Druva for Microsoft Azure VMs

Druva's agentless, SaaS-based platform delivers air-gapped, cyber-resilient backups for Microsoft Azure Virtual Machines (VMs). With built-in immutability, zero infrastructure, and unified cloud protection, Druva empowers organizations to recover faster, reduce storage costs, and simplify operations—without relying on fragmented native tools.

The challenge

Legacy and native backup tools were designed for operational recovery—not cyber resilience. When primary data and backups reside in the same Azure tenant—without identity isolation or robust ransomware protection—organizations face heightened risk of data loss, compromise, and extended downtime. Managing protection across regions and subscriptions is complex and lacks centralized visibility, creating operational overhead. At the same time, costly storage redundancy without deduplication inflates costs. As cloud environments scale, these limitations increase risk, reduce efficiency, and strain IT resources.
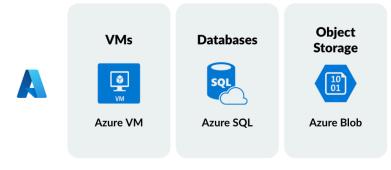
The solution

Druva provides secure, efficient, and simplified backup and recovery for Azure VMs through a fully managed SaaS platform. Designed for zero trust and built to scale, Druva removes the infrastructure, egress fees, and management complexity of native tools—delivering fast, reliable recovery from ransomware, insider threats, or operational failure. Extend protection to Azure SQL, Azure Blob, Azure Files, Microsoft 365, Entra ID, Dynamics 365, and integrate with Microsoft Sentinel.

Business challenges

- Co-location of primary data and backup
- No identity access isolation or immutability
- No cyber recovery or threat detection capabilities
- Cloud sprawl with fragmented visibility
- Too many disconnected tools and services
- Redundant storage costs and surprise egress charges
- Soaring storage costs as you scale

Key benefits

- Immutable, air-gapped backups
- Secure by design, not by implementation
- Fast, clean, reliable recovery—with built-in rollback
- Threat hunting, quarantine, and 24/7/365 monitoring
- Cyber recovery with in-line scanning for IOCs and malware
- Cut Azure backup costs with deduplication
- Simplified protection across regions and subscriptions
- Multi-cloud protection and cross-cloud resilience

VMs — Azure VM
Databases — Azure SQL
Object Storage — Azure Blob

druva
Data Security Cloud

Fully Managed SaaS Platform
Zero Trust Recovery Vault
Choose AWS or Azure for Cloud Storage

Zero Infrastructure. Zero Egress. Zero Headaches.

Key features

Security

Air-gapped, immutable backups

Backups are stored outside your Azure tenant in Druva's isolated cloud storage, ensuring they remain safe from ransomware and IAM compromise.

Zero trust recovery vault

Separates data and control planes to prevent attackers from altering or deleting backups—even with elevated credentials.

Data lock

Prevents backup modification or deletion—even by admin users—to guarantee data integrity and compliance.

Data anomaly detection

Machine learning establishes baselines and flags suspicious deviations, such as mass deletions or encryptions.

Rollback actions

Instantly restore deleted or compromised backups within a configurable window to recover quickly from ransomware or accidental deletions.

Cyber recovery

Makes every recovery a cyber recovery. Ensures only clean data is restored by scanning backup sets for malware or IOCs.

Threat hunting

Proactively scans backup data for signs of ransomware or unusual activity, enabling early threat detection before recovery.

Quarantine

Automatically isolates suspicious snapshots to prevent reintroducing compromised data during restoration.

24×7 Managed Data Detection & Response with Safe Mode

Around-the-clock threat monitoring and expert-guided response to accelerate investigation and recovery from backup-based threats. Lock down consoles during an attack to block deletions and contain blast radius.

Simplicity

Auto-discovery across subscriptions

Easily onboard Azure subscriptions, discover VMs, and apply protection policies based on business SLAs.

Cross-subscription and cross-region recovery

Restore VMs or files across regions or subscriptions to ensure rapid recovery from regional outages, account compromise, or cyber attacks.

File-level recovery

Quickly recover individual files and folders from any backup—no need to restore the entire VM.

Cyber recovery

Achieve up to 1.8TB/hr restore speeds from fully air-gapped, immutable backups. Ensures clean data by scanning backup sets for malware/IOCs prior to restore.

Savings

Lower Azure backup storage costs

Avoid expensive vault storage tiers like GRS and RA-GRS by using Druva's efficient cloud storage.

Deduplication of data

Reduce storage costs by deduplicating backup data across all workloads and locations at the source.

No egress charges

Data transfers for backups and restores across Azure regions or to Druva's cloud are completely free from Azure egress charges.

To learn more, visit:

https://www.druva.com/solutions/azure-vm-backup