataPlatform for Cloud

3+ Nodes

Small, Medium, Large, X-Large
(capacities per node)

Cloud Edition

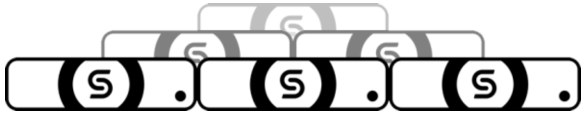
Edge

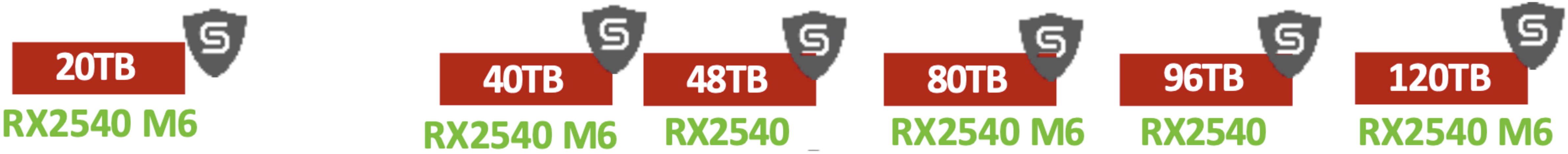
Core

Cloud

*It is possible to scale beyond 24 nodes with support assistance

Link to all certified platform vendors and models are found HERE





TM

kapacitás / 1 node

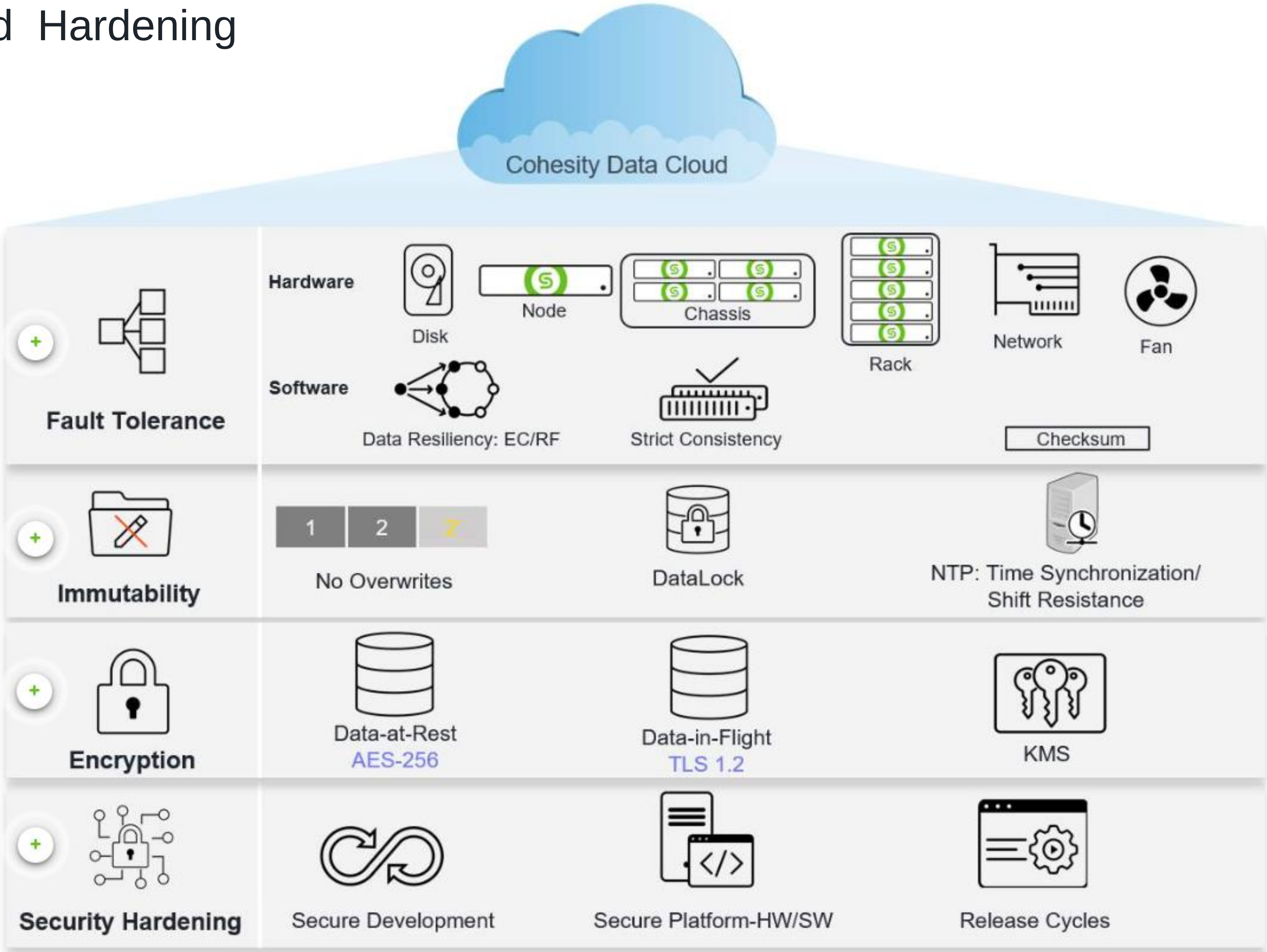
COHESITY

Cyber Resiliency

Cyber Resilience Framework

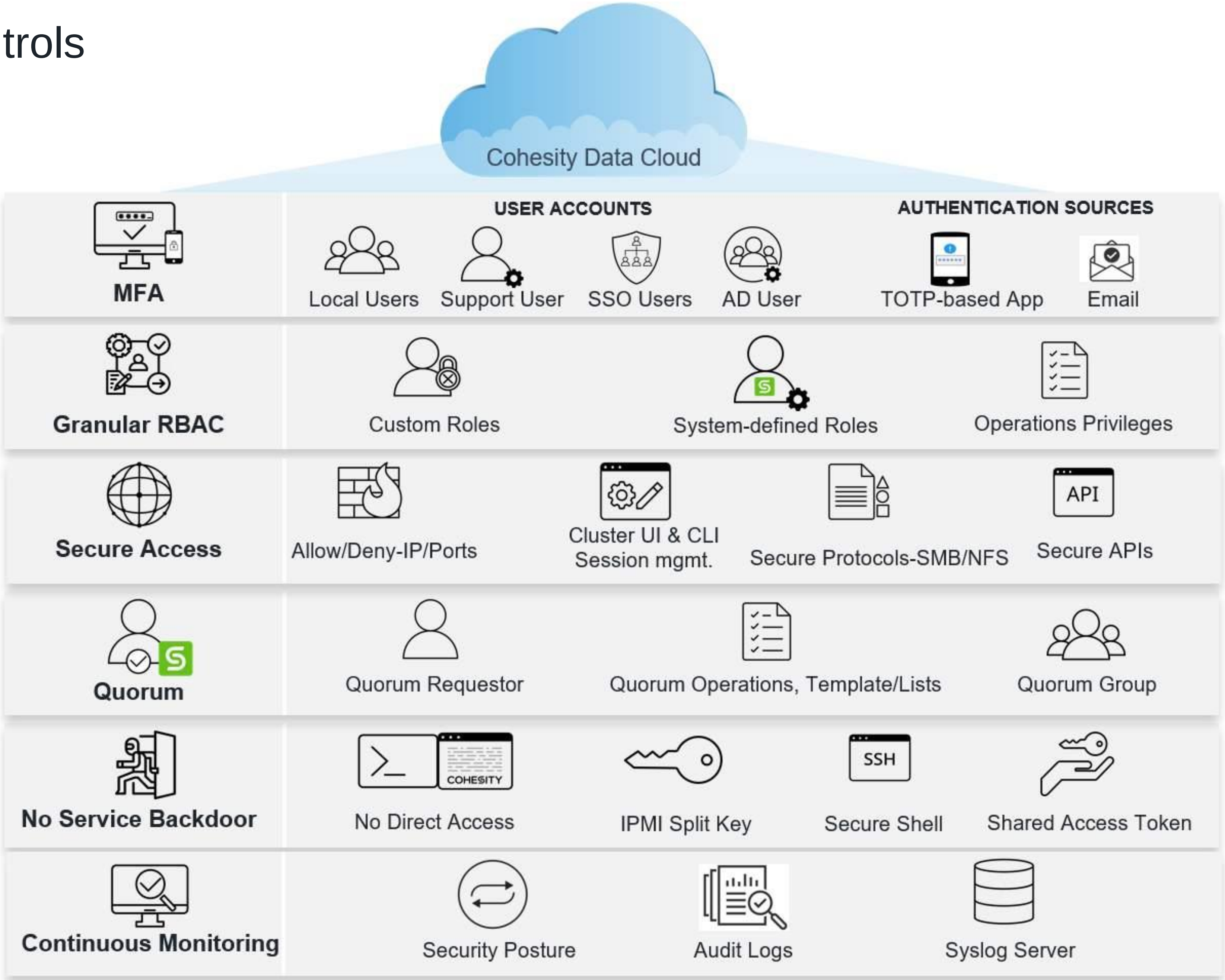
NIST

Resiliency and Hardening with Cohesity



COHESITY

Zero Trust Controls



Cohesity Data Cloud

MFA — USER ACCOUNTS: Local Users, Support User, SSO Users, AD User — AUTHENTICATION SOURCES: TOTP-based App, Email

Granular RBAC — Custom Roles, System-defined Roles, Operations Privileges

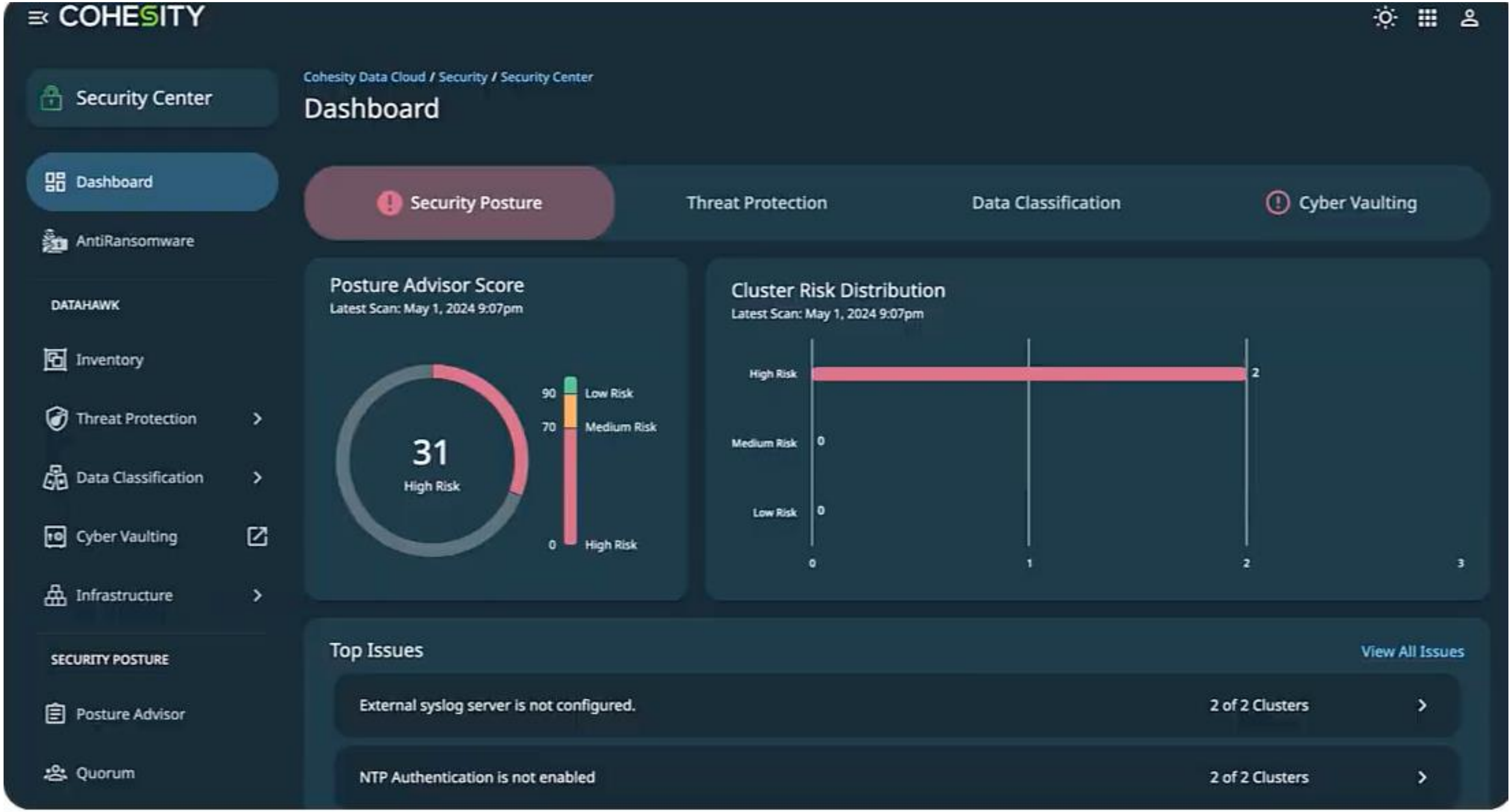
Secure Access — Allow/Deny-IP/Ports, Cluster UI & CLI Session mgmt., Secure Protocols-SMB/NFS, Secure APIs

Quorum — Quorum Requestor, Quorum Operations, Template/Lists, Quorum Group

No Service Backdoor — No Direct Access, IPMI Split Key, Secure Shell, Shared Access Token

Continuous Monitoring — Security Posture, Audit Logs, Syslog Server

Secury Dashboard / Security Posture



External syslog server is not configured. 2 of 2 Clusters

NTP Authentication is not enabled 2 of 2 Clusters

https://www.cohesity.com/demos/interactive/

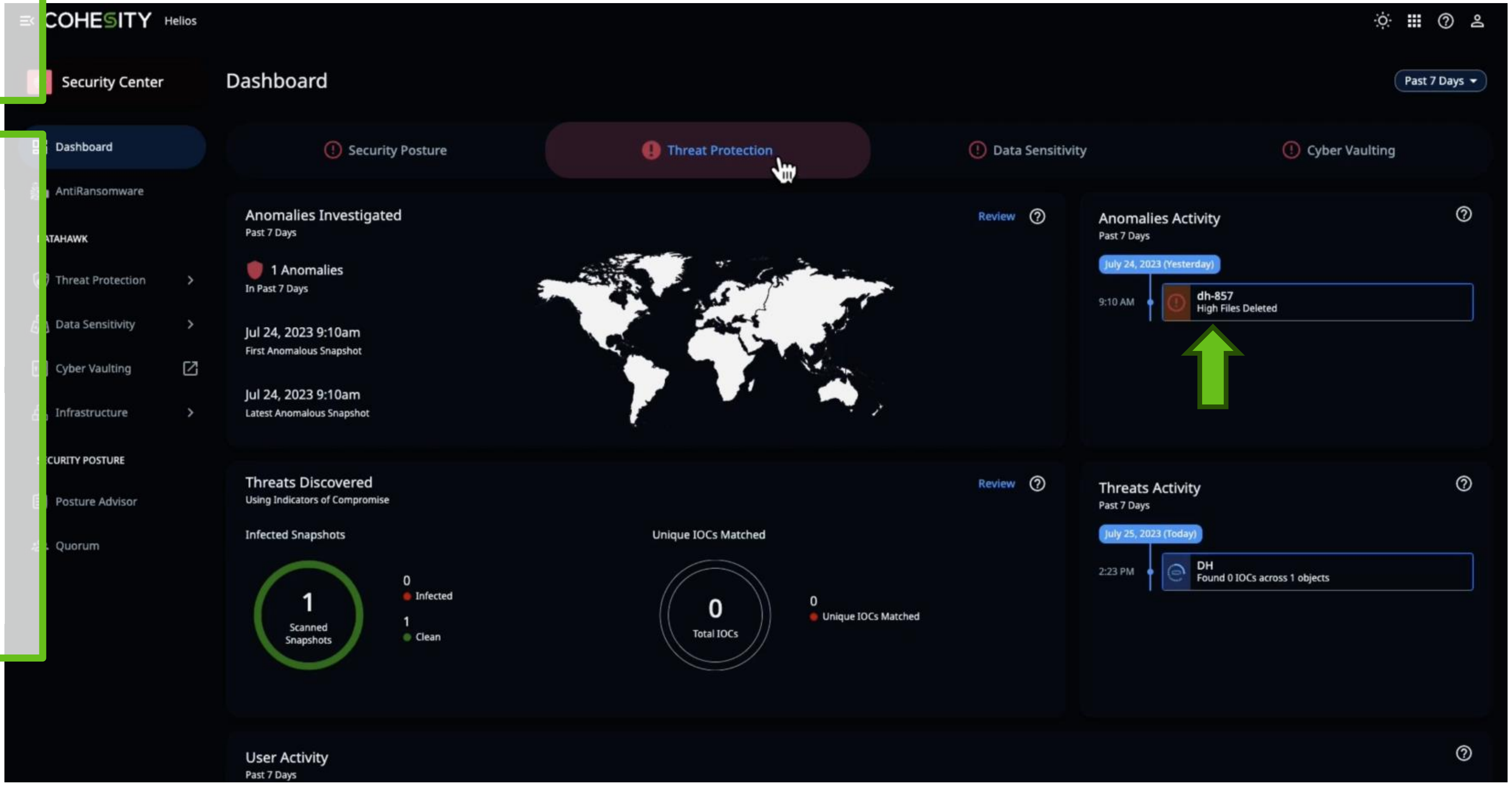
Cohesity Threat Protection

Qualys

Cohesity leverages threat feeds from Qualys to scan from over 100,000 IOCs

1 Customers can leverage all these IOCs to scan their backups

2 Threat feed is updated daily, eliminating the need for manual scanning rules and feed updates.



COHESITY Helios

Security Center

Dashboard

Past 7 Days

Anomalies Investigated
Past 7 Days

1 Anomalies
In Past 7 Days

Jul 24, 2023 9:10am
First Anomalous Snapshot

Jul 24, 2023 9:10am
Latest Anomalous Snapshot

Review

Anomalies Activity
Past 7 Days

July 24, 2023 (Yesterday)

9:10 AM dh-857
High Files Deleted

Threats Discovered
Using Indicators of Compromise

Review

Infected Snapshots

1 Scanned Snapshots

0 Infected

1 Clean

Unique IOCs Matched

0 Total IOCs

0 Unique IOCs Matched

Threats Activity
Past 7 Days

July 25, 2023 (Today)

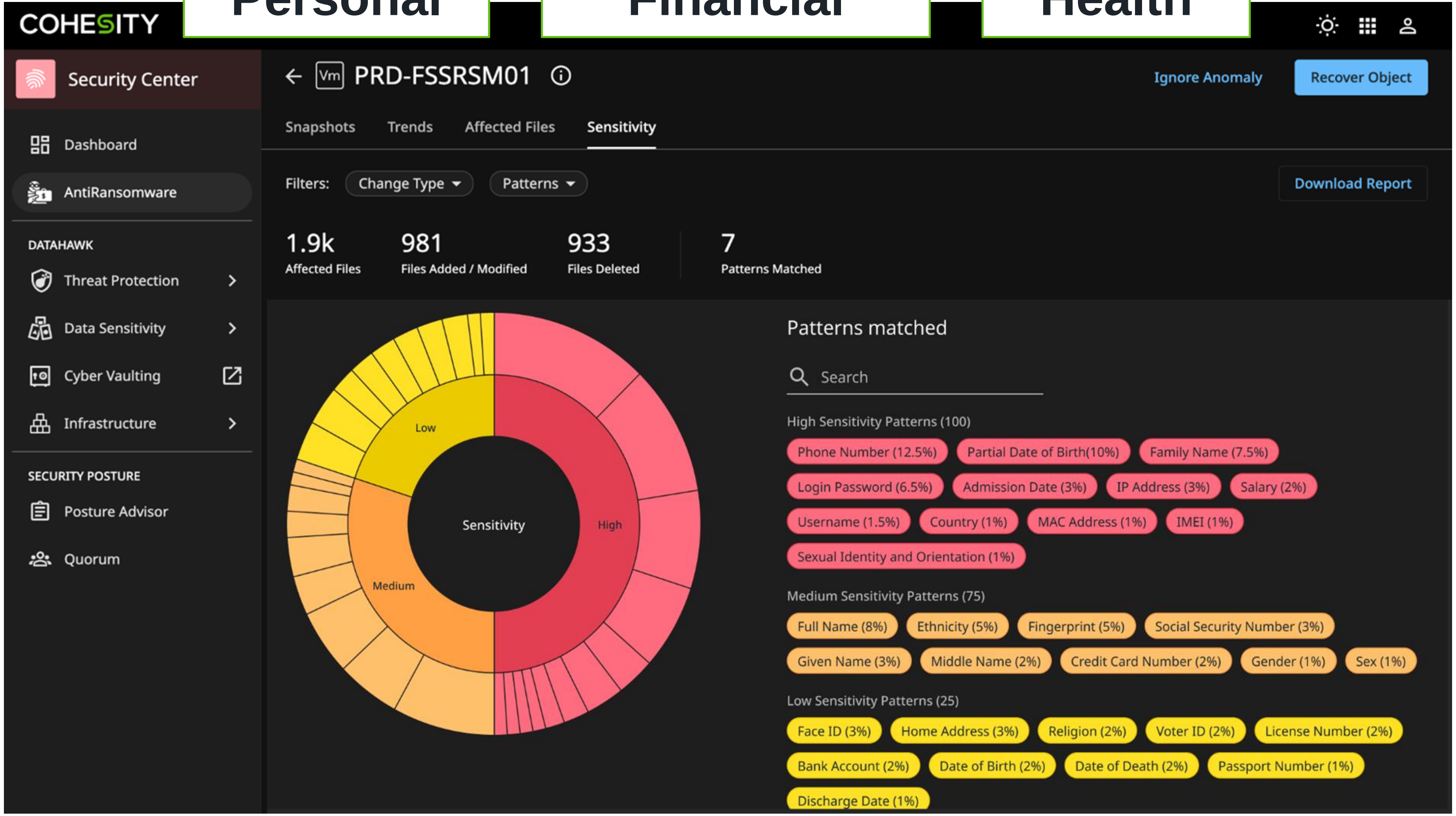
2:23 PM DH
Found 0 IOCs across 1 objects

User Activity
Past 7 Days

Advance Pattern Matching

Data Classification

Personal | Financial | Health



PRD-FSSRSM01

Filters: Change Type ▾ Patterns ▾

1.9k Affected Files

981 Files Added / Modified

933 Files Deleted

7 Patterns Matched

Patterns matched

High Sensitivity Patterns (100)

Phone Number (12.5%) | Partial Date of Birth(10%) | Family Name (7.5%) | Login Password (6.5%) | Admission Date (3%) | IP Address (3%) | Salary (2%) | Username (1.5%) | Country (1%) | MAC Address (1%) | IMEI (1%) | Sexual Identity and Orientation (1%)

Medium Sensitivity Patterns (75)

Full Name (8%) | Ethnicity (5%) | Fingerprint (5%) | Social Security Number (3%) | Given Name (3%) | Middle Name (2%) | Credit Card Number (2%) | Gender (1%) | Sex (1%)

Low Sensitivity Patterns (25)

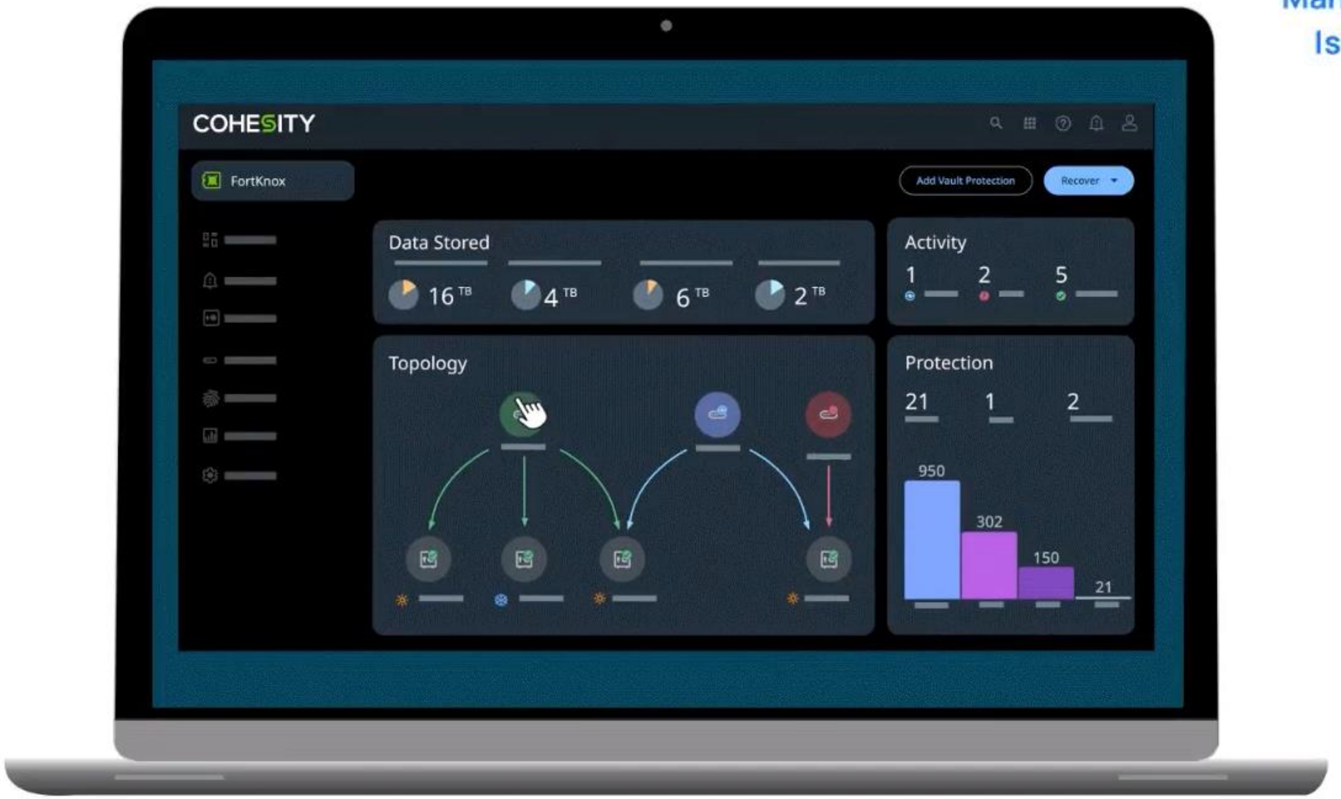
Face ID (3%) | Home Address (3%) | Religion (2%) | Voter ID (2%) | License Number (2%) | Bank Account (2%) | Date of Birth (2%) | Date of Death (2%) | Passport Number (1%) | Discharge Date (1%)

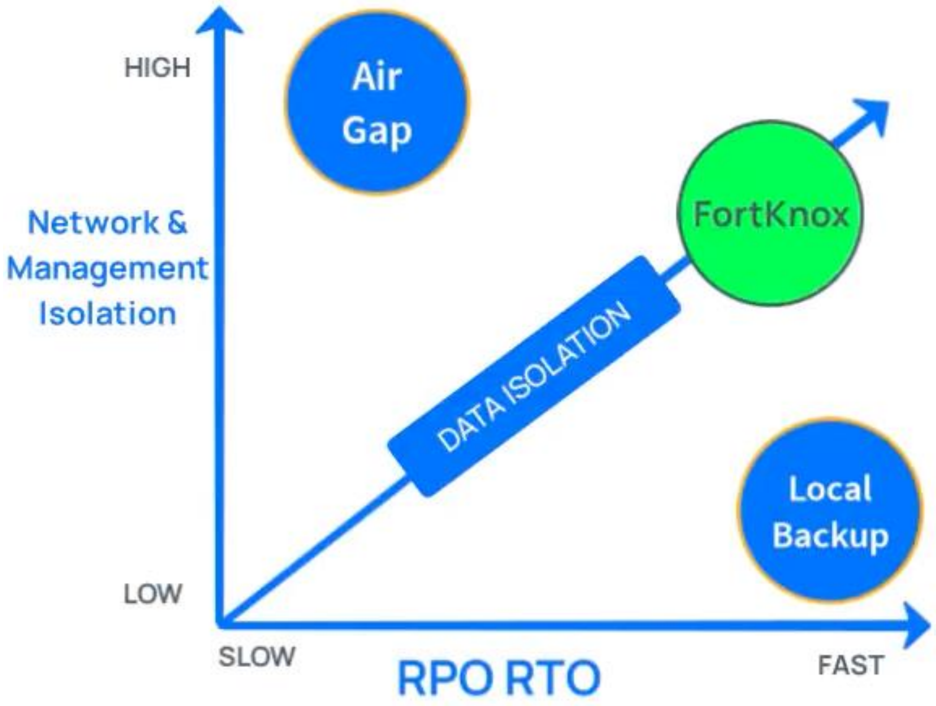
BigID

COHESITY

Data Isolation: Cohesity FortKnox

FortKnox = Fast & Secure Data Isolation
FortKnox requires Quorum

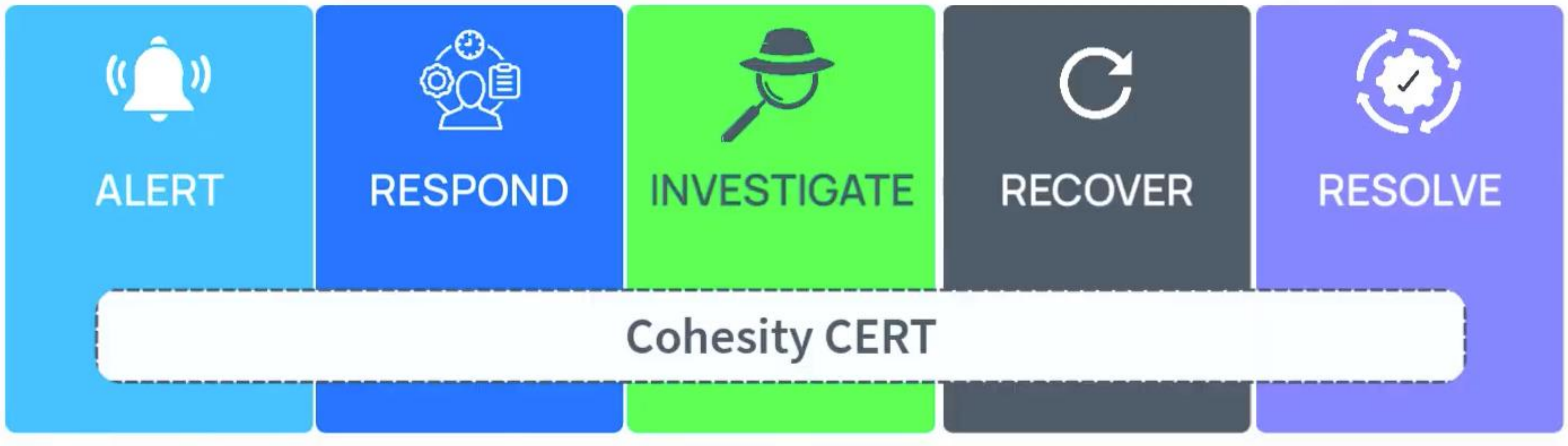




COHESITY

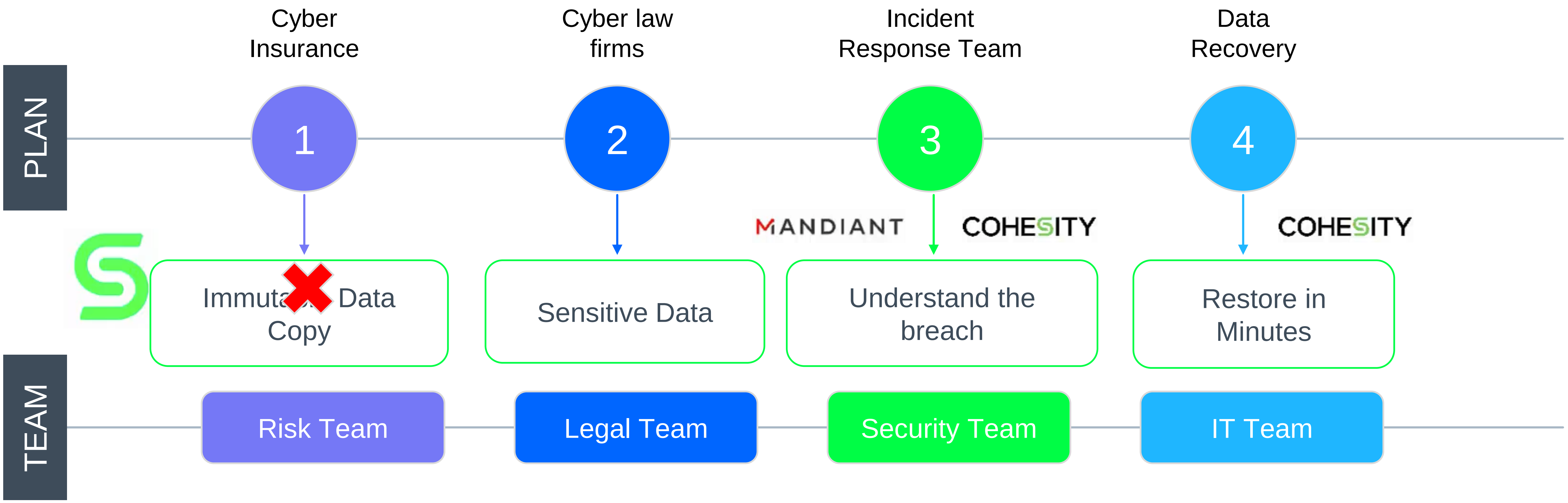
Cyber Resiliency / Navigating Cyber Events

Cyber Event Response Team



Customers should open a support case with Cohesity CERT as soon as an attack is confirmed

Effective Cyber Event Response & Risk Mitigation



PLAN

TEAM

Cyber Insurance

1

Immuta✖ Data Copy

Risk Team

Cyber law firms

2

Sensitive Data

Legal Team

Incident Response Team

3

MANDIANT

COHESITY

Understand the breach

Security Team

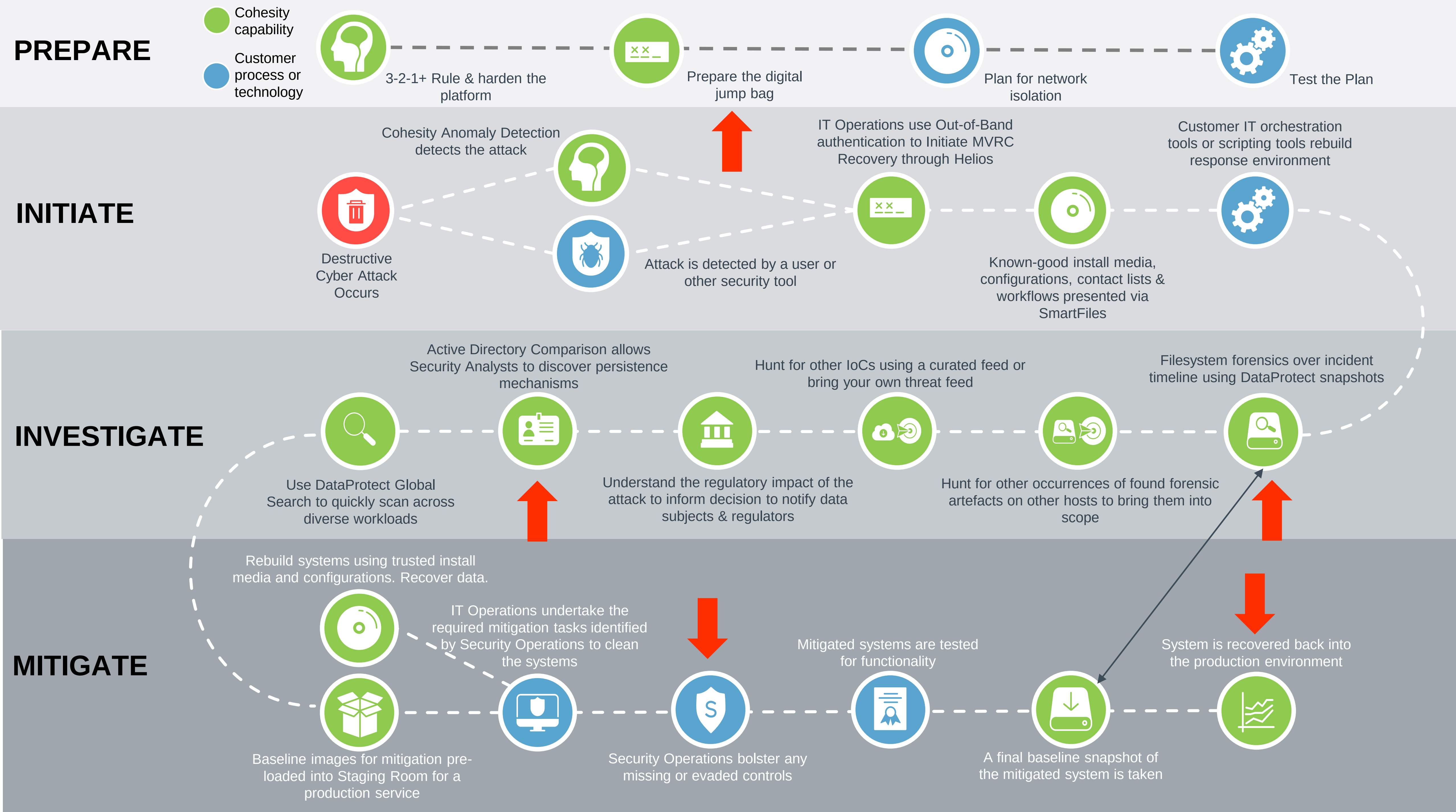
Data Recovery

4

COHESITY

Restore in Minutes

IT Team



🟢 Cohesity capability

🔵 Customer process or technology

PREPARE

3-2-1+ Rule & harden the platform

Prepare the digital jump bag

Plan for network isolation

Test the Plan

INITIATE

Destructive Cyber Attack Occurs

Cohesity Anomaly Detection detects the attack

Attack is detected by a user or other security tool

IT Operations use Out-of-Band authentication to Initiate MVRC Recovery through Helios

Known-good install media, configurations, contact lists & workflows presented via SmartFiles

Customer IT orchestration tools or scripting tools rebuild response environment

INVESTIGATE

Use DataProtect Global Search to quickly scan across diverse workloads

Active Directory Comparison allows Security Analysts to discover persistence mechanisms

Understand the regulatory impact of the attack to inform decision to notify data subjects & regulators

Hunt for other IoCs using a curated feed or bring your own threat feed

Hunt for other occurrences of found forensic artefacts on other hosts to bring them into scope

Filesystem forensics over incident timeline using DataProtect snapshots

MITIGATE

Rebuild systems using trusted install media and configurations. Recover data.

Baseline images for mitigation pre-loaded into Staging Room for a production service

IT Operations undertake the required mitigation tasks identified by Security Operations to clean the systems

Security Operations bolster any missing or evaded controls

Mitigated systems are tested for functionality

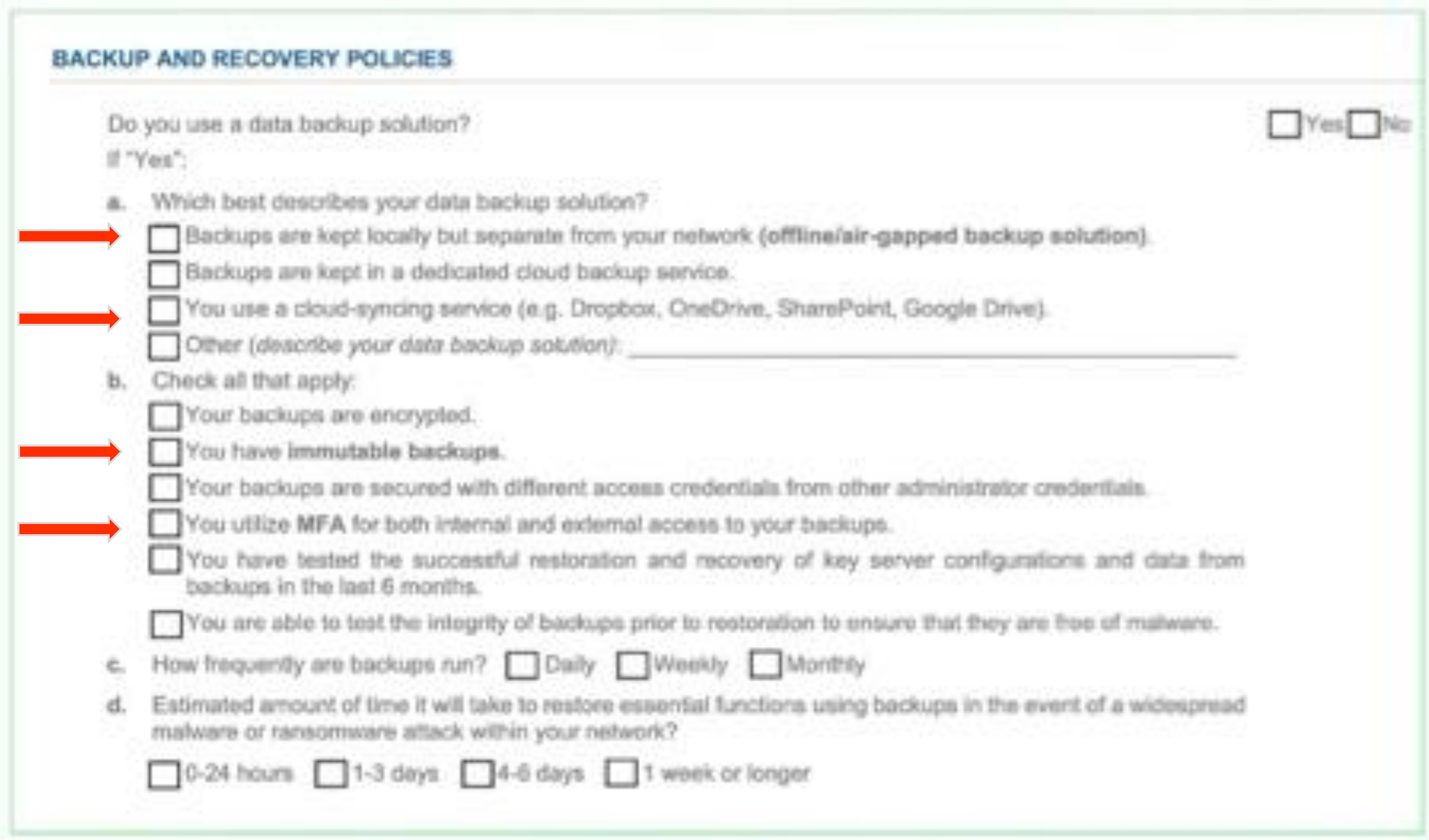
A final baseline snapshot of the mitigated system is taken

System is recovered back into the production environment

Call to Action / Házi feladat!

COHESITY

Cyber Insurance form



BACKUP AND RECOVERY POLICIES

Do you use a data backup solution? □Yes □No

If "Yes":

a. Which best describes your data backup solution?

□ Backups are kept locally but separate from your network **(offline/air-gapped backup solution)**.

□ Backups are kept in a dedicated cloud backup service.

□ You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive).

□ Other *(describe your data backup solution)*: ____________________

b. Check all that apply:

□ Your backups are encrypted.

□ You have **immutable backups**.

□ Your backups are secured with different access credentials from other administrator credentials.

□ You utilize **MFA** for both internal and external access to your backups.

□ You have tested the successful restoration and recovery of key server configurations and data from backups in the last 6 months.

□ You are able to test the integrity of backups prior to restoration to ensure that they are free of malware.

c. How frequently are backups run? □ Daily □ Weekly □ Monthly

d. Estimated amount of time it will take to restore essential functions using backups in the event of a widespread malware or ransomware attack within your network?

□ 0-24 hours □ 1-3 days □ 4-6 days □ 1 week or longer

Házi feladat: A mentésekkel kapcsolatban:

1. Használnak MFA-t ? (Ha van, de nem, akkor lsz kapcsoljátok be!)

2. Használnak multi-person authorizációt / quorum-ot a kritikus műveletekhez ?
   Képes lenne erre a mentő software-ük?

3. Van WORM másolatuk az adatokról ? (Ha van lehetőség, akkor lsz kapcsoljátok be, felhőbe is!)

4. Képes a mostani tárolójuk Immutable adattárolásra ? SmartFiles!

5. Van külső helyszínen másolatuk az adatokról (air-gap) ?

Házi feladat: A mentésekkel kapcsolatban:

1. Van-e leírt / átbeszélt Ransomware helyreállítási terv?

2. Van-e összekészítve egy “digital jumpbag” ? Cohesity SmartFiles!
   - Az alap SW csomagok, amivel fel lehet majd építeni egy tiszta szobát a sérülés megértésére.
   - Amiben benne vannak a minimiálisan szükséges rendszerek a válaszadásra
   - Kommounikációs csomagok

3. Kapnak segítséget Ransomware helyzetben a gyártótól? (Cohesity CERT team)

4. Helyreállítási folyamathoz van-e elképzelés? (Cohesity Celan Room solution)

Érdekes olvasnivaló

Use Cohesity for Your Veeam Backup Repository
https://docs.cohesity.com/HomePage/PDFs/Cohesity-Solution-Guide-Veeam-Backup-Repository.pdf
(Ratmir Timashev – Object First)

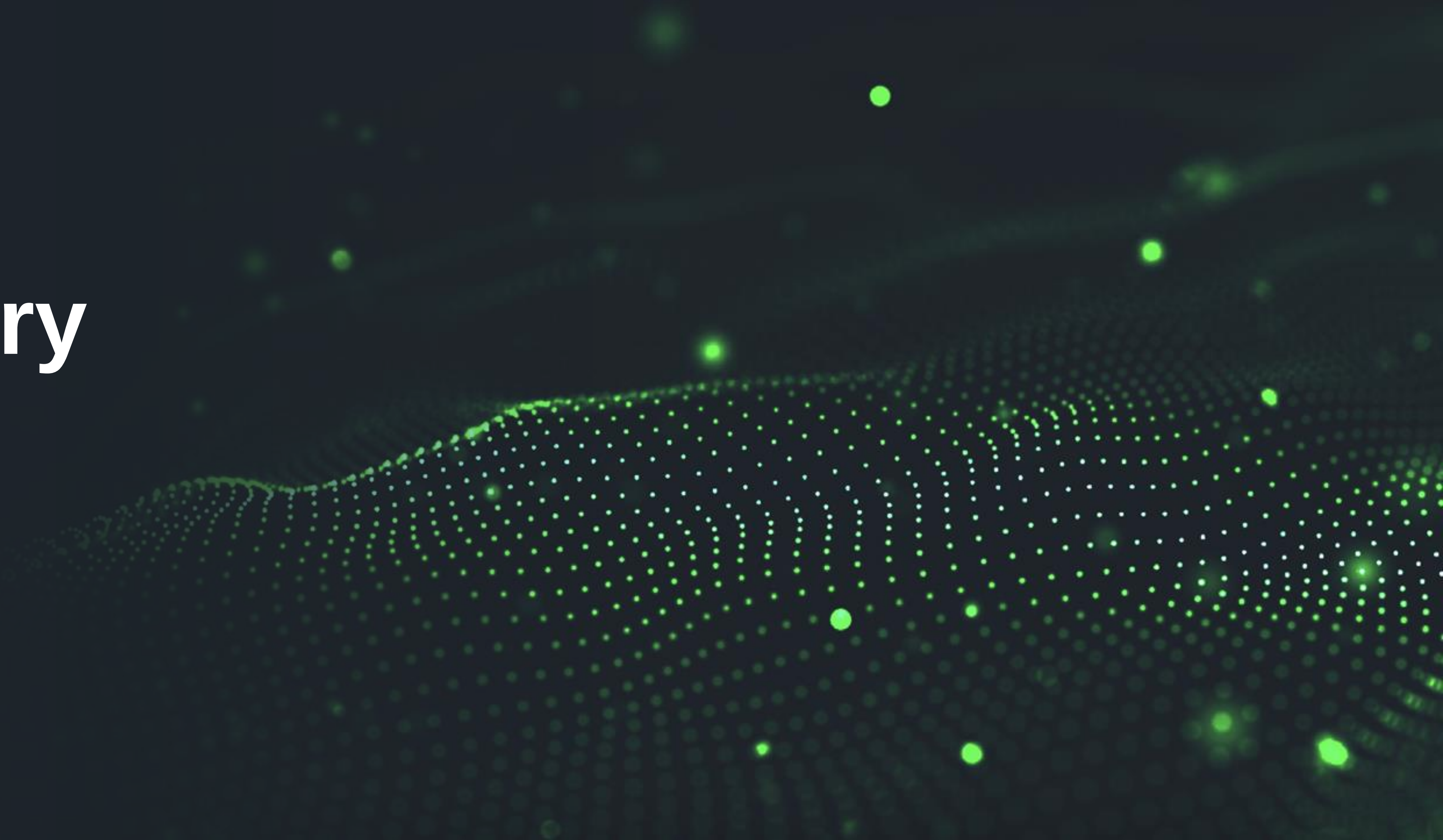
Use Cohesity for Your Commvault Storage Libraries
https://docs.cohesity.com/HomePage/PDFs/Cohesity-Solution-Guide-CommVault.pdf

Use Cohesity as HPE NonStop Systems Backup Repository
https://docs.cohesity.com/HomePage/Content/ExternalFiles/TechGuides/Cohesity-Solution-Guide-HPE-NonStop-Systems-Backup-Repository.pdf

Use Cohesity for Your IBM Spectrum Protect Storage Pools
https://docs.cohesity.com/HomePage/PDFs/Cohesity-Solution-Guide-IBM-Spectrum-Protect.pdf

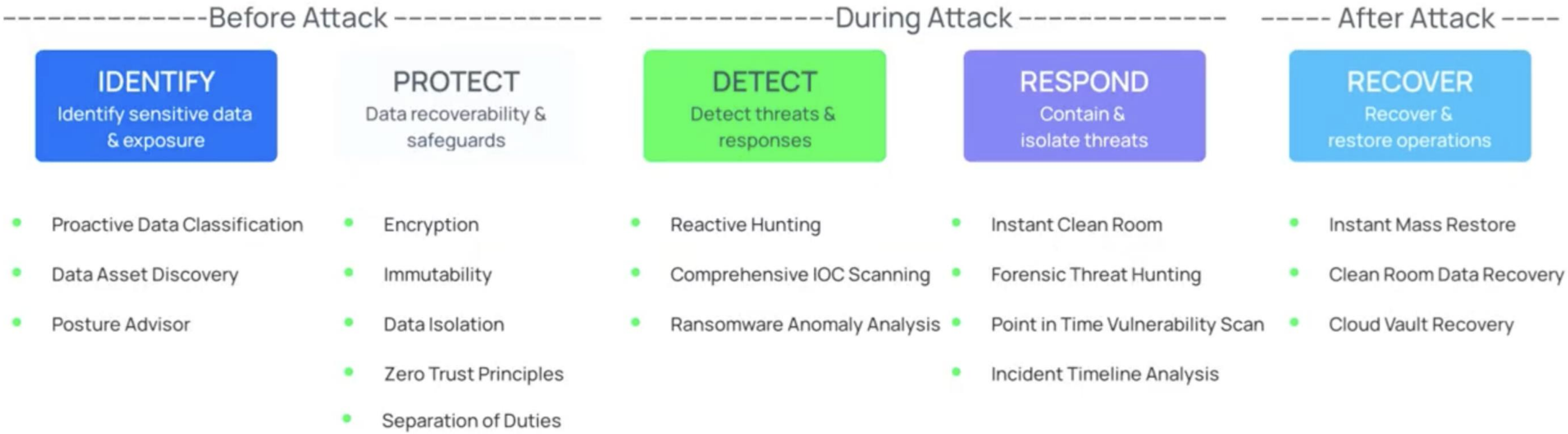
COHESITY

Summary



RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
NIST
CYBERSECURITY FRAMEWORK

Cohesity’s Team Sport Approach to Modern Data Security



-------------Before Attack -------------

IDENTIFY
Identify sensitive data & exposure

- Proactive Data Classification
- Data Asset Discovery
- Posture Advisor

PROTECT
Data recoverability & safeguards

- Encryption
- Immutability
- Data Isolation
- Zero Trust Principles
- Separation of Duties

-------------During Attack -------------

DETECT
Detect threats & responses

- Reactive Hunting
- Comprehensive IOC Scanning
- Ransomware Anomaly Analysis

RESPOND
Contain & isolate threats

- Instant Clean Room
- Forensic Threat Hunting
- Point in Time Vulnerability Scan
- Incident Timeline Analysis

----- After Attack ----

RECOVER
Recover & restore operations

- Instant Mass Restore
- Clean Room Data Recovery
- Cloud Vault Recovery

COHESITY

Cohesity Data Cloud Delivers Superior Outcomes

Speed

Decreased backup times by **45%**

10x faster data recovery times compared to legacy infrastructure

97% faster file restores

Security

$0 ransomware paid in multiple cases

$2M saved in cyber insurance costs

17% more threats detected

Scale

Support **40K+** M365 users

Billions of objects

Multi-PB cloud cyber vaulting

Protection for VMware, Oracle, Physical & SAP HANA at **PB scale**

Simplicity

Retire **18** systems in favor **1** modern platform

Each FTE manages **63%** more VMs

36% more efficient security and backup teams

Smarts

48% less time to remediate threats

45% less staff time to detect threats

26% more productive compliance teams

Source: Customer case studies, IDC

COHESITY

Thank You

COHESITY