# druva

Druva for Microsoft 365 backup

Druva provides a comprehensive, scalable, and cost-effective SaaS platform to protect Microsoft 365 data, including Exchange Online, OneDrive, SharePoint, and Teams from common risks like accidental deletion, file corruption, insider attacks, ransomware, and non-compliance with data retention, legal hold, and eDiscovery. Druva's platform supports other cloud applications and endpoints.
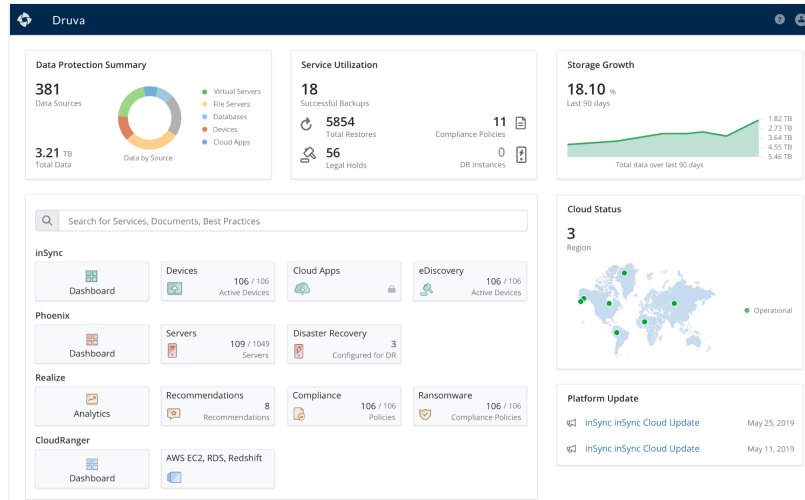
Manage all of your workloads from a single pane of glass

Data backup and retention

Easy-to-use centralized console

Intuitive interface allows global visibility of Exchange Online, One Drive, Sharepoint, Teams, and endpoint backup snapshots. Easily automate backups without end-user intervention.

Flexible retention

Druva offers optional unlimited or customizable data retention for Microsoft 365 to meet data retention and compliance needs.

Cloud to cloud with zero infrastructure

Microsoft 365 files are backed up directly from Microsoft Azure to the Druva Cloud Platform on AWS. Druva customers do not have additional cloud storage or hardware costs. Agentless architecture improves recovery performance and avoids taxing your WAN bandwidth or latency.

Agentless data protection

Microsoft 365 files are backed up directly from Microsoft Azure to the Druva Cloud Platform on AWS. The configuration is straightforward — connect to your Microsoft 365 tenant using an admin account and specify backup parameters — no agents required.

### First full and forever incremental backup

Only one full back is ever needed because of Druva's patented global dedupe technology. Subsequent backups take less time and consume less storage space.

Flexible backup schedule

Druva's profile-based architecture enables independent backup frequencies for different user groups.

Large file support

There are no limits to the size of an individual file that can be protected and restored with Druva's cloud architecture.
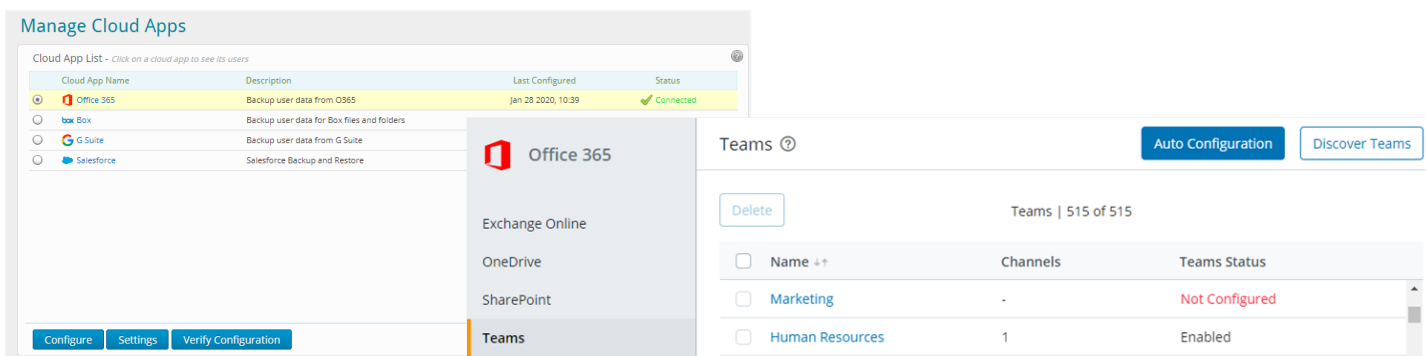
Comprehensive support for cloud applications

Backing up in-use or open files

Druva's unique technology enables backup of files that may be open and in use during backup runtimes, ensuring all files are protected.

Multi-geo support

With AWS storage regions across the globe, backups can be stored, retained, processed, and managed within a specific country or region to meet your latency and data residency requirements.

Data retention of inactive and terminated employees

Druva retains data for inactive and terminated employees, eliminating the need to purchase and maintain additional Microsoft 365 licenses or invest in more expensive pricing plans.

Reliable backups

Dedicated algorithms, including error-checks and retries, ensure backup completion and data integrity, regardless of Microsoft throttling.

Data recovery

User self-serve restore support

Users are empowered to restore Exchange Online and OneDrive without IT admin intervention.

Search and restore

Quickly identify content for recovery based on metadata such as filetype, owner, date created, email subject, and date modified.

Point-in-time recovery

Recover quickly from any time-based snapshots using a simple and intuitive interface.

Granular files and metadata restore

Perform granular recovery of Exchange Online emails, folders, calendars, One Drive files, Sharepoint site with metadata, timestamp, and permissions.

Bulk and folder level restore

Druva allows recovery of multiple Microsoft 365 files and object metadata from any point-of-time snapshots.

Restore to any location

Restore data from any backup snapshot to an alternate destination.

Restore chain of custody/audit trail

Druva maintains a tamper-proof log of all the admin restore activities and locations, which is admissible as evidence in a court of law.

Restore API

Druva APIs can be leveraged by third-party applications for restoring objects programmatically, eliminating the need for manual intervention.

Data security and privacy

Digital envelope encryption

Druva-managed keys use enterprise-grade digital envelope encryption in-transit (256-bit TLS) and at-rest (AES 256-bit) for the highest levels of data security and

privacy of your Microsoft 365 backup data. Alternatively, use your own AWS Keys to secure your Microsoft 365 backup sets.

Granular access controls

Global or Profile admins can be set up to support delegation of backup and restore responsibilities to different groups to prevent data loss attributed to disgruntled employees/rogue admins.

Audit tracking and logging

Ensures visibility and trackability of restores for files containing sensitive and proprietary information.

FedRAMP compliance

If you are a contractor of the US Federal Government, Druva is FedRAMP compliant and can protect your Microsoft 365 GCC environment.

Security certifications

Druva is compliant with SOC 1, ISAE 3402, SOC 2, SOC 3, ISO 27001, PCI DSSLevel 1 (Cloud), and HIPAA regulations.

Data and metadata separation

Druva stores Microsoft 365 data, metadata, and encryption keys separately for an additional layer of security that extends beyond data encryption.

Data privacy

To fully protect sensitive data privacy, Druva is designed so that your own Druva admins as well as Druva employees may not view end user data stored in the Druva Cloud Platform.

Ransomware recovery

Data isolation for ransomware recovery

To recover from data corruption of customers' Microsoft 365 environment Druva provides "data cocoon" – true isolation of backup data from customer-controlled storage environments.

Unlimited retention

Druva offers unlimited retention for Microsoft 365, enabling ransomware recovery from a clean snapshot, even if the malware has been present in your environment and infecting your data for months.

Security investigations

Federated search of metadata attributes enable Information Security teams to search through Microsoft 365 files across users, end-devices, and storage locations, to track infected files, determine sequence of events, and analyze scope and location of attack.
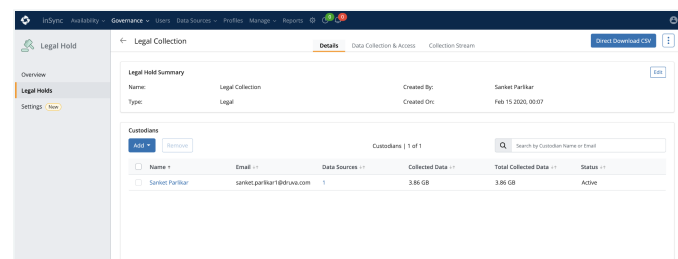
eDiscovery and legal hold

Unified legal hold

Unified legal hold management enables proactive collection and preservation of Microsoft 365 and endpoints data and its electronic chain of custody, until it is extracted, processed, and analyzed in an eDiscovery platform.

eDiscovery ecosystem support

Druva integrates with market-leading, cloud-native eDiscovery tools to seamlessly collect, preserve, and upload data relevant to legal matters into eDiscovery platforms for review, analysis, and production.

Federated metadata search across all workloads for ransomware and security investigations, eDiscovery, and compliance

Centrally manage and automate legal hold across workloads

Pre-culling for minimized, relevant data-sets

Pre-cull eDiscovery data by dimensions such as time-range and keywords, so that only the most relevant, minimized data-set is provided for downstream analysis by the legal team.

Fastest download times

Fastest in our category eDiscovery data-download times so that data can be quickly provided to the downstream legal team.

Legal and forensics investigations

Federated search of metadata attributes enable IT admins to quickly locate Microsoft 365 content for legal and forensic investigations and discovering custodians.

Preserve departing employees' data

Druva enables you to preserve departing employees' data, which may be relevant for present and future eDiscovery needs. This eliminates the need to pay for maintaining their Microsoft 365 licenses, obtaining higher M365 editions or quarantining their devices.

Compliance

GDPR, CCPA, and HIPAA support

Proactively monitor, with out-of-box, predefined, customizable compliance templates for potential violations of key global regulations like GDPR, HIPAA, CCPA, and be alerted of these risks to quickly remediate violations.

Customize and add compliance templates

Easily customize pre-built compliance templates for global regulation and PII, or create your own templates for governance policies, including regulation or internal data governance policies.

Defensible deletion
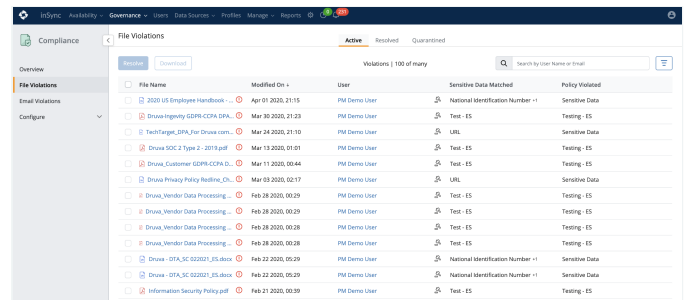
You can act on Druva's alerts to potential compliance violations by deleting files containing prohibited information from the backup, Microsoft 365 source, or both. User-generated content such as Mailbox or OneDrive data can be erased using metadata identifiers to comply with "Right to be Forgotten," such as the one contained in GDPR Article 17.

Search for sensitive data

Federated search of metadata attributes enable IT admins to quickly locate Microsoft 365 files across all users and end-devices, in order to locate sensitive files or confidential documents that should be acted on such as defensible deletion or restricted use.

Data retention and DR compliance

The Druva Cloud Platform allows you to comply with industry data-retention regulation, via indefinite and customizable retention, and with industry disaster recovery (DR) regulations, which require full data isolation.

Centrally monitor and address compliance violations

Druva helps some of the world's largest organizations protect their investment in Microsoft 365, as well as other key data workloads from data loss and compliance violations — all from a single pane of glass.

Check out druva.com/solutions/microsoft365 — find out how we can help you close the gaps in Microsoft 365 data protection, to keep your employees productive and meet your business continuity SLAs.