Druva Identity Resilience for Microsoft Active Directory (AD)

Identity resilience starts with behavioral insights. Druva delivers fully managed, cloud-native protection for Active Directory. Minimize disruption and downtime with air-gapped, immutable backups, surgical rollbacks, and automated forest recoveries.

Microsoft Active Directory (AD) remains the operational heart of most enterprises, controlling access to servers, endpoints, and applications across the environment — and syncing identities to cloud providers like Microsoft Entra ID and Okta. When AD is disrupted by ransomware, accidental deletion, corruption, or infrastructure failure, the business impact is immediate: users can't authenticate, apps can't authorize, and operations grind to a halt.

The Challenge: The "Identity Gap"

Many organizations still protect AD using legacy or native tools (for example, Windows Server Backup) that were not designed for modern cyber threats or high-pressure recoveries. This creates an "Identity Gap" between the sophistication of today's attacks and the tooling available to restore identity services quickly and safely.

Common risks include:

- **Single Point of Failure:** If AD is encrypted or corrupted, authentication and access to critical services can stop across the enterprise.
- **Slow, Monolithic Restores:** Lack of built-in capabilities requires admins to endure highly manual processes that prolong downtime.
- **Lack of Granular Visibility:** Native tools create dangerous blind spots, allowing subtle attacks and rogue account creations to go unnoticed until the damage is already done.
- **High Operational Complexity:** Forest recovery can be cumbersome and error-prone, requiring specialized expertise and manpower during a crisis.

The Solution

Druva Identity Resilience for Microsoft Active Directory is a fully managed SaaS solution that delivers secure, isolated backups and simplified recovery workflows designed specifically to restore trust and function in the face of AD outages and identity-based attacks.

Customer Benefits

- **Unified Management:** Protect hybrid identity environments (AD, Entra ID, Okta) from a single, cloud-native platform.
- **Air-Gapped and Immutable Protection:** Tamper-proof and isolated backups to withstand credential compromise and ransomware.
- **Automated Forest Recovery:** Orchestrate entire rebuilds or AD forests and re-establish your "root of trust" after deletion, corruption, or attack.
- **Reduced Recovery Time:** Move from days of manual rebuild toward automated, friction-less recovery.
- **Granular Control:** Restore only what objects you need without restarting Domain Controllers or performing broad rollbacks.
- **Audit-Ready Operations:** Demonstrate proof of recoverability for compliance needs with immutable logs and reporting.

© Copyright 2026 | Druva Inc. | druva.com

Use Cases

Cyber and Disaster Recovery (Ransomware, Outages, Corruption)

- **Scenario:** Domain Controllers are encrypted, the Global Catalog is corrupted, or a major infrastructure event breaks the forest.
- **Druva:** Automate forest-level restores to accelerate RTO and prevent reinfection.

Operational Recovery (Human Error)

- **Scenario:** An admin deletes an OU, breaks a GPO, or overwrites critical objects.
- **Druva:** Granular object-level restore to recover precisely what changed without rolling back the entire domain.

Compliance and Audit Readiness

- **Scenario:** Auditors require evidence of recoverability and tracking of identity-related actions.
- **Druva:** Immutable audit logs and reporting for backup/restore actions help in compliance audits.

Hybrid Identity Recovery

- **Scenario:** A cyberattack, infrastructure failure, or human error compromises your Active Directory and Entra ID environments, halting access to critical business resources.
- **Druva:** Rapidly restore hybrid AD and Entra environments within minutes from a single pane of glass.

Key Features

- **Comprehensive Coverage:** Protect Users, Groups, Devices, Contacts, OUs, GPOs, AD FS, and Domain Controller configurations.
- **Automated Schedules:** Flexible schedules (daily/weekly, etc.), with default daily full system state on each DC.
- **Forest-Level Recovery:** Automated, full rebuilds of one or multiple forests.
- **Secure Storage:** Encryption in transit (TLS 1.2+) and at rest (AES-256); supports Druva KMS and BYOK.
- **Granular Object Restore:** Restore Users, Groups, Devices, and OUs without restarting DCs.
- **Clean Recoveries:** Pre-incident restore points that prevent malware reinfection.
- **GPO Restore:** Restoration for individual GPOs, links, or all GPOs.
- **Centralized Dashboard:** Backup status, success/fail rates, and utilization across Domain Controllers.
- **Role-Based Access Control:** Purpose-built roles (e.g., Cloud Admin and Active Directory Admin).
- **Alerting:** Notifications for backup failures and restore activities via email.
- **Audit Logging:** Immutable logs for critical events and administrative actions.

Why Druva?

Druva delivers fully managed SaaS data security and resilience — eliminating infrastructure overhead while strengthening cyber readiness across critical platforms. Druva extends that proven approach to identity resiliency with AD protection designed for fast, confident recovery.

Visit druva.com/use-cases/saas-apps-and-endpoints/identity-resilience/active-directory to learn more.

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, X (formerly Twitter), and Facebook.