

Securing Azure Local with SaaS Data Protection

Druva Resilience Cloud protects Azure Local as a fully managed SaaS service, with no backup servers, storage, or software to deploy at any site. Backup data and the console that governs it both sit outside your environment, so a compromise of your clusters or your Azure tenant reaches neither. Recovery is not tied to the hardware or the site that failed.

The Azure Local Protection Challenge

Organizations are extending Azure into data centers and edge locations through Azure Local, but data protection lags behind. Traditional Hyper-V backup tools and native snapshots are fragmented and hardware-dependent, often running inside the same environment they protect. An attacker who reaches administrator credentials reaches the backups too.

Business Challenges

Siloed Tools

Azure Local managed apart from Azure workloads, leads to harder management and compliance.

Ransomware Vulnerability

Snapshots sit in the environment they protect and fall with it during an attack.

Operational Complexity

Remote sites configured once, rarely validated, and unmonitored until a restore fails.

Hardware Dependency

Recovery waits on replacement hardware, or on standby capacity paid for and rarely used.

How Druva Secures Azure Local

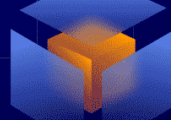
Druva Resilience Cloud treats Azure Local as an extension of the Azure estate rather than as a standard server, allowing organizations to apply consistent policies, from the same console, and with the same protection model used for cloud-native workloads.

Key Benefits of Druva for Azure Local

- **Backups Outside the Blast Radius:** Backup data and its management both sit outside your environment. A compromise of your Azure Local clusters or your Azure tenant reaches neither.
- **Hardware-Independent Recovery:** Restore full VMs to the original host, another host in the cluster, a Hyper-V host at a different site, or a Hyper-V host running in Azure.
- **Operational Simplicity:** No backup servers, storage, or software at any site. No patching, sizing, or maintenance windows.
- **Unified Governance:** Standardize backup and retention policies across Azure VMs, Azure Files, Azure Blob, and Azure Local through an Arc-aligned console.
- **Predictable Economics:** Up to 40% lower TCO, unlimited restores (zero egress fees), and no multi-year commitment required to get consumption-based pricing.

How Druva Protects Azure Local Workloads

Backup data moves directly from the Azure Local environment into the Druva Resilience Cloud. It does not land in customer-owned storage first, and it is not reachable from the production network or the local hypervisor control



plane. Protection is cluster-aware, using resilient change tracking to keep backup windows short over constrained site links.

Because the backup data lives in the Druva Resilience Cloud rather than at the site it came from, recovery does not wait on replacement hardware. Restore to surviving infrastructure elsewhere in the estate, or stand up a Hyper-V host in Azure and recover there. The recovery target is a decision made during the incident, not one provisioned for in advance.

Azure Local Protection

- **Automated VM Backups:** Cluster-aware protection for Hyper-V VMs on Azure Local, with no backup hardware.
- **Change Block Tracking:** Incremental-forever backups that keep backup windows short.
- **Granular Recovery:** Full VM, virtual disk, and file-level restore from the same recovery point.
- **Flexible Restore Targets:** Original host, alternate host or cluster, another site, or a Hyper-V host in Azure.

Why Druva is Different

Most backup platforms now offer a SaaS control plane. Far fewer move the data plane out with it. When backup data sits under customer-managed keys inside customer IAM boundaries, immutability holds only until someone with enough privilege revokes the key. These foundational capabilities are built-in and available to all customers regardless of license.

Separation and Isolation

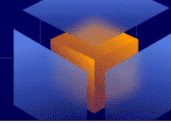
- **Operational Isolation (Control and Data Planes):** Both management and data planes sit outside your production environment, eliminating the blast radius of a primary system compromise.
- **Data Hardening (Air-Gap and Immutability):** Backup data is physically isolated from production networks and written to immutable, tamper-proof storage to prevent unauthorized alteration.
- **End-to-End Encryption:** Data is encrypted in transit and at rest.
- **Druva Safe Mode:** Locks down retention and deletion operations during a suspected breach.

Intelligent Operations

- **Dru SRE Agent:** Monitors backup health, identifies issues, and recommends actions to improve recovery readiness.
- **Managed Data Detection and Response (MDDR):** 24/7 expert monitoring and threat containment.
- **Druva MCP:** Extend backup intelligence into Microsoft Copilot to monitor operations without leaving Copilot.

Economics

- **Global, Source-Based Deduplication:** Minimizes bandwidth consumption to make edge protection viable over constrained links and ensures cloud recovery is practical and scalable.
- **Zero Egress Fees:** Recover and test with complete cost predictability: no data transfer or restore charges, ever.



SaaS Data Protection for Microsoft Workloads

Azure Local is often the trigger point for organizations to move toward platform standardization. Druva Resilience Cloud provides a scalable platform for the entire [Microsoft ecosystem](#), protecting Azure Local along with Azure VMs, Files, Blob, Microsoft 365, and Entra ID. By consolidating protection of these environments with the Druva Resilience Cloud, organizations can achieve consistent security postures and simplified compliance across their entire Microsoft environment.

SoFi protects cloud workloads and Hyper-V servers from one console and cuts data protection costs by 25% after switching.

Get Started Now!

Take the next step in securing your Azure hybrid environment:

- [Request a Personalized Demo](#) with a solution expert.
- [Take a Product Tour](#) to see Druva in action.
- [Start your 30-day Free Trial](#), experience zero-infrastructure protection today.

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 Resilience Cloud is the leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Resilience Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva Resilience Cloud enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by nearly 7,500 customers, including 75 of the Fortune 500, Druva Resilience Cloud safeguards business data in an increasingly interconnected world. Visit druva.com and follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).