druva

Securing your Microsoft 365 data protected by Druva

Contents

Microsoft 365 Data Resiliency Use Case(s) 2

Security Overview 3

Understanding the relationship between the two Platforms 3

- Microsoft 365 user permissions requirements 4
- Initial deployment of the Druva app in Azure 4
- Microsoft 365 App Data Consenting Permissions 5
- Azure AD Sign-In Activity (Interactive) 5
- Sign-In Activity (Non-Interactive) 6

Securing Your Microsoft 365 Account 7

Druva Cloud Platform Security 8

Druva Cloud Platform Microsoft 365 Data Protection 9

druva

Securing your Microsoft 365 data protected by Druva

Microsoft 365 Data Resiliency Use Case(s)	Microsoft 365	Druva	Capabilities
Restore user's primary mailbox to a prior point in time	✗	✓	Druva provides customers with a point-in-time backup enabling restore of mailboxes and associated online archive mailboxes. Customers can maintain multiple snapshots per day with unlimited retention or customized retention. M365 does not allow for the restore of a mailbox to a prior point in time.
Immutable copy of user's email: active, online archive and recoverable items and OneDrive	✗	✓	Druva's WORM architecture (write once read many) maintains backups with added Data Lock functionality. This ensures that even admins with the Cloud Admin role cannot delete backup snapshots. M365 can place content on legal hold ensuring the content not be deleted but it does not ensure the content cannot be modified or encrypted.
Recover a Microsoft Team (membership, teams settings and SharePoint) to a prior point in time	✗	✓	Druva protects Microsoft Teams, membership and associated SharePoint site collections. Customers can restore back in place, to another team or create a completely new team with an existing team backup. M365 retention for a team and corresponding app data (groups, spo, etc.) is not consistent. Content such as chat that is deleted cannot be restored back to the same team..
Recover a user's OneDrive to a prior point in time Recover an entire SharePoint site collection to a prior point in time	✗	✓	Druva is not dependent on 365 policies. Customers can maintain forever backups or customize a retention policy. OneDrive and SharePoint files(only) restores are dependent on version history and files must remain in the recycle bin. A user is an admin of their OneDrive and can purge deleted data from the 1st and 2nd stage recycle bins. Malware has been reported to modify the number of versions saved while leaving the remaining versions of a file encrypted.
Recover a user's OneDrive without the user being logged into 365	✗	✓	Druva administration allows for 1 or more admins with RBAC to restore user data (OneDrive, Exchange Online), SharePoint, Groups and Teams data. All restores are executed using the Microsoft API Services layer. No user login is required.
An admin in 365 has created a dynamic policy for sensitivity labels inadvertently overwriting previously tagged (and approved) labels in a SharePoint site collection. Restore sensitivity labels for a file or files in OneDrive or SharePoint to a prior point in time	✗	✓	Druva restores files and metadata for OneDrive and SharePoint including sensitivity and retention labels to a prior point in time.

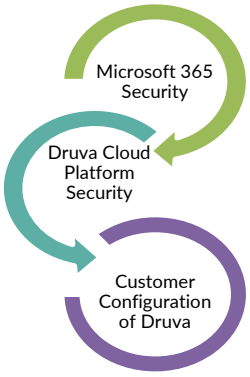
Securing your Microsoft 365 data protected by Druva

Security Overview

Security is of the utmost importance for any organization. When protecting Microsoft 365 data, addressing security on multiple levels is imperative. Coupled with a customer's Microsoft 365 security practices, Druva's platform security architecture and customer-configurable security features close the gaps to protect the customer's backup data.

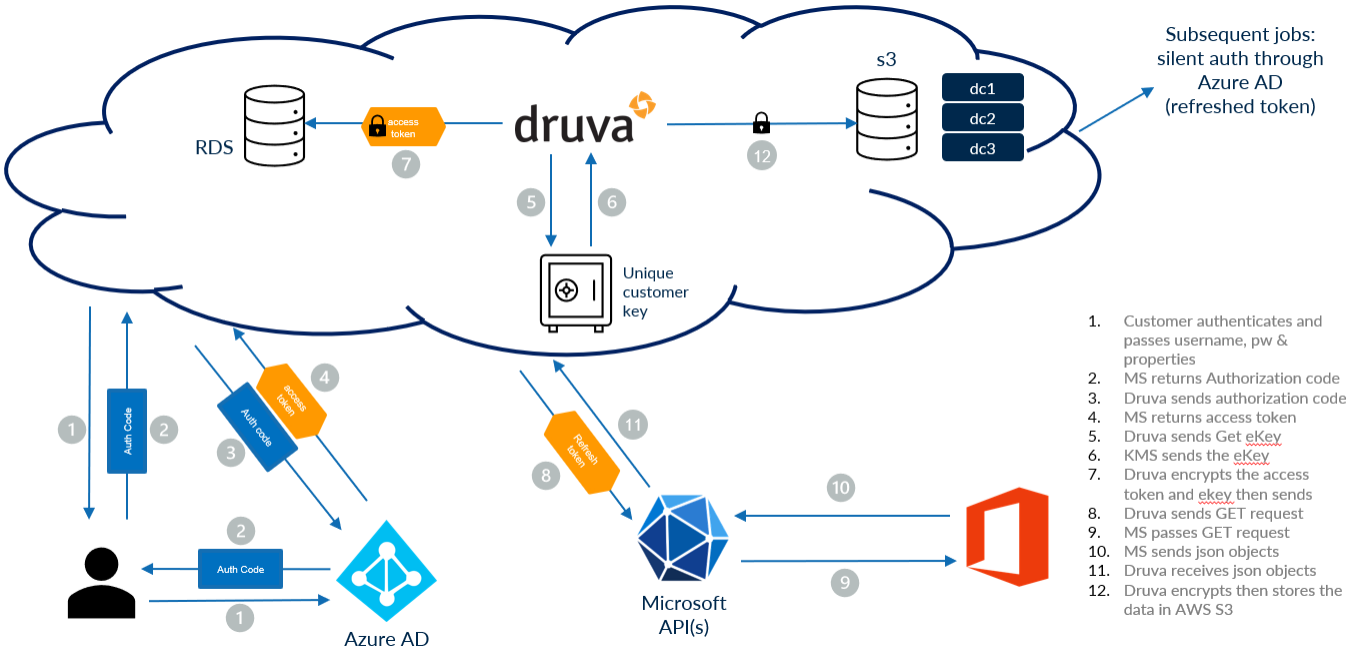
A customer can optimize their Microsoft 365 tenant security to enforce a higher degree of integrity for 3rd party vendors. Druva interacts with customer data via Microsoft 365 API layer and Identity services.

Let's look at how best to secure customer backup data for Microsoft 365.



Understanding the relationship between the two Platforms

Data transactions between the DCP and the customer's Microsoft 365 tenant are encrypted in flight and at rest. Druva employees cannot access customer data as it is encrypted with unique customer keys. No customer data is ever used for any purposes either internal or external. DCP highly recommends its customer utilize MFA and/or Azure AD conditional access policies. For those companies that have yet to implement them, DCP can still protect Microsoft 365 data. If changes are made to the customer's Azure AD conditional access policies, the customer may have to re-authenticate within DCP.

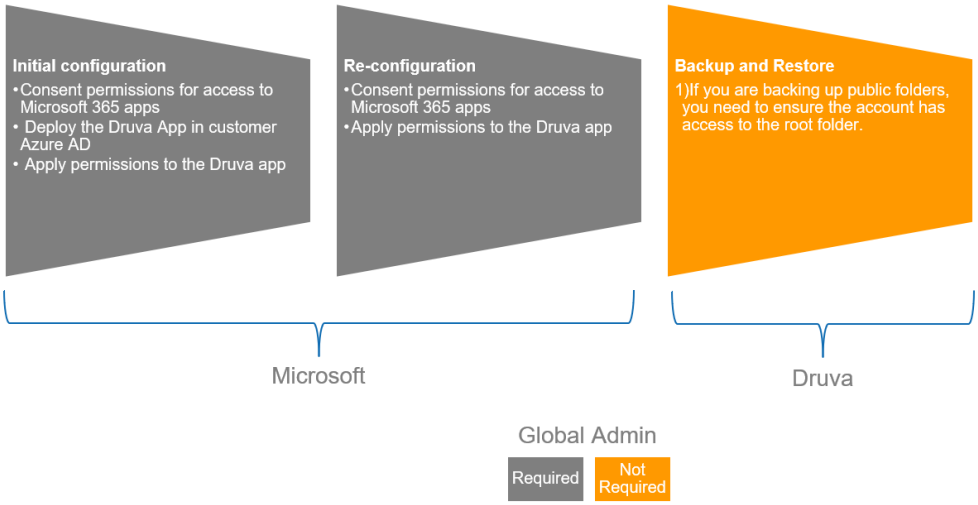


w/ or w/o Conditional Access Policies, MFA

Securing your Microsoft 365 data protected by Druva

Microsoft 365 user permissions requirements

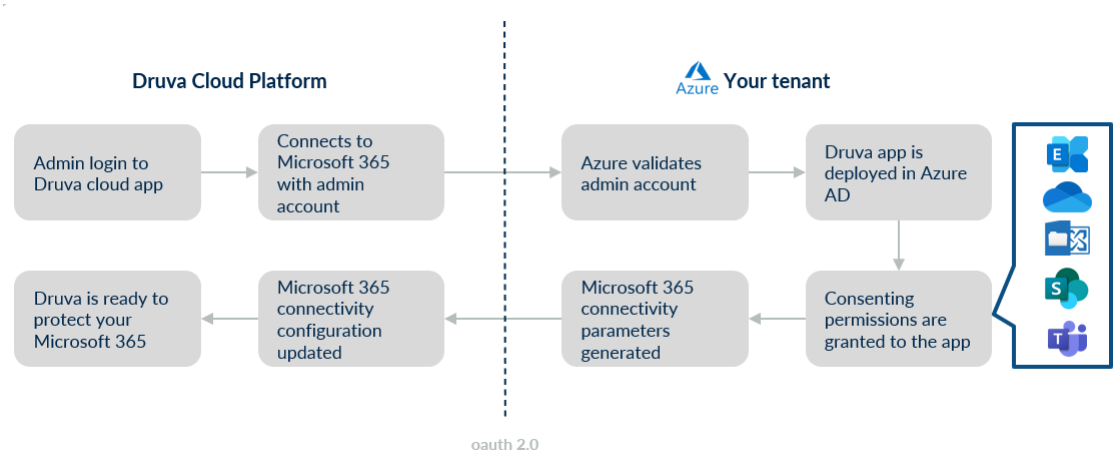
Specific functions within Azure require the authenticated user to have global admin privileges. Those actions occur during the initial configuration of a customer's instance in DCP as well as subsequent re-configurations. After successful connection and configuration to the customer's tenant, the global admin permissions associated with the account should be removed by the company admin. DCP actions such as backup and restore are not dependent on elevated permissions in the customer's Microsoft 365 tenant. If a company is protecting Exchange Online public folders, the user would require permission to access the root folder.



Initial deployment of the Druva app in Azure

During the initial connection from Druva to the Microsoft 365 tenant, a user account with the Global Admin role is required to complete the connection. There are three core functions being completed during this initial connection:

1. Druva App is deployed in the customer Azure AD Enterprise Applications
2. Global administrator consents to permissions granted to the Druva app. The permissions are app-based and enable the Druva app to connect to the specific Microsoft 365 API(s).
3. Permissions are applied to the Druva app

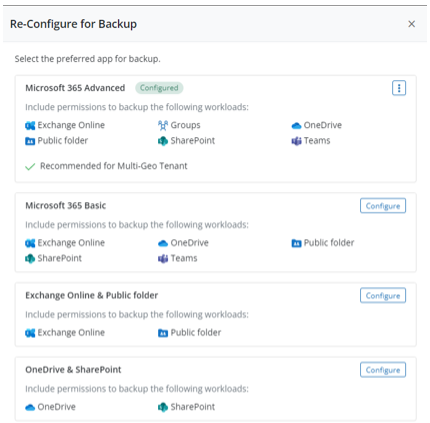


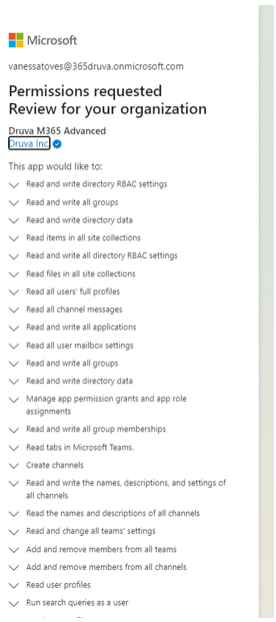
Securing your Microsoft 365 data protected by Druva

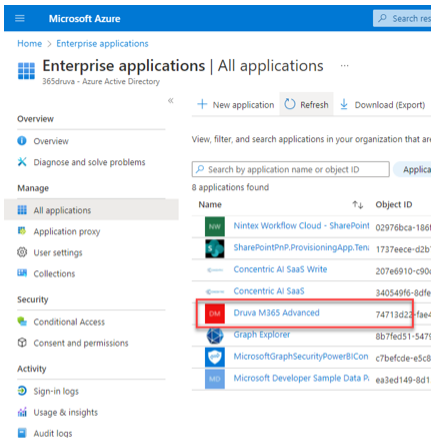
Microsoft 365 App Data Consenting Permissions

Customers have the flexibility of choosing one of 4 options when backing up their Microsoft 365 data. The company admin can choose from the following apps during the initial configuration:

1. Microsoft 365 Advanced (Exchange Online, M365 Groups, OneDrive, Public Folders, SharePoint and Teams)
2. Microsoft 365 Basic (Exchange Online, OneDrive, Public Folders, SharePoint and Teams)
3. Exchange Online & Public Folders
4. OneDrive & SharePoint



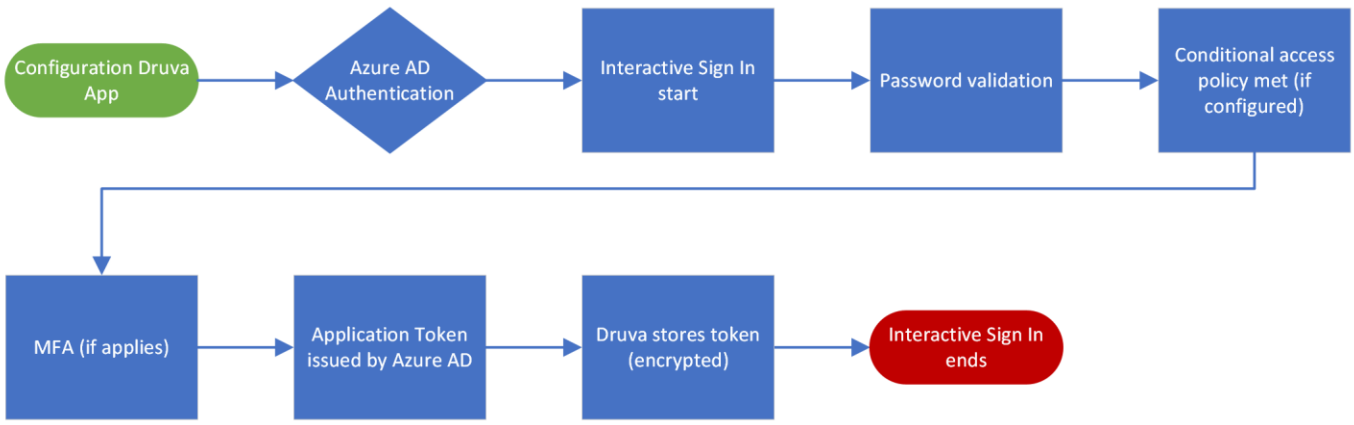




[View the detailed api permissions used by Druva]

Azure AD Sign-In Activity (Interactive)

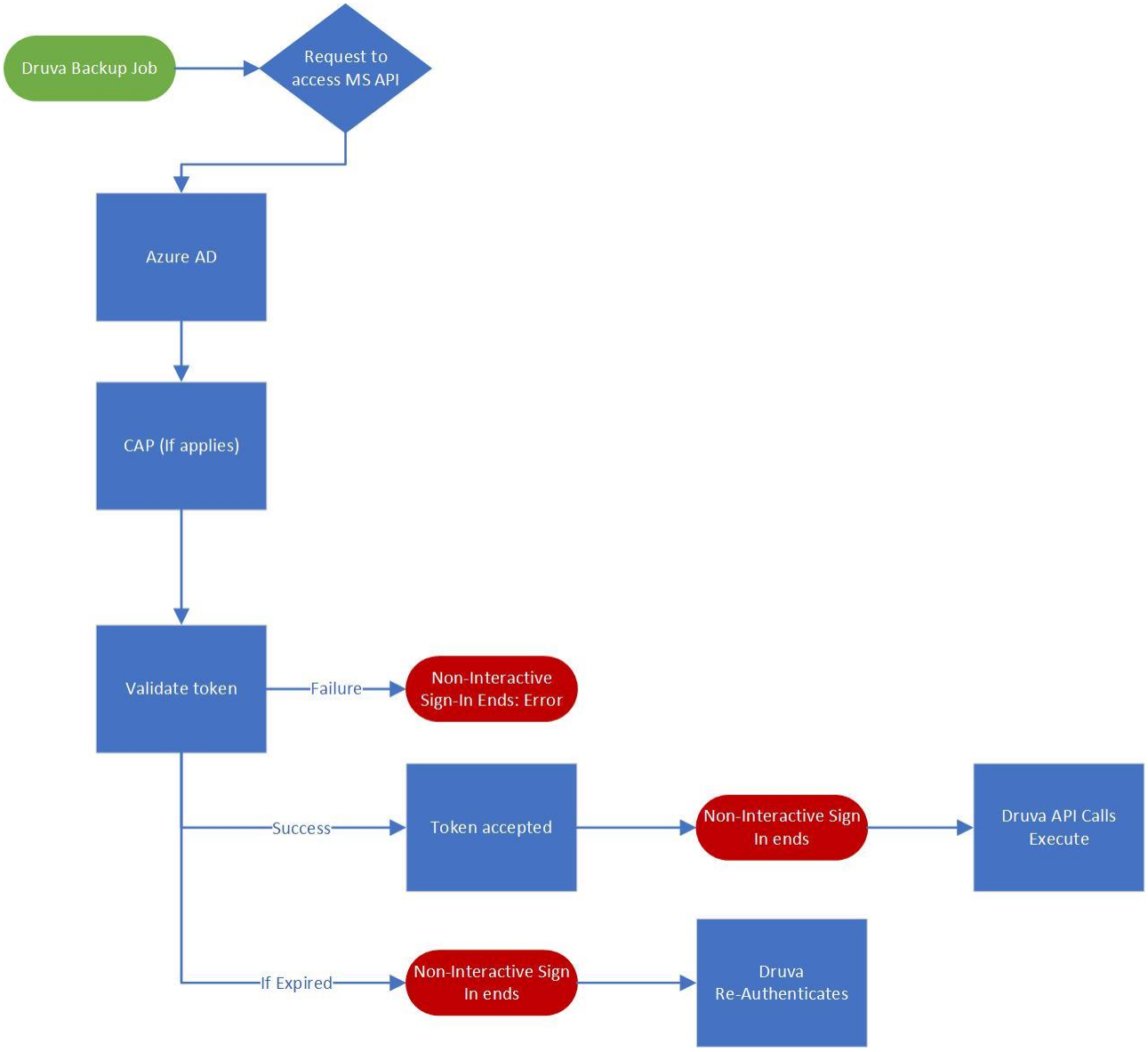
The DCP admin will configure the connection type to the customer's tenant. This initial login will result in an interactive sign-in event in Azure AD. Subsequent reconfigurations or adding an additional connection will also result in an interactive sign-in event in Azure AD.



Druva Authentication Process with Azure (Interactive)

Sign-In Activity (Non-Interactive)

Behind the scenes, backup and restore jobs will log non-interactive sign-in events in Azure AD. The number of sign-ins directly correlates to the number of mailboxes, OneDrive, SharePoint site collections, teams, etc. Success and failure events are to be expected. An example of a “failure” event could be if the refresh token presented for a backup or restore has expired. Azure AD will reject the connection and request re-authentication. Druva will initiate an authentication job and the refresh token will be issued back to Druva for that specific job.



Securing Your Microsoft 365 Account

Now that there's an understanding of the relationship between the two platforms, you can choose how to secure the account and access the data in DCP. The following are guidelines for security measures for the Microsoft 365 account.

Dedicated account	Create one or more alert policies.
Create a dedicated account that is to be used for the backup and restoration of data with Druva. With a dedicated account, you can restrict access using Microsoft security features. • The account used to configure access to your M365 data does NOT require a direct login to the DCP. In fact, for companies that configure SSO, this ensures if this account is compromised, direct login access to the backup data is NOT possible. • After the initial configuration or subsequent re-configurations, this account does NOT require elevated permissions like Global Admin or other elevated roles in Azure. • If you are not protecting public folders, this account does NOT require a Microsoft 365 license.	Alert policies are excellent methods of maintaining visibility to what the account used to connect to the DCP should not be doing. This account should not be accessing your M365 data via a browser, creating mail/forwarding rules, downloading files via OneDrive sync, etc. As an additional layer of visibility and security, we recommend you create one or more alerts utilizing your service desk ticketing system email. All activity by Druva is generated through the Druva app. Link Examples of alerts: • Created group • Downloaded files to computer • The account deletes a file • Share file externally • Create mail forward/redirect rule • Accessed file
Enable MFA	**Secure on-premises privilege (Hybrid)**
Enable MFA for the account used to prevent unintended use. Microsoft also recommends utilizing app-based authentication vs. SMS or Call authorization	Secure on-premises privilege (Hybrid) **Link**
Conditional Access Policy	**Monitor Azure activity logs**
Druva validates the Conditional Access policies enabled for your Microsoft 365 tenant during the Microsoft 365 app configuration to authenticate and provide conditional access to users. • Druva's Conditional Access Policy Support • Configure Microsoft 365 app with Conditional Access Policy	The Azure Monitor activity log is a platform log in Azure that provides insight into subscription-level events. The activity log includes information like when a resource is modified or a virtual machine is started. Link Additionally, you can use the paid service feature of Microsoft Sentinel to ingest and monitor Azure Activity. **Link**

druva

Securing your Microsoft 365 data protected by Druva

Druva Cloud Platform Security

Druva keeps enterprise data completely secure from end to end by adhering to proven standards that protect your data's privacy and safeguard it from external threats. Developed with security as a foundational cornerstone, Druva's solutions are engineered to ensure data protection at every step—transmission, storage, and access.

View detailed security information such as the information below at https://security.druva.com/

Secure multi-tenancy	Data in flight	Data at rest
The Druva Cloud Platform provides a secure, multi-tenant environment for customer data, thereby resulting in complete data isolation for each customer. This secure multi-tenancy is realized by: • Logical segmentation of each customer tenant • Encrypting data of each customer using a unique 256-bit AES encryption key	Druva is designed from the ground up with the understanding that endpoints often connect over WANs and VPN-less networks for backup activities. The Druva Cloud Platform always encrypts data in transit with 256-bit TLS 1.2 encryption, ensuring enterprise-grade security over these networks.	Druva secures data at rest (in storage) with 256-bit AES encryption. The data encryption keys used are unique to each customer and utilize an envelope encryption mechanism to protect the data encryption key itself. The use of a unique encryption key for each customer provides an additional layer of crypto-segmentation on top of Druva's logical segmentation for each customer tenant.
Digital envelope encryption	**Data sharing**	**Operational security**
Druva Cloud Platform is modeled after digital envelope encryption. Digital envelope encryption is comprised. of two encryption keys: • The first key is the Data Encryption Key (DEK) • The second key is the Key Encryption Key (KEK)	Druva's patented deduplication technology, where files are split into individual blocks and only unique blocks are sent to the service globally across all devices. These unique blocks are stored in object storage without any identifying metadata, while block reference data and associated source file metadata are stored in a separate object-based NoSQL database.	Druva employees have no access to any of a customer's instances. Access to cloud infrastructure by Druva employees is limited to the cloud operations team that adheres to strict rules and regulations defined under the Druva security policies document. This access is granted to enable the successful completion of security patching, service upgrades, and monitoring tasks.

druva

Securing your Microsoft 365 data protected by Druva

Druva Cloud Platform Microsoft 365 Data Protection

Druva provides a secure, scalable 100% SaaS platform for the enterprise that protects Microsoft 365 data.

Single Sign-On	Administrator Password Policy	MFA
Druva inSync supports SAML for exchanging authentication and authorization data between security domains. Link	A Password Policy is a set of rules that encourage the use of strong passwords for ensuring added data security. DCP supports and recommends strong password policies. Link	Multifactor Authentication allows you to verify the administrator's identity by using a combination of two different authentication steps. Link
Role-based access control	**Azure AD integration**	**Multiple M365 Data Configurations**
RBAC is a method of regulating access to specific DCP functions Examples include: Disable Snapshot Deletion, Access Sensitive Data Governance or Create and Import Users Link	Druva supports the management of user data to integrate using Azure AD. Customers can control via mapping(s) using Azure AD attributes or groups to control what users are protected.. Link	Druva supports the principle of least privilege by enabling a customer to select one of four different configuration methods. Customers select which Microsoft 365 apps to protect. Link
Geofencing for Admins	**Geofencing for Users**	**Audit Trails Admins and Users**
The Geofencing policy within DCP empowers you to restrict access from outside your corporate network. Link	Restrict users from performing restore functions while off its corporate network. Link	Audit Trails captures the activities performed by the administrators in the console and logs them. Link
Idle Session Timeout	**Sensitive Data Governance**	**eDiscovery Download Client**
The idle session timeout feature represents the amount of time the administrators within your organization can remain inactive on Druva product consoles. Link	DCP enables you to proactively track, monitor, and get notified of data compliance risks in your organization. Link	With the eDiscovery Download Client, you can download custodian data to a server or a device. eDiscovery Download Client enables you to parallelly download data to multiple devices. Admins Link
Data Privacy Policy	**Data Privacy End Users**	**Permissions Transparency**
By default, administrators can access user data and logs across your organization. However, you can: Prevent all administrators (including yourself) from accessing user data or logs. Link	Allows users from preventing administrator access to data and allow users to prevent administrator access to the logs on user devices. Link	Our commitment is to only have access to the data that is being protected and to use the permissions required by Microsoft APIs to support backup (read) and restore (write). Link