

COHESITY

**Adatvédelem újragondolva:
reziliencia, egyszerűség és AI a vállalati
adatok mögött**

andras.pulai@cohesity.com
Fsas Technologies Day

Az MI-alapú adatbiztonság vezetője

Our Mission: *A világ adatának: védelme és biztonságossá tétele. Kereshetőség.
A világ legnagyobb vállalatainak biztosítunk hibatűrést!*

Erre fókuszálunk:

Data Protection

- Sokféle adatforrás
- Nagyvállalati skálázódás
- Rugalmas licenclés

Data Security

- Ultra-gyors Threat észlelés
- Posture Management
- Egyszerű kibervédelem

Data Insights

- GenAI fájl adatokra
- Keresés & analízálás
- reporting

Ezt értük el:

\$1.7B
bevétel

**100+
EBs**
védett adat

1600
Patents

2x
K+F a
legközelebbi
versenytárhoz
képest

19.4%
pical
részesedés
(vezető)

140
helyen a
világon

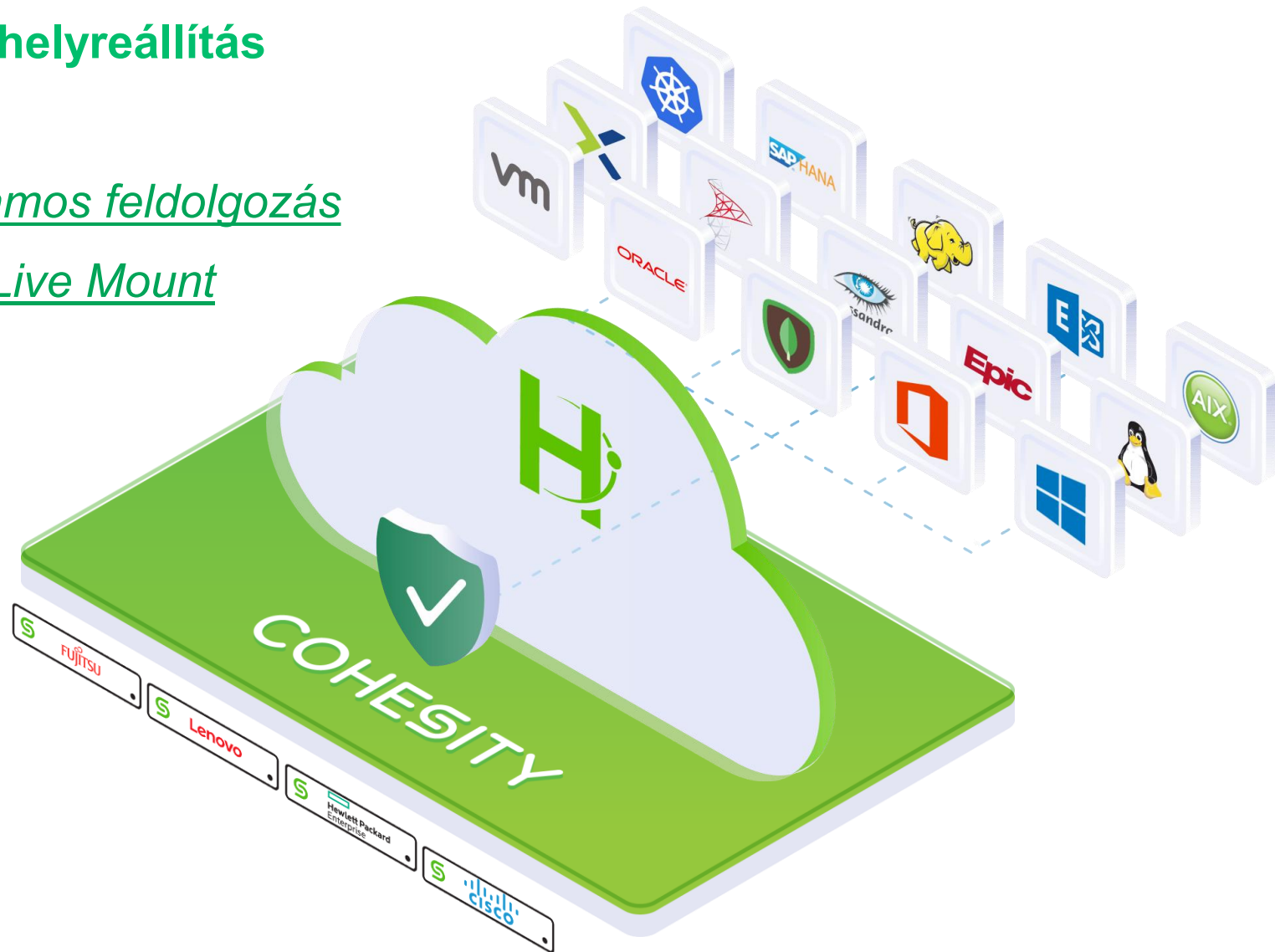
12000
ügyfél

3000
partner

Leader
Gartner MQ

Cohesity Data Protect

- Radikálisan egyszerű mentés és helyreállítás
- Házirend alapú automatizálás
- Gyors elosztott mentés – Párhuzamos feldolgozás
- Azonnali tömeges visszaállítás – Live Mount
- Zero Trust képességek (titkosítás, nem-módosítható adatok, SoD, RBAC, MFA, törlés elleni védelem, stb.)
- Anomália észlelés
- Fenyegetettségek megfogása – Snapshot és fájl szinten
- Előfizetesként vagy SAAS-ként elérhető



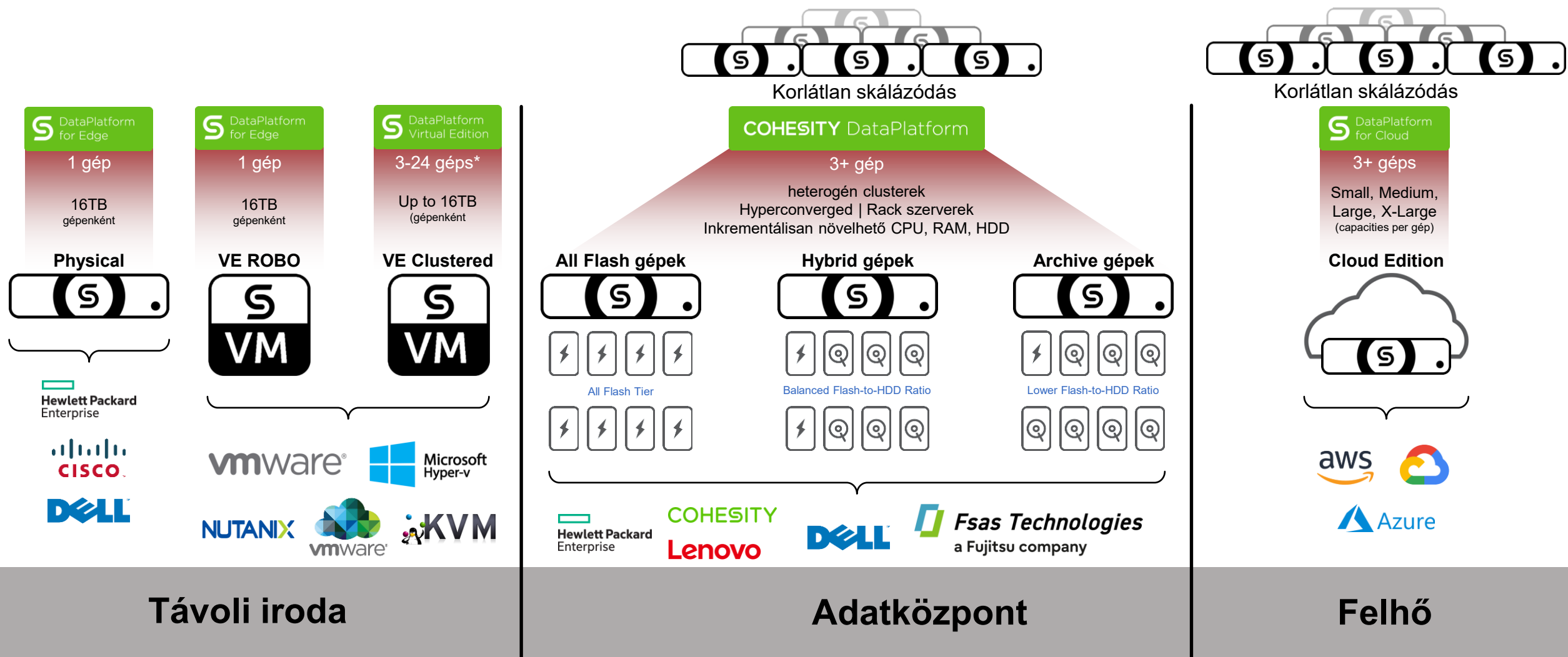
Cohesity Smart Files

= Fájl- és objektumtárolás

- **Software Defined**
 - Korlátlan skálázódás
- **Optimalizált hatékonyság**
 - Kapacitás és adatkezelés
- **Multiprotocol támogatás**
 - NFS, SMB, S3, Public Clouds
- **Könnyen kezelhető**
 - Szabályzat-alapú és egységes menedzsment
- **Beépített adatkezelés**
 - Elemzés, keresés, migráció, adat klasszifikáció, archiválás
- **Integrált alkalmazások**
 - Clusteren futtatható külön appok



Cohesity Data Platform: Kiváló skálázódás és rugalmasság



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



Áttekintés a platformról

További
építőelemek

Data



Analytics & Insights



Infrastructure



Mobility



Encryption



Adatbiztonsági
ökoszisztéma

Data Security Posture Management



Data Loss Prevention



Threat Feeds



SIEM / SOAR / XDR



Vulnerability Management



Identity Access Management



Managed Security Services



Data Platform



Cohesity Data Cloud

MI-alapú adatbiztonsági és menedzsment platform

Forrás
rendszerek

Virtual & Physical



Storage



Databases / NoSQL



Clouds / SaaS Apps

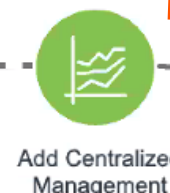
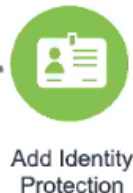




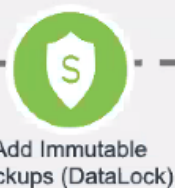
Cyber Resilience

Protect Data

-  Cohesity capability
-  Cohesity scanner
-  Customer process or technology



Ensure Recoverability



Detect Threats



Practice Recovery



Reduce Data Risk



Egyszerű kezelőfelület / mentési házirendek

Cluster
← US-NYC-01

Dashboards

Data Protection

Protection

Recoveries

Sources

Policies

Runbooks

Infrastructure

SmartFiles

Test & Dev

Marketplace

Policies

Target Type

Policy ↑	Protection Groups	Protected Objects	Backup
Bronze Backup 1d Retain 30d DataLock 30d	0	0	
Gold Backup 4h Retain 1w DataLock 1w	0	0	
MVRC - Dial Tones Backup 1d Retain 2w DataLock 2w Replicate Cloud Vault	9	64	
Protect Once Retain 2w Backup One Time	0	0	
Silver Backup 12h Retain 2w DataLock 2w	0	0	
Tiered Protection - Replicate and Archive Backup 1d Retain 2w DataLock 3d Archive	2	0	
Vaulting Policy - US East Backup 1d Retain 2w DataLock 3d Archive Cloud Vault	8	5	

Target Type ▾

🔍

Mentési házirendek

WORM funkció: 

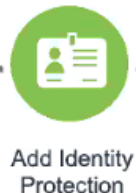
Törlés is tiltva van:

DataLock 1w

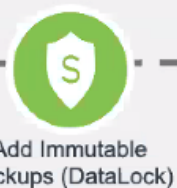
Policy ↑	
	Bronze  Backup 1d Retain 30d DataLock 30d
	Gold  Backup 4h Retain 1w DataLock 1w
	MVRC - Dial Tones  Backup 1d Retain 2w DataLock 2w Replicate Cloud Vault
	Protect Once Retain 2w Backup One Time
	Silver  Backup 12h Retain 2w DataLock 2w
	Tiered Protection - Replicate and Archive  Backup 1d Retain 2w DataLock 3d Archive
	Vaulting Policy - US East  Backup 1d Retain 2w DataLock 3d Archive Cloud Vault

Protect Data

-  Cohesity capability
-  Cohesity scanner
-  Customer process or technology



Ensure Recoverability



Detect Threats



Practice Recovery



Reduce Data Risk



Az AD sebezhetőségeket biztosan ki fogják használni

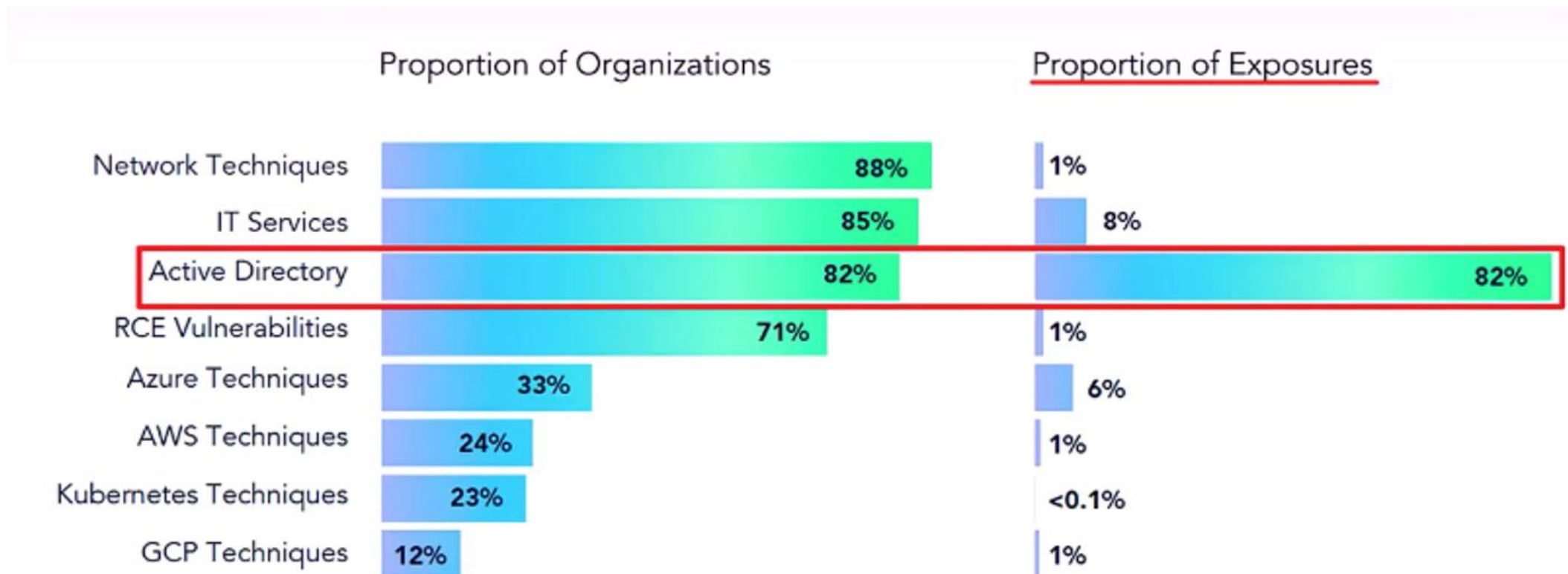


Figure 8: Categories of techniques targeting exposures identified by attack path analysis

Forrás: "Navigating the Paths of Risk: The State of Exposure Management in 2023"

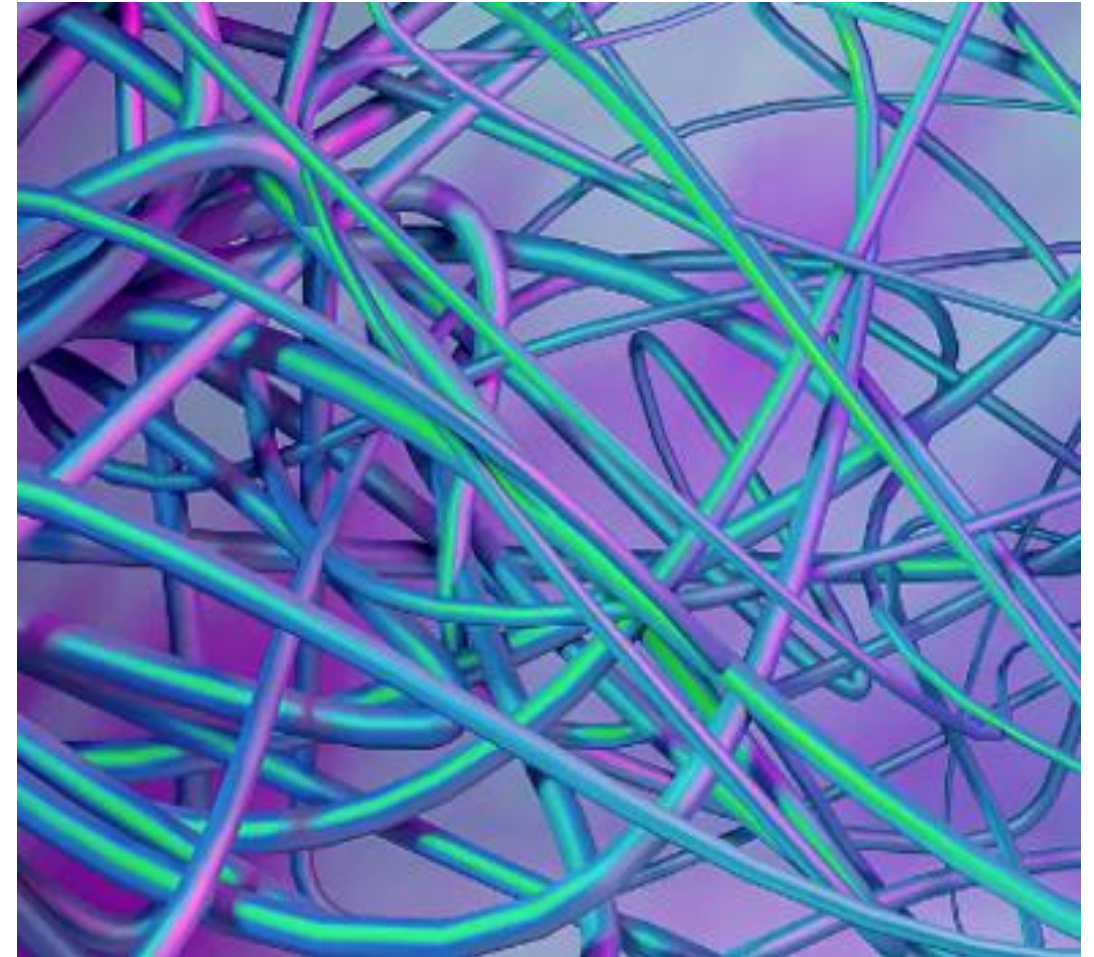
Változó konfiguráció → Növekvő támadási felület

Egy szokásos AD forest elhamarkodott döntések évtizedes gyűjteménye...

- Évtizedek óta működik
- Kicsit több jog mint kellene, hogy működjön
- Nincs felügyelet:

Ha valami elavult – jó eséllyel bent marad

Ez mind növeli a támadási felületet



Active Directory Forest helyreállításának lépései

1. Húzd ki a hálózati kábeleket minden DC-ről, vagy kapcsold ki a hálózatot
2. Kapcsold a DC-eket a visszaállításhoz egy privát hálózatba (Ő, igen – globális privát VLAN-t hozz létre)
3. Minden doménre: Az első írható DC nem jogos visszaállítása
4. Hitelesítés visszaállítása a SYSVOL-ról azon a DC-n
5. Remediate malware
6. Nullalázz vissza az összes adminisztrátori fiók jelszót
7. FSMO-k lefoglalása
8. Minden írható DC metaadat-tisztítása, kivéve a célzott magerdő DC-eket
9. DNS konfigurálása az erdőgyöker DC-n
10. Távolítsd el a globális katalógust minden DC-ről. (Várj a globális katalógus eltávolítására)
11. Töröld a DNS NS rekordokat azokról a DC-kről, amelyek már nem léteznek
12. Töröld a DNS SRV rekordokat azokról a DC-kről, amelyek már nem léteznek
13. Emeld a rendelkezésre álló RID poolok értékét 100 ezreccsel
14. Érvénytelenítsd a jelenlegi RID poolt minden DC-re
15. Kétszer is visszaállítsd a root DC számítógépes fiókját
16. Kétszer is reset **krbtgt** fiókot (Ekkor már magerdő van)
17. Windows idő konfigurálása
18. Hozzáadj GC-t egy DC-hez minden OS verzióhoz minden domainben (várj a GC-k létrejöttésére)
19. Készíts biztonsági mentést az összes DC-ről a magerdőben
20. Hozz létre egy IFM csomagot minden OS verzióhoz, minden domainben futnak a DC-k
21. Építsünk magerdőt további DC-kkel a 0. / 1. szintű műveletek támogatására
22. Minden DC-t a magerdővé való áthelyezés esetén: Tisztítsd meg a (korábbi) DC-t /FORCEREMOVAL segítségével, vagy építsd újra az operációs rendszert
23. IFM csomag küldése a szervernek (várj...)
24. Vegyék le a DC-t a nyilvános hálózatról, és tedd fel a magerdő hálózatra.
25. Futtass egy DCPROMO IFM-et (Napok telnek el, amíg tisztítod és újjáépíted a DC-eket) (Most már elég nagy erdőd van az alapvető műveletekhez)
26. Ellenőrizd a teljes erdő egészségét
27. A helyreállított erdő áthelyezése vállalati hálózatba
28. Indítsd újra az összes szervert és klienst, hogy kényszerítsd a kommunikációt az új erdővel

Fontos szempontok



A kézi helyreállítás hajlamos

hibare, és gyakran további ciklusokat igényel a hibák kijavításához, ami tovább hosszabbítja az idővonalat



Szükséges személyzet a manuális AD

erdőhelyreállításhoz:

Core AD csapat, minden adatközpont operátorai, valamint egyéb külső támogatás
(Becslések szerint 10-15 IT támogató dolgozó áll az átlagos vállalati területen)

Az általános mentés csak a 3. lépést automatizálja, így a helyreállítási folyamat többi része többnyire manuális feladat



Ez a legfontosabb különbség

Cohesity Identity Resilience esetén:

Napok vagy hetek helyett percek

Teljesen automatizált Forest helyreállítás - elkerülve az emberi hibákat,
90%-kal csökkentve az állásidőt ,
és megszüntetve az újrafertőződés kockázatát.

Az ADFR 7 kattintásos AD helyreállítása:

1. Kattints a **Recover** gombra
2. Indítsa el az erdőhelyreállítást
3. Biztonsági készletek listázása
4. Válaszd ki a **Backup Set** a visszaállításhoz
5. Kattints **Folytatás** gombra
6. Kattints **Folytatás** gombra
7. Kattints a **Helyreállítás indítására**

A Semperis ADFR-hez
Csak 1-2 AD admin kell

Active Directory ellenálló képesség növelése

Active Directory Forest Recovery



Csökkenti az AD helyreállítási idejét
Biztosítja az üzlet folytonosságát egy erős helyreállítási stratégiával.

- Autamtikus, gyors, kiekrüli az emberi hibákat,
- megváltoztathatatlan mentéseket használ
- több Forest helyreállítása néhány óra alatt.
- Malware kiszűrése
- A betörési utáni elemzések / vizsgálatok felgyorsítása az újrafertőzés megelőzése érdekében.

Forest Druid (OPEN)



Proaktívan azonosítsuk és zárjuk kritikusan támadási útvonalakat

- Zárja a támadási vektorokat, amelyek a 0-as szintű elemeket célozzák meg.
- Pontos azonosítjuk melyek a valódi 0. szintű elemek.
- Hatékonyan csökkenti a túlzott jogosultságokat az AD-n belül.
- A támadási lehetőségeket a súlyosság alapján rangsoroljuk, nem azok gyakorúsága szerint.
- Monitorozza a kritikus Active Directory komponenseket.

Purple Knight (NYITOTT)



Kiértékeli és segít javítani az Active Directory biztonsági állapotát.

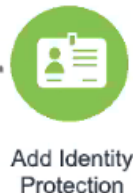
- Átfogó auditokat végez az Active Directory sebezhetőségeket keresve
- A community által megismert AD fenyegetéseket tudjuk használni.
- Hozzáférés AD biztonsági tanácsokhoz a Semperis szakemberektől.
- Azonosítja azokat a hibás konfigurációkat, amelyek gyakori támadási módszerekhez sikerességéhez vezetnek.



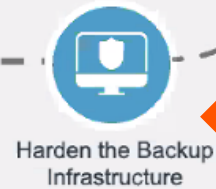
<https://www.cohesity.com/forms/semperis-purple-knight/>

Protect Data

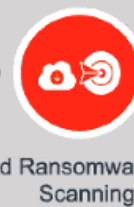
-  Cohesity capability
-  Cohesity scanner
-  Customer process or technology



Ensure Recoverability



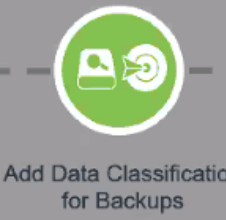
Detect Threats



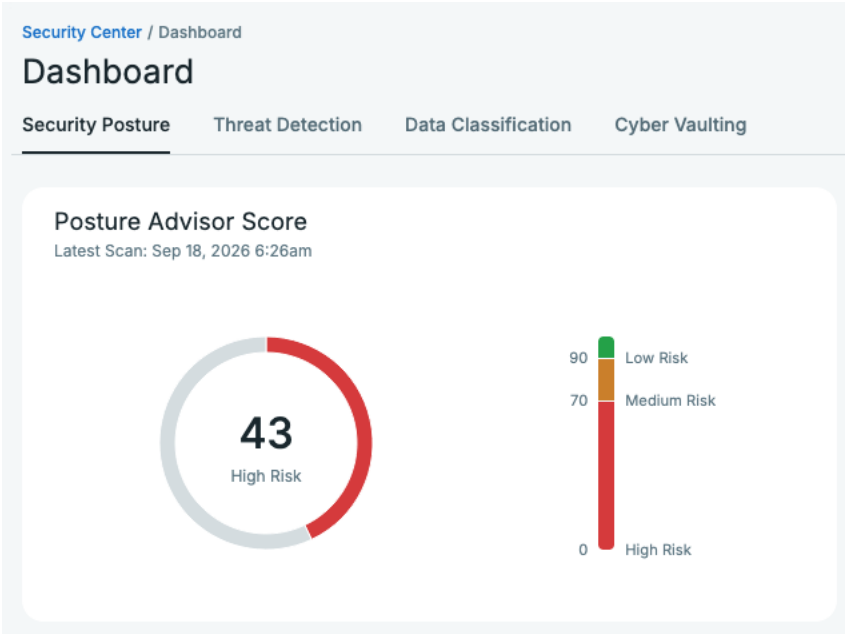
Practice Recovery



Reduce Data Risk



A backup rendszer megerősítése / hardening



Security Posture –
áttekintés, hogyan is állunk

Top Issues – mire kell odafigyelni

Top Issues

[View All Issues](#)

Support User Two-factor authentication is not enabled.	8 of 8 Clusters	>
External syslog server is not configured.	6 of 8 Clusters	>
Audit Log retention period is less than 6 months.	6 of 8 Clusters	>
Sudo access for support user is not disabled.	4 of 8 Clusters	>
Login banner is not enabled. It is displayed before login.	3 of 8 Clusters	>

Vaulting

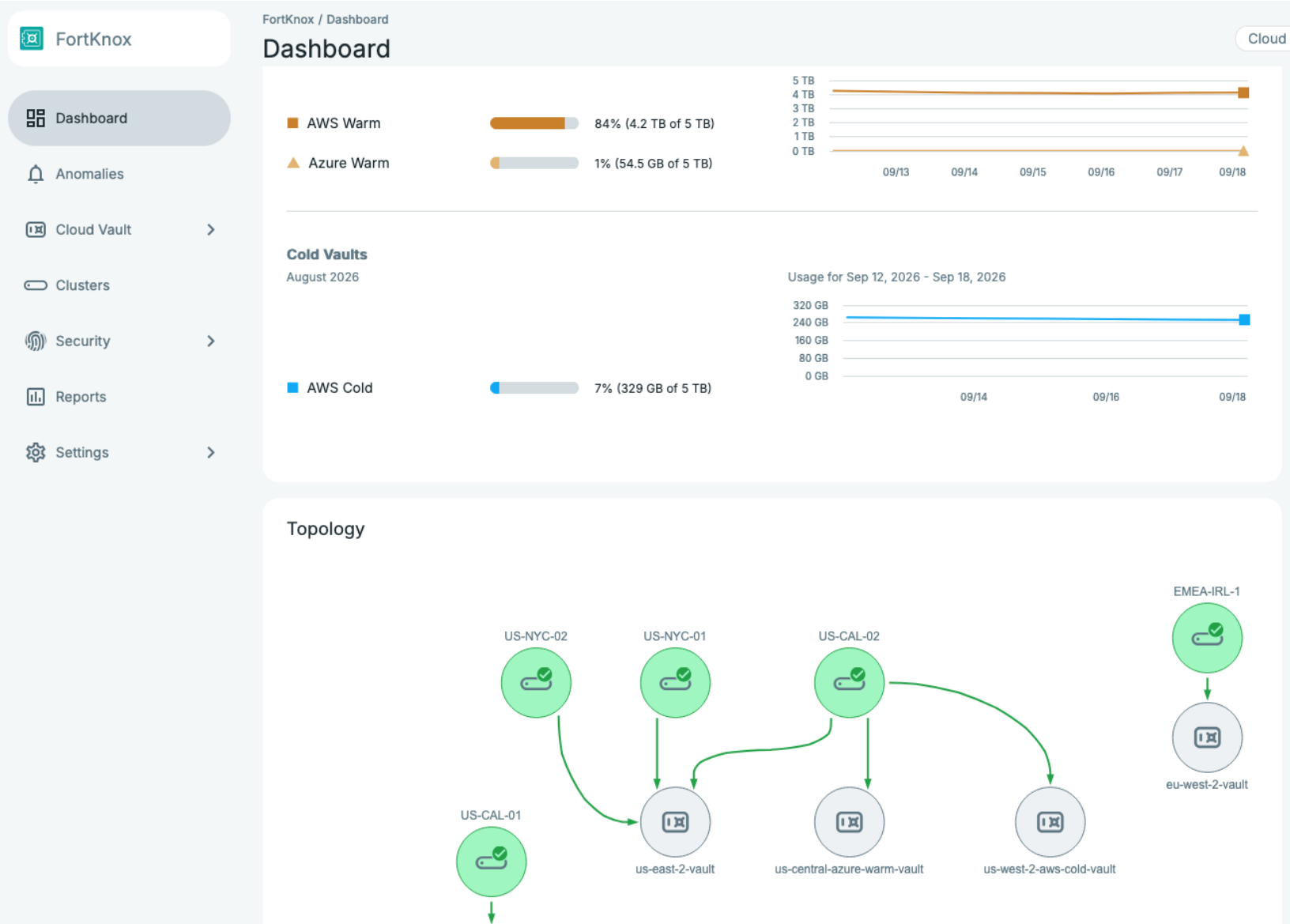


Vaulting

Adat külön zónában

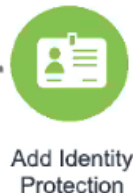
- Földrajzilag
- Authentikációs szempontból

Multi-Person
Authorizáció

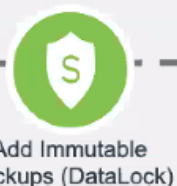


Protect Data

-  Cohesity capability
-  Cohesity scanner
-  Customer process or technology



Ensure Recoverability



Detect Threats



Practice Recovery



Reduce Data Risk



Anomaly Detection

Summary

Rules

Dashboard

Anomaly Detection

Inventory

Threat Detection >

Data Classification >

Cyber Vaulting 

Scan Order Configuration

Security Posture >

Sensitive Data Posture

User Activity >

Integrations

REDLab News

Alerts

Audit Logs

Systems with Affected Objects



Objects with Anomalous Snapshots

Filters:

Object Type ▾

System ▾

☐ Object	System	Anomalous Snapshot ↓	Anomaly Strength	Threat Detection
☐  core-apps-NYC-Win-284 Source: vCenter-US-NYC-01.hellosdemo.local	US-NYC-02	Sep 15, 2026 4:10am	 28%	 3 Threats
☐  core-apps-NYC-Win-581 Source: vCenter-US-NYC-01.hellosdemo.local	US-NYC-02	Sep 11, 2026 4:16am	 22%	No Scan
☐  core-apps-NYC-Win-715 Source: vCenter-US-NYC-01.hellosdemo.local	US-NYC-02	Sep 10, 2026 4:10pm	 33%	 6 Threats
☐  core-apps-NYC-Win-956 Source: vCenter-US-NYC-01.hellosdemo.local	US-NYC-02	Sep 10, 2026 4:11am	 29%	 6 Threats
☐  core-apps-NYC-Win-844 Source: vCenter-US-NYC-01.hellosdemo.local	US-NYC-02	Sep 9, 2026 4:14pm	 23%	No Scan

Az észlelt anomáliák miatt automatikusan indul egy threat-scan

core-apps-NYC-Win-715

Anomalous Snapshot: Sep 10, 2026 4:10pm

[Recover](#)

Dashboard

Anomaly Detection

Inventory

Threat Detection >

Data Classification >

Cyber Vaulting 

Scan Order Configuration

Security Posture >

Sensitive Data Posture

User Activity >

Integrations

Snapshots Trends Affected Files Sensitivity Threats



33%

Anomaly Strength

US-NYC-02

Affected System

vCenter-US-NYC-01.heliosdemo.local

Affected Source

Filters:

Tag ▾

Type ▾

Assessment ▾

Snapshot ↓

Data Written

Entropy

■ Sep 10, 2026 4:10pm

Threats Matched

Critical Anomaly Detected

6.8 GiB



0.72



■ Sep 10, 2026 3:57pm

Threats Matched

High Sensitivity Detected

113.2 MiB



0.08

▲ Sep 10, 2026 3:45pm

21.9 MiB

0.04

● Sep 10, 2026 3:38pm

20.9 MiB

0.04

● Sep 10, 2026 3:31pm

24.6 MiB

0.05

Látszik, hogy nő a mentett adat mennyisége és az entriópia: ez baj!

GTI = Google Threat Intelligence

Scan Details

 **Succeeded**
Status

1/1
Scanned Objects

41m 5s
Duration

Affected Items

1
Objects

1
Snapshots

3
Unique Files

3
Threats Found

Filters: Files Objects Threat Feed Threat Matched

File Path	File Hash	Object	Snapshot	Threat Feed	Threat Matched	GTI Assessment
 /C/th_test_files_smart_sca...	239cbfbb3c84a420...	 core-apps-NYC...	Sep 18, 2026 4:15am	Default Threat Library	YARA Rule: G_Upl... Family ID: malware--9...	 Malicious 30/100
 /C/th_test_files_smart_sca...	239cbfbb3c84a420...	 core-apps-NYC...	Sep 18, 2026 4:15am	Default Threat Library	YARA Rule: G_Upl... Family ID: malware--9...	 Malicious 30/100
 /C/th_test_files_smart_sca...	cb52031e47382e34...	 core-apps-NYC...	Sep 18, 2026 4:15am	Default Threat Library	YARA Rule: M_Ba... Family ID: malware--4...	 Malicious 80/100

Items per page 10 1 - 3 of 3 < >

Ime a gyanús fájlok!
Linkekkel a virustotal.com-ra

Threat Library



YARA Rules

Hash Feeds

Hash Configuration

Malware Scanner

Custom Hash Feeds

SHA-256 File Hashes ⓘ

Hashes in Threat Library
0

Last Updated
-

Manage

Hash feeds:

- CISA
- Cohesity RedLab
- Google
- Open Source

Built-in Hash Feeds

CISA ⓘ

Hashes in Threat Library
457

Last Updated
Sep 18, 2026

Cohesity REDLab ⓘ

Hashes in Threat Library
497

Last Updated
Sep 18, 2026

Google Threat Intelligence ⓘ

Hashes in Threat Library
4000

Last Updated
Sep 18, 2026

Open Source ⓘ

Hashes in Threat Library
500

Last Updated
Sep 18, 2026

Az AI itt is tud segíteni:



Security Center

Dashboard

Anomaly Detection

Inventory

Threat Detection

Data Classification

Cyber Vaulting

Scan Order Configuration

Security Posture

Sensitive Data Posture

User Activity

Integrations

REDLab News

Alerts

Audit Logs

Security Center / Anomaly Detection

Anomaly Detection

SummaryRules

Past 30 Days

Systems with Affected Objects

1Affected Sources

49Anomalous Snapshots

1Affected Protections

Aug 17, 2026 4:05amFirst Anomalous Snapshot

1Affected Systems

Sep 15, 2026 4:10amLatest Anomalous Snapshot

Objects with Anomalous Snapshots

Filters: Object TypeSystem

Object	System	Anomalous Snapshot	Anomaly Strength	Threat Detection	Sensitive Patterns
☐ core-apps-NYC-Win-284 Source: vCenter-US-NYC-01.hellosdemo.local	US-NYC-02	Sep 15, 2026 4:10am	28%	3 Threats	1 High of 11
☐ core-apps-NYC-Win-581 Source: vCenter-US-NYC-01.hellosdemo.local	US-NYC-02	Sep 11, 2026 4:16am	22%	No Scan	1 High of 11
☐ core-apps-NYC-Win-715 Source: vCenter-US-NYC-01.hellosdemo.local	US-NYC-02	Sep 10, 2026 4:10pm	33%	6 Threats	1 High of 11
☐ core-apps-NYC-Win-956 Source: vCenter-US-NYC-01.hellosdemo.local	US-NYC-02	Sep 10, 2026 4:11am	29%	6 Threats	1 High of 11
☐ core-apps-NYC-Win-844 Source: vCenter-US-NYC-01.hellosdemo.local	US-NYC-02	Sep 9, 2026 4:14pm	23%	No Scan	1 High of 11

AI összefoglaló az eseményről

Cyber Recovery Assistant

> Reasoning



Summary

In the past 30 days, there were 80 anomaly alerts detected across your environment, all on the US-NYC-02 cluster protecting VMware workloads. Anomaly strengths range from 6 to 33, with most alerts in the moderate range (around 20–30).

Key Findings

- Total alerts (past 30 days): 80
- Environment: All alerts are on VMware (kVMware) workloads from source `vCenter-US-NYC-01.heliosdemo.local`.
- Cluster concentration: All alerts are on cluster US-NYC-02.
- Anomaly strength range:
 - Maximum: 33
 - Minimum: 6
 - Majority between 20–30, indicating consistent moderate anomalies rather than extreme spikes.
- Affected objects pattern: Alerts are distributed across many `core-apps-NYC-Win-*` VMs, suggesting broad coverage rather than a single isolated asset.

Details (Top 5 recent alerts)

Object Name	Cluster	Environment	Alert Time (UTC)	Latest Anomalous Snapshot (UTC)	Latest Clean Snapshot (UTC)	Anomaly Strength
core-apps-NYC-Win-284	US-NYC-02	VMware	2026-09-15 01:58:03	2026-09-15 02:10:17	2026-09-15 01:45:53	28
core-apps-NYC-Win-581	US-NYC-02	VMware	2026-09-11 02:04:36	2026-09-11 02:16:50	2026-09-11 01:52:28	22
core-apps-NYC-Win-715	US-NYC-02	VMware	2026-09-10 14:10:13	2026-09-10 14:10:13	2026-09-10 13:57:21	33
core-apps-NYC-Win-956	US-NYC-02	VMware	2026-09-10 02:11:40	2026-09-10 02:11:40	2026-09-10 01:58:06	29
core-apps-NYC-Win-844	US-NYC-02	VMware	2026-09-09 14:02:32	2026-09-09 14:14:32	2026-09-09 13:50:24	23

...and 75 more alerts over the last 30 days, mostly with anomaly strengths in the 20–30 range on similar `core-apps-NYC-Win-*` VMs.

Recommendations

- **Prioritize higher-strength alerts:** Start with objects like `core-apps-NYC-Win-715` and `core-apps-NYC-Win-956` (strength ≥ 29) for deeper investigation (file changes, entropy, and classification/threat scans).
- **Correlate with sensitive data and threats:** For the most recent high-strength alerts, consider running data classification and threat scans on the affected snapshots to see if sensitive data or indicators of compromise are present.
- **Trend review:** If you want, I can next summarize snapshot trends (entropy, compression, file-change counts) for one of these alerts to understand how the anomaly evolved over time.

Suggestions:

Summary of the top 3 Anomalies

Anomaly with highest count of affected files

Analyze the most recent Anomaly

Anomalies with strength greater than 50 but less than 90.

Summary of the top VMware alerts



Past 30 Days



49

Anomalous Snapshots

Aug 17, 2026 4:05am

First Anomalous Snapshot

Sep 15, 2026 4:10am

Latest Anomalous Snapshot

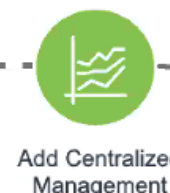
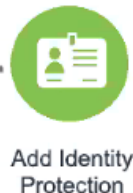
erns

Ask a question



Protect Data

-  Cohesity capability
-  Cohesity scanner
-  Customer process or technology



Ensure Recoverability



Detect Threats



Practice Recovery



Reduce Data Risk



digital

Object Type

Source

Protection Group

Storage Domain

Digital Jump Bag

Storage Domain: DefaultStorageDomain | Protection Group: Digital Jump Bag | Last Backup:12 hours ago | Size: 98.8 MiB

Digital jumpbag – az elsősegély csomag

Digital Jump Bag

Browse on Indexed Data

Sep 22, 2026 7:46pm

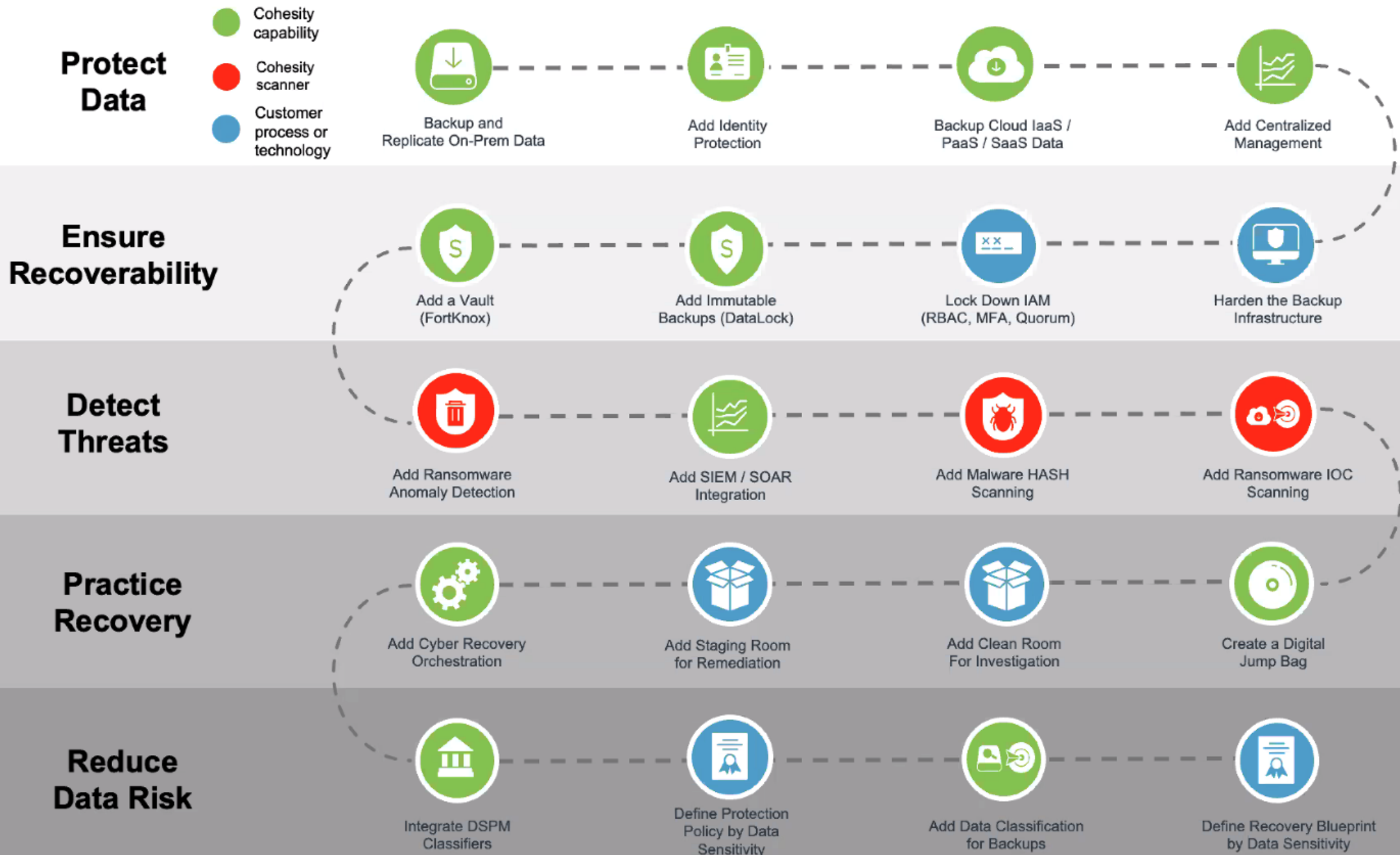
Name	Size	Last Modified
Company Policy		Oct 30, 2024 10:00pm
Contacts		Oct 30, 2024 10:07pm
ISO		Oct 30, 2024 9:40pm
Network Config		Oct 30, 2024 10:13pm
Product Documentation		Oct 30, 2024 10:22pm
RunBook.txt		Aug 15, 2024 9:59pm

MVC: Minimal Viable Company:

- “Mini vállalat” amit el lehet indítani 24h belül
- ”Mini vállalat” -> mini szolgáltatások

MVRC / Digital Jumpbag

- Minimum Viable Response Capability
- Minimum válaszadási képesség
- Response értsd: ellencsapás



Veeam: <https://www.cvedetails.com/vendor/15994/>

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2019	0	0	0	0	0
2020	2	0	0	0	0
2021	0	0	0	0	0
2022	2	1	1	0	0
2023	1	0	0	0	0
2024	10	3	2	1	0
2025	6	0	1	0	0
2026	9	0	2	0	0
Total	30	4	6	1	



GitHub

<https://github.com> › [SentinelXofficial](#) › [CVE-2026-44963](#) ⋮

CVE-2026-44963 — Veeam Backup & Replication RCE

9 Jun 2026 — CVE-2026-44963 is a Remote Code Execution (RCE) **vulnerability** in **Veeam Backup & Replication** caused by insecure deserialization of untrusted data ...



GitHub

<https://github.com> › [HORKimhab](#) › [CVE-2026-44963](#) ⋮

HORKimhab/CVE-2026-44963 - Veeam

This **repository** is for **educational** and authorized security research only. It is designed to help users learn about: Security **vulnerabilities**; Sandbox and ...



GitHub

<https://github.com> › [advisories](#) ⋮

A vulnerability in Veeam Backup & Replication allows a...

3 Dec 2024 — A **vulnerability** in **Veeam Backup & Replication** allows a low-privileged user to start an agent remotely in server mode and obtain credentials, ...

Köszönöm a figyelmet

andras.pulai@cohesity.com



COHESITY

© 2025 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.