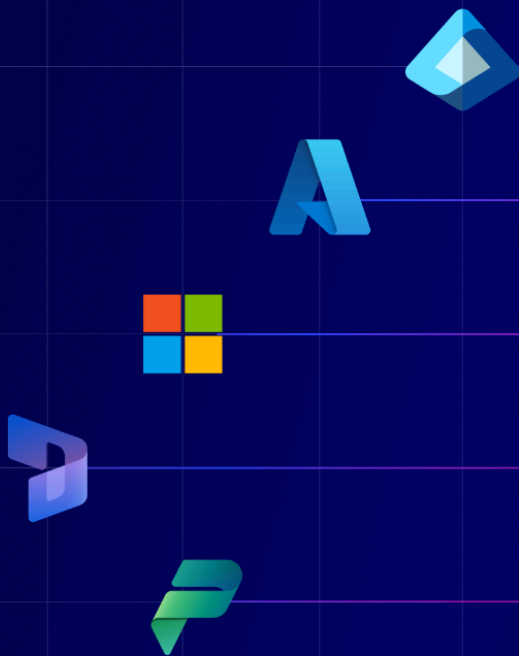




One Solution, Cyber Resilience for All Things Microsoft

Protect Microsoft & Azure workloads
against evolving threats with just one
unified, fully managed SaaS solution



Introduction

Microsoft has become the operational backbone of the modern enterprise. Email, collaboration, file services, identity, analytics, business applications, and cloud infrastructure increasingly run across Microsoft 365, Microsoft Entra ID, Active Directory, Power Platform, Dynamics 365, and Azure. As adoption expands, so does the blast radius of data loss, cyberattack, accidental deletion, misconfiguration, and compliance failure.

That shift changes what organizations need from data protection. A workload-by-workload approach is no longer enough. Native capabilities may help with service availability and basic retention, but they do not create an independent, unified, cyber-resilient data protection layer across the Microsoft estate. Security teams need confidence that backup data is isolated. IT teams need granular recovery. Governance teams need long-term retention, auditability, and defensible workflows. And the business needs all of it to work together.

A modern Microsoft data protection strategy must do more than recover deleted files. It must help organizations protect productivity, preserve business continuity, strengthen cyber resilience, simplify operations, and reduce risk across SaaS, identity, and cloud infrastructure.

This is where Druva delivers a different approach.

The Evolution of Microsoft Data Protection

From Native Gaps to Unified Cyber Resilience

Historically, backup was evaluated through the lens of operational recovery: restore a mailbox, recover a file share, roll back a VM, or recover from a regional outage. That model breaks down in today's Microsoft environments.

The challenge is no longer limited to a single application or a single restore event. Microsoft environments are deeply interconnected. A compromised identity can block access to Microsoft 365 and Azure. A ransomware event can affect collaboration data, endpoint data, and cloud workloads simultaneously. A governance issue can span SharePoint, OneDrive, Exchange, Power BI, Power Apps, Power Automate, Dynamics 365, and Azure storage. What used to be separate backup problems are now part of the same resilience problem.

Modern Microsoft data protection must therefore extend beyond traditional backup and recovery to include five core capabilities:

1. **Data protection, availability, and fidelity:** Data must remain accessible, accurate, and recoverable across Microsoft workloads without dependence on native retention windows or fragmented tooling.
2. **Governance, risk, and compliance:** Organizations need policy-driven retention, defensible deletion, audit trails, and legal hold readiness across a growing mix of data sources.
3. **Data visibility and observability:** Teams need insight into where Microsoft data lives, how it changes, and what activity may indicate risk.
4. **Threat detection and cyber readiness:** Backup data must be protected from ransomware, insider threats, and credential compromise, while also contributing to faster investigation and cleaner recovery.
5. **Accelerated response and recovery:** Recovery must be granular when possible, broad when necessary, and clean when cyberattacks are involved.

An ideal solution brings these capabilities together in one operational model. That is the difference between backup as a point product and cyber resilience as a platform.

A Comprehensive Approach

Druva Data Security Cloud for Microsoft and Azure

Druva delivers a 100% SaaS, fully managed approach to securing Microsoft data. Instead of requiring separate tools, backup infrastructure, agent sprawl, and custom processes for each workload, Druva provides a unified platform to protect Microsoft 365, Microsoft Entra ID, Active Directory, Dynamics 365, Power Platform, Azure VMs, Azure SQL, Azure Blob, Azure Files, Windows endpoints, Windows Server, and more.

This approach matters because Microsoft environments do not operate in silos. Users move across Microsoft 365 and OneDrive. Access depends on Entra ID and Active Directory. Business processes rely on Dynamics 365, Power BI, Power Apps, and Power Automate. Azure infrastructure underpins critical applications and data services. When protection is fragmented, response is fragmented too.

Druva helps organizations replace that fragmentation with a consistent operating model built around:

- **Unified policy management** across Microsoft workloads
- **Air-gapped, immutable backups** isolated from the production environment
- **Granular and point-in-time recovery** for business-critical data
- **Zero-trust principles and role-based access controls**
- **Centralized visibility and reporting** for IT, security, and compliance teams
- **Cloud-native scale without infrastructure overhead**
- **Expanded storage choice and data residency flexibility** for Azure-aligned requirements

The result is a simpler and more resilient foundation for protecting Microsoft environments at enterprise scale.



Foundational Security Across All Microsoft Workloads

A modern Microsoft strategy starts with foundational controls that apply consistently across workloads.

Air-gapped, immutable protection

Druva stores backup data in isolated, tamper-resistant storage to help protect against ransomware, malicious deletion, and credential compromise. This gives organizations an independent recovery layer that is separate from the primary Microsoft environment.

Zero-trust administration

Role-based access control, policy enforcement, and strong administrative guardrails help reduce the risk of over-privileged access and unauthorized changes to backup data.

Strong encryption and auditability

Druva protects backup data in transit and at rest while maintaining detailed audit logs to support security investigations, compliance reviews, and operational accountability.

Granular recovery at scale

Whether the issue is a deleted mailbox item, a damaged Power Platform asset, a broken group membership, or a compromised VM, Druva enables teams to recover the right data with speed and precision.

Operational simplicity

Because Druva is SaaS-based and fully managed, organizations avoid the ongoing burden of backup servers, patching, capacity planning, and infrastructure lifecycle management.

Cost efficiency and cloud flexibility

Global deduplication, automated lifecycle management, and zero egress fee recovery help reduce cost while preserving recovery readiness. For many Microsoft-centric organizations, the ability to align with Azure purchasing and residency needs adds further operational value.

Securing Microsoft 365

Protecting Productivity and Collaboration Data

Microsoft 365 is where business moves fastest and where data loss is often first discovered. Exchange Online, OneDrive, SharePoint, Teams, Groups, Planner, and related services contain communications, working files, shared knowledge, and operational context that cannot simply be recreated.

The challenge is that native Microsoft 365 protection is not designed to function as a complete backup and cyber recovery strategy. Retention windows vary by service. Granular recovery can be limited. Administrative recovery paths may be cumbersome. And versioning or recycle bins do not create a truly independent, immutable copy of data.

Druva helps close these gaps with a purpose-built Microsoft 365 protection model that includes:

- Automated, policy-based backups across Microsoft 365 workloads
- First full, forever incremental architecture for efficient protection
- Smart backup methods that reduce unnecessary API calls and resource consumption
- Self-service and admin-led restore options
- Granular recovery for emails, folders, calendars, files, sites, and related metadata
- Secure recovery to alternate locations with auditability
- Unlimited or extended retention aligned to business and compliance requirements
- Federated search for investigations, eDiscovery, and governance workflows



For organizations with large-scale Microsoft 365 environments, Druva Microsoft 365 Backup Express adds another option for ultra-fast recovery of Exchange, SharePoint, and OneDrive data using Microsoft 365 Backup Storage while remaining centrally managed through the Druva platform.

This combination gives organizations both breadth and speed: broad Microsoft 365 coverage with the ability to accelerate recovery for the data that matters most.

Why native collaboration features are not enough

Collaboration features are valuable, but they are not a substitute for cyber-resilient backup. OneDrive version history, for example, supports collaboration workflows, but it does not provide the same assurance as an immutable, independent backup copy. If versions are altered, encrypted, or deleted, or if recovery is discovered too late, native recovery may not meet business continuity needs.

Druva gives organizations a cleaner recovery path by maintaining protected data outside the primary collaboration plane.

Protecting Identity

Microsoft Entra ID and Active Directory

In Microsoft environments, identity is foundational. If identity is disrupted, users cannot access Microsoft 365, Azure resources, or downstream applications. That makes Entra ID and Active Directory more than administrative systems; they are operational dependencies.

Microsoft Entra ID

Druva Identity Resilience for Microsoft Entra ID helps organizations protect and recover critical identity data with a policy-driven model. This includes users, groups, memberships, roles, enterprise applications, app registrations, administrative units, conditional access policies, and privileged identity configurations.

The value is not just object recovery. It is functional recovery. Druva restores settings and relationships so organizations can re-establish trusted access with less manual reconstruction and less risk of reintroducing bad state.

This is especially important in scenarios involving:

- Cyber compromise
- Misconfiguration
- Accidental deletion
- Identity service disruption
- Governance and portability workflows

Active Directory

Active Directory remains the operational heart of many enterprises, especially in hybrid environments. When AD is corrupted, encrypted, or misconfigured, business impact is immediate.

Druva Identity Resilience for Microsoft Active Directory provides:

- Air-gapped, immutable protection for AD backups
- Granular object restore for users, groups, devices, and OUs
- GPO recovery without broad rollback
- Guided forest-level recovery for catastrophic events
- Immutable audit logs and role-based administration
- Centralized management for hybrid identity environments

Together, Entra ID and Active Directory protection help organizations recover trust, not just data. That is a critical distinction when identity has become a primary attack path.

Protecting Business Applications and Analytics

Dynamics 365 and Microsoft Power Platform

Microsoft environments are no longer only about productivity. They now hold operational systems of record and decision-making systems that directly affect revenue, service, and execution.



Microsoft Dynamics 365

Dynamics 365 often contains critical CRM and ERP data. Yet native recovery approaches can make restore operations slow, broad, and difficult to validate.

Druva helps organizations protect Dynamics 365 with:

- Granular recovery of entities, records, relationships, and metadata
- Customizable retention beyond native limits
- Search and compare capabilities to identify unexpected changes and bulk deletions
- Restore options that support production or sandbox workflows
- Air-gapped protection that helps preserve data integrity during cyber events

This enables a more precise recovery model for a system where operational downtime and data inconsistency can have immediate business consequences.

Microsoft Power Platform

Microsoft Power Platform is increasingly becoming the intelligence, application, and automation layer of the enterprise. Druva extends protection to assets that organizations depend on for executive reporting, custom low-code applications, process automation, and operational insight across Power BI, Power Apps, and Power Automate.

Many organizations still rely on manual exports, solution downloads, or inconsistent processes to preserve Power Platform content. That creates risk because manual methods do not capture the full environment, miss critical dependencies, or provide policy-driven recovery.

Druva addresses this with:

- Automated discovery of Power Platform assets across Power BI, Power Apps, and Power Automate
- Policy-based backup and retention
- Protection for reports, dashboards, semantic models, custom apps, automated workflows, and data connectors
- Point-in-time and granular recovery
- Air-gapped, immutable storage for cyber resilience
- Unified management alongside broader Microsoft workloads

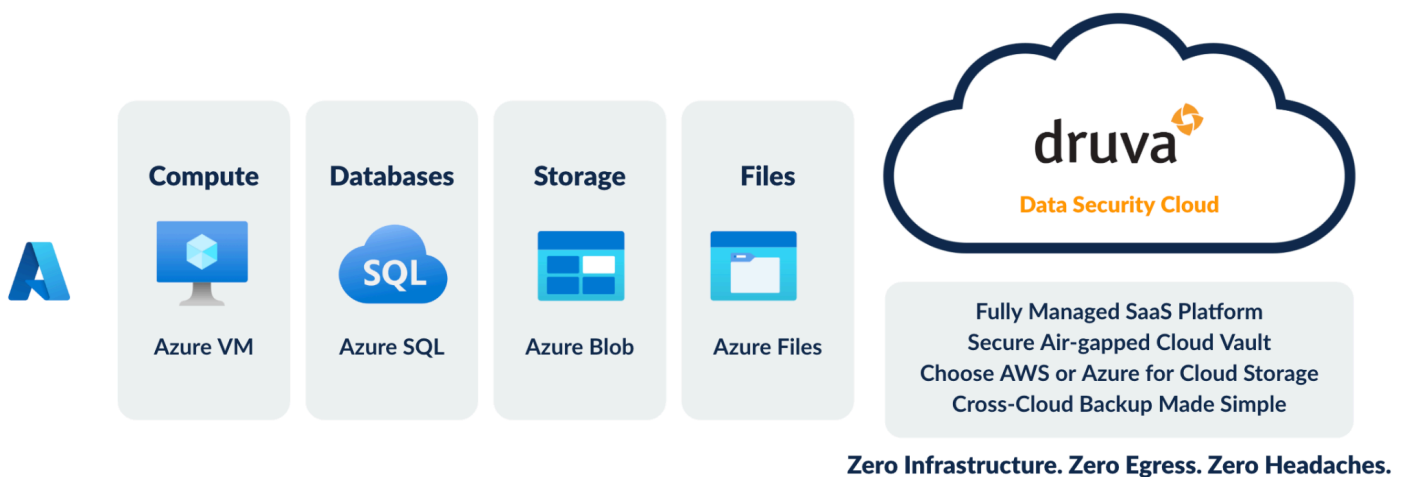
For organizations that treat Power BI as the intelligence layer of the business, backup can no longer be manual, partial, or best effort.

Securing Azure Workloads

A Unified Approach to Cloud Infrastructure and Data Services

Azure adoption continues to expand, but native recovery and storage resilience strategies are not always sufficient for modern cyber resilience requirements. When primary data and backup data remain too closely coupled, organizations increase their exposure to ransomware, credential compromise, operational complexity, and rising storage costs.

Druva brings a unified, cloud-native approach to Azure protection across infrastructure and data services.



Azure VMs

Druva protects Azure virtual machines with agentless, SaaS-based backup and recovery designed for cyber resilience. Key capabilities include:

- Air-gapped, immutable backups stored outside the Azure tenant
- Zero-trust separation of data and control planes
- Built-in rollback and quarantine options
- Recovery intelligence for cleaner restores

- Threat watch and threat hunting for backup-based investigation
- Simplified protection across regions and subscriptions
- No egress fee recovery and reduced storage overhead through deduplication

Azure SQL

For Azure SQL environments spanning Azure VMs, SQL databases, and managed instances, Druva provides:

- Agentless protection with policy-driven automation
- Full backup support plus Change Data Capture where applicable
- Isolated Copy Protection for workloads where CDC is restricted or unsupported
- Transactionally consistent recovery points
- Fast restore to the same or alternate region or tenant
- Long-term retention and compliance-ready recovery workflows

Azure Blob

Azure Blob contains high-value object data that is often protected through operational mechanisms rather than true backup. Druva adds a stronger recovery layer with:

- Agentless backup with no proxies or infrastructure
- Air-gapped, immutable protection outside the Azure tenant
- Granular object and metadata restore
- Metadata-driven search for faster recovery
- Flexible restore to alternate subscriptions or regions
- Multi-cloud backup storage flexibility to support resilience and compliance goals

Azure Files

For Azure Files, Druva delivers:

- Simply protect Azure Files SMB shares (SSD Premium and HDD Standard)
- Direct, agentless protection for Azure Files over public networks
- Secure protection for Azure Files in private networks using the Druva Quantum Bridge
- Centralized backup, retention, and recovery policies
- File-, folder-, and share-level restore
- Recovery to the same or alternate subscription and region
- Encrypted, immutable storage isolated from production
- Unified governance and reporting across Azure workloads

Across Azure VMs, Azure SQL, Azure Blob, and Azure Files, Druva gives customers a consistent operating model for secure recovery without introducing more infrastructure.

Governance, Compliance, and Operational Simplicity

As Microsoft data sprawls across collaboration services, identities, business applications, endpoints, and Azure resources, compliance and governance become harder to operationalize.

Druva helps organizations simplify this challenge through:

- Centralized policy control across workloads
- Long-term retention aligned to internal and external requirements
- Detailed audit trails for backup and restore activity
- Federated search across protected data
- Legal hold and eDiscovery workflows for Microsoft 365 and endpoint data
- Data residency and region alignment options to support regulated industries

- Defensible deletion and data governance support for privacy requirements

Operationally, the advantage is just as important. A SaaS model removes the overhead of maintaining backup infrastructure while giving teams a central console for visibility, reporting, and policy enforcement. That improves consistency, reduces administrative burden, and helps security, IT, and compliance teams work from the same system of record.

Why a Unified Microsoft Strategy Matters

Organizations rarely fail because a single restore feature is missing. They struggle because recovery becomes fragmented across too many tools, too many consoles, and too many assumptions about what native protection will cover.

A unified Microsoft data security strategy changes that.

With Druva, organizations can:

- Reduce operational complexity without sacrificing control
- Improve cyber readiness with isolated, immutable backup data
- Restore faster and more precisely across Microsoft services
- Strengthen governance with centralized retention, search, and auditability
- Optimize costs through SaaS delivery, deduplication, and zero egress fee recovery
- Support long-term Microsoft and Azure strategies without adding more infrastructure

Conclusion

The Microsoft estate now spans far more than email and file sharing. It includes collaboration data, identity systems, analytics assets, CRM and ERP data, cloud infrastructure, storage services, databases, and hybrid operational dependencies. Protecting each one in isolation creates gaps. Protecting them together creates resilience.

Druva brings that unified approach to life with a cloud-native platform built to protect Microsoft workloads and Azure environments with air-gapped security, immutable recovery data, operational simplicity, and policy-driven control.

For organizations looking to standardize on a modern Microsoft data security strategy, the path forward is clear: move beyond fragmented native and point solutions, and adopt a platform built for the way Microsoft environments actually operate today.

Next Steps

Evaluate where your current Microsoft data protection model still depends on native retention, manual exports, fragmented recovery workflows, or infrastructure-heavy backup tooling. Then identify where a unified SaaS platform can improve recovery readiness, reduce complexity, and strengthen cyber resilience across the Microsoft ecosystem.

Druva helps organizations protect productivity, recover identity, preserve business applications, and secure Azure workloads through one modern platform.

See why Druva was recognized as a [2025 Gartner® Magic Quadrant™ Leader](#) for Backup and Data Protection Platforms, and [start a risk-free 30-day free trial](#). No credit card required!

For More Information

druva.com/use-cases/cloud-native/microsoft-and-azure

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](#).