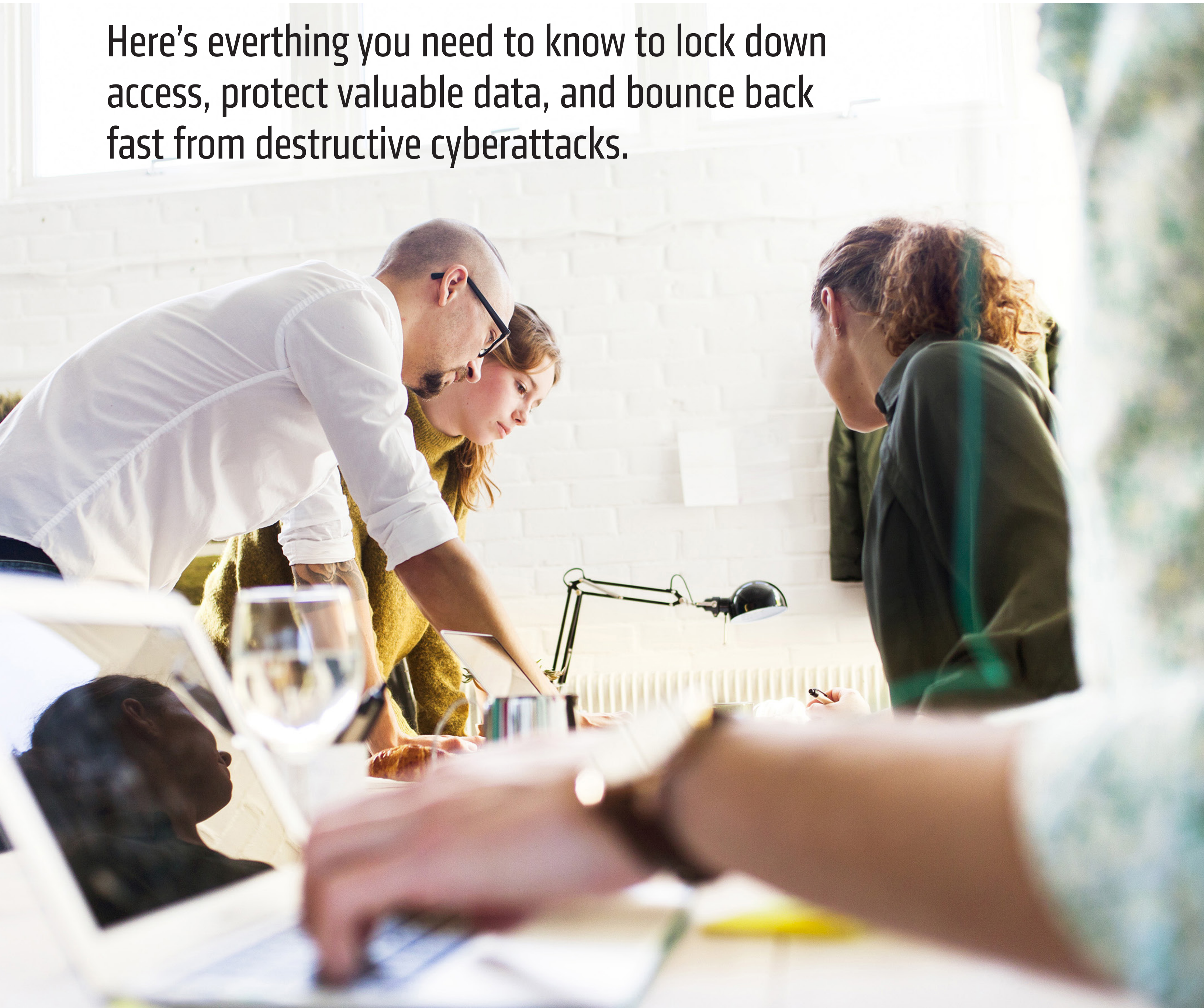
COHESITY

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?

Active Directory (AD), the foundation of enterprise identity, acts as a central nervous system that enables authentication, authorization, and access to critical applications and services. Because of its interconnected nature, AD remains one of the most targeted attack surfaces. Complicating matters is the recovery effort post-incident. After a compromise, restoring AD is notoriously slow, complex, and error-prone—conditions that can increase the risk of reinfection and extend downtime.

Here's the hard truth: When AD goes down, business grinds to a halt. That's why organizations like yours invest in identity resilience—modern solutions purpose-built for the protection and rapid recovery of AD.

> *“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:

- **Withstand identity attacks:** Detect, respond, and recover when credentials are compromised.
- **Secure critical data and infrastructure:** Keep your crown jewels out of reach even if attackers bypass traditional defenses.
- **Reduce downtime:** Ensure business operations can be recovered securely and seamlessly from an identity-attack.

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 identifying and closing security gaps, continuously monitoring for attacks, and implementing a tested AD recovery plan to be prepared to bounce back from the worst-case scenario. 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 resilience as simply another workload to back up and recover when needed. This is a dangerously outdated mindset. Cybercriminals know this, which is why many target backup infrastructures in their ransomware attacks. A modern approach that extends cyber resilience to identity and access systems combines protection and secure recovery throughout every step of the attack lifecycle. Here's what separates a true enterprise-ready identity resilience solution from the rest:

Proactive AD hardening: Identity resilience starts before the breach. Active Directory (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 regular security posture assessments of your AD. This can help to detect any vulnerabilities and prioritize remediation. By implementing these fixes and continuous monitoring, proactive hardening ensures attackers hit roadblocks before they can weaponize your identity systems.

Protection that stands up to attacks: 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 AD is compromised, downtime ripples across every business function. Recovery speed matters, but so does recovery integrity. Simply restoring AD without validating its trusted risks reintroducing malware or backdoors, leading to repeat infections and dreaded doom loops. An effective solution should combine application-only protection, orchestrated, rapid recovery with automated malware scanning of AD backups. These guarantees can reduce downtime during a recovery process but also prevent persistent infections with a recovery you can trust.

Granular recovery options: Not every AD 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 separated Forest and granular recovery tools ensures that there is a clear separation of duties between help-desk type requests and full-on cyber events.

Future-proofing for hybrid environments: Identity is no longer confined to on-prem AD. Entra ID is rapidly becoming a crucial part of enterprise identity architecture. You need a future-proof resilience solution to run seamlessly across hybrid identity environments, protecting both AD and Entra ID. For many organizations, Entra ID is synched with AD, meaning that to successfully and securely restore Entra ID, you need the ability to protect and recover AD first. Entra ID is a separate application from AD with a one-way sync from on-prem to the cloud, without the on-prem protection you only have the second half of a solution.

Forensics support to prevent future attacks: Recovery without insight leaves you vulnerable to repeat incidents. A modern solution should embed forensic capabilities that allow teams to identify attack vectors. 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 cyber 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. When it comes to 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 backups?
2. Can you demonstrate full recovery in less than a day?
3. How do you verify that recovered AD is free from malware or compromise?
4. Can you recover AD without internet access?
5. Do you support hybrid identity environments (on-prem AD + Entra ID)?
6. Can your solution run full forest recoveries in an automated manner and adhere to the Microsoft Recovery Runbook?

Warning signs to look out for

! 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. 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
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				
Hybrid AD (on-prem + Entra ID) Support				
Ability to recover without internet access				
Post-breach forensics				
Scalability (multi-forest/global)				
24/7 expert 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.

The right identity resilience solution goes beyond backups. It hardens AD against compromise, delivers lightning-fast recovery, and helps you close backdoors for trusted malware-free restorations. To learn more about identity resilience and how it could help secure your most vulnerable identity system, talk to your Cohesity account team today.

COHESITY

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