

Cyber Resilience Across Clouds

Simplify cloud-native data protection across AWS and Azure with no hardware, no agents, and no silos.

The challenge

As cloud adoption accelerates, organizations are shifting critical workloads to AWS and Azure. But legacy backup systems — built for on-prem environments — and native tools like AWS Backup and Azure Backup weren't designed for today's cloud-native demands. These tools lack true air-gapped security, cross-cloud flexibility, and cost-efficient scalability.

Meanwhile, ransomware threats and compliance pressures are intensifying. Native and legacy tools fall short in providing cyber resilience and scalable protection. Additionally, rising storage costs driven by hidden egress fees and inefficient replication are forcing enterprises to seek better solutions.

The Solution

Druva provides a cloud-native, fully managed SaaS platform purpose-built for AWS and Azure environments. It delivers immutable, air-gapped, and policy-driven data protection, eliminating the need to manage infrastructure or worry about hidden costs. Druva simplifies operations and secures workloads at scale — without sacrificing compliance or flexibility.

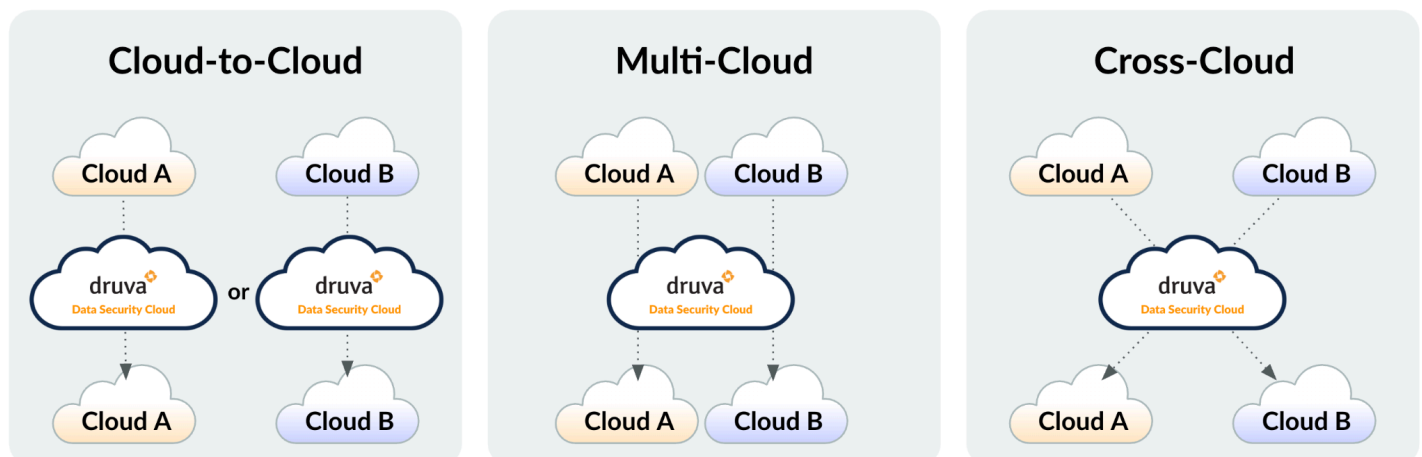
Business challenges

- **Security Risks:** Native tools store backups in the same cloud, making them vulnerable to ransomware and accidental deletion.
- **Lack of Cross-Cloud Protection:** No way to move or store data across clouds, leading to vendor lock-in and cloud concentration risks.
- **Rising Cloud Storage Costs:** Native replication is expensive, with added egress and storage fees that drive up TCO.
- **Operational Complexity:** Managing multiple tools adds time, cost, and risk — especially in hybrid or multi-cloud environments.

Key benefits

- **Immutable, Air-Gapped Data Security:** Safeguards against ransomware, insider threats, and compliance failures.
- **True Cross-Cloud Backup:** Seamlessly protect AWS and Azure workloads with no vendor lock-in.
- **Up to 40% Cost Reduction:** Global deduplication and zero egress fees slash storage costs.
- **Agentless, Fully Managed SaaS:** No hardware, software, or maintenance required.
- **Built-In Compliance & Cyber Resilience:** Includes threat detection, legal hold, and automated policy controls.

Ideal for Every Cloud Strategy



How It Works

Druva's SaaS-native architecture provides a unified platform to simplify and secure cloud data. Whether you're operating in AWS, Azure, or across both, Druva ensures air-gapped, policy-driven protection and seamless recovery — with no infrastructure to deploy or manage.

The Benefits

Cloud-to-Cloud Data Protection

For organizations fully in AWS or Azure, Druva offers air-gapped, immutable backups within the same cloud ecosystem. This ensures scalable, policy-driven protection and fast recovery — unlike native tools that store backups alongside production data and lack advanced controls.

Multi-Cloud Data Protection

Enterprises using both AWS and Azure gain a unified platform with Druva. Agentless deployment and global policy automation reduce complexity while maintaining robust data security across environments, simplifying operations, and improving control.

Cross-Cloud Data Protection

Industries like finance, healthcare, and government require resilience beyond a single cloud. Druva enables secure cross-cloud backup across AWS and Azure while maintaining compliance — ensuring availability even in the face of provider outages or regional incidents.

Lift-and-Shift Data Protection

Organizations migrating SQL, Oracle, or file servers to the cloud need enterprise-grade protection. Druva secures these workloads with air-gapped backups and storage-efficient deduplication, ensuring seamless protection and recovery across Amazon EC2 and Azure VMs.

Proactive Cyber Defense and Threat Hunting

Druva delivers advanced threat hunting and recovery tools to strengthen cloud security. Organizations can detect threats in backed-up data using on-demand threat hunting and assess infection timelines using rich metadata, accelerating response and recovery efforts.

Identity Resilience for Cloud Native

Cloud-native identity resilience requires managing a mix of Okta, Entra ID, and Active Directory across AWS and Azure. Druva bridges identity management and cyber recovery, unifying protection on a hardened platform. This delivers immutable security, intelligence, and orchestrated recovery for proactive cyber-readiness and absolute recovery.

Why Druva?

Druva is the only 100% SaaS platform offering secure, cross-cloud backup with built-in cyber resilience. Unlike traditional or native solutions, Druva eliminates infrastructure complexity, delivers cost efficiency, and empowers organizations to scale protection confidently.

- **No hardware, no software, no complexity** – Fully managed SaaS platform with agentless deployment.
- **Air-gapped, immutable protection** – Resilient against ransomware and insider threats.
- **Cross-cloud backup** – Unified protection for AWS and Azure workloads.
- **Cost optimization** – Up to 40% storage savings with zero egress fees and global deduplication.
- **Regulatory compliance** – Simplifies governance for regulated industries.

For More Information

druva.com/use-cases/multi-cloud-resiliency

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 industry's leading SaaS platform for data security, and the only vendor to ensure data protection across the most common data risks backed by a \$10 million guarantee. Druva's innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Security Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).