COHESITY

THE IDENTITY LAYER IS GROUND ZERO FOR CYBERATTACKS

*Why security and IT leaders must **prove** they can recover identity infrastructure*

INTRODUCTION

Enterprise identity was supposed to make your life simpler. Organizations first centralized digital access in the late 1960s and early 1970s, giving them one place to decide who got in and what they could touch. LDAP and platforms like Active Directory later turned that idea into a single source of truth for the entire network. It worked beautifully.

That's exactly the problem.

That single source of truth is now the single easiest way in. Attackers don't break in anymore. They log in, with stolen credentials and legitimate access, and walk straight to your most critical systems. Nothing trips. No alarm sounds. They're using the same door your employees use every morning, which makes this a fundamentally different problem than the one most security programs were built to solve.

For years, you built your defenses around a perimeter: a wall meant to keep intruders out. The wall still stands, but attackers have stopped climbing it. **Compromising your identity infrastructure is easier, quieter, and more reliable, which is why identity has replaced the network perimeter as the primary battleground.** Most security stacks were never built to fight on this ground.

The numbers are not subtle. In 2024, 79% of attacks were malware-free: no virus to catch, just social engineering, stolen credentials, and trusted remote tools slipping past detection. In 2025, that figure climbed to 82%, as attackers leaned even harder on valid credentials, trusted identity flows, and approved SaaS integrations to move across domains undetected (CrowdStrike Global Threat Report). The trend line points in exactly one direction.

This is the uncomfortable place any serious security program now has to start. The system you built to control access to everything has quietly become the easiest way into everything. That's not a reason to panic. It's a reason to protect identity first, and to be able to prove you can recover it, before anything else.

Why enterprise identity Is under attack

To an attacker, identity is the highest-value, lowest-effort target in your enterprise, because one compromised credential can unlock everything behind it. Identity isn't just another vector. It's the one vector a modern attacker is actively hunting for.

But here's the catch: almost nothing in your stack was built to stop this. EDR, firewalls, and network segmentation are all designed to catch someone breaking in, not to question someone who logged in with valid credentials. To your defenses, the attacker looks exactly like your employee.

And the blind spot only grows. Most Active Directory environments are decades old. Years of quick fixes, forgotten accounts, and quiet misconfigurations have piled up in the background where nobody is looking. That pile isn't just technical debt. It's an unlocked window, and it's precisely what attackers go looking for first.

Hybrid identity makes it worse. Most organizations now run a mix of on-premises Active Directory and cloud identity providers like Entra ID and Okta, and every connection between them widens the attack surface. Worse still, a weakness in Entra ID or Okta often traces straight back to Active Directory, because Active Directory is usually the single source of truth everything else trusts. Crack the foundation, and the whole structure moves.

ACTIVE DIRECTORY IS AT THE CORE OF ENTERPRISE IDENTITY

Active Directory has run enterprise identity for over 25 years, and it remains in place at 90% of organizations worldwide. Most cloud identity providers are federated or synced to it, which means that even as you adopt newer platforms, Active Directory is still the foundation holding all of them up.

In fact:

- Adversaries breach a domain controller in more than 78% of human-operated intrusions.
- In 35% of those cases, the domain controller becomes the point from which ransomware spreads across the entire environment.

When the attack comes, Active Directory is often the one thing standing between you and recovery. Consider what that means: if you can't log into your own backup solution, you can't start recovering anything. Attackers understand this perfectly, which is why they increasingly hit your backup systems and your Active Directory at the same time. Take out both, and you no longer have a bad day. You have a hostage situation.

And the clock is merciless. A full Active Directory forest recovery can take days or even weeks, and every hour of downtime can cost organizations up to $730,000 per hour (*Forrester, The Total Economic Impact™ of Quest Recovery Manager for Active Directory Disaster Recovery Edition*).

Traditional backup tooling won't save you here. It can copy individual domain controllers and files, but it can't orchestrate the precise, ordered steps required to rebuild an entire Active Directory forest. Backing up the pieces isn't the same as being able to put them back together.

SUPPORTING DATA

32%

surge in identity-based attacks, H1 2025. 97% were password spray or brute-force

(Microsoft Digital Defense Report 2025)

22%

of breaches involved stolen credentials over-all; 88% of attacks on basic web applications specifically involved stolen credentials

(Verizon 2025 Data Breach Investigations Report)

35%

of cloud incidents were driven by valid account abuse

(CrowdStrike 2025 Global Threat Report)

Identity is the foundation of MVC and trust, now and in the future

A Minimum Viable Company (MVC) is the smallest, leanest version of an organization required to survive and maintain essential operations. When organizations are hit with a cyber incident, they don't fail to recover because their backups break. They often fail because they try to recover everything at once or in the wrong order.

The layer most organizations miss centers on trust and control, and identity sits squarely at the intersection of both. It's the skeleton key to the enterprise. If you can't establish a trusted identity, you can't safely restore anything else.

Identity and access management (IAM) is responsible for three core functions:

- **Identity lifecycle management:** Automates onboarding, role updates, and deprovisioning so access stays accurate as people join, change roles, and leave.
- **Authentication:** Verifies that someone is who they claim to be, typically through multifactor authentication (MFA) and single sign-on (SSO).
- **Authorization:** Grants each authenticated user the specific access they need to do their job, while restricting everything else.

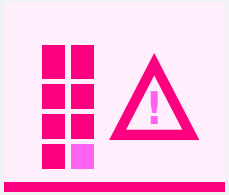
Put those three functions together and Active Directory, Entra ID, and Okta stop being plumbing and become the operational backbone of your business. They authenticate every employee, every application, and every transaction. This leads to one simple, uncomfortable truth: if identity infrastructure goes down, the business goes down with it.

And this operational backbone is about to get a lot more exposed. As organizations rush to adopt AI and agentic workflows, those agents depend on identity infrastructure to operate securely, and that shift is already visible in the data: 93% of organizations already use or plan to use AI agents for sensitive security tasks like password resets and VPN access (Semperis, May 2026).

Here's the part that should get your attention: these agents often borrow the identities of the employees who prompt them to carry out tasks and access sensitive data. Every one of them is a new set of keys. The stakes for securing, protecting, and recovering identity have never been higher.

SUPPORTING DATA

Active Directory and Entra ID are used by over 90% of enterprises worldwide (Semperis).



Active Directory is involved in 9 out of 10 cyberattacks, not because it's poorly built, but because it's everywhere (*Cohesity CERT*).

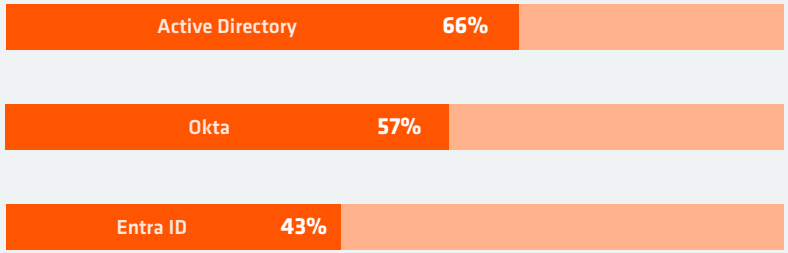
The intersection of identity, business continuity, and cyber resilience

Traditional business continuity planning treats identity like electricity: infrastructure you assume will be on when you flip the switch. That assumption is exactly where organizations get destroyed. Identity doesn't get to be an assumption anymore. It needs its own recovery plan.

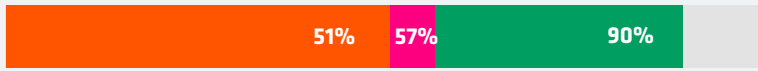
Cyber resilience flips that assumption on its head. It treats identity as the first thing that will be attacked and the first thing you must be able to bring back (independently, tested, isolated, and trusted) even when everything around it is compromised. The gap between "we assume it will work" and "we have proven it will" is exactly where organizations lose days or weeks after an attack. They can restore their files just fine. They just can't log a single person in to use them.

For security, IT, and executive leaders, the takeaway is blunt: business continuity and cyber resilience only succeed when proactive identity security and identity recovery are planned, tested, and resourced as disciplines of their own. Never assume they'll happen automatically while you restore everything else.

SUPPORTING DATA



Disaster recovery plans include Active Directory for only 66% of organizations, Entra ID for 43%, and Okta for 57%, leaving a large share of continuity plans with a blind spot at the identity layer itself *(Semperis, Nov 2025).*



90% of organizations scan for identity vulnerabilities, yet only 51% have remediation procedures, and just 57% automate identity recovery *(Semperis, Nov 2025).*

The cost of inaction

Let's talk about the price of waiting, because waiting is a decision too, and it's the most expensive one on the table. Not just financially, but operationally and reputationally.

That cost isn't one bill. It's three, and they compound:

- **The breach bill:** incident response, regulatory fines, and legal exposure
- **The downtime bill:** lost productivity, blocked revenue, and repeat attacks while the identity layer stays exposed
- **The trust bill:** rising cyber insurance premiums, executive liability, and deal risk

And waiting doesn't freeze the meter. The identity attack surface is among the most targeted in the enterprise, and one that traditional defenses can't keep pace with, so the price of inaction doesn't stay static. It climbs every quarter you leave it unaddressed. Delay isn't caution. It's compounding interest on a debt you never chose to take.

SUPPORTING DATA

Over three years, organizations can face a successful identity attack costing $1.2 million, manual monitoring of hybrid identity costing $109,000, and lost productivity and downtime from manual Active Directory recovery costing $3.9 million. *(Forrester Total Economic Impact study).*

The global average cost of a data breach is $4.44 million, but credential-based breaches cost roughly $4.67 million and take about 292 days to identify and contain, the slowest of any attack vector *(IBM Cost of a Data Breach 2025).*

Ransomware economics are shifting, but not painlessly: the median ransom payout fell to $115,000, and 64% of victims refused to pay, meaning more organizations are absorbing the operational cost of recovery instead of the ransom itself, adding more pressure on identity recovery speed *(Verizon DBIR 2025).*

8 out of 8 major cyber insurers now ask and validate identity-specific security and resilience when underwriting cyber policies, and demonstrating strong identity hardening directly correlates to lower premiums and higher coverage *(Cohesity, "Identity resilience is critical for cyber insurance").*

These aren't unrelated data points. They're the itemized breach bill and downtime bill, with the trust bill closing in right behind them as insurers tie premiums directly to your identity posture. Every one of them gets more expensive the longer identity stays unaddressed. You'll pay this bill regardless. The only question is whether you pay a little now, on your terms, or all of it later, on the attacker's.

CONCLUSION

Identity-based compromise now shows up in nearly every major breach, and the pattern never changes. Attackers don't break in. They log in with valid credentials and trusted identity flows and move undetected across environments never built to catch them. Then they steal your data, seize your systems, and deploy their ransomware.

None of this is inevitable.

What separates the organizations that recover in hours from the ones that spend weeks rebuilding trust in their identity services has nothing to do with luck, and nothing to do with how much they spent. It comes down to a single decision: whether they built identity resilience as its own discipline, across the entire attack lifecycle, before they ever needed it.

So treat identity resilience as what it has become: not optional, but a core requirement of enterprise security. Identity is your front door, your foundation, and your recovery bottleneck all at once. A patchwork of point tools will always fall short. So will any continuity plan that simply assumes identity will be there when the moment comes. The only strategy that survives contact with a real attack is the one you've tested and proved before you needed it.

The good news is that you can get ahead of this. You can accelerate cyber resilience for your most critical identity systems.

And we can help.

Learn more about how Cohesity can help build and strengthen identity resilience

Get a free identity security assessment to identify vulnerabilities and gaps across Active Directory, Entra ID, and Okta

COHESITY

6100036-001 EN 8-2026