

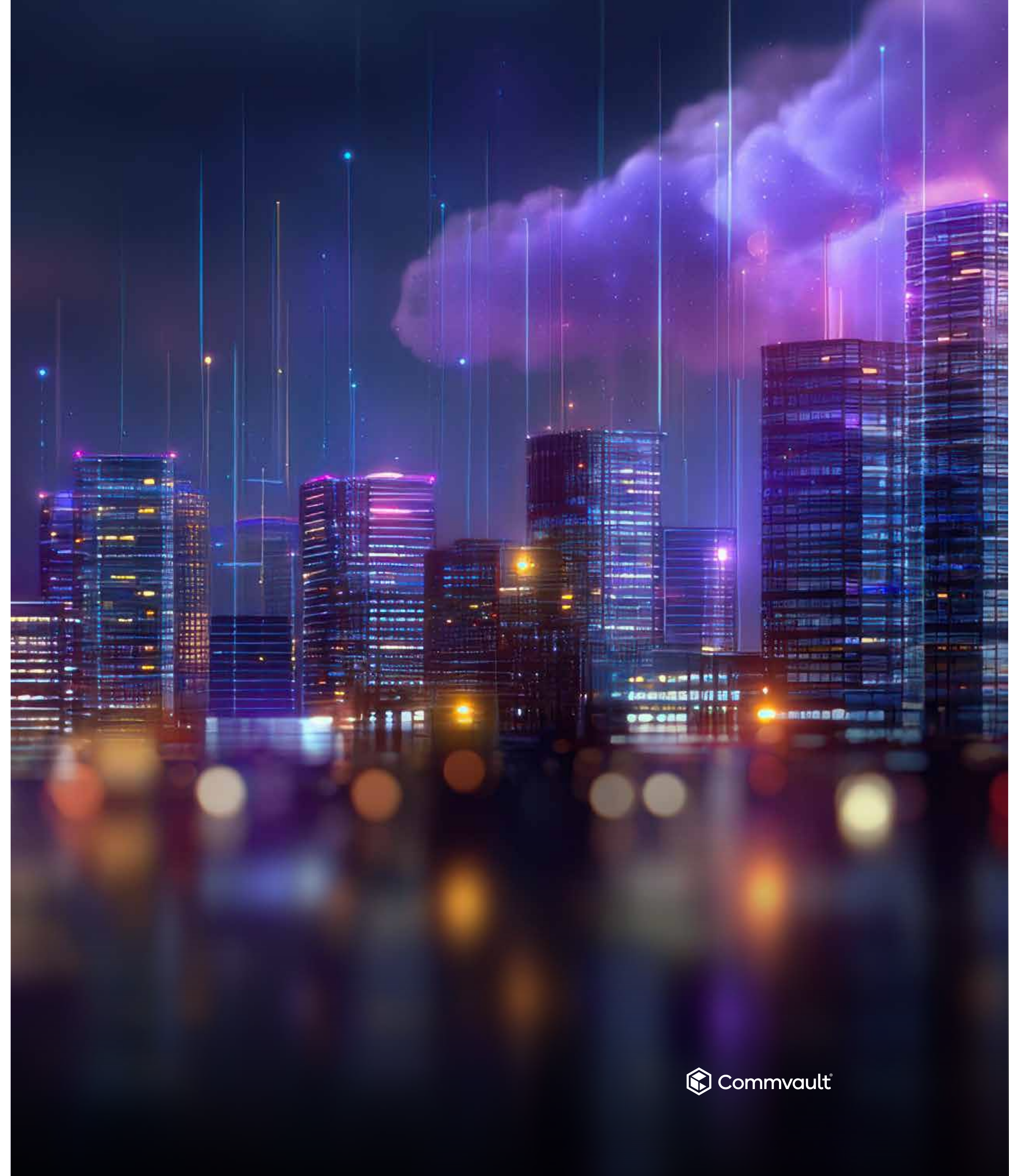
The Identity Recovery Gap

Why Restoring Access Isn't Restoring Trust

5 Pillars for Recovering Trusted Identity After Compromise

A Readiness Report for CIOs and CISOs

READINESS REPORT ISSUE 7 OCTOBER 2026



Executive Summary

Identity used to be a gate. Now it is the foundation everything else stands on. Seventy-nine percent of cyberattacks start with compromised identity,¹ and 82% of organizations have experienced at least one identity-based attack in the past year.² When identity breaks, every system, application, and user that depends on it breaks with it.

Most identity programs are built to answer yesterday’s question: Can we stop the attack? That question still matters, but it is no longer sufficient on its own. Frontier AI – a term encompassing the most advanced AI tools and models – has compressed the timeline. Now, some adversaries can begin lateral movement in as little as four minutes after a credential is compromised.³ Prevention alone cannot keep pace. The question every CIO and CISO needs an answer to now is different: Can we restore trusted identity after prevention fails?

This report helps reframe identity from a data security control into critical recovery infrastructure. It examines why identity availability is not the same as identity recoverability, and it lays out the five pillars – Assessment, Protection, Detection, Readiness, and Recovery – that organizations need to help close the gap between restoring identity systems and restoring trust.

79%
of cyberattacks start with compromised identity¹

82%
of organizations have experienced at least one identity-based attack in the past year²

¹ The State of Ransomware 2026, Sophos
² 2025 Future of Identity Security Report, ConductorOne
³ 2026 Annual Cyber Threat Report, ReliaQuest



How Does Today's Identity Security Compare to Yesterday's?

For years, identity security has answered one question: Can we stop identity attacks? More than likely, the answer was “Yes,” using a combination of multi-factor authentication, conditional access, and privileged access management.

While stopping an identity attack still matters a great deal, it is no longer the deciding factor that determines whether a business can survive an incident or not.

Today's pressing question is more nuanced: Can we restore trusted identity after an identity attack succeeds?

The distinction is not academic. Identity has become the primary attack surface and attack vector in the enterprise – 79% of modern breaches involve compromised identities, according to Sophos.⁴ When identity breaks, authentication breaks, and every application and system that depends on them breaks, too.

Frontier AI is compounding the problem. Attacks are faster and more autonomous, and some adversaries can begin lateral movement within as little as four minutes of an initial compromise.⁵ Detection and containment windows that once measured in hours now measure in minutes.

Most organizations may not be prepared. Only 24.7% have documented and tested their Active Directory (AD) and Entra ID recovery capabilities.⁶ The rest are operating on hope, not evidence.

⁴ The State of Ransomware 2026, Sophos

⁵ 2026 Annual Cyber Threat Report, ReliaQuest

⁶ Resilience Operations: The Discipline That Makes Readiness Provable, IDC (commissioned by Commvault), July 2026

Executive Takeaways

Prevention alone is not enough.

Build detection, response, and recovery into your identity program, too.

Put identity in your critical-service recovery plan

Map the identities, permissions, and access relationships the business needs to recover, not just the applications.

Recovery begins with trust.

Restoring systems and data means little if the identities accessing them are still compromised.

Identity availability is not the same as identity recoverability.

You need to restore a known-good identity state, not just bring identity services back online.

Validate recovery, don't assume it.

Test identity recovery regularly against realistic compromise scenarios.

The Target Challenge:

Can you quickly and safely recover trust after identity compromise?

Ask your team:

Can we securely access the systems we need to recover when identity itself is compromised?

Do we know what a known-good identity state actually looks like?

Have we tested identity recovery under realistic attack conditions – not just in theory?

The Five Pillars of Identity Resilience

Closing the identity recovery gap takes more than a better backup. Successful practitioners view it as a continuous discipline built on five pillars: Assessment, Protection, Detection, Readiness, and Recovery. Each pillar addresses a different part of the gap.

1. Assessment

Know Your Risk Before Attackers Do

You cannot protect what you cannot see. Assessment means regularly identifying the data security misconfigurations, such as excessive privileges and insecure settings, that give attackers their opening – before they use it.

The scope of what needs assessing keeps growing. According to the Cloud Security Alliance, 75% of organizations in 2025 engaged two or more identity providers, while 11% relied on five or more,⁷ underscoring the growing complexity of identity management in multi-cloud and hybrid environments. In addition, another report found that non-human identities outnumber human identities 144 to 1.⁸ The takeaway? Each one of those identities is a potential blind spot.

Yet 69% of security leaders admit they lack full visibility into identity vulnerabilities, and 55% lack visibility into admin access across their organization.⁹

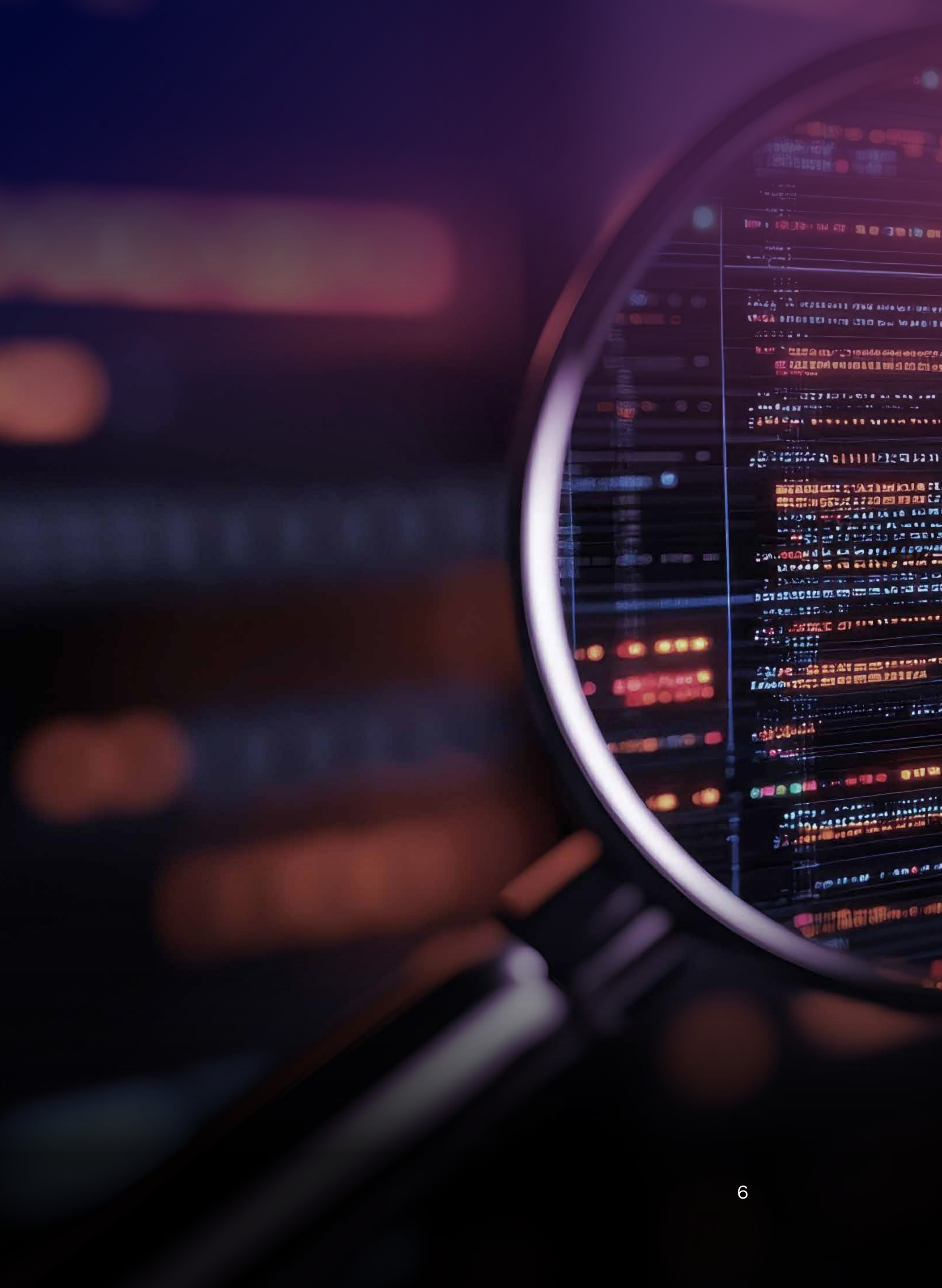
What to require

Frequent vulnerability assessment across your identity provider environments, with risk prioritized by impact and mapped to clear remediation guidance – not a point-in-time audit that’s outdated the day after you run it.

⁷ The State of Multi-Cloud Identity Survey 2025, Cloud Security Alliance

⁸ The NHI & Secrets Risk Report H1 2025, Entro Security

⁹ 2025 State of Identity Security, Cisco Duo



2. Protection:

Keep a Clean, Trusted Copy of the Truth

If your identity infrastructure and configuration data can be altered or deleted by the same compromised credentials that caused the breach, you don't have protection – you have a single point of failure.

Protection means maintaining secure, immutable, isolated copies of critical identity infrastructure and configuration, so there is always a version of the truth that attackers cannot touch.

Non-human identities make this harder to keep current. Service accounts and non-human identities get regular rotation or audits at just 34% of organizations, and continual review at only 11%,¹⁰ according to Sophos – a gap that creates exactly the kind of stale, unmonitored accounts attackers rely on for persistence.

What to require

Immutable, isolated backups of identity infrastructure across every provider you run – AD, Entra ID, Okta, and beyond – protected in storage that cannot be modified by compromised credentials.

¹⁰ [The State of Identity Security 2026](#), Sophos



3. Detection: Catch It While It's Happening

Identity attacks are quiet by design. Attackers who steal valid credentials look like legitimate users, which is exactly why they can evade traditional defenses.

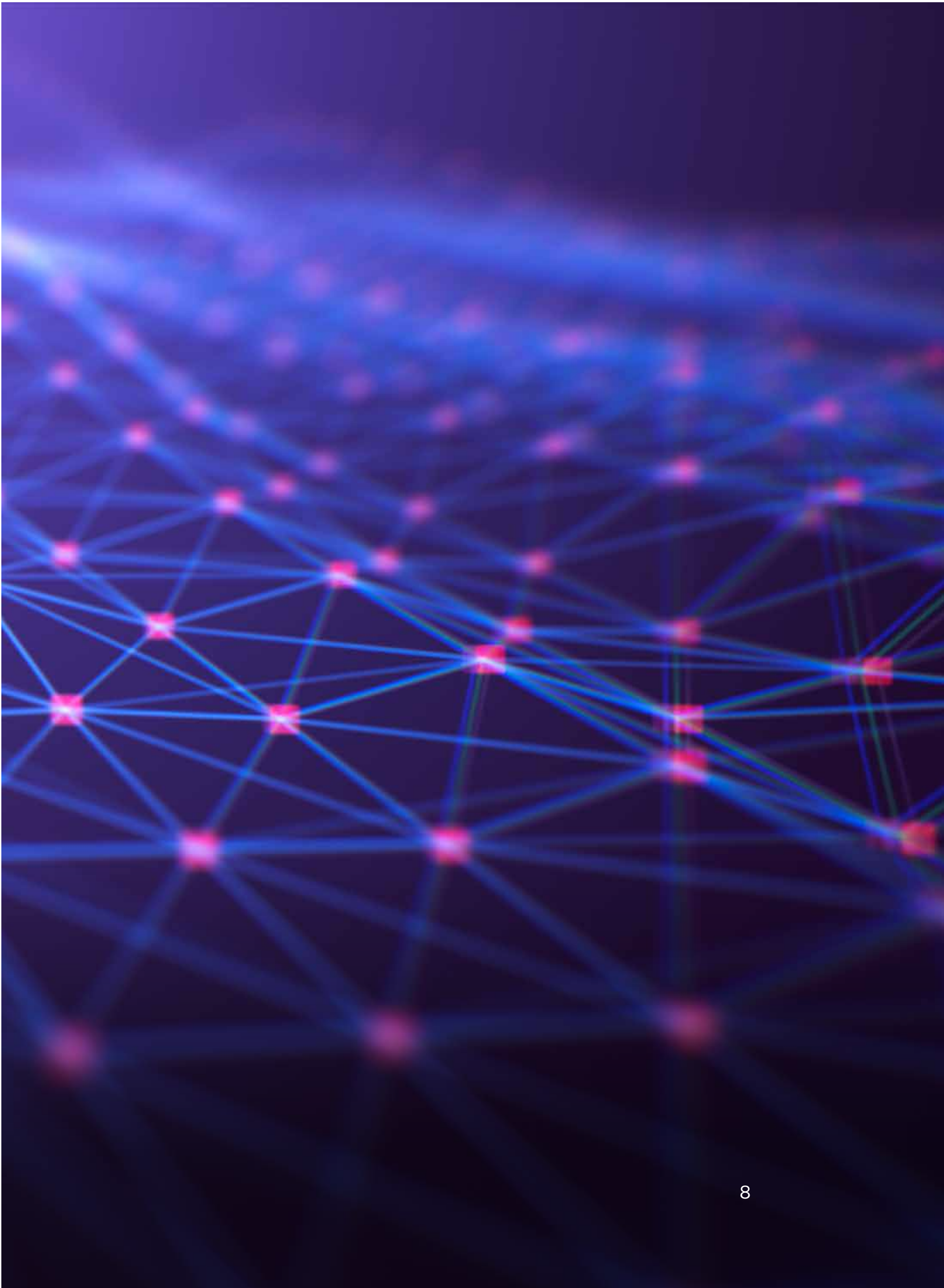
Detection means continuously monitoring for material changes, privilege escalation, and anomalous behavior across the identity environment. It also requires surfacing high-risk events immediately, with enough context to act.

Data illustrates how high the stakes already are. In 2026, organizations took an average of 247 days to identify and contain a breach, contributing to a record \$4.99 million global average breach cost.¹¹ The prolonged detection window highlights why identity attacks remain so effective and why continuous monitoring is essential to identify abnormal activity before attackers can establish persistence and expand their access.

What to require

Real-time auditing that captures who changed what, when, and where – with instant rollback of unauthorized or malicious changes, not just an alert for someone to investigate later.

¹¹ Cost of a Data Breach Report 2026, IBM



4. Readiness

Prove Recovery Before You Need It

An untested recovery plan is a hypothesis, not a capability. Readiness means regularly exercising identity recovery in a clean, isolated environment before an incident forces the question.

Most organizations are not there yet. Nearly 60% of organizations have limited or no cleanroom implementations, according to IDC, which means many organizations that do recover may be recovering directly into production, increasing the risk of reinfection from whatever compromised them in the first place. Only 24.7% report documented and tested AD and Microsoft Entra ID recovery capabilities.¹²

What to require

A consistent testing cadence, run in isolated environments, that validates your recovery workflows and clean restore points – so the first time you test recovery isn't during a live incident.

¹² Resilience Operations: The Discipline That Makes Readiness Provable IDC (commissioned by Commvault), July 2026



5. Recovery

Return to a Known-Good State, Fast

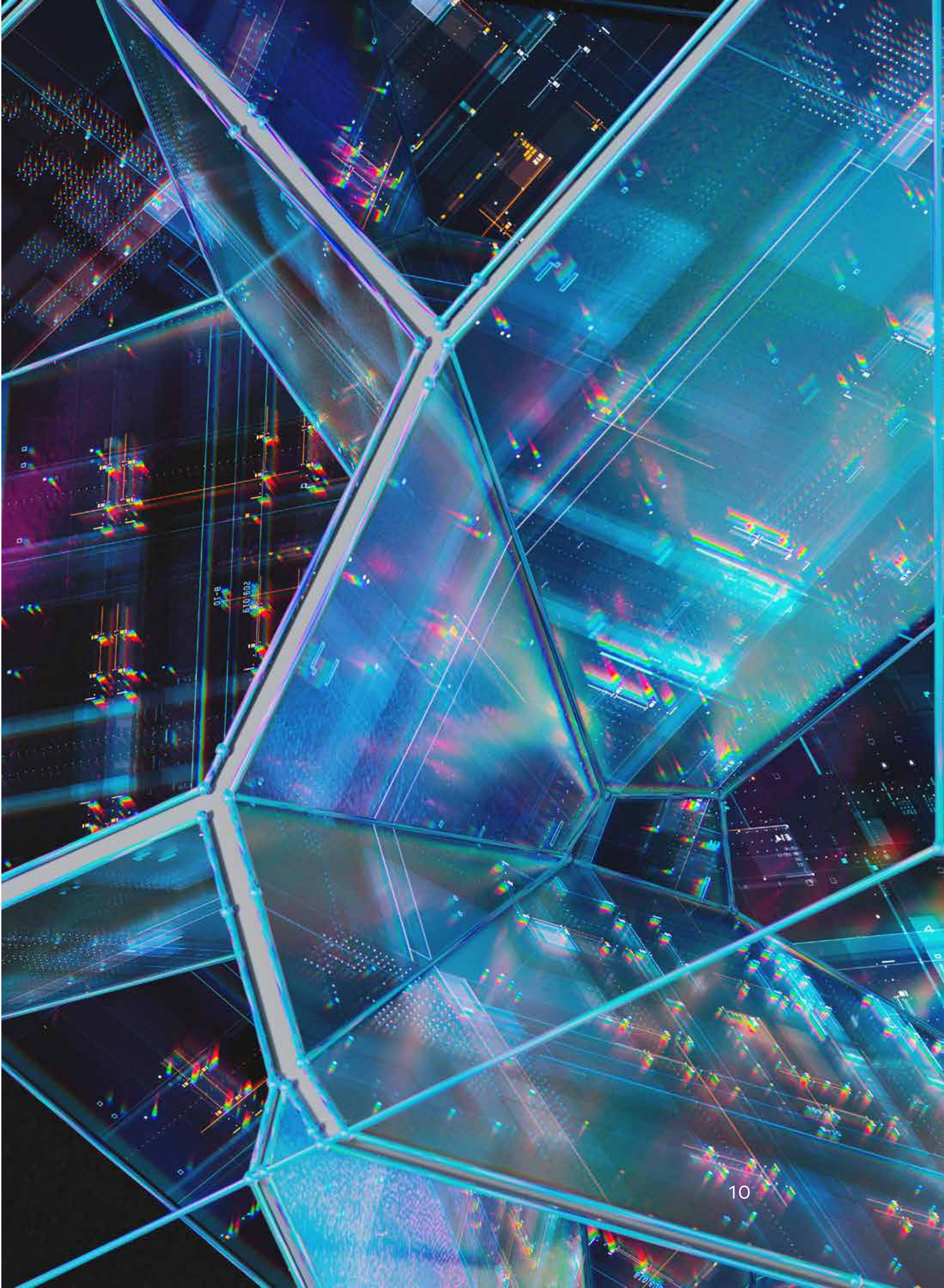
Detection without recovery may leave you watching the attack unfold. Recovery means rapidly restoring forests, domains, configurations, or individual objects to a known-good state – with the speed, precision, and confidence to help avoid reinfection.

The cost of getting this wrong may be steep, and specific to identity. Seventy-one percent of organizations experienced at least one identity-related breach in the past 12 months, averaging 3 attacks per affected organization, according to Sophos. The average cost to rectify an identity breach was \$1.64 million, with a median cost of \$750,000. Two-thirds of ransomware victims (67%) reported that the ransomware incident was the same event as their most significant identity attack – establishing a direct pipeline from identity compromise to ransomware impact.¹³

What to require

Multiple recovery paths - granular rollback for targeted remediation, and full forest recovery for worst-case scenarios - so the scope of your response matches the scope of the incident, not the other way around.

¹³ The State of Identity Security 2026, Sophos



The Identity Recovery Checklist

Before you face a potential incident, evaluate your organization against all five:

Assessment

Are you regularly identifying misconfigurations and exposures that attackers commonly exploit across every identity provider you run?

Protection

Do you maintain immutable, isolated copies of identity infrastructure that can help protect against compromised credentials?

Detection

Can you see material changes and privilege escalation as they happen, with enough context to act?

Readiness

Have you tested identity recovery in an isolated environment, under realistic attack conditions?

Recovery

Can you restore a known-good identity state - not just bring identity services back online - fast enough to matter?

As highlighted earlier, achieving identity resilience requires more than a single tool or a single moment. It takes a continuous loop: Assess to help reduce risk, protect to help preserve a trusted baseline, detect to help catch what slips through, regularly test to help prove readiness, and recover to help restore trust – then feed what you learn back into your assessment. Miss one step, and the model (and your resilience) may break.

Conclusion

Prevention will always matter. But prevention was never designed to answer what happens after an attack succeeds. That is: Can we come back, and can we trust what comes back?

Organizations that can answer **yes** – with evidence, not hope – will be better positioned to recover after the identity systems the rest of the business depends on are tested for real.

Additional Resources

The [Commvault Identity Resilience Assessment](#) will help you assess where you stand.

The [Identity Resilience Health Check](#) is a self-guided check against the six requirements every identity resilience strategy needs.

[Get Real About Identity Resilience eBook](#) will outline the business case and threat landscape behind this report.

Join [The CxO Exchange](#) on the [Readiverse](#) to connect with CIOs and CISOs that are building resilient identity operations.