Identity Resilience

Secure, protect, and recover AD and Entra ID throughout the entire attack lifecycle

Josef Honc, Senior Principal Sales Engineer

COHESITY

Cohesity Identity Resilience

Active Directory Forest Recovery
powered by Semperis

Cohesity Cloud Protection Services

Identity Threat Detection and Response (ITDR)
powered by Semperis

Continuous monitoring and rapid recovery from ransomware, insider threats, cyberattacks, and operational disruptions

Cohesity Identity Resilience brings leading Semperis technologies

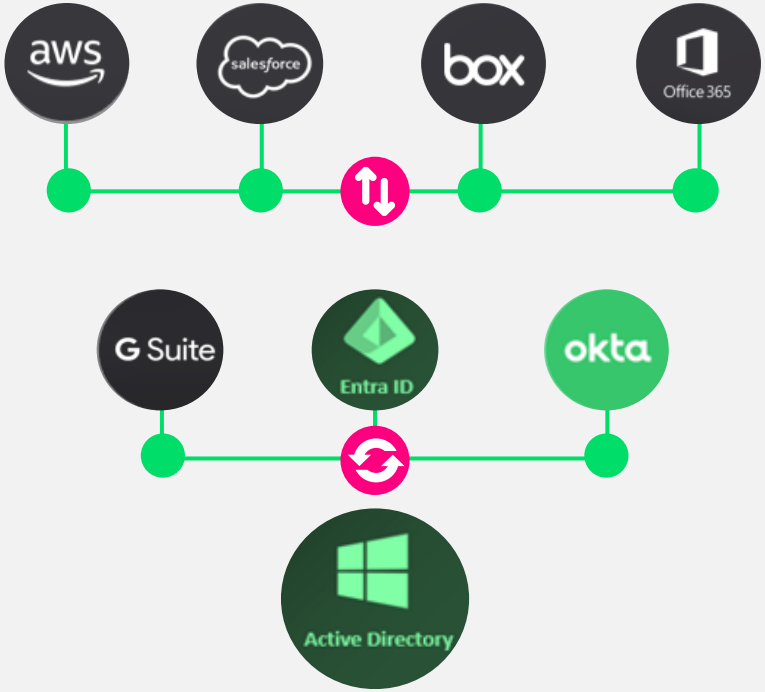
Trusted by the world's largest brands

COHESITY

What does Active Directory do?

Handles the **Four As** of identity and access management (IAM)

- ✓ **Authentication**: Who you are
- ✓ **Authorization**: What you're allowed to access
- ✓ **Account** management
- ✓ **Audit**: Proving who did what (sign-in logs, etc.)



For **90% of enterprises,** identity starts with AD.

Cohesity Identity Resilience

Powerful identity security and fast, malware-free recovery

Prevent identity-based attacks

Continuously monitor, get real-time alerts, and automated remediation cross your identity environment.

Cut downtime

Restore AD and Entra ID in a few clicks with automated recovery using immutable Cohesity backups.

Eliminate malware

Avoid reintroducing malware by recovering identity to a known-secure state.

Speed forensics

Accelerate post-breach forensics to prevent follow-on attacks.

If AD isn’t secure, nothing is.

AD is the core identity system for 90% of businesses worldwide

AD is a primary attack target, involved in 9 out of 10 breaches

Without AD, business operations come to a halt

Standard recovery approaches don't work with AD

Malware reintroduction

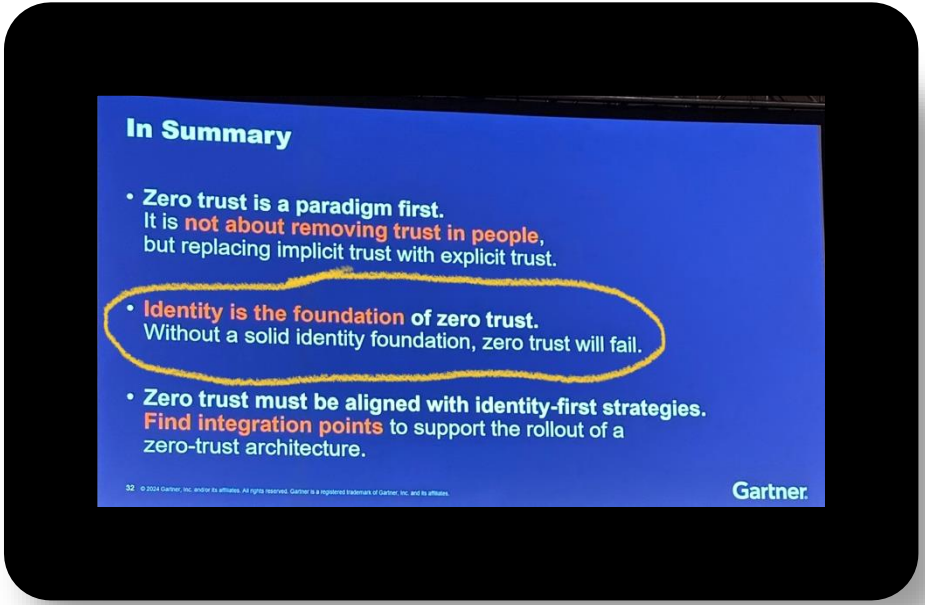
Lack of trust in the environment

Prolonged recovery

Recovering from identity-related attacks requires a different approach, with identity-specific technology, processes, and people

“**Identity is the foundation of zero trust.** Without a solid identity foundation, zero trust will fail.”

—John Watts, “Demystifying Zero Trust in an Identity First Strategy”



“*Stop* working on zero trust if you haven’t addressed identity first.”

What happens when AD is attacked?

Obvious effects

- All DCs have malware on them (OS,SYSVOL)
- Some DCs are not functional

Not-so-obvious effects

Changes in the service to provide control or persistence

- Privileged group membership changed
- Permissions changed (e.g. AdminSDHolder)
- Group Policy objects (GPOs) changed
- Hidden objects (Deny Read ACE)
- Back doors inserted (Mimikatz,DCSHADOW)

Manual Active Directory forest recovery steps

1. Pull the network cables from all DCs or otherwise disable network
2. Connect DCs to be restored to a private network (*Oh yes - establish a global private VLAN*)

For each domain:

3. Nonauthoritative restore of first writeable DC
4. Auth restore of SYSVOL on that DC
5. Remediate malware
6. Reset all admin account passwords
7. Seize FSMOs
8. Metadata cleanup of all writeable DCs except for targeted seed forest DCs
9. Configure DNS on the forest root DC
10. Remove the global catalog from each DC. *(Wait for global catalog to be removed)*
11. Delete DNS NS records of DCs that no longer exist
12. Delete DNS SRV records of DCs that no longer exist
13. Raise the value of available RID pools by 100K
14. Invalidate the current RID pool for every DC
15. Reset the computer account of the root DC twice
16. Reset krbtgt account twice *(You have a seed forest at this point)*
17. Configure Windows Time
18. Add GC to a DC for each OS version in each domain *(Wait for GCs to be created)*
19. Take a backup of all DCs in the seed forest
20. Create an IFM package for each OS version, in each domain your DCs are running
21. Build out seed forest with additional DCs to support Tier 0 / Tier 1 operations

For each DC to be repromoted into the seed forest:

22. Clean up the (former) DC using /FORCEREMOVAL or rebuild OS
23. Send IFM package to server (wait…)
24. Take the DC off the public network and put it on the seed forest network.
25. Run a DCPROMO IFM *(Days pass while you clean and rebuild DCs) (Now you have a large enough forest to support basic operations)*
26. Verify health of the full forest
27. Move restored forest to the corporate network
28. Reboot all servers and clients to force communications with the new forest

Important considerations

Manual recovery is error-prone and often requires additional cycles to correct missteps, extending the timeline even further

Required staff for manual AD forest recovery:
Core AD team, operators at every datacenter, plus other external support (Estimated 10-15 IT support staffers in average enterprise)

General purpose backup only automates step 3, leaving the rest of the recovery process a mostly manual effort

KEY COMPETITIVE DIFFERENTIATOR

COHESITY

Comparing a manual process to Cohesity Identity Resilience

From days/weeks to minutes

Orchestrated, fully automated forest recovery process—avoiding human errors,

reducing downtime by 90%,

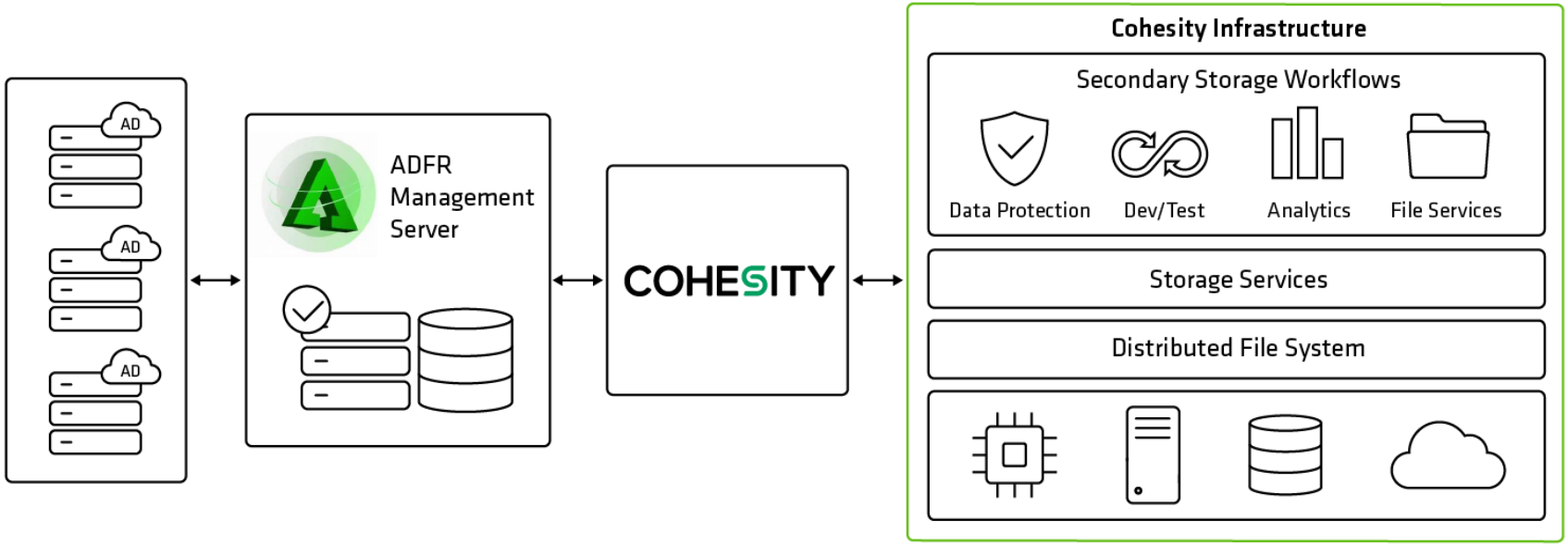
and eliminating the risk of malware reinfection.

ADFR's 7-click automated AD recovery:

1. Click **Recover**
2. Start **Forest Recovery**
3. List **Backup Sets**
4. Select **Backup Set to recover**
5. Click **Continue**
6. Click **Continue**
7. Click **Start Recovery**

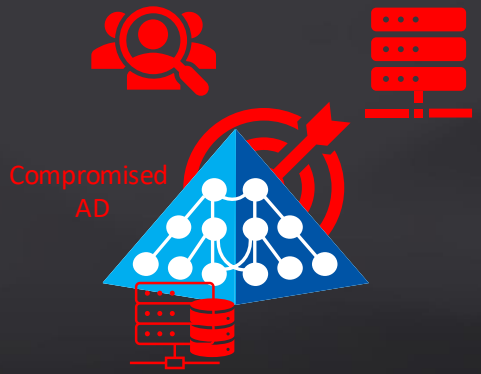
Required staff for Semperis' ADFR:
Only 1-2 AD admins

ADFR integrated with Cohesity Data Cloud provides greater resilience



Timeline of the AD Cyber Recovery

Compromised Network



Days 1 2 3 4 5

Identity under attack: Steps to recovery

1 Get a minimal backup of the compromised forest

Install Active Directory Forest Recovery (ADFR)

- Management server
- Agents on a minimum set of DCs

Take a backup

- ADFR backs up AD and leaves the OS (and its malware) behind
- Flexible recovery from any hardware platform to any hardware platform

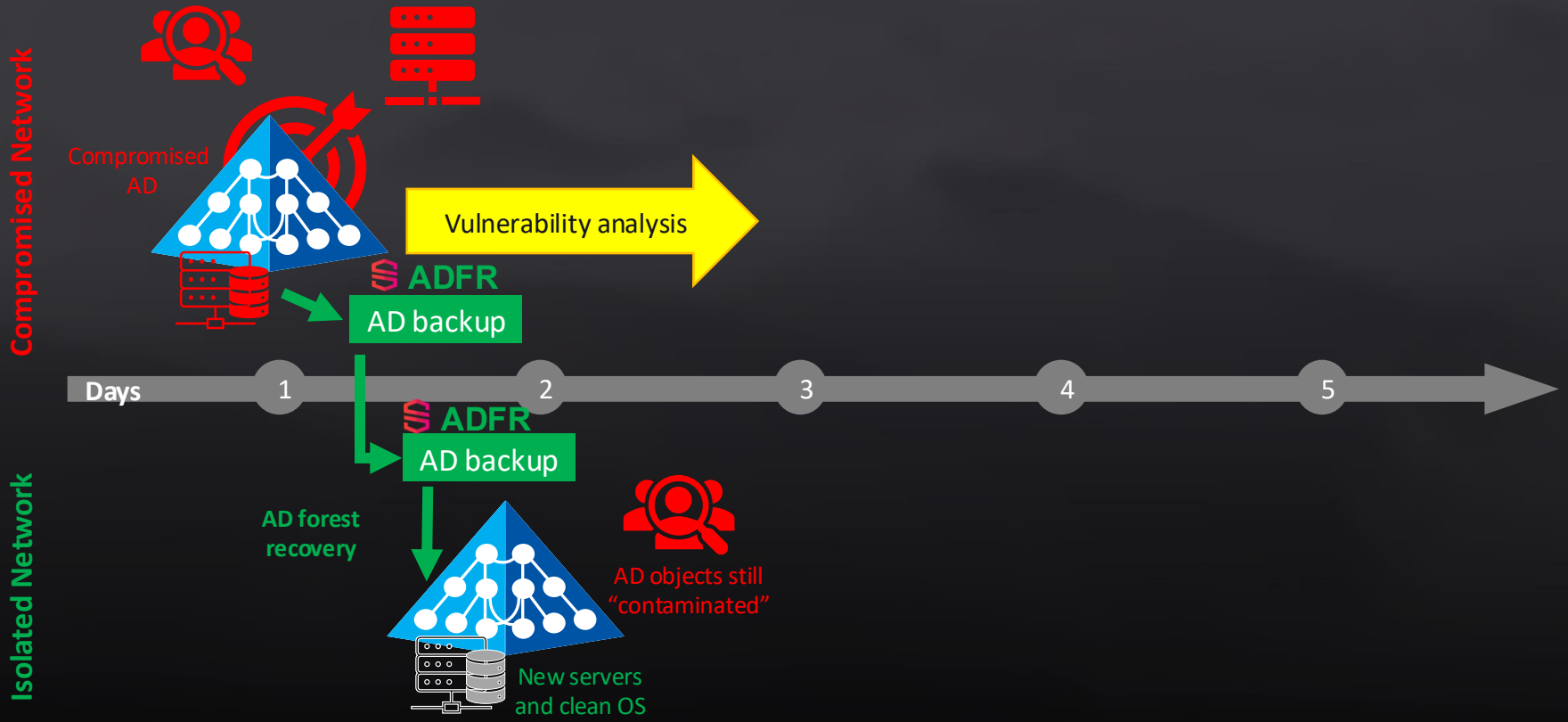
Timeline of the AD Cyber Recovery

Identity under attack: Steps to recovery

2 Recover the compromised forest to an isolated recovery environment (IRE)

- Create an isolated network and provision fresh (=malware free) VMs with ADFR agents
- Make the ADFR management server and backups available in the isolated network
- Perform an automated, high-speed **AD forest recovery to a minimum forest** using ADFR to the new, malware-free servers in the isolated network

Timeline of the AD Cyber Recovery



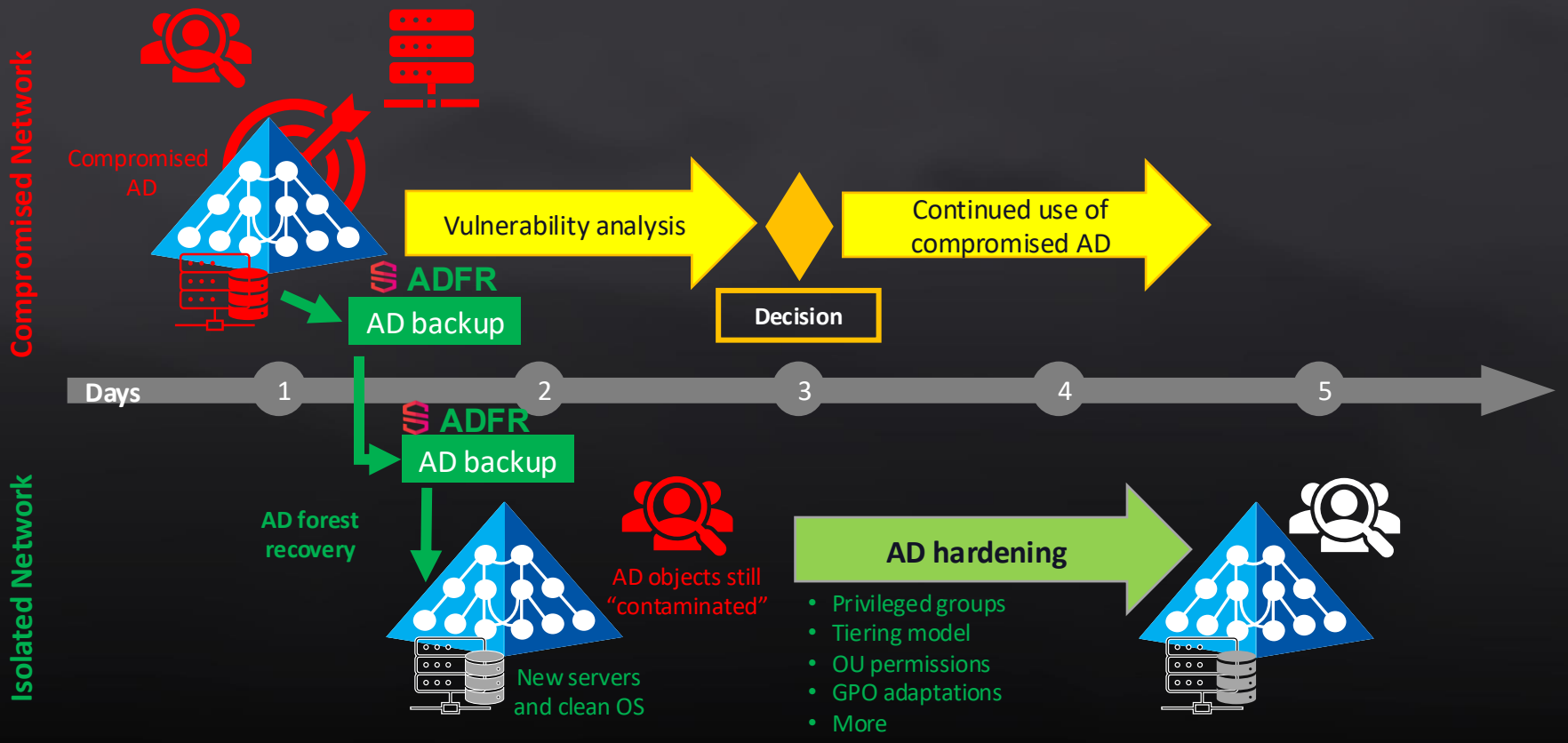
Identity under attack: Harden the recovery forest

3 Harden the contaminated AD service

You have a recovery forest with clean DCs, *but the service is still untrustworthy*

- Run Purple Knight Post Breach Edition to discover threat actor ingress and control of the AD service
- Run Purple Knight and Forest Druid (free Semperis tools) for an overall vulnerability assessment
- Remediate most critical items, focusing on probable threat actor penetration techniques
- If time, apply security best practices such as admin tiering

Timeline of the AD Cyber Recovery

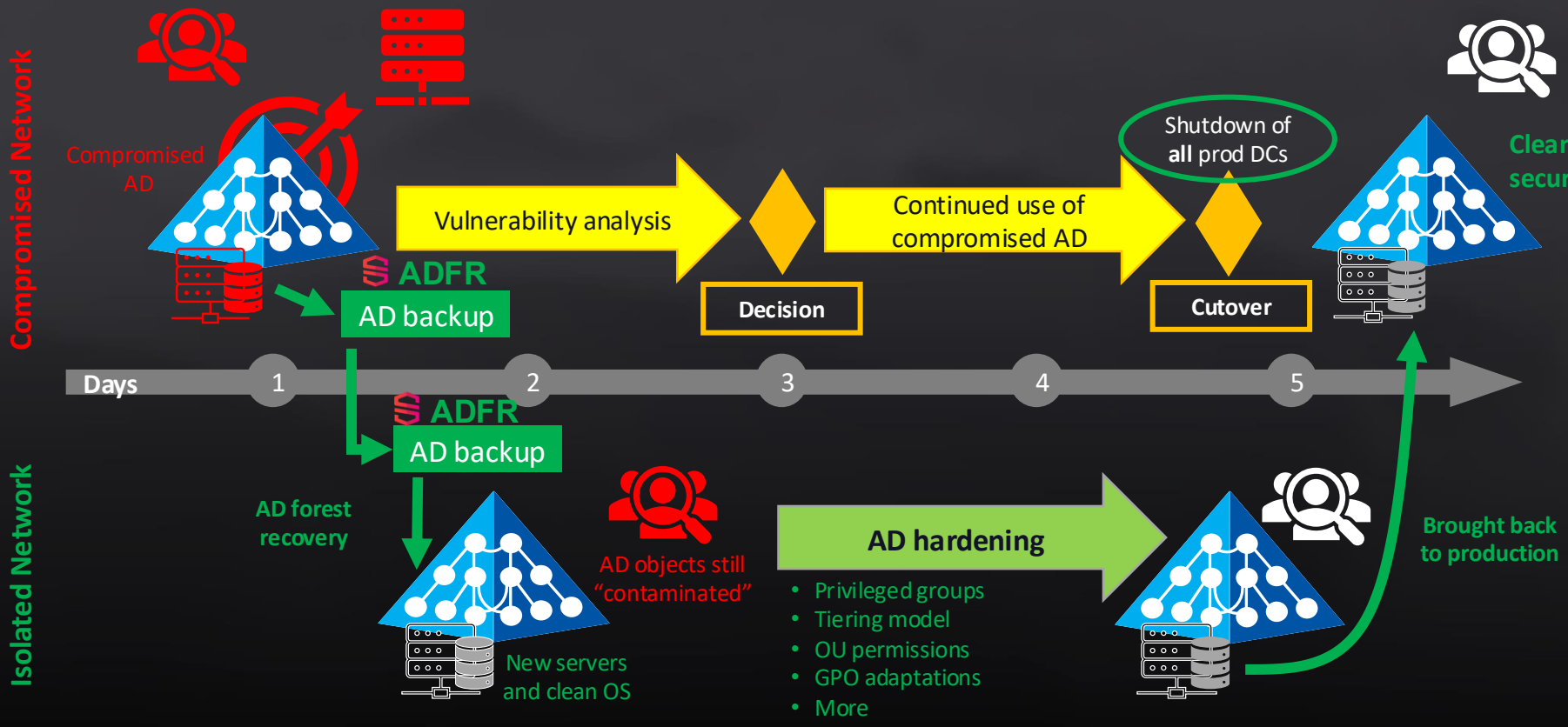


Identity under attack: Cut over to the new forest

4 Bring back recovered AD to production

- Shut down existing production forest (!)
- Update recovery forest DNS resolvers to production DNS
- Open isolated network to production network
- Register recovery forest DCs in DNS
- Reboot all domain-joined servers and PCs

Timeline of the AD Cyber Recovery



Assess Your Current AD Environment

Proven tools to quickly and accurately gauge your risk from identity-related cyber attacks

Forest Druid

Close the paths that attackers use to target tier 0 assets.

https://www.cohesity.com/forms/semperis-forest-druid/

- Identify the true Tier 0 perimeter
- Cut down excessive privileges
- Prioritize attack paths by severity, not commonality
- Monitor what matters
- Save time and resources

Purple Knight

Asses your Active Directory security to avoid common attacks.

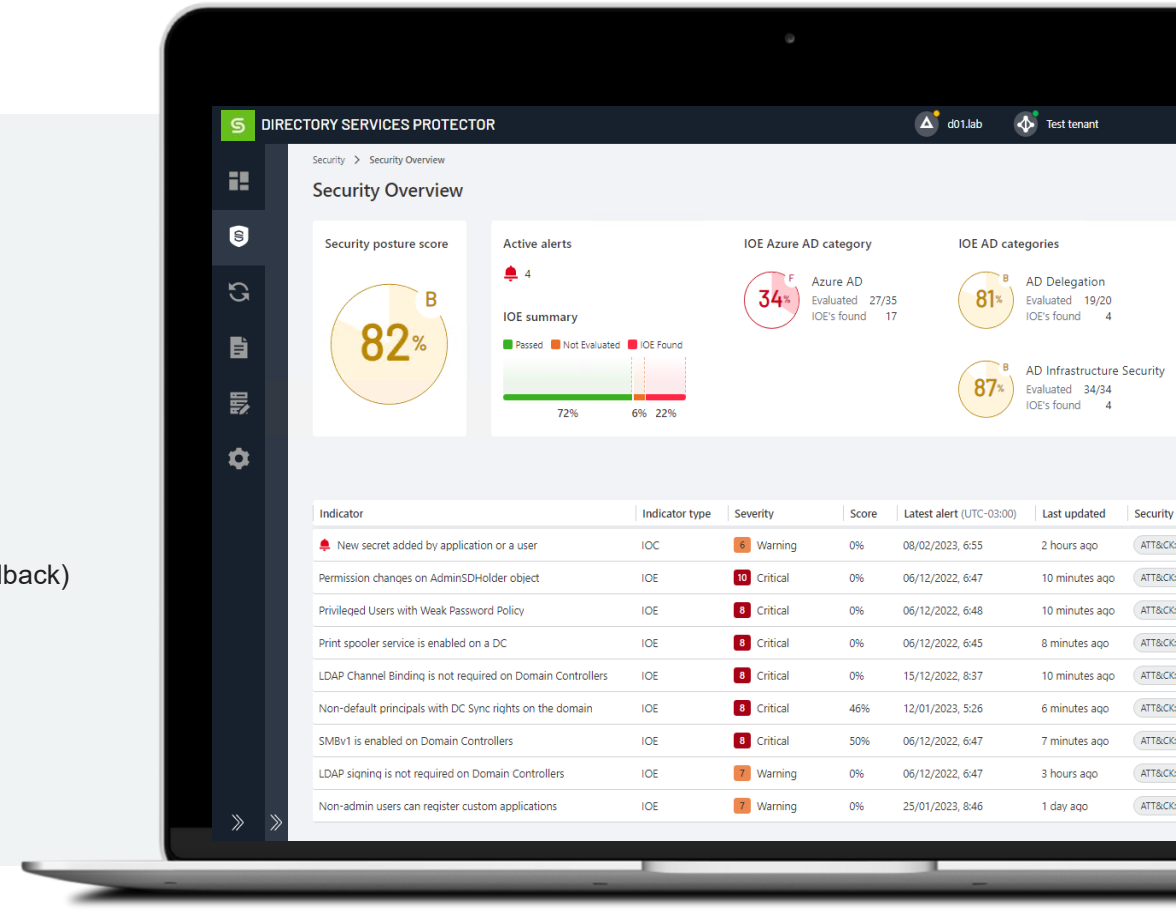
https://www.cohesity.com/forms/semperis-purple-knight/

- Audit your Active Directory for security
- Community-driven AD threat intelligence
- Get AD security guidance from Semperis experts

Now Available…

DIRECTORY SERVICES PROTECTOR

- Continuous vulnerability assessment
- Tamperproof tracking
- Real-time security alerts
- Auto-remediation (malicious change rollback)
- Compliance reporting



Identity Resilience Critical Capabilities

Advanced identity resilience check list

- ❑ Recovery tools that require no internet access
- ❑ Active Directory backups that are decoupled from the operating system
- ❑ Recovery processes that are automated and require no manual intervention
- ❑ Ability to analyze attack paths leading to Tier 0 assets (including Active Directory and Cohesity storage clusters)
- ❑ Tamper-proof multi-source change tracking & rollback
- ❑ Inventory and monitoring of highly targeted service accounts
- ❑ Active Directory backups that are immutable
- ❑ Ability to recover 'minimum viable business' in hours
- ❑ Guaranteed malware-free recovery
- ❑ Flexible restore targets
- ❑ Pre- and post-breach forensics to evict bad actors
- ❑ 24/7 Incident Responders on standby

**Capabilities in black are specific to Cohesity Identity Resilience*

Advice to prospects and customers: Require competitors to prove competency in these scenarios

	REQUIREMENT	DETAILS
DEPLOYMENT	Solution must be deployable on a standalone server	Customers in large environments and isolated networks should not be required to deploy virtual infrastructure to backup distributed and potentially isolated environments.
	Solution must not require internet connectivity for management, configuration, or restores	During an incident, internet connectivity likely will be disabled. The administration and recovery experience for the solution must be the same with or without the internet connection.
OPERATIONS	Solution must embrace Zero Trust identity model: only designated users should be able to manage AD forest backup and recovery	Platform Global Administrator accounts should not be able to administer or recover Tier 0 assets. Only designated AD personnel should access these environments for true Zero Trust separation of duties.
	Solution agent must not require domain service account privileges	The service account on the domain controllers must not rely on domain services and elevated privileges to perform actions.
	Restore activities should be performed on local console—assume no internet connectivity	Internet connectivity will likely be disabled during an attack.
	Restore process must be able to be paused at strategic points	During a recovery, it must be possible to pause the process at strategic points to perform forensic analysis and remediation.
	Must have the ability to bring AD online while Global Catalog rebuild is still occurring	Large complex environments require significant time to rebuild and replicate the GC database. To accelerate RTO, DCs must be accessible prior to a full sync completion.

Thank You

josef.honc@cohesity.com

COHESITY