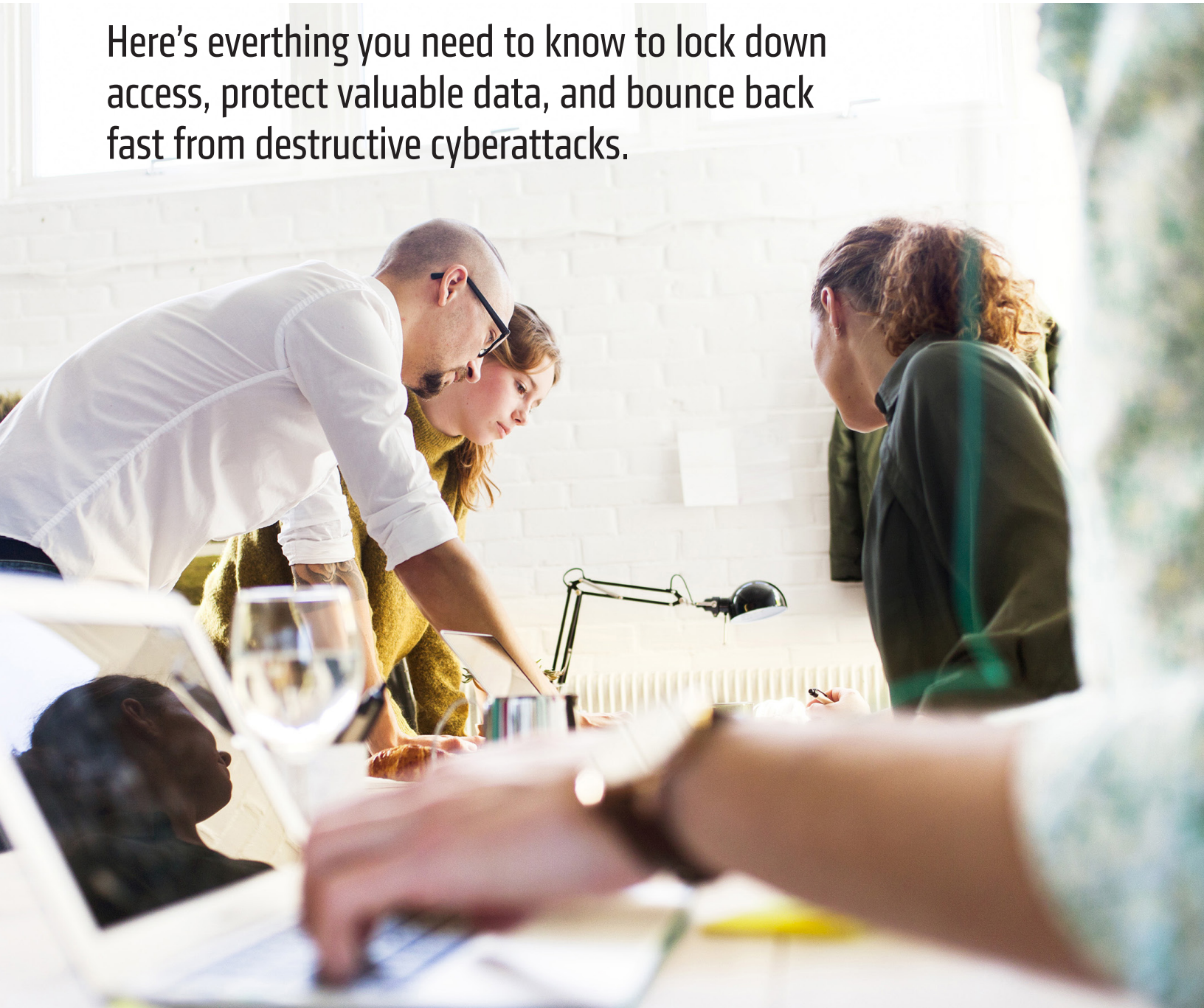
COHESITY

AN EXECUTIVE'S GUIDE TO EVALUATING IDENTITY RESILIENCE SOLUTIONS

Here's everthing you need to know to lock down access, protect valuable data, and bounce back fast from destructive cyberattacks.



Your identity and access management systems are a prime target for bad actors.

Why?

9 out of 10 cyber-attacks involve identity and access management (IAM) systems. It's the most attacked part of any organization's infrastructure.

An identity system of record is a high-value target because compromising it provides attackers with access to virtually any resource in the organization. That's why identity resilience is a cornerstone of a comprehensive cyber resilience strategy. To rapidly restore a minimum viable company, identity services must be among the first workloads returned to a trusted state because so many critical systems and business processes depend on them.

For most organizations, the primary IAM and source of truth for other identity providers is on-prem Microsoft Active Directory (AD). Cyber recovery of AD, especially in complex environments that include multiple forests, is a challenging process that requires specialized expertise; it is not "just another workload." In addition to AD, you most likely have some mixture of Entra ID and Okta.

As you look to bolster your defenses against cyber-attacks you must ensure that you have an end-to-end identity resilience strategy across all your critical identity services.

> ***"No organization can be 100% safe from cyberattacks—so you need to invest in resilience, the ability to bounce back from a breach."***

Identity resilience ensures your business can:

- **Detect and remediate identity threats:** Detect identity-based attacks in progress and automatically rollback risky changes that can't wait for human intervention with identity threat detection and response (ITDR).
- **Cleanly recover identity services and restore trust:** Bring back your identity services without bringing back the attackers and/or backdoors that lead to persistent reinfection.
- **Reduce downtime:** Identity is key for access and authentication. When it falls, business grinds to a halt. Ensure business operations can be recovered securely and seamlessly from an identity-attack to reduce downtime.

No organization can be 100% safe from cyberattacks —so you need to invest in resilience, the ability to bounce back from a breach. Your organization should improve and expand identity resilience by continuously detecting and remediating identity-based attacks and implementing a proven recovery strategy that brings back AD, Entra ID, and Okta clean and fast under any circumstance. This guide will help you evaluate solutions, ask the right questions, and make a confident investment in securing your identity infrastructure against today's threats.

What to look for in an identity resilience solution

When evaluating options, it's tempting to think of identity as simply another workload to back up and recover when needed. This is a dangerously outdated mindset. A modern approach that extends cyber resilience to identity and access systems combines advanced proactive security and clean recovery throughout every step of the attack lifecycle. Here's what separates a true enterprise-ready identity resilience solution from the rest:

Advanced ITDR: Identity resilience starts before the breach. IAM systems like AD is often the first system attackers target because it provides the keys to the kingdom. Simply backing it up isn't enough. Your solution should be able to provide continuous monitoring of the security posture of your identity environment through Identity Threat Detection and Response capabilities. This can help to detect any vulnerabilities to harden your identity infrastructure and automate remediation. Automated rollback and remediation of malicious changes that can't wait for human intervention can reduce the chances of a successful attack. By implementing these continuous threat detection and remediation and proactive hardening, you can ensure attackers hit roadblocks before they can weaponize your identity systems.

Protection that stands up to attacks: If a compromise occurs, it's important to ensure that your identity infrastructure can be recovered via clean backup data. Attackers know that backups are the last line of defense, which is why they actively engage in double extortion schemes or attempt to encrypt, modify, or delete them—leaving you largely defenseless and forced to pay exorbitant ransoms. Your identity resilience solution must provide immutability by design—ensuring AD backups can't be tampered with even if attackers gain domain admin credentials. WORM storage, quorum-based approvals, and cryptographic verification are critical capabilities for resilient backups. If your protection layer doesn't stand up when adversaries are inside your network, you don't really have protection.

Fast, malware-free recovery: When identity is compromised, downtime ripples across every business function. Recovery speed matters, but so does recovery integrity. Simply restoring identity without validating its trusted risks reintroducing malware or backdoors, leading to repeat infections and dreaded doom loops. An effective solution should combine automated, orchestrated, rapid recovery of AD, Entra ID, and Okta . For AD specifically, recoveries should be decoupled from the OS to make sure that compromised credentials and malware isn't brought back. This can reduce downtime during a recovery process by preventingpersistent infections with a recovery you can trust.

Granular recovery options: Not every identity incident requires a full restore. Granular recovery saves time and reduces disruption by giving you options for object-level, attribute-level, and forest-level recovery. Having both forest and granular recovery tools ensures that there is an appropriate solution for both help-desk type requests and full-on cyber events.

Protection across hybrid identity: Identity is no longer confined to on-prem AD. Entra ID and Okta is rapidly becoming a crucial part of enterprise identity architecture, especially for access to cloud apps. You need a future-proof resilience solution to run seamlessly across hybrid identity environments, protecting both AD , Entra ID, and Okta. For many organizations, Entra ID and Okta are synched with AD, meaning that to successfully and securely restore Entra ID and Okta, you need the ability to protect and recover AD first. Entra ID and Okta are separate applications from AD with one-way syncs from on-prem to the cloud, without the on-prem protection you only have the second half of a solution. Your identity resilience solution should also encompass protection and recovery capabilities to ensure Entra ID and Okta is secure and cleanly recoverable to ensure cloud identity continuity.

Post-breach forensics to validate trust and prevent future attacks: Recovery without insight leaves you vulnerable to repeat incidents. A modern solution should embed forensic capabilities that allow teams to validate whether a recovery is clean. This not only aids post-incident investigations but crucially informs preventative measures–helping enterprises strengthen their defenses and meet compliance or regulatory reporting requirements. Without the due diligence post-recovery, you are at risk for a follow-up attack. Forensics should not be an afterthought. It's an integral part of identity resilience.

Ability to recover without internet access: In the case of a catastrophic outage or cyber-attack, you cannot assume that you'll have stable or secure internet access. Your identity resilience solution needs to be able to successfully bring back your critical identity systems without internet availability so that you can cleanly restore and bring systems back online in every circumstance.

24/7 incident response support: Identity is a unique and complex workload, especially when it comes to recovering it. For cyber recovery of critical identity infrastructure, it is key to make sure the vendor of the solution has proven expertise in protecting, securing, and recovering identity and can give the customer the guidance needed. Every recovery situation can vary, and the proper response support and forensics from seasoned veterans is key to ensuring that your organization can recover from the most catastrophic identity attacks or outages confidently and quickly.

Critical questions to ask vendors

1. How do you prevent attackers from tampering with or deleting AD, Entra ID or Okta backups?
2. Can you demonstrate full recovery of your entire identity infrastructure in less than a day?
3. How do you verify that recovered AD, Entra ID, or Okta is free from malware, backdoors, or didn't bring back compromised credentials?
4. Can you recover identity with the same experience and UI without internet access?
5. Do you support hybrid identity environments (on-prem AD + Entra ID + Okta)?
6. Can your solution run full forest recoveries for AD in an automated manner and adhere to the Microsoft Recovery Runbook?
7. Does your solution hunt for identity-specific threats to detect and evict bad actors before a compromise occurs?

Warning signs to look out for

- No ability to decouple the OS during the recovery. Bringing back the OS with your identity data can bring back malware and backdoors.
- No ability to target any physical/virtual source for recovery. Requiring an exact patch level can lead to prolonged downtime.
- No identity forensics and incident response expertise (IFIR) for 24/7 incident response support.
- No identity security capabilities. Resilience includes risk reduction before impact and mitigating threats to prevent compromise.
- Solutions relying only on native Microsoft tools. These are manual, slow, and unreliable when you need it the most.
- Backups stored in production. Attackers can wipe them and leave you without anything to recover with.
- No orchestration or automation for parallel recoveries of multiple domain controllers (DCs). Without it, this forces admins to follow lengthy, manual steps during a time of high stress and chaotic environment.
- The solution is reliant on having secure and stable internet access. You cannot assume or rely on having an internet connection during a cyber-attack or recovery.
- No ability to test recovery. If you can't rehearse it, you can't trust it.

Vendor evaluation checklist

Use this scorecard during vendor conversations:

Requirement	Vendor 1	Vendor 2	Vendor 3	Notes
Recovers multiple DCs in parallel (for AD)				
Target any physical/virtual source for recovery				
Immutable, isolated AD backups				
Object to forest-level recovery granularity				
Automated forest recovery workflows				
Proactive hardening to identify and close attack paths				
Malware/corruption detection in backups				
Tamper-proof multi-source change tracking & rollback				
Inventory and monitoring of highly targeted service accounts				
Hybrid AD (on-prem + Entra ID) support				
Ability to recover without internet access				
Post-breach forensics				
Scalability (multi-forest/global)				
24/7 expert identity incident response support				

The bottom line

Identity-based compromise is at the heart of nearly every major breach. That's why accelerating cyber resilience when it comes to your critical identity systems is no longer optional—it's foundational to enterprise security.

A proven identity resilience solution goes beyond backups. It hardens identity against compromise, defends against identity attacks and threats, delivers lightning-fast trusted recoveries, and helps you close backdoors for trusted malware-free restorations. To learn more about identity resilience and how it could help secure your most critical identity services, talk to your Cohesity account team today.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500064-004-EN 7-2026