Druva for Microsoft 365 Backup & Cyber Resilience

As your organization relies more heavily on Microsoft 365, protecting this business-critical data from loss, corruption, and cyber threats is non-negotiable. While Microsoft ensures infrastructure availability, it doesn't guarantee data security and recoverability. That's your responsibility. Druva provides a 100% SaaS-based, air-gapped, and scalable protection for Microsoft 365 that's purpose-built for today's cyber resilience demands.

The Challenge: Microsoft's Native Protection Isn't Enough

According to Microsoft's Digital Defense Report 2024, over 600 million cyberattacks target the Microsoft ecosystem every day. Yet native Microsoft 365 tools offer only basic retention, not true backup. The risk is real—21% of organizations report data loss despite having M365 backup policies, and 70% of ransomware incidents specifically target backups. Alarmingly, 43% of ransomware victims saw their backups encrypted, leaving them without a clean path to recovery. This widening gap between attack volume and protection capability exposes organizations to critical risks. As a result, customers often report the following experiences:

- **Short Retention Periods:** Microsoft 365 retains deleted data for only 14 to 93 days, with no flexibility to extend, leaving you unprotected once the window closes.
- **No Granular Recovery:** Native tools lack the ability to restore specific emails, files, or chats, forcing inefficient, broad rollbacks that disrupt users and delay recovery.
- **Ransomware Lockout & Malicious Deletions:** Without air-gapped or immutable backups, ransomware can encrypt or erase both live and backup data, making clean recovery nearly impossible.
- **Malicious Insider or Admin Threats:** A compromised or rogue admin can change retention settings or delete both primary and backup data, with no way to undo or trace the damage.
- **Operational Complexity:** Managing protection across Microsoft 365 workloads requires multiple admin consoles and scripts, making recovery slow, error-prone, and resource-intensive.

The Solution

Druva delivers a fully managed, 100% SaaS data protection and cyber resilience platform, purpose-built to secure Microsoft 365 against ransomware, insider threats, accidental deletion, and compliance risks. It provides resilient protection across a wide range of Microsoft workloads, including Exchange Online, OneDrive, SharePoint, Teams (including private chats), Planner, Groups, Entra ID, and more, all managed through a single, scalable platform.

Key Features & Benefits

Data Backup & Retention

- **Automated Backups**: Create custom backup policies to define backup and retention schedules, and automate Microsoft 365 backups with Druva, ensuring consistent, policy-driven protection across all workloads.
- **First Full, Forever Incremental Backups**: Create just one full backup. Druva's global deduplication ensures all future backups are incremental, saving time, bandwidth, and storage without compromising protection.
- **Air-gapped, immutable backups**: Druva stores Microsoft 365 backups in an isolated, air-gapped architecture with built-in immutability, preventing unauthorized access or tampering. The backups can be stored, retained, and managed within a specific country or region to meet enterprise latency and data residency requirements.
- **Smart Backups**: Druva's Smart Backup detects and protects only changed SharePoint content, reducing API calls and resource consumption.
- **Performance Optimization with Auxiliary Apps:** Dynamically deployed microservices scale out backup operations, optimizing backup performance intelligently to avoid throttling.
- **Lightning-fast Backup & Restore**: Druva's Microsoft 365 Backup Express solution delivers high-speed, large-scale recovery for Exchange, SharePoint, and OneDrive — with zero throttling and ultra-low RPOs/RTOs.

Data Recovery

- **Self-Serve Restore:** Users can independently restore Microsoft 365 data without relying on IT administrators.
- **Point-in-Time & Granular Recovery**: Quickly locate data using metadata search or select the specific snapshot to perform full or granular recovery of emails, folders, calendars, and files.
- **Flexible & Secure Restores**: Recover data to alternate locations, maintain a tamper-proof audit trail for legal compliance, and leverage APIs for programmatic restore automation.

Security & Privacy

- **Advanced Encryption**: Druva uses enterprise-grade digital envelope encryption (256-bit TLS in-transit and AES 256-bit at-rest) to secure Microsoft 365 backup data, ensuring maximum data privacy and security. It also supports Bring Your Own Key (BYOK) for added control using AWS KMS keys. Druva separates data, metadata, and encryption keys for added protection, ensuring that sensitive user data remains inaccessible to administrators.
- **Data Immutability**: The Data Lock feature prevents any modification or deletion of backups, ensuring true data immutability.
- **Strengthen Security Posture**: Enforce conditional access policies to align with Microsoft Entra ID restrictions, ensuring secure and compliant authentication. Monitor sensitive activities through built-in audit logs, analyze detailed reports for end-to-end visibility, and leverage real-time insights from the Security Center dashboard to proactively manage risks and strengthen your security posture.
- **Data Anomaly Detection**: Druva's patented AI-driven anomaly detection feature identifies suspicious activity, empowering organizations to respond swiftly and protect their critical data assets from cyber threats.
- **Quarantine Snapshot:** Automatically isolate suspicious files during Microsoft 365 backups to prevent unauthorized access or restoration. Enable secure, compliant recovery with admin-led investigation and control.
- **Recover Lost Data**: Druva's rollback feature enables swift recovery from ransomware or accidental data loss by restoring Microsoft 365 content to a known-good state from a secure cache retained for up to 7 days.
- **SIEM Integrations:** Druva captures every download and restore action, providing Microsoft Sentinel with detailed data insights to accelerate threat detection, investigation, and response - including deep integration with Copilot Security for AI-powered analysis.

Ransomware Recovery

- **Always-On Threat Monitoring:** Druva's Managed Data Detection and Response (MDDR) service helps you stay ahead of cyber threats with 24/7/365 real-time surveillance and AI-driven detection, accelerating response and ensuring clean recovery.
- **AI-Guided Investigation:** Druva's Dru Investigate feature uses AI-powered investigation and deep backup telemetry to help IT admins and security teams investigate cyber threats within their backup environment.
- **Unlimited Retention**: With unlimited retention for Microsoft 365, Druva enables recovery from clean snapshots, even if ransomware has been present for months.
- **Federated Search for Investigations**: Druva's federated search allows security teams to track infected files, analyze attack scope, and investigate events across Microsoft 365 users, devices, and storage.
- **Curated Recovery**: Druva creates tailored snapshots with the cleanest, safest file versions for seamless OneDrive and SharePoint restores.

eDiscovery & Legal Hold

- **Unified Legal Hold**: Druva enables proactive collection and preservation of Microsoft 365 and endpoint data with an electronic chain of custody. You can also preserve data belonging to departing employees, ensuring it remains available for current and future eDiscovery needs without incurring ongoing Microsoft 365 licensing costs.
- **eDiscovery Ecosystem Integration**: Druva integrates with leading cloud-native eDiscovery tools (Exterro, OpenText) to collect, preserve, and upload relevant data for legal review, analysis, and production.
- **Federated Search Capabilities**: IT admins can perform unified searches across Microsoft 365 and endpoints to locate sensitive data, support compliance, and streamline legal, forensic, and ransomware investigations.

Compliance

- **Comprehensive Compliance Support**: Druva offers built-in support for key global regulations like GDPR, CCPA, HIPAA, and FedRAMP, with proactive alerts and remediation for potential violations. Druva platform is also compliant with SOC 1, ISAE 3402, SOC 2, SOC 3, ISO 27001, PCI DSSLevel 1 (Cloud), and HIPAA regulations.
- **Customizable Governance Policies**: Use Druva's predefined compliance templates to create custom governance policies that meet both industry regulations and internal compliance requirements.
- **Data Governance & Defensible Deletion**: Address compliance violations by securely deleting prohibited data to support "Right to be Forgotten" requests under regulations like GDPR Article 17.
- **Retention & Security Certifications**: Ensure compliance with data-retention and disaster recovery regulations, while benefiting from certifications like SOC 2, ISO 27001, and PCI DSS Level 1.

Next Steps

Check out the Microsoft 365 solution page to discover how Druva closes your data protection gaps.

- Explore how Druva protects Microsoft Azure and the broader ecosystem: Visit the Webpage
- Try Druva's data security for Microsoft 365 for yourself: Tour the Product
- Get started with Druva with a 30-day free trial

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