druva

The Resilience Paradox
Restoring Trust After Identity Compromise

Whitepaper
Q426-20603

Executive Summary

As organizations accelerate cloud adoption, operationalize AI, and support distributed workforces, digital identities are the connective tissue of every business process. Every user, autonomous agent, and application depends on authentication and authorization to function.

At the same time, identity has become the primary attack vector. Modern adversaries prefer to log in rather than break in. Instead of exploiting software vulnerabilities first, bad actors compromise credentials, abuse privilege inheritance, manipulate OAuth relationships, or leverage non-human identities (NHIs) to gain illegitimate access.

This shift has created a resilience paradox. Without a trustworthy identity layer, business continuity is a myth. Users cannot access applications. Operations stall. Recovery workflows cannot proceed.

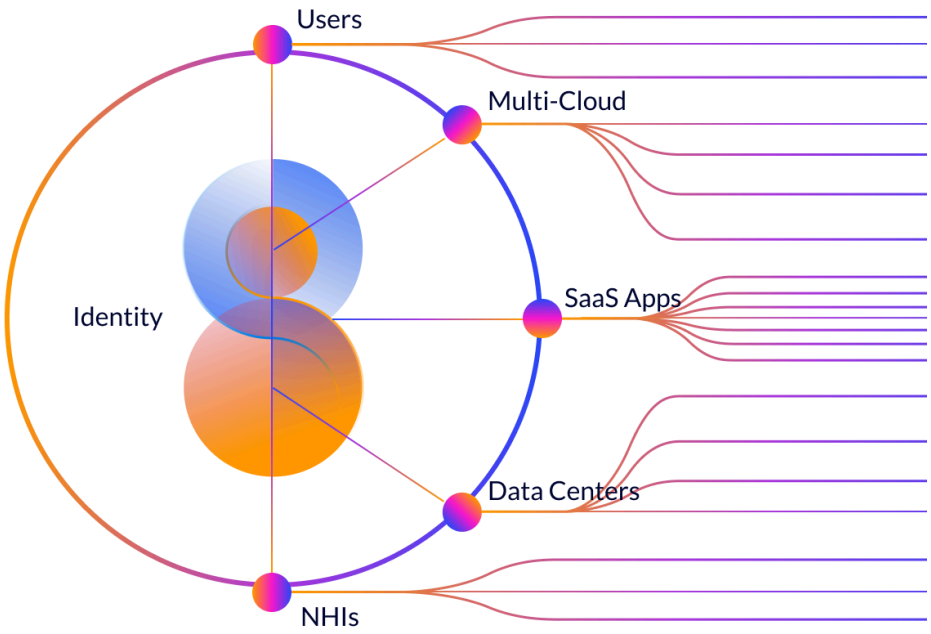
This whitepaper explores:

- Why identity is now a Tier 0 asset
- The anatomy of identity-based attacks
- Where traditional backup strategies fall short
- Why Identity Resilience
- How Druva enables organizations to restore trust across the identity-layer

Identity as a Mission-Critical Asset

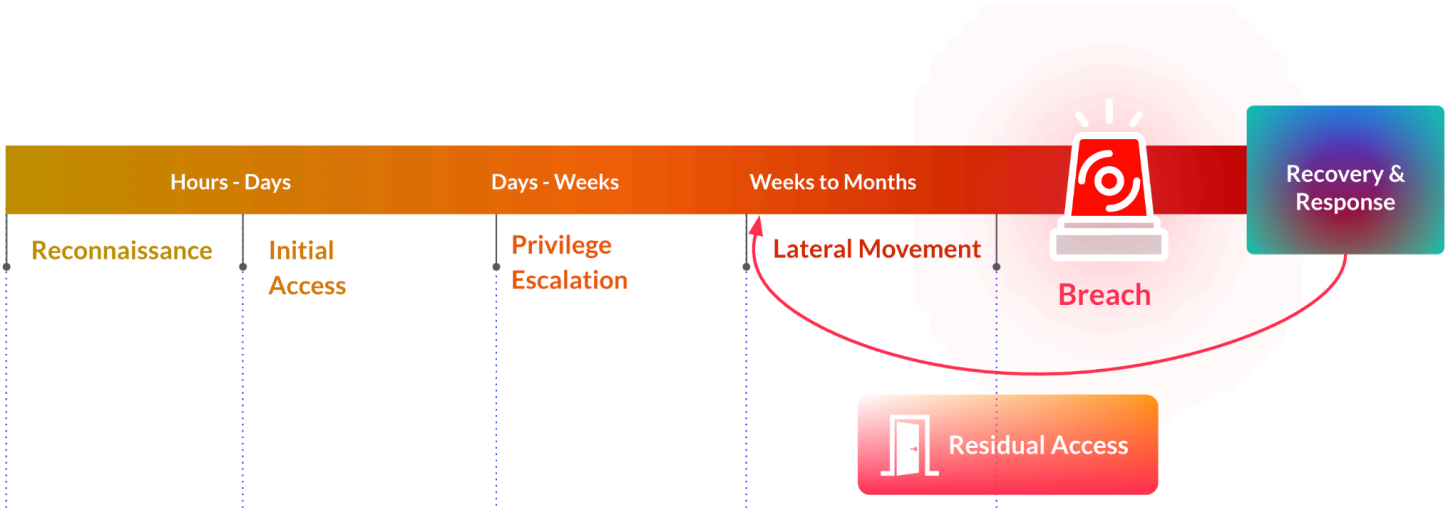
Identity providers (IdPs) such as Okta, Entra ID, and Active Directory (AD) now function as the control plane of the modern enterprise. They determine who has access to what and why. They authorize human users, govern NHIs, and serve as the authentication backbone for every app and workload.

As Tier 0 assets, IdP environments sit at the highest level of operational dependency. If identity is compromised, the entire enterprise is at risk. Without a functioning identity layer, access is severed, and restoring other systems is nearly impossible. Trustworthy access must be re-established before applications, data, or infrastructure can safely come back online. In this sense, identity is not simply another workload; it is the root of trust upon which all recovery depends.



The Anatomy of Identity-Based Attacks

Identity-centric attacks are stealthy by design. They exploit legitimate access pathways rather than obvious vulnerabilities, making detection, response, and clean restoration significantly more difficult. Often, by the time ransomware is deployed or data is compromised, the identity fabric itself has already unraveled.



Reconnaissance

An attacker typically begins with reconnaissance, acquiring credentials through phishing campaigns, infostealer malware, or dark web marketplaces.

Initial Access

With valid credentials in hand, the adversary disguises themselves as a legitimate user to map directory structures, enumerate roles, and analyze privilege paths.

Privilege Escalation

Privilege escalation often follows. Misconfigurations are exploited. OAuth grants are abused. High-privilege accounts are targeted.

Lateral Movement

Malicious changes are introduced quietly, blending into normal administrative activity to hide in a crowd. Persistence mechanisms are also established to ensure residual access.

Breach

The attack escalates. Ransomware is deployed. Data is extorted. Accounts and systems are locked down to maximize operational disruption and damage.

Recovery & Response

Recovery efforts begin as teams restore access, data, and systems—yet, hidden backdoors unknowingly reintroduce threat actors back into environments.

Why Traditional Backup Falls Short

Traditional backup solutions were designed to recover data from operational disruption, natural disasters, or site failure and do not account for the modern nature of cyber threats. They assume that the environment into which objects are restored is fundamentally secure and trustworthy. Yet, when identity is under attack, that assumption breaks down. Put differently, operational recovery fails when identity is compromised.

Restoring users, groups, or configurations without accurately validating their relationships and verifying a clean state can inadvertently reintroduce compromise. Orphaned accounts or hidden backdoors may remain active, enabling bad actors to quickly regain access immediately after recovery.

This reinfection loop is one of the most costly and frustrating outcomes of recovering from identity compromise. Recovery appears successful, only for the adversary to re-emerge using residual access. This underscores the paramount need for businesses to have effective and verifiable ways to restore IdP environments while truly uprooting and severing adversary access.

Embracing A Forward-Thinking Mindset

To effectively mitigate identity-based threats, organizations must evolve beyond conventional, object-centric backup methodologies. Identity Resilience represents a fundamental shift in mindset.

It marks the necessary evolution of treating identity not as a workload to be protected, but as critical infrastructure required by organizations to survive an attack. Data security and recoverability play an essential role in this equation, delivering an immutable foundation and high-fidelity signals necessary to clearly understand risk, withstand compromise, and rapidly reinstate trusted access to users, environments, and applications.

Existing Data Protection Challenges

- Fragmented coverage
- Lack of observability
- Native gaps
- Script-heavy solutions
- Limited recoverability
- Reinfection loops

Druva Identity Resilience

Druva Identity Resilience is purpose-built to defend identity as the foundational layer of the modern enterprise. We provide centralized protection, recovery, and detection across Okta, Entra ID, and Active Directory, safeguarding disparate Identity Provider (IdP) environments from our immutable, fully managed cloud-native platform.

This is all underpinned by our identity-aware insights, powered by Dru MetaGraph, which demystifies the identity layer and provides organizations with clear context on which activities matter, why they matter, and what action to take next.

The result is confidence when you need it most: the ability to purge threats, prevent reinfection, and safely re-establish a trusted identity layer—all delivered with the simplicity, security, and savings of enterprise-grade SaaS.

Unified Protection

Centralizes governance and recoverability across Okta, Entra ID, and Active Directory within a single SaaS platform. This eliminates hybrid silos and establishes a consistent source of truth across identity environments. This brings clarity, confidence, and compliance to today's volatile and high-risk identity layer.

Cyber Recovery

Enables precise, identity-first restoration. Through granular rollbacks, automated orchestration, and validation gates, organizations can re-establish a trusted authentication layer before restoring applications and data. This sequencing accelerates recovery while preventing reinfection.

Detection and Response

Provides contextualized insight into identity risk. By continuously assessing identity states and behaviors, Druva surfaces high-fidelity signals around privilege drift, persistence mechanisms, and suspicious access patterns, driving informed action grounded in evidence, n guesswork.

Identity-Aware Insights, Powered by Dru MetaGraph

Unlike conventional tools that treat identity as static objects, our graph-powered architecture maps and analyzes the intricate relationships between human users, NHIs, and the data we protect in the data center, across clouds, and at the edge. This provides a precise view into identity states and deviations over time to inform more effective protection, containment, and response outcomes across the entire identity fabric.

Key Benefits

- Consistently protect, govern, and recover hybrid IdP environments
- Understand identity-centric risks and drive evidence-based response
- Determine clean restore points, enforce validation gates, and reinstate access
- Uproot adversaries, eliminate reinfection loops, and surgically seal backdoors

Next Steps

Organizations that treat identity as recoverable infrastructure — not merely another workload to protect — will be positioned to withstand the next generation of cyber threats.

Visit druva.com to learn how Druva Identity Resilience can help you establish a hardened root of trust and accelerate secure recovery across your enterprise. Schedule a demo to experience identity-first resilience in action.

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com