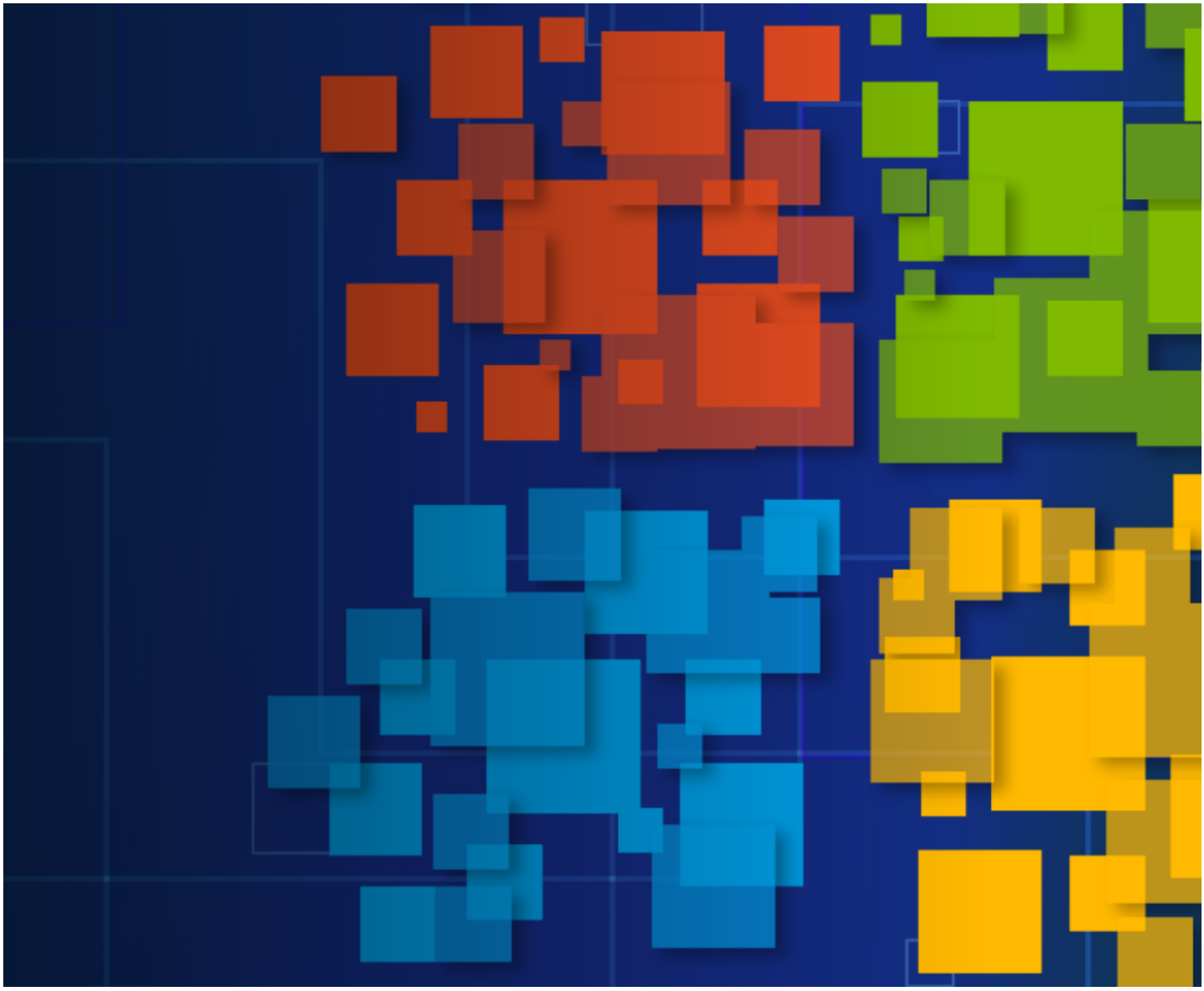
druva

White paper



Guide to Microsoft Teams Data Protection

How companies solve the multi-dimensional challenges of protecting Teams data

Q122-20269

Business risks

Evolving features, support for third-party application integrations, guest users, and new points of integration make Teams a complex ecosystem for data protection and data governance. Companies that use Teams must contend with these vulnerabilities:

- No native backup and SLA-driven data recovery
- Accidental sharing and deletion of Teams data by employees and administrators
- Protecting data from targeted ransomware and malware attacks on Teams

Druva advantages

- Flexible, automated, first full and incremental backups of data, and metadata
- Quick and granular data restore – point-in-time snapshots; restore data in-place or as a copy
- Data immutability with truly isolated backup copies stored on AWS; point-in-time snapshots for recovering data following a ransomware infection
- Federated search, intuitive administrative dashboards, and unlimited retention for efficient data governance and control

Key challenges

Growth in Microsoft Teams reached unprecedented proportions over the course of 2021 and continue to grow. With more than 270 million daily active users as of January 2022, Teams has ushered in a novel approach to hybrid work as well as challenges in managing and protecting huge volumes of data being generated by users. The biggest concerns with Teams data protection are:

- **Complexity:** There are several moving parts to Teams, such as chats, channels, tabs, voice, video, rich presence, screenshare, and whiteboard. Data gets generated across these diverse applications and stored across SharePoint Online, OneDrive, and Exchange Online. Teams also supports integration with 180+ third-party applications, allowing them to push notifications and data into Teams. This heterogeneity makes backing up and restoring Teams data challenging and highly complex.
- **Evolving API support:** The application programming interface (API) for Teams data backup is still evolving, with Microsoft not supporting the backup of certain data types, such as non-document data shared over chat (i.e. animated GIFs), data delivered through webhooks, and whiteboard data. Until recently, voice and video content recorded and stored in Stream could not be backed up. But, with Microsoft moving the data storage location to OneDrive and SharePoint in 2021, it is now possible to backup audio and video content.

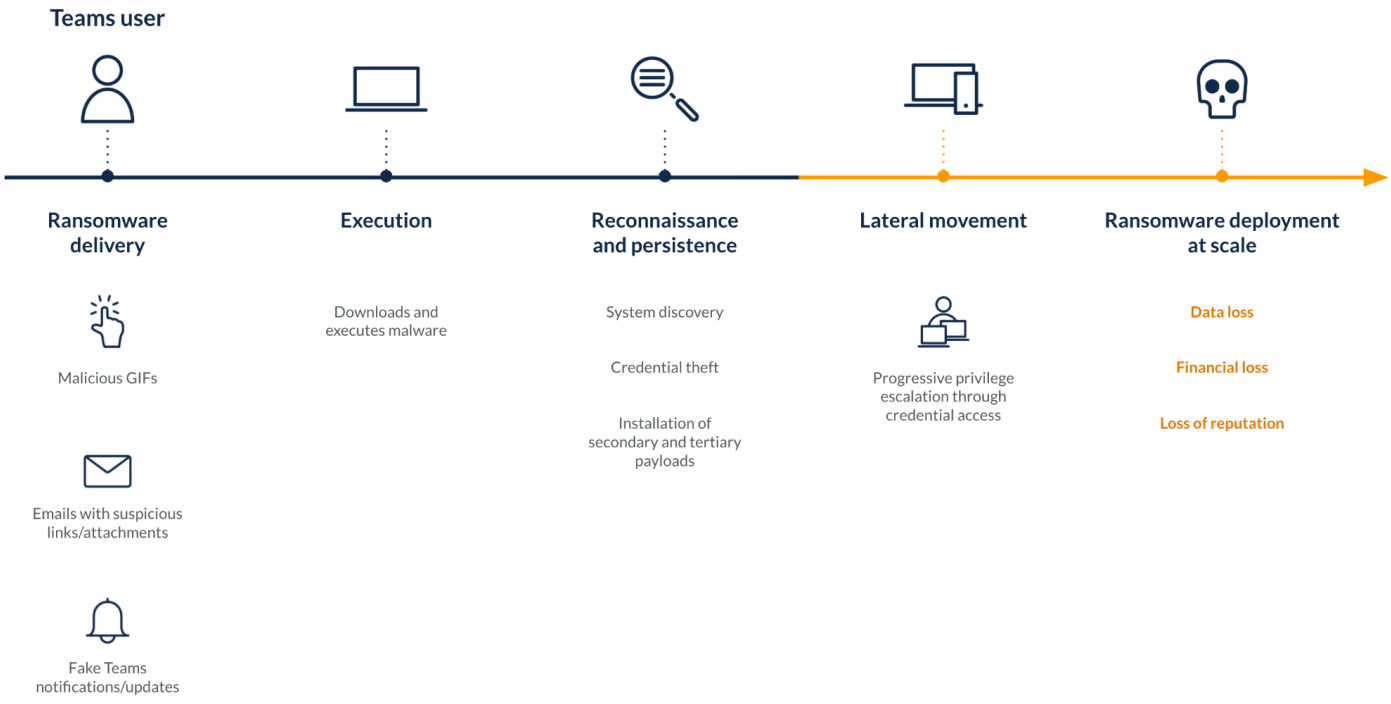
Teams data storage locations in Microsoft 365 and API support for backups

Data source	Where is the data stored?	APIs for third-party backup
Personal chat messages	Exchange Online	Can be backed up as part of Exchange Online / No API for in-place restore
Group chat messages	Exchange Online (Group email)	Can be backed up as part of Exchange Online email groups / No API for in-place restore
Channel conversations	Exchange Online Groups	Can be backed up as part of Exchange Online email groups
Non-doc data shared over chat	Not stored as part of chat files	No backup API available
Docs data shared over chat	OneDrive (1:1/Group)	Can be backed up as part of OneDrive backups
Docs shared over Teams channels	SharePoint	Can be backed up as part of SharePoint backups
Private channel messages	Exchange Online	Can be backed up using APIs
Emails sent to Teams channels	Exchange Online	Can be backed up using APIs
Channel messages posted via webhooks	Azure Cosmos DB	No backup API available
Teams meeting recording	OneDrive/SharePoint	OneDrive and SharePoint storage will support backups
Teams calendar	Exchange Online	Can be backed up as part of Exchange Online

Teams wiki	SharePoint Online	Can be backed up as SharePoint data
Teams whiteboard data	Azure	No backup API available. Roadmap to move this to OneDrive in October 2021.

- **Accidental deletion of data:** In August 2020, KPMG reported that personal chat histories of 145,000 Microsoft Teams users were inadvertently deleted by an administrator. Accidental deletion of Teams data by both employees and administrators is a cause of concern for many organizations. Microsoft Teams fosters collaboration and data sharing, but these come with the risk of users accidentally sharing confidential information with unauthorized third parties or providing a backdoor entry into the organization by inviting guest users to their Teams chats/meetings. Though it is recommended that organizations continuously audit what is being shared across Teams, and especially with guest users, this just adds to the administrative burden.
- **Data loss from ransomware and malware:** In late 2020, Microsoft issued a warning that attackers were using fake Teams updates to deliver malware into customer networks. Over the course of the last several months, there has been a rise in the number of Teams-specific attacks across a number of organizations as ransomware and malware can be delivered through a number of routes into the application – directly via chats (as URLs, documents with malicious URLs, GIFs), or through Exchange Online emails. Microsoft's native threat protection tool, Microsoft 365 Defender, can scan URLs in emails and attachments delivered via emails. However, URLs delivered directly to Teams chats are not scanned for malware.

Microsoft Teams ransomware attack chain



- **Compromised Teams profiles:** Microsoft recently released a patch for a severe flaw found in Teams that would allow bad actors to breach a user's account. Compromised Teams profiles pose an immense danger to organizations as these accounts provide legitimate access to confidential data. Microsoft acknowledges that there has been a recent spurt in the number of cybersecurity threats targeted at its users. It has a Compromise Recovery Security Practice (CRSP) team to help organizations recover post-breaches. However, the CSRP team focuses only on recovering control over the customer environment, recovering applications after a ransomware attack, and advanced threat hunting, NOT data recovery. Microsoft does not make any assurances for recovering/restoring customer data residing within Teams and the broader Microsoft 365 ecosystem in the event of permanent data loss.

- **Rule-based native data loss prevention:** For data loss prevention (DLP), Microsoft offers only basic, mostly rule-based options:
    - 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.

Limitations in native data restore in Teams

While Microsoft does provide a number of features for retaining data across the Microsoft 365 ecosystem, these are not without some significant gaps that can make data restore complex, manual, risk-prone, and time consuming.

Gaps in Teams data restore

Teams data	Restore option	Limitations
Files stored in SharePoint	Gives users access to version history. If deleted, restore from Recycle Bin within 93 days after which it moves to second stage Recycle Bin for another 93 days. End-user recovery.	Not a true backup. Files can be altered, deleted, and encrypted. Versioning is not equal to backup.
Conversations and chat history	Stored in Exchange Online and not recoverable directly. However, using eDiscovery tools, this content is searchable and can be manually downloaded one file at a time. End-user recovery.	Long, manual recovery even for individual files. No bulk recovery and restore possible.
Tabs, connectors	No recovery option if these get deleted, but can be reconfigured by admin.	Even if tabs and connectors are reconfigured, no guarantee that the underlying resources are available.
Conversations and content in channels	Data stored in SharePoint and OneDrive. Directly recoverable from Teams for up to 21 days. End-user recovery.	Longer retention times possible based on SharePoint and OneDrive configuration.
Entire Teams	Involves recovering the associated Microsoft 365 Group. Can be recovered from Exchange Online for up to 30 days (soft delete). End-user and admin recovery supported (from different locations).	Hard deleted Teams have no recovery option.
User deleted messages	Permanent deletion after 21 days.	No long-term retention options.
Bulk export of Teams chat messages	API limitations for bulk exports.	Restricted to 200 RPS per app per tenant and 600 RPS for an application.

Microsoft retention policies for Teams

Microsoft allows retention policies to be applied to Teams chats messages and channel messages. In addition to these, embedded images, tables, hypertext links, links to other Teams messages and files, and card content can also be retained for compliance purposes. However, there are a number of elements that cannot be retained using a retention policy, such as code snippets, recorded voice memos from the Teams mobile client, thumbnails, announcement images, reactions from others in the form of emoticons and emails, and files used with Teams. Though Teams data gets stored across SharePoint, OneDrive, and Exchange Online, existing retention policies configured within these applications are not automatically applied to Teams content. For example, Microsoft says "Teams chats and channel messages are not included in retention policies that are configured for Exchange user or group mailboxes."

Customers need to have an E3 or an E5 license if they want to use retention policies.

The solution

Druva delivers comprehensive, enterprise-class backup and data protection for Microsoft OneDrive, Exchange Online, SharePoint, and Microsoft Teams. Druva complements Microsoft 365 by filling data protection gaps without dedicated hardware, software, or resources. The secure 100% SaaS platform ensures that company data is open and accessible to unified governance policies and ransomware protection, while providing critical insights into business-critical Microsoft 365 data and projects.

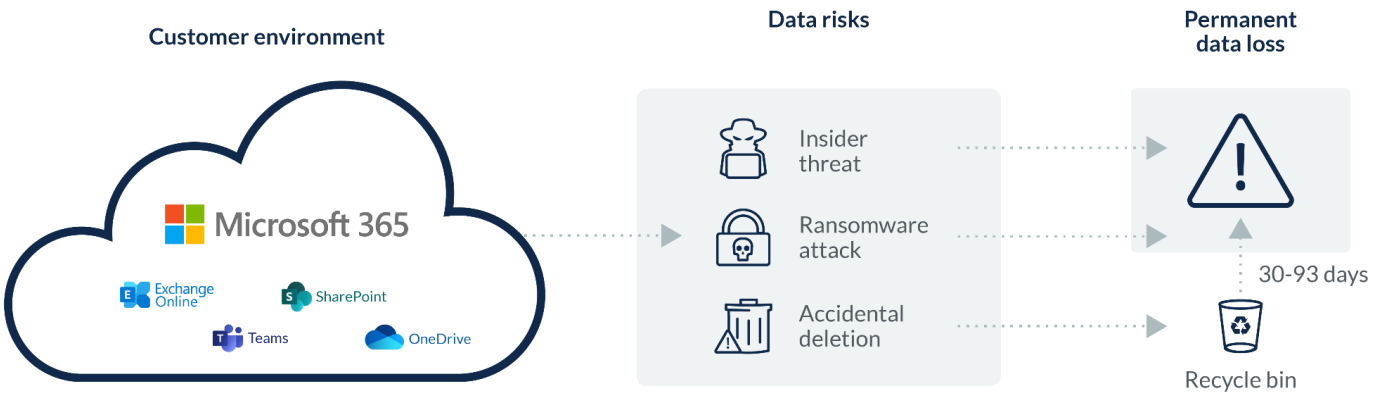
In addition, Druva addresses critical gaps in native Microsoft Teams data retention policies. With Druva, Microsoft 365 customers can back up:

- All Teams data within all of its channels (standard or private) including date of creation, Teams name, members, permissions assigned to Team members and guests, and more
- Files, Wiki, OneNote, and tabs within a channel
- Conversations or posts within a channel

Druva supports **in-place restore** (to the same Team from where the data was backed up), and **restore as a copy** (channel to a new channel, and Files and folders to a new file/folder within the channel) for the following:

- An entire Team
- Only Teams' settings
- An entire channel or any file, folder within a channel
- Preview messages in a post
- Entire channels' folders
- File folders
    - Individual files within the file folder
- Wiki folders
    - Individual Wiki files within the Wiki folder

Druva data protection for Microsoft Teams



The benefits

- **Best-in-class protection for Teams data:** Druva eliminates the complexity associated with protecting Teams data by providing a single 100% SaaS platform to back up and recover your data with just a few clicks. Customers rely on Druva for speed, simplicity, zero hardware or maintenance, and significant cost savings.
- **Protection from permanent data loss:** Relying on just native Microsoft data protection capabilities can make organizations vulnerable to data loss. Never worry about native retention time periods or storage quota excesses. Druva allows customers to go back in time to recover just the data they need.
- **Recover from data corruption:** Recover quickly without losing the latest changes to Teams files, chats, or messages. Druva auto-replicates your backup data into three separate locations for true backup immutability.
- **Secure by design:** Druva provides complete protection immediately — deploying in only 15 minutes. Automated, complete 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 — including Teams, OneDrive, SharePoint, and Exchange.
- **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.
- **Limitless dynamic scaling:** Data protection scales to meet your needs based on use.
- **Stringent security and compliance:** Druva is certified for or compliant with important regulations and frameworks such as SOC 2 type II, HIPAA, FIPS 140-2 and FedRAMP ATO, among other audits and attestations.
- **Comprehensive global deduplication:** Druva uses less than half of the storage used by other data protection solutions enabling customers to receive an up to 50% reduction in TCO.
- **All-inclusive, simple consumption-based pricing:** No operational expenses, hardware, or software costs. No maintenance, infrastructure, or transaction costs. One price for service and storage.
- **Excellent customer service and support ratings:** Druva features an NPS score of 89.

For more information

Druva was named a leader in the Forrester New Wave for SaaS Application Data Protection; read the report to learn more. Discover how Druva fills the gaps in native Microsoft 365 data protection by visiting druva.com/solutions/microsoft-365-backup. Or, sign up for a live demo or free trial to see Druva in action.

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 enables cyber, data and operational resilience for every organization with the Data Resiliency Cloud, the industry's first and only at-scale SaaS solution. Customers can radically simplify data protection, streamline data governance, and gain data visibility and insights as they accelerate cloud adoption. Druva pioneered a SaaS-based approach to eliminate complex infrastructure and related management costs, and deliver data resilience via a single platform spanning multiple geographies and clouds. Druva is trusted by thousands of enterprises, including 60 of the Fortune 500 to make data more resilient and accelerate their journey to cloud. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.