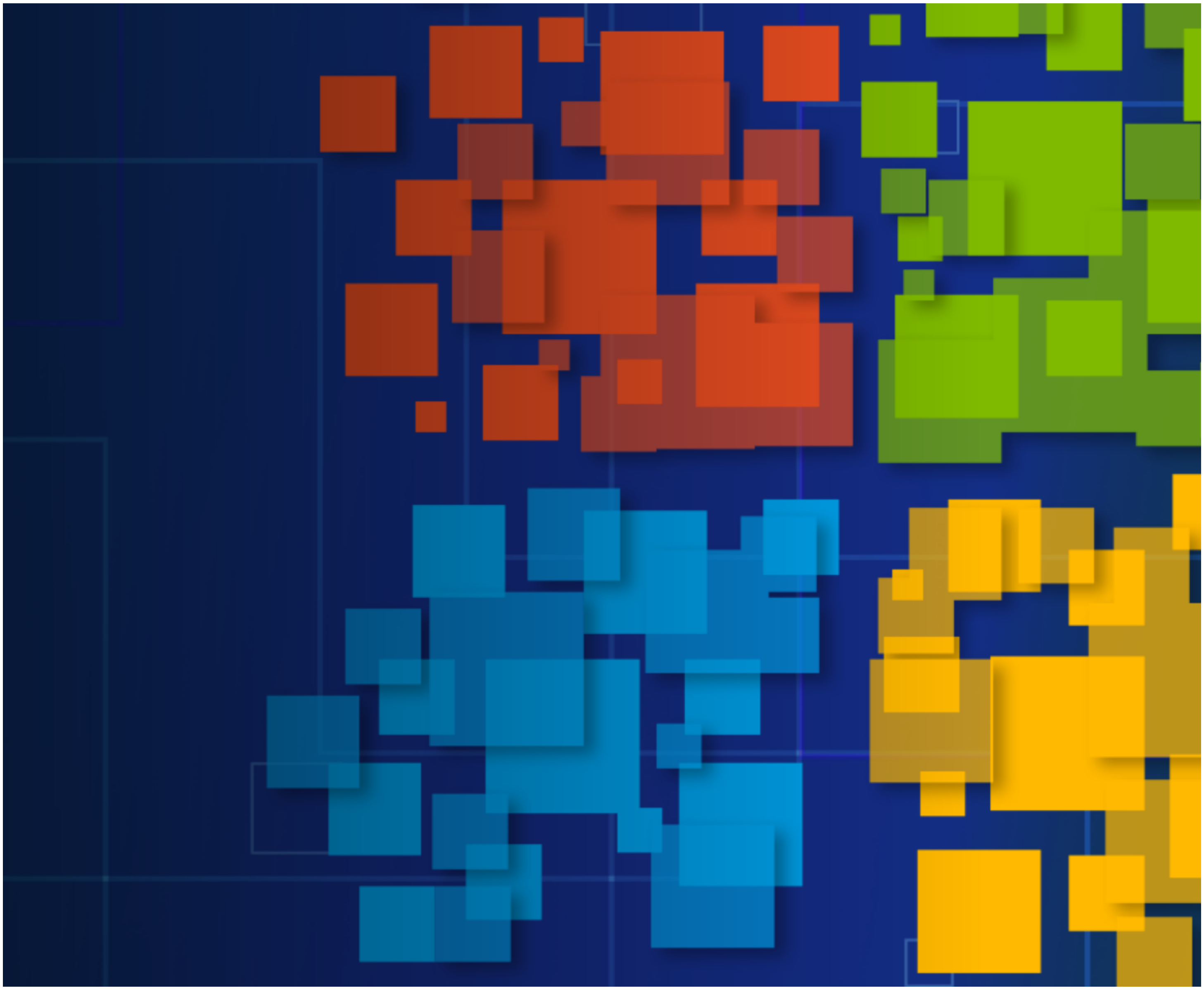
White paper



Overcome native data protection gaps in Microsoft 365

Key challenges with Microsoft 365 native data protection
and how Druva addresses them

The challenge

Native Microsoft data storage offers a number of great features and also some significant gaps. Versioning, replication, recycle bin, and retention policies do not fully secure customer data from risks. Without a true cloud data protection solution, customers are likely to face the following challenges in protecting Microsoft 365 data:

- **Gaps** in Microsoft's retention policy expose sensitive data to risk
- **Data loss** arising from security holes in Microsoft 365
- **Limited data availability** and control
- **Non-compliance**, regulatory fines

Shared responsibility model and customer implication

Microsoft states that under its shared responsibility model, the customers own their data and identities across all of the Microsoft 365 applications. It is worth noting that Microsoft SLAs are built around service guarantees and not data retention.

As a Microsoft customer, you own the responsibility for:

- **Data**
- **Endpoints**
- **Account**
- **Identity and access management**

Microsoft's shared responsibility model (Source: Microsoft)

Responsibility	SaaS	PaaS	IaaS	On-prem	
Information and data	●	●	●	●	**Responsibility always retained by customer**
Devices (mobile and PCs)	●	●	●	●	
Accounts and identities	●	●	●	●	
Identity and directory infrastructure	◑	◑	●	●	**Responsibility varies by service type**
Applications	○	◑	●	●	
Network controls	○	◑	●	●	
Operating system	○	○	●	●	
Physical hosts	○	○	○	●	**Responsibility transfers to cloud provider**
Physical network	○	○	○	●	
Physical datacenter	○	○	○	●	

○ Microsoft ● Customer

From a SaaS data protection perspective, customers will need to ensure:

- **Data availability** — that there is always a copy of their data stored in a different fault domain
- **Full data retention and control** over data access, protection, and governance
- **Business-critical data is protected** from common Microsoft 365 data loss events such as accidental deletion, malicious insiders, and data modification
- **There are security guardrails in place** against external threats such as ransomware and malware as well as non-malware threats such as email fraud, credential phishing, and compromised supply chain attacks
- **On-demand, timely, and fast eDiscovery** and legal hold
- **Compliance** — including automated compliance monitoring, logs, and audits from both internal and external governance, risk, and compliance (GRC) departments

Native Microsoft 365 data retention policy gaps

Data retention policy	Microsoft (E3 & E5)
Content directly provided/created by admins and users (Word, Excel, PowerPoint, Outlook, and OneNote; passwords, certificates, encryption keys, storage keys)	● Active deletion* scenario: 30 days ● Passive deletion** scenario: 180 days
Exchange Online inbox and folders	● Soft deletion: 30 days ● Hard deletion: Admin recovery possible for single items if enabled previously
SharePoint Online	● 93 days from the time data is deleted from its original location ● Hard deletion: No end-user recovery possible. Admin can contact Microsoft for site restoration (library level restore possible based on retention policy and if version history is turned on)
OneDrive for Business	● Restore deleted files from Recycle Bin: 30 days (library level restore possible based on retention policy and if version history is turned on. Restores after 30 days possible based on retention policy) ● Restore deleted files from Second Stage Recycle Bin: 30 days ● Recovering permanently deleted files: 30 days
Departed employee	● Permanent deletion after 30 days once the employee account is deleted and if content has not been restored from OneDrive and Exchange Online
End user identifiable information (DOMAIN/UserName or user@domain)	● Active deletion scenario: 180 days (only by tenant administrator) ● Passive deletion scenario: 180 days
Personal data (Globally Unique Identifiers/GUIDs, Persistent Unique Identifiers/PUIDs, or Security Identifiers/SIDs) & session IDs	● Active deletion scenario: 30 days ● Passive deletion scenario: 180 days

**Tenant with active subscription*

***Tenant whose subscription has ended. Retention policies are available only for E3 & E5 licenses.*

Modifications to retention policies can take up to seven days to become effective. Microsoft retention policies are not data backups by themselves. But E3 and E5 license customers can take advantage of in-built immutability within the service to keep data for the duration the business needs. However, these are highly policy-driven and can result in a customer keeping everything, which can have enormous storage and cost implications.

Retention policies are not designed to enable easy access to the backed up data and quick restore. For example in Exchange Online, if the data under a retention policy is modified or permanently deleted (either from its original location or from the Deleted Items folder) during the retention period, it is automatically moved to the Recoverable Items folder in Exchange or in Preservation Hold for SharePoint and OneDrive for 14 days. But these secure locations and the retained content is not visible to most users. After the 14 days, data stored in Recoverable Items or Retention Hold folders are permanently deleted.

Unraveling “unlimited” storage

Remember that even though OneDrive for Business offers unlimited storage for E3/E5 customers with >5 users, once users exceed the standard 1TB (and another 5TB that can be granted by admins), admins have to request Microsoft support to increase/remove the limit. This is a set process and can be time consuming especially if you have a higher volume of users.

SharePoint Online has limited native built-in backup capability. Customers can enable file versioning and retention, allowing them to go back and look at old file versions, or recover deleted files, but that data also comes off their SharePoint Online allocation, which is 1TB storage per tenant plus 10 GB per license. However, Teams, Planner, and various other Microsoft 365 services actually create sites in SharePoint Online tenant for storage, and files stored in those services count toward the tenant capacity. Customers can buy additional storage at US$0.20 per GB per month. However, this can get very expensive as 1TB will cost ~$205/month.

Security holes risk Microsoft 365 customer data

All of Microsoft’s native security is tooled around the goal that data cannot be removed from the service. Microsoft 365 is a combination of multiple applications, creating a honeypot of sensitive data and files that can be exploited. This has been proved by the several intentional data and identity thefts it faced, especially over the last one year.

Ponemon Institute’s Data Breach Study says that Microsoft accounts are the #1 target of phishing campaigns. Detecting privilege-based attacker behaviors and gaining full visibility over their Microsoft 365 infrastructure is still a big challenge for customers. Native security controls in Microsoft 365 cannot detect or block today’s sophisticated phishing, ransomware or zero-day attacks due to its lack of threat isolation and limited link protection capabilities.

For data loss prevention (DLP), Microsoft offers only basic, mostly rule-based:

- Detection methods (as against powerful machine learning techniques of third-party security vendors that use correlation, behavioral analysis, natural language processing/NLP, and anomaly detection)
- Incident management
- Remediation workflows

Once data is removed from the service, there is zero recourse for customers that solely rely on OneDrive for their backup needs.

Microsoft 365 native security features and risks

Security features	Microsoft 365 E5	Risk
Accidental data loss	• Offers conditional data loss prevention over email but these are very limited in scope • Organizations must create, test, and continuously fine-tune DLP policies manually, resulting in high costs and resources • Manual creation of DLP rules can also lead to risk	• Data loss, data exfiltration • Loss of proprietary and confidential data • IP and financial loss • Loss of reputation and customers that could even result in business closure • Risk of non-compliance

Insider risk	• No dedicated functionality but some support available as part of DLP	• Data loss, data exfiltration
External attacks such as ransomware, advanced spear phishing, business email compromise, supply chain compromise, domain impersonations, and account takeover	• No dedicated functionality for this risk, but just complementary protection which makes detection sporadic and inconsistent	• Compromised user credentials. Injection of ransomware into the environment. • Financial fraud

Note: E3 license holders need to add on advanced security for additional costs.

Microsoft states that, “point-in-time restoration of mailbox items is out of scope for Exchange Online,” [1] which means if you do not have third-party backup, there is no way customers can recover this data.

A third-party data protection service like Druva stores your data in a completely different fault domain (AWS instead of Azure) to ensure its separation from the production environment. Customers can always get a clean snapshot of their data even if they fall victim to internal or external attacks, or if the Microsoft 365 service has an outage.

The complexity of data recovery in Microsoft 365

One of the biggest challenges in Microsoft 365 is data recovery which is manual, complex, and resource-intensive. Microsoft’s fundamental approach to data recovery is to empower users first to recover data from accidental deletion, with longer-term or admin-driven restores being a more complex process. It takes a lot to just understand the several recovery options available across the different applications and execute these for data recovery. Exchange Online alone has Search Mailbox, eDiscovery, and PowerShell cmdlets to recover data. Unlike Druva, there is no single dashboard to view, manage, govern, and restore data across multiple applications. The available options for restore all require significant configuration, taxing the scant resources of IT organizations. Another common issue is that multiple versions of the same file are stored in SharePoint and OneDrive, which can make recovery even more cumbersome.

Contrast this with the highly efficient recovery routes provided by Druva, allowing quick and granular data recovery. Searchable backups for granular file recovery significantly optimizes recovery time and precision.

Support for eDiscovery, legal hold, and compliance

Microsoft stipulates several restrictions — across both its Core eDiscovery (for E3 and below) and Advanced eDiscovery (available only with E5) products — to placing legal holds across applications. The process of identifying and delivering electronic information that can be used as evidence in legal cases can be complicated. There are also several gaps in the eDiscovery process such as:

Challenges with Microsoft 365 eDiscovery

➔ Copying data from Microsoft 365 storage to Azure Blob (for larger files) can cause long wait times

➔ Microsoft’s data throttling limit is 2 GB/hour which can delay exporting results

➔ Data export limited to 2 TB/day per organization

➔ Data view/download limits

➔ Index limits of 100 MB per file (any files more than this size will show a processing error)

➔ Excel file viewer limit is 4 MB

➔ Review download limit set for specific documents is 3 MB or 50 documents

➔ Automatic purging of data after two weeks

[1] Microsoft, “Backing up email in Exchange Online,” April 15, 2021.

In private contracts, Microsoft is known to stipulate that not more than 15 percent of an organization's inboxes can be on concurrent legal hold at any given point in time.

Microsoft offers a number of compliance features through its Core eDiscovery and Advanced eDiscovery licenses. Admins can create, configure, and turn-on alert policies using the security and compliance center (it takes up to 24 hours for the policies to work as these need to be synced to the alert detection engine).

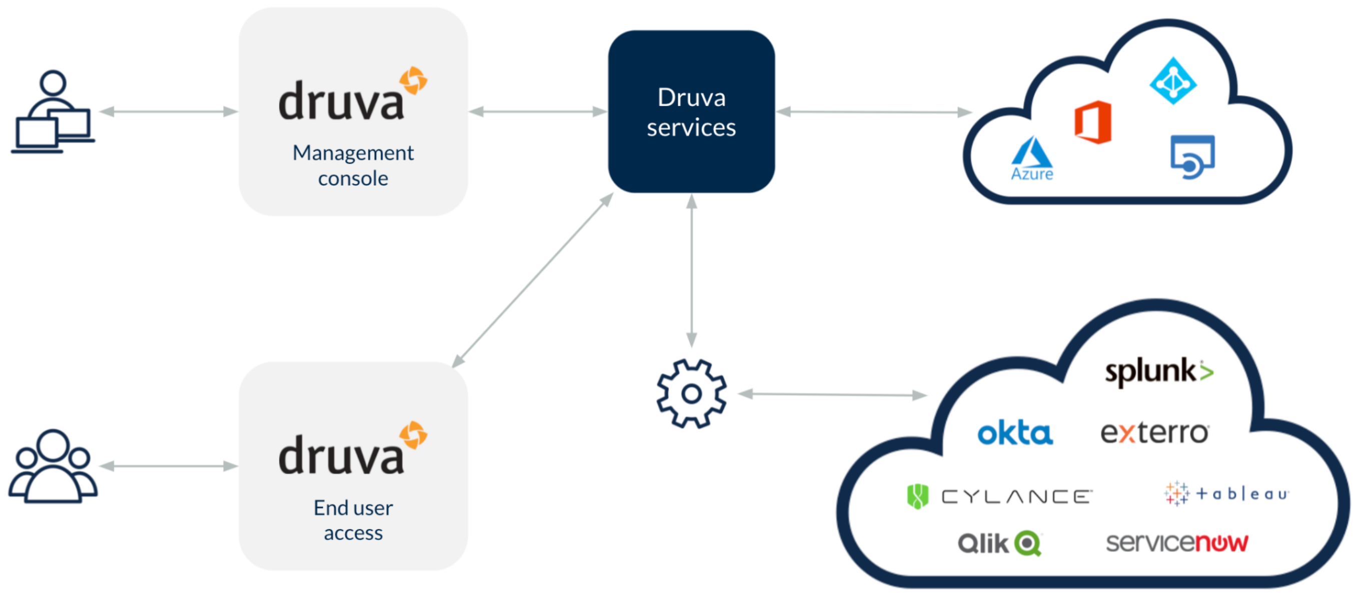
Customers can pull activity logs using the Unified Audit Log interface in the Security and Compliance Center. But, the challenge is the interface can only display pages with up to 150 logs with the maximum number of logs capped at 5,000. Most of the logs are hidden in JSON format, and it takes specialist tools to collect and filter this data. Larger customers tend to invest significantly in hiring specialist firms to collect Microsoft 365 logs for audit purposes.

The solution

Druva addresses the above critical gaps in Microsoft 365 data protection by providing a single, unified, cloud-native platform that brings together simplicity, scale, ease of use, and flexibility to the customer. Built on the high-performance AWS architecture, the Druva Cloud Platform delivers quick value to Microsoft 365 enterprise license customers. With Druva, Microsoft 365 customers can:

- **Elastically scale** compute and storage resources as their Microsoft 365 backup grows
- **Unify Microsoft 365 backups** into a single data pool that simplifies search, eDiscovery, and legal holds
- **Implement admin-driven control** and management of data backups and retrieval
- **Leverage intelligent classification** and federated search for quick recovery
- **Benefit from built-in ransomware protection** as admins can always restore the latest clean version of data from the backup
- **Ensure immutability** for data in flight and at rest via encryption
- **Restore clean copies** of their data from air-gapped backups
- **Enforce automatic compliance monitoring**, and uniform policies across geographically distributed data locations
- **Overcome Microsoft throttling** and performance issues with Druva's novel workarounds for these challenges
- **Achieve robust interoperability** with current cloud tools/tech stack (bi-driectional API integrations with third-party cloud tools such as SOAR, SIEM, and ticketing systems

Druva data protection for Microsoft 365



Business challenges	Druva differentiators
• Business risk and data availability • Lack of understanding of what is a 'true' backup and where Microsoft 365 falls short • Poor visibility on native data protection options for backup/restore options, performance, retention policies, and the associated hidden costs	• Cloud-to-cloud data protection for Microsoft 365 • Platform simplicity, centralized management, great UX • Lower total cost of ownership (TCO), performance SLAs • Support for multiple applications and use cases like ransomware recovery, eDiscovery, legal hold, and compliance • Integrations with third-party tools for threat intelligence, eDiscovery, and workflow • Support for multiple compliance regulations and local data residency needs

The benefits

- **Reduce cost and complexity of cloud backups:** Unlike legacy data protection solutions that require considerable hardware, software, and ongoing maintenance costs, Druva for Microsoft 365 has no associated infrastructure costs. Unlimited storage for all your backups lets you spend less for Microsoft cloud storage. High performance and availability SLAs minimize hidden costs arising from service disruptions.
- **Protection from permanent data loss:** Never worry about native retention time periods or storage quota excesses that can cause permanent data loss. Allows customers to go back in time to recover data that was deleted a while back.
- **Recover from data corruption:** Recover from data corruption without losing the latest changes to OneDrive files or SharePoint resources.
- **Secure by design:** Built-in data immutability, encryption, ransomware protection, and guardrails against data loss events ensure customer data in the cloud is protected whether in motion or at rest across multiple Microsoft 365 applications.
- **Retain control over your data:** Complete control of your organization's backup data, isolated from the primary source. Search across snapshots even when data loss specifics are not available.
- **Overcome native Microsoft eDiscovery challenges:**
    - **Instant restores:** Zero wait time for accessing eDiscovery data. Helps organizations stay prepared for presenting litigation data on-demand.
    - **Cost savings:** Save on Microsoft per user license costs by storing ESI (Electronically Stored Information) data on Druva.
    - **Unlimited and unrestricted data access:** Unlimited quantity of data export for eDiscovery. No need to race against time to download ESI data for processing.
    - **No throttling delays:** No data transfer rate restrictions for gathering case relevant information quickly. 5x faster downloads than Microsoft native eDiscovery.

For more information

druva.com/solutions/microsoft-365-backup

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300

Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva® delivers Data Protection and Management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted by thousands of companies worldwide, including over 50 of the Fortune 500. Druva is a privately held company headquartered in Sunnyvale, California, and is funded by Sequoia Capital, Viking Global Investors, CDPQ, Neuberger Berman, Tenaya Capital, Riverwood Capital, and Nexus Partners. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.