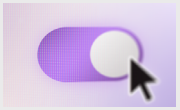
Commvault

eBOOK

GET REAL  ABOUT IDENTITY RESILIENCE: THE NEW  IMPERATIVE  FOR ENTERPRISE CYBER DEFENSE 

With most breaches tied to compromised credentials, organizations must move beyond prevention to build true identity resilience.

Identity systems like Microsoft Active Directory (AD), Entra ID, and Okta are the crown jewels of enterprise IT, authenticating users and controlling access to critical business systems. From workstation logins to physical building access, identity systems enable the seamless operation of organizations, making it the ultimate prize for cybercriminals.

But here's what most organizations don't realize: Traditional protection and recovery approaches for identity systems are fundamentally inadequate in today's threat landscape. The truth about identity resilience goes far beyond simple data protection: It requires a comprehensive strategy that anticipates sophisticated attacks and enables rapid recovery to a trusted state – at the speed of business.

When identity systems are unavailable or compromised, it can severely disrupt line-of-business applications and processes, blocking user access to vital systems and resources.

This is where identity resilience becomes critical. Identity resilience isn't just about backing up your directory – it's about building an identity infrastructure that can withstand, adapt to, and rapidly recover from sophisticated attacks while maintaining business continuity.

IDENTITY: THE PRIMARY ATTACK SURFACE

The reality of modern cyber warfare is that identity infrastructure has become the primary battleground. Attackers are no longer forcing their way in – they're logging in, using compromised credentials to gain legitimate access. Once inside, they can quietly move laterally across the environment, escalate privileges, and undermine recovery mechanisms before anyone even realizes what's happened.

The statistics paint a stark picture of the current threat landscape.

88%

of web application attacks used stolen credentials.[1]

82%

of organizations experienced at least one identity-based attack in the past 12 months.[2]

57%

of cyberattacks started with compromised identity.[3]

1 2025 Data Breach Investigations Report, Verizon
2 2025 Future of Identity Security Report, ConductorOne
3 The Identity Crisis Report, Varonis

IDENTITY ATTACKS ARE STEALTHY, SCALABLE, AND HARD TO DETECT

Identity-based attacks are especially dangerous because of their subtlety. By impersonating legitimate users, adversaries can blend into normal activity and evade traditional defenses.

Despite the variety of tactics used, these attacks share a common objective: exploit identity to gain authorized access and remain undetected.

Credential theft
(phishing, token theft, malware)

Privilege escalation through misconfigurations

Abuse of excessive permissions

Persistence via directory manipulation or backdoor accounts

Today, AI-enabled automation has accelerated these attacks to escalate privileges and move laterally faster. Organizations have less time than ever to detect compromise, contain impact, and recover.

THE COMPLEXITY OF IDENTITY PROTECTION

Identity sprawl impacts visibility and control.

Identity information exists everywhere – across on-premises systems, cloud platforms, SaaS applications. This explosion of identity data increases both visibility gaps and potential entry points for attackers.

Siloed tools create blind spots.

Identity risk is managed across disconnected tools and teams, making it harder to prioritize, spot issues early and slower to respond when incidents occur.

Complexity expands the attack surface.

Modern enterprises operate across complex, interconnected, and interdependent identity systems spanning on-premises and cloud environments, expanding the attack surface and making recovery harder.

Lack of resilient recovery.

Many recovery approaches are slow and complex, often forcing reliance on compromised backups or manual rebuilds, prolonging downtime and increasing risk.

These trends are converging to create a new operating reality:

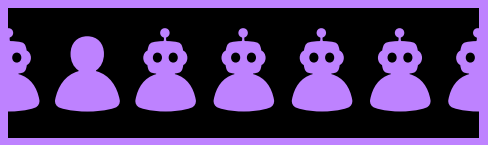
Identity is the most targeted layer of the enterprise.

Attacks are faster, quieter, and more difficult to detect.

Identity and access management (IAM) environments are more complex and interconnected than ever.

Fast, clean recovery is both more critical and more challenging than before.

144:1



ratio of non-human identities to human identities.[4]

75%

of organizations use multiple identity providers to manage enterprise identity.[5]

4 The NHI & Secrets Risk Report H1 2025, Entro
5 The State of Multi-Cloud Identity Survey, Strata

THE IMPACT OF IDENTITY-BASED ATTACKS ON ORGANIZATIONS

The importance of prioritizing identity resilience is evident when you consider its cascading effect on other workloads. Applications, file systems, email services, and databases all rely on identity for proper authentication and user access.

When identity systems are unavailable or cannot be trusted:

Workforce and customers cannot authenticate.

Applications and services become unavailable.

Recovery timelines extend to weeks or months.

Identity resilience recognizes this fundamental dependency. Because nearly everything in modern businesses relies on identity, building resilient identity infrastructure becomes the cornerstone of organizational resilience. This goes far beyond simply restoring identity systems after an attack occurs.

By establishing identity resilience practices, organizations may be able to better maintain control over their networks and systems even during active attacks, enforce data security and access policies, and provide a stable foundation that supports rapid recovery of other systems and services.

THE COST OF IDENTITY COMPROMISE

Financial losses

Identity-based attacks often result in financial impact that extends well beyond initial remediation. Organizations face immediate costs such as incident response, recovery, and downtime, alongside longer-term losses such as lost revenue and declining customer trust.

Reputational damage

Identity-related breaches can directly impact customer confidence and brand trust. Negative publicity and perceived security gaps can lead to customer churn, reduced loyalty, and long-term damage that is difficult to fully rebuild.

Operational disruption

Because identity underpins access to critical systems, attacks can halt business operations at scale. Employees, partners, and customers lose access to applications and services, productivity declines, and recovery efforts potentially impeded.

Regulatory exposure

When identity systems are compromised, unauthorized access to sensitive data can trigger serious regulatory and compliance consequences. Organizations may face fines, legal action, and increased scrutiny, particularly in highly regulated industries like finance and healthcare.

50%

of organizations reported security breaches linked to compromised machine identities in the past year.[6]

51%

experienced delays in application launches.[6]

44%

experienced an outage or disruption that negatively impacted customer experience.[6]

43%

of attackers were able to gain unauthorized access to data, networks, and systems.[6]

6 2025 State of Machine Identity Security Report, CyberArk

REAL WORLD IDENTITY BASED DISRUPTION: HOW SOCIAL ENGINEERING BROKE RETAIL AT SCALE

In 2025, a financially motivated threat group used coordinated social engineering tactics to compromise identity systems across multiple retail organizations in the United Kingdom, including the large global chain Marks & Spencer.[7]

Rather than exploiting software vulnerabilities, attackers targeted IT help desks and support processes – impersonating employees to reset credentials, bypass multi-factor authentication, and gain privileged access. Once inside, they moved quickly to escalate permissions, access internal systems, and disrupt operations.

In some cases, attackers leveraged this access to deploy ransomware, exfiltrate data, and interfere with business-critical services, demonstrating how identity compromise can rapidly evolve into full-scale operational disruption.

The breaches are estimated to have a total financial impact of

$592M[7]

Retail operations, supply chains, and customer-facing systems experienced significant outages and degradation.[7]

46 DAYS:

Time M&S paused online sales after the attack.[8]

7 The Hacker News
8 Reuters

HOW A HELP DESK CALL CAUSED MILLIONS IN DAMAGE

In a widely reported 2023 incident, MGM, a major hospitality and entertainment organization was brought to a standstill through social engineering.

Attackers impersonated an internal user and contacted the IT help desk, successfully convincing support personnel to reset credentials and grant access to privileged accounts. From there, they escalated access, moved laterally across systems, and ultimately disrupted core operations.

This example reinforces a key principle of identity resilience: Organizations must be prepared to rapidly detect and contain identity-based attacks, restore trusted access, and re-establish operations without prolonged disruption.

The attack cost the company over $100 million in losses due to system downtime – as well as $45 million in class action lawsuits related to the attack and a 2019 data breach.[9]

Customers expressed concerns about security and operational reliability.[10]

The incident triggered regulatory scrutiny and investigations related to compliance reporting and response practices.[10]

9 The Record
10 Inszone Insurance Services

THE SOLUTION: BUILDING IDENTITY RESILIENCE

ESSENTIAL COMPONENTS OF AN IDENTITY RESILIENCE STRATEGY

Identity resilience is the ability to rapidly detect, contain, and recover from identity attacks and other incidents while maintaining secure and dependable access for users and applications.

Core elements of a comprehensive identity resilience strategy include:

Proactive assessment to identify and prioritize risks and strengthen security posture.

Real-time monitoring and roll back capabilities, enabling faster detection and response to identity-based attacks.

Proven ability to restore identity infrastructure quickly and with confidence to a trusted state.

Visibility, response, and recovery across both on-premises and cloud-based identity providers.

HOW COMMVAULT® DELIVERS COMPREHENSIVE IDENTITY RESILIENCE

Building identity resilience requires a modern, unified approach. Commvault Cloud helps enable organizations to protect and rapidly recover identity systems – including AD, Entra ID, and Okta – against threats such as corruption, accidental deletion, and ransomware.

With a comprehensive approach to identity resilience, Commvault helps empower organizations to proactively assess risk, detect and contain threats in real time, and recover their identity provider environments quickly and confidently to a trusted state.

Vulnerability assessments

Helps you identify misconfigurations and exposures across your AD environment – such as excessive permissions and non-expiring credentials – and prioritize risks with clear, actionable remediation guidance, enabling you to strengthen your security posture and reduce risk.

Immutable protection

Helps protect identity backups in tamper-resistant storage that is designed to prevent modification or deletion by compromised credentials.

Real-time auditing and detection

Helps continuously monitor identity changes, including privilege escalation, persistence techniques, and anomalous behavior, enabling you to investigate and instantly roll back malicious or unauthorized changes.

Granular recovery

Helps restore exactly what is needed, down to specific users, groups, Organization Units, and even individual attributes, without impacting on the broader environment.

Automated, orchestrated recovery at scale

Helps you recover entire AD forests, multiple domains, and domain controllers through coordinated, automated workflows designed for complex, distributed environments.

Integrated recovery testing

Helps you gain confidence in cyberattack readiness through regular test recovery workflows, which help you validate your recovery plans and improve resilience.

BEYOND IDENTITY: THE COMPLETE CYBER RECOVERY STRATEGY

Staring down a cyberattack or ransom situation is a harrowing experience. Restoring identity systems is the first step in most cases, and finding ways to automate the otherwise time- and resource-intensive process can help jumpstart the recovery process and bring back the business quickly. Even better is when your identity recovery is built on the same platform the rest of your cyber recovery relies on.

True identity resilience extends beyond just identity provider protection – it integrates easily with your broader cyber recovery strategy. Unifying the cyber recovery and rebuild process on a common platform enables easy coordination, automation, and orchestration that spans more than just identity recovery – you can orchestrate the recovery of apps, data, clouds, and infrastructure.

This will help your teams work together to rebuild your systems following cyberattacks and disasters, and build resilience that delivers continuous business.

Learn more about Commvault® Identity Resilience

commvault.com | 888.746.3849 | get-info@commvault.com