

Industry-First Identity Protection for the Hybrid Enterprise

Identity resilience starts with behavioral insights. Druva is fully managed, cloud-native, built for identity-first recovery.

The Challenge: Identity is Tier 0 infrastructure

Identity providers (IdPs) are the verifiable gateway for users to access all digital tools, making them Tier 0 assets and the linchpin of the modern IT ecosystem. However, this critical role makes them a primary target. Compromised IdPs can serve as a Trojan horse, enabling attackers or rogue insiders to escalate privileges, propagate attacks, steal data, deploy ransomware, or sever widespread access to critical systems. Without a clean and functional IdP, restoring any business-critical workload is nearly impossible, leading to extended downtime and mounting costs.

Despite this clear and escalating risk, many businesses remain vulnerable by relying on conventional backup approaches that don't address modern identity-based threats. Organizations must adopt a security-centric strategy that closes the gap between identity management and data protection. This approach proactively mitigates risk while ensuring the reliable, full-fidelity recovery of digital identities exactly when needed. Current challenges include siloed protection across platforms like Okta, Entra ID, and AD; limited visibility into risk; and critical gaps in native backup, which contribute to manual, script-heavy restoration processes that can lead to reinfection loops and recovery latency extending downtime from hours to weeks.

Why Identity Resilience?

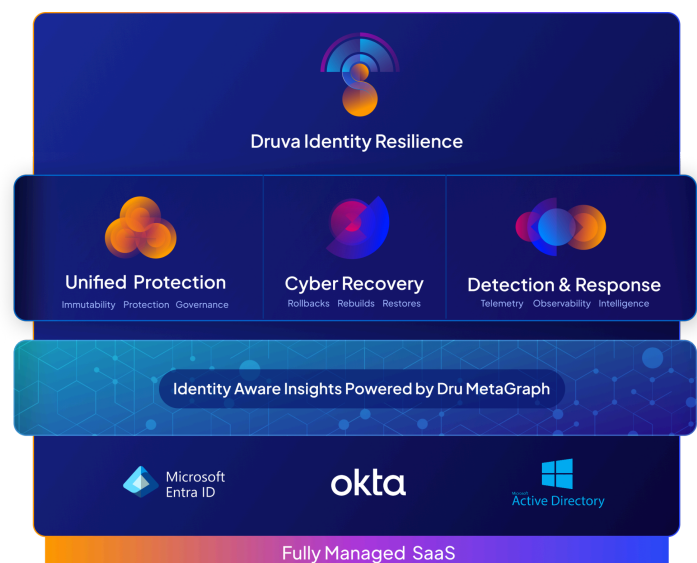
Identity Resilience marks a fundamental shift from reactive protection to proactive defense. It treats identity not as a perimeter to be defended, but as critical infrastructure required by organizations to survive an attack. Advanced data protection and recoverability play an essential role in this equation, delivering an immutable foundation necessary to secure business data, withstand compromise, and rapidly reinstate trusted access to users, non-human identities (NHIs), agents, environments, and applications.

Introducing Druva Identity Resilience

Unlike solutions that treat identity as an isolated workload, **Druva Identity Resilience** delivers comprehensive protection broadly across Okta, Entra ID, and Active Directory through a fundamentally different, identity-aware approach.

At the core of this is **Dru MetaGraph**, our common data graph that continuously assesses user activity, privileges, access paths, relationships, and the data we protect to model the identity layer as a dynamic system over time. This architectural understanding unlocks high-fidelity signals around malicious behaviors such as abuse, privilege drift, and persistence mechanisms.

Teams can use this context to assess suspicious human identities or NHIs, visualize changes and blast radius, and determine the trusted state that existed before compromise. With layered security, built-in intelligence, and accelerated response, Druva's fully managed SaaS platform delivers the missing layer of intelligence — revealing which identity-based risks matter and what actions should follow — to guide response, containment, and recovery.





Unified Protection — Get an immutable source of truth that centralizes protection, governance, and compliance to guarantee recovery-readiness across fragmented on-premises, cloud, and hybrid IdP environments — all from a fully managed SaaS platform.



Cyber Recovery — Reimagine resilience with identity-first cyber recovery that combines guided containment recommendations with granular, curated rollback options to purge persistent threats and restore identities to trusted pre-compromise states.



Detection & Response — Move beyond guesswork with AI-powered behavioral assessment that connects suspicious identity activity, visualizes blast radius, and contextualizes changes against attacker techniques to accelerate investigation and response.

Supported Identity Platforms

Okta

- Automated backups for key Okta objects, attributes, and relationships, establishing a trusted source of truth.
- Instantly restore your entire tenant or specific objects to their pre-attack state using an immutable, air-gapped backup.

Microsoft Entra ID

- Protection for critical identity objects and configurations used across Microsoft cloud services and beyond.
- Fast restores that re-enable access for users and applications, reducing downtime and ensuring business continuity.

Active Directory (AD)

- Backup security for critical AD objects, attributes, and components across domain and forest environments.
- Surgical object-level restore and automated forest-level recoveries to bounce back from outage, deletion, or attack.

Key Features & Benefits

- **Unified Hybrid Continuity & Policies:** Achieve total resilience with a single, converged solution that protects Okta, Entra ID, and Active Directory, while enabling orchestrated recoverability across the entire enterprise workload estate. Eliminate security "seams" and prevent "security drift" by enforcing trusted policies and uniform configurations across the entire hybrid identity fabric.
- **Orchestrated Identity-First Recovery:** Drastically reduce downtime with comprehensive rollback, restore, and forest-level recoveries. Automate and orchestrate workflows to unblock downstream application recovery and get users, AI agents, and business operations back online faster.
- **AI-Powered Behavioral Insights:** Get the distinct advantage of Druva's unique data foundation to accurately assess identity behaviors and fast-track investigation without relying on manual log analysis. Map identity relationships over time, understand suspicious behavior and propagated changes, and pinpoint possible persistence, privilege escalation, and changes to conditional access policies
- **Guided Cyber Recovery:** Quickly assess suspicious human or NHI activity, visualize impacted objects, leverage evidence-backed context for containment, and rapidly recover back to last known trusted states.
- **Clean-State Integrity & Reinfection Prevention:** Break the reinfection loop by rolling environments back to guaranteed, verifiable clean states. By surgically identifying and closing hidden backdoors during recovery, organizations can restore operations with absolute confidence while uprooting access for bad actors and rogue internal users.
- **Tamper-Proof Immutability:** Minimize the threat of internal and external attacks with logical isolation and immutability that prevents data tampering, alteration, or deletion, ensuring a pristine source of truth for trusted recovery.

Differentiators

- **Single-Codebase:** As a 100% homegrown solution, we eliminate the "Frankenstein" complexity to ensure seamless interoperability, uniform protections, and a consistent user experience across the entire Druva platform.
- **Data Visibility:** Our SaaS native architecture provides a unified "source of truth" across the identity landscape for improved telemetry and cross-workload visibility—ensuring data-rich insights and instant scalability without management overhead.
- **SaaS Resilience:** Druva's SaaS-delivered platform offers a light-touch experience for organizations to secure their entire identity fabric—without the operational overhead, egress costs, or security vulnerabilities of managing backup hardware.
- **Trusted Recovery:** We ensure data integrity and verifiable recoveries through rapid, high-fidelity restoration that preserves and reinstates the integrity of IdP environments. This includes both surgical object rollback and at-scale forest-level reconstruction that quickly rebuilds complex environments back to pristine golden states. Recommended recovery plans identify clean snapshots and provide granular object-level rollback options, allowing administrators to review and tailor recovery before execution.
- **Embedded AI:** AI-powered analysis turns identity metadata, activity, permissions, and configuration changes into actionable insight—helping administrators understand suspicious behavior, assess impact, and make more informed containment and recovery decisions.

Learn More

With 90% of breaches utilizing compromised credentials, Druva bridges the gap between identity management and cyber recovery. Unifying protection for Okta, Entra ID, and Active Directory into a single, hardened, and trusted platform, Druva delivers immutable security, actionable intelligence, and orchestrated recovery. Organizations get proactive protection with enhanced cyber-readiness across the entire identity layer, ensuring operations remain secure, data remains accessible, and recovery remains absolute.

Learn more: visit druva.com/use-cases/saas-apps-and-endpoints/identity-resilience

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

Druva is the resilience foundation for the AI enterprise, helping organizations secure and recover from connected risk across data, cyber, identity, and AI. The Resilience Cloud is a fully managed, cloud-native SaaS platform that delivers air-gapped and immutable protection across cloud, SaaS, on-premises, endpoint, and edge environments. Powered by Dru MetaGraph, Druva's graph-powered intelligence layer, the platform connects critical business context so customers can understand risk, respond faster, recover cleanly, and govern data with greater confidence.

Trusted by nearly 7,500 customers, including 75 of the Fortune 500, Druva helps safeguard the critical information and systems businesses depend on in an increasingly connected world. Visit druva.com and follow us on [LinkedIn](#) and [Facebook](#).