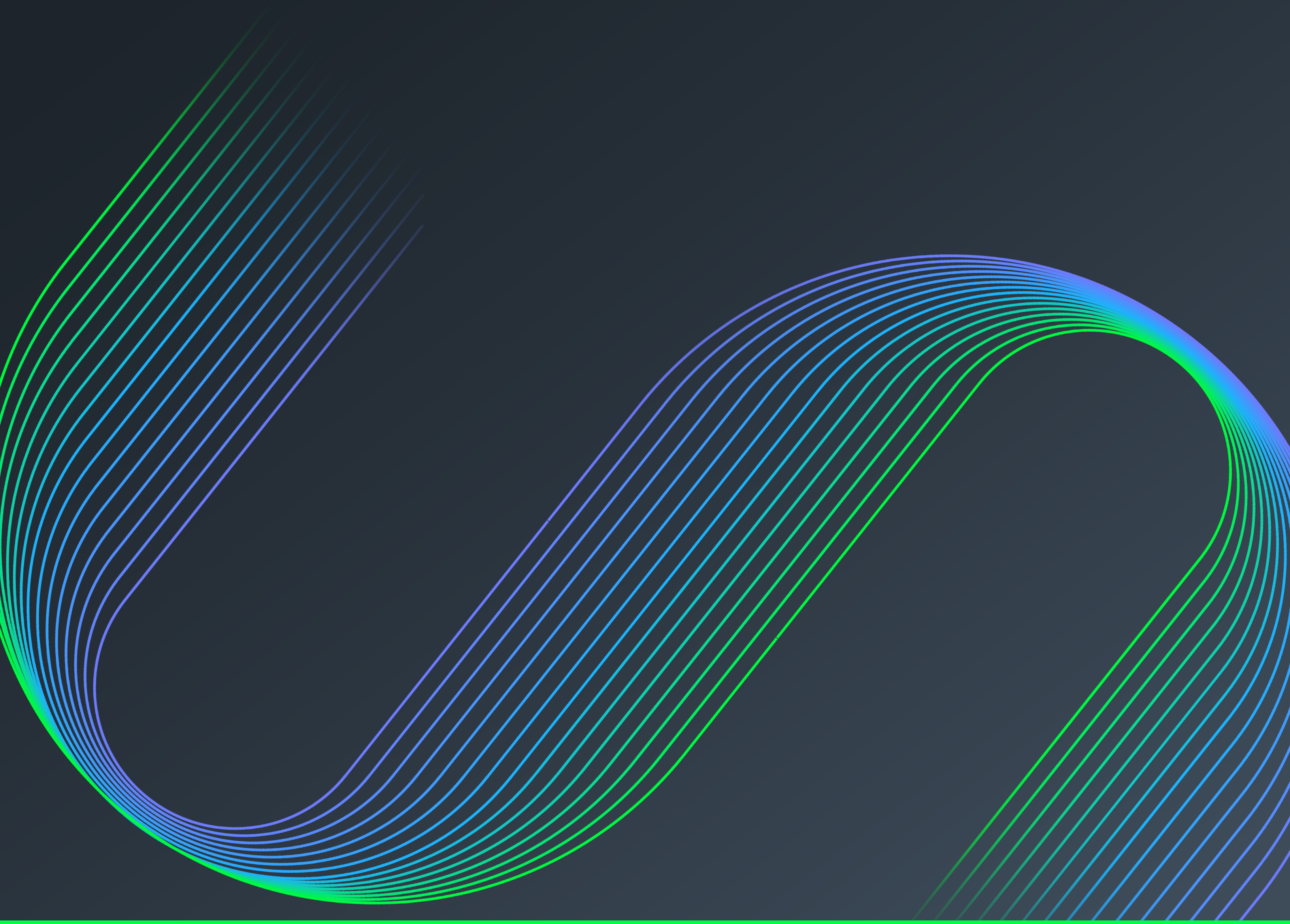
COHESITY

A comprehensive guide to

Ransomware protection for Microsoft 365

Improve your organization’s cyber resilience



Contents

Data security matters

If your business relies on Microsoft 365 (M365), collaboration minutes and user count aren't the only things you should be keeping an eye on. Ransomware is on the rise, and your sensitive data in M365 will increasingly be coming under attack.

Bad actors are already looking to infect your data with malware and encrypt it, demanding that your organization pay ransom to get it back. Beyond that, cybercriminals will be hoping you have limited protection on your sensitive data in M365 so they can potentially exfiltrate, or steal, it before using it to extort payments as a way of preventing its public disclosure. That technique is quickly becoming part of "double-extortion" ransomware schemes.

Whatever their plan, ransomware attackers can badly damage your bottom line and brand reputation. Stay one step ahead. Microsoft guidance for countering ransomware targeting your M365 data is simple: Regularly backup content and data. Store using third-party apps and services.[1] This is good advice. But it's likely not enough.

Keep reading to discover why and how to improve your ransomware protection for M365 >

59% of companies were hit by ransomware

in the past year.[2]

34% say malicious deletion from a cyber attack

is the most common causes of SaaS data loss.[3]

[1] Microsoft Service Agreement, Section 6b

[2] Sophos, 'The State of Ransomware 2024,' 2024.

[3] Enterprise Strategy Group "Data Protection for SaaS," 2023

Understanding shared responsibility

As a hyperscale cloud and application provider, Microsoft operates a shared responsibility model. What that means in practice is that Microsoft commits to high infrastructure reliability and availability service levels, robust infrastructure security, and limited data protection, including some data retention policies and versioning that we'll cover next. It never commits to ensuring the availability of your content. That's a broad-brush view of its share of responsibility.

Your responsibility share is just as important to maintaining your brand reputation and customer trust. You own your content. So your cloud data is your responsibility to protect in the short and long term—to meet your business and regulatory requirements. It's also on your organization to recover your data quickly should it be attacked. Your in-house share of responsibility for M365, a mission-critical environment, is the number one reason to consider following best-practice advice and going beyond basic M365 protection to add third-party apps and services that protect your data from ransomware attacks.

Although Microsoft has some built-in ways to retain data after deletion or modification, these capabilities simply aren't robust, immutable backups (more on that later).

Native M365 protections at a glance

Data protection is important for the M365 apps serving your key business operations. Here's a brief look at what Microsoft has built in:

Exchange Online	• Retention default for deleted items is 14 days, up to 30 days, if configured • Retention default for deleted email boxes is 30 days
OneDrive	• Retains deleted items for 93 days by default for Site Collection Recycle Bin • Retains deleted items for 30 days by default for a User's Recycle Bin • Recovery of data back to a point in time for up to 30 days, if configured
SharePoint	• Retains deleted items for 93 days by default for Site Collection Recycle Bin • Retains deleted items for 30 days by default for a User's Recycle Bin • Retains backups of deleted items for an additional 14 days • Admins can recover deleted site collections + contents within 90 days
Teams	• Message retention default ranges from 1–7 days • Other data types have limited retention based on the services providing them

Keep in mind that each M365 service also relies on Microsoft Azure Active Directory at its core, so it's also important to have a plan to back up that repository as well to be able to rapidly restore end-user access.

Ransomware is lurking

Malware can infiltrate a system and hide for weeks or months to further spread to other systems before launching a full attack. Moreover, versioning as you'll discover, just isn't suitable to recover from ransomware because restores have to happen from a specific point in time on the entire data set—rather than on individual files—to ensure your restored data is free of ransomware infection.

Ransomware-as-a-Service (RaaS) is pay-for-use malware. It lets attackers use a platform that provides the necessary ransomware code and operational infrastructure to launch and maintain a ransomware campaign.[4]

A note about backups vs. versioning

If you need more evidence native M365 alone isn't robust enough backup for your data, consider how it retains data. Unlike true backup solutions, M365 uses a technique that works more like version control—which is managing multiple revisions of the same information or files. Put another way, versioning happens on an individual file basis and each file has a different file version history. The challenge with this approach is that ransomware attacks happen at specific points in time and negatively impact a large number of files at once.

Let's look at an example in Figure 1 on the next page. A new PowerPoint presentation created today is on version 2 while a years-old sales forecast spreadsheet is on version 1278 (if everything is even set up to keep so many versions). This type of versioning retention makes it difficult, if not impossible, to restore or roll back thousands of files at once to a particular point in time across documents to the time before an attack.

24% reported data loss due to misunderstanding data retention and deletion policies.[5]

And,

Only 2% say they could recover their data and restore business processes within 24 hours of an attack.[6]

[4] Ransomware trends, statistics and facts heading into 2024," 03 Jan 2024.

[5] Enterprise Strategy Group "Data Protection for SaaS," 2023

[6] Cohesity Global Cyber Resilience Report 2024

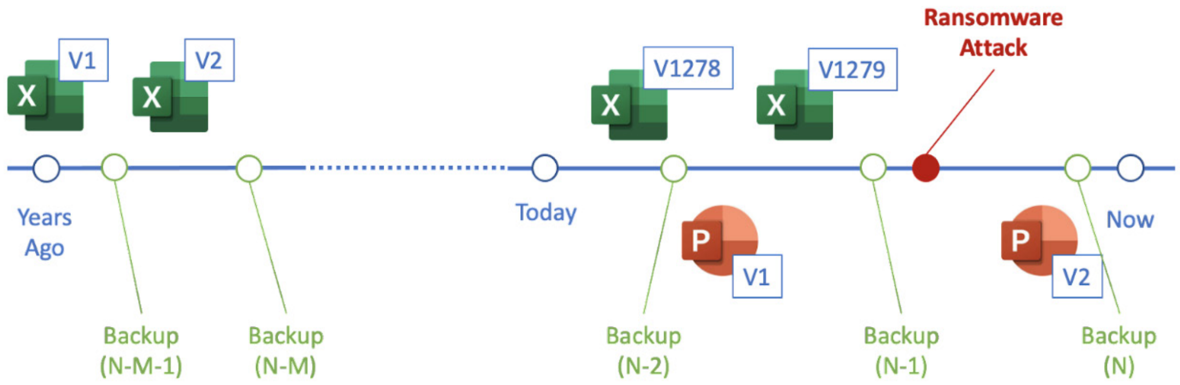


Fig. 1: Backups vs. versioning comparison timeline

A modern backup and recovery solution gives your organization fine-grained control over how long you can keep data and also allows you to restore all of your data—on a per-snapshot basis—to a specific point in time, for example, just before an attack or compromise. This way you're assured your team has a clean copy of all your files and data at their fingertips for rapid recovery.

Streamlining compliance and meeting internal requests

New and changing government regulations have heightened the need for your organization to be agile when it comes to adjusting data retention policies. In regulated industries such as healthcare, financial services, and government, for example, teams are now regularly being required to keep data beyond seven years (and sometimes even forever).

Any organization that's been in a legal dispute also understands the value of flexible retention policies. eDiscovery can take months, even years, and involve M365 data such as emails and documents. Without flexibility in how long you retain and how quickly you can retrieve your data, you could be putting your organization at risk of non-compliance or fines related to meeting legal discovery requests.

Executives are also adjusting internal company guidelines more often to meet business needs and protect data in the cloud era. They're establishing policies that include moving data offsite or to another cloud for maximum protection and minimum vendor lock-in. You'll want to be sure you have a plan in place to keep your data protected in case of an M365 service interruption or you someday decide to move away from M365 to another cloud provider.

Evaluating current M365 protections

If your organization has adopted M365, the defaults may have worked so far. Now consider these questions as a way to decide if they'll be enough for your future:

- Are you protected if M365 is compromised and the only copies of your data are in Microsoft's cloud?
- What would happen to your organization's brand and reputation if data was exfiltrated and leaked to the public or dark web?
- How would you restore data needed for eDiscovery or a legal situation that arises months or years from now?
- How do you support recovery time and recovery point objectives (RTOs/ RPOs) without Microsoft offering service-level agreements (SLAs)?
- How are you addressing compliance regulations for your data? How do you plan to demonstrate compliance if you are attacked?
- What solutions do you have to migrate data back on-premises or to another service, if needed?
- What are your options for backing up M365 data to another cloud for cyber resilience and isolating data if Microsoft's cloud is attacked?

Do any answers to these questions give you pause? The default M365 protections may put your business or data at risk.

Diving into disaster: How ransomware causes chaos

Despite apps having basic versioning and retention capabilities, cybercriminals find vulnerabilities. Here are common ways they've targeted M365 with ransomware.

Infection

Remember those emails from the wealthy prince promising millions of dollars upon response? Email is still one of the top infection vectors ransomware exploits. Simply by clicking on a link or downloading a document is enough to trigger malware that encrypts data and systems in homes and businesses.

Seven in ten organizations (71%) experienced at least one successful phishing attack in 2023 compared to 84% in 2022, according to 2023 State of the Phish report.[7] And while this seems like good news, some of the consequences have become more severe (e.g., penalties and fines).

Recently, Retirement Clearinghouse, an organization offering retirement account consolidation services, reported a data breach that affected approximately 10,500 individuals. A phishing attack on an employees email caused the breach, leading to potential unauthorized access to personal data. Infection through email—including Exchange Online—is a common vector for attackers to gain access to enterprise systems. Once bad actors gain access, their ransomware moves laterally using compromised credentials to attack by exploiting the vulnerabilities of unpatched systems.

Popular examples of malicious emails seen recently in threat signals include:

- **Phishing** (also spear-phishing): Attackers look to trick someone into sharing sensitive information by sending notifications of urgency to click on a link, for example, to reset a password. Upon entry of their credentials on a fake domain, victims are often redirected to a legitimate site, such as the M365 login page, to retype their credentials, completing the theft and scam.

- **Malware delivery**: When a compromised message is received and opened, it can be linked to a malicious web site that delivers the malware to a business computer. Alternatively, an infected document may include macros that download ransomware in the background, turning systems into weapons to attack others in the environment.

Cerber ransomware is a notable example of attackers focusing on Microsoft (Office) 365 users to deliver phishing emails.[8]

[7] 2024 State of the Phish – Today's Cyber Threats and Phishing Protection

[8] AFI. "Can Ransomware Hit Your Microsoft 365 Data?" 22 April 9, 2023.

Despite doing everything right with foundational M365 protections, including correctly configuring Mail Flow rule(s) for SCL spam detection, anti-spam, anti-phishing, safe links, safe attachments, multi-factor authentication and anti-malware settings, some emails from bad actors still make it into enterprise mailboxes. The challenge is even more acute with OneDrive and SharePoint files which are at higher risk of being encrypted.

When attackers strike, you want to be sure you can recover quickly, according to business SLAs. If your enterprise has expectations of a recovery SLA (RTO and RPO) and a preferred format of recovery from unexpected disruption such as a ransomware attack, you will need a data protection solution to align with business needs and ensure recoverability. That means making backup protection for your entire M365 suite including Exchange Online emails part of your IT plan.

Data encryption

For years, data encryption has been ransomware attackers' go-to strategy. Cybercriminals lock up production data and demand a large-sum payment before promising to give teams an encryption key (or often, a set of keys to dig through) to decrypt and free their data. For example, OneDrive and SharePoint are already in bad actors' grips. These collections can be encrypted in several ways. For example, infected local files are synced from a user machine to OneDrive or SharePoint, or directly from a server that encrypts and syncs files at scale. Even if you could rollback your files with versioning, the process is tedious and can't address point-in-time recovery—often a business-critical requirement. In all cases, an immutable backup and recovery system is an effective countermeasure.

Data theft and exfiltration

Beyond imaginable success has emboldened ransomware attackers and they have become more creative. Cybercriminals are now not only encrypting files and data, but also stealing them. They are illegally removing large amounts of data (exfiltration) and targeting the sensitive and confidential information including customer credit card numbers and personally identifiable information (PII) with the goal of threatening to leak it publicly or sell it on the dark web to extort even larger-sum payments from victimized organizations.

The ransomware double-extortion threat is ideal for M365 data and terrifying for businesses. With M365 and other SaaS apps providing easy online access and simple sharing controls, cybercriminals have great opportunities—many with fewer obstacles. To combat them, organizations need to proactively monitor the apps and users accessing data for behaviors indicative of cybercriminal actions.

In 2024, ransom payments averaged $2 million, up from $400,000 in 2023.[9]

Of those hit by ransomware, 94% said that the cybercriminals attempted to compromise their backups.

57% of those attempts were successful.[10]

[9] State of Ransomware 2024," 2024

[10] Sophos, "State of Ransomware 2024," 2024

Actionable steps to reign in data and lower risk

Built-in M365 safeguards are not equivalent to modern data backup. They do not provide a multilayered approach to M365 ransomware protection either. Be better prepared to counter ransomware attacks with a modern back up and recovery solution that empowers you to perform three key steps to properly defend your data.

1. Meet SLAs and simplify hybrid cloud operations

In addition to strengthening your data protection, BaaS includes a comprehensive, enterprise-grade feature set that lets you decide when, where, and how long to keep important information. This gives your organization the most choice and flexibility in how you protect your data and meet business requirements today and tomorrow.

Single management plane

Many organizations use multiple tools to manage and protect their data, leading to silos that create gaps in protection, which hackers can exploit. Newer solutions will not only simplify protection by combining data management and security capabilities onto a single platform, but also provide global visibility into your M365 data and other workloads. With a bird's-eye-view you can quickly spot abnormalities and react.

Unified backup (M365 plus other data sources)

Because you may not want to move every workload to the cloud for business advantage or compliance reasons, adopt a data protection solution that allows you to back up M365, other SaaS and cloud data sources as well as on-premises workloads such as VMs and databases.

Flexible retention

When it comes to meeting complex compliance requirements, there's no better option than modern third-party backup. It lets you control how long you need to keep M365 data (for months or even years) and manages those policies for you. Also flexible long-term retention—beyond M365 defaults—helps ensure your organization can recover data from any point in time if disruption occurs.

Pricing flexibility

A robust data management strategy will also consider factors beyond ransomware in decisions about which backup solution to choose. For example, aligning the budget for M365 backup with how your organization operates is critical. Will you pay by number of users, matching backups to M365 plans, or will you consolidate backup data across a variety of sources and pay by capacity. Most BaaS solutions are optimized for pricing flexibility. Another consideration is whether you can purchase it through the Microsoft Azure Marketplace to help offset Microsoft Azure Consumption Commitment (MACC).

2. Secure backups

Now that cybercriminals have realized data retention repositories and backups are like insurance policies, it's incumbent on your organization to do more to safeguard your valuable backup data. For best results, choose a BaaS offering with stringent security controls. Moreover, consider BaaS where data is retained in a separate cloud service outside of Microsoft and does not charge extra for data egress, so if you choose, you can use it to create a form of data separation while eliminating vendor lock-in.

Immutable backups

For cybercriminals, targeting production data is still a primary goal. Yet more often, they are also now attempting to encrypt or delete backups to disable any ability you might have to recover your production data quickly after an attack. A replace with modern BaaS solution that features immutability helps prevent both scenarios because data is in an immutable snapshot that can't be accidentally or maliciously altered, changed, or manipulated.

Write once, read many (WORM)

WORM empowers your team to create and apply a time-bound lock on data through policies and then assign them to selected jobs to enhance immutability for protected data. As this is a protection that neither security officers nor security administrators can modify or delete, you don't have to worry as much about potential insider threats. This is a replace with modern data management capability that M365 doesn't natively provide.

Access controls

Look for a solution that takes a comprehensive approach incorporating Zero Trust Security principles such as granular role based access, Multi-Factor Authentication, Single Sign-On, immutable snapshots, privileged access management, and Quorum. These security measures define who can view or change data, helping to ensure that sensitive information is protected from unauthorized access.

Separate backup data from production

Storing your backup data outside of the Microsoft cloud can help achieve one form of "off-site" data separation while also helping thwart ransomware payments. BaaS helps you balance your RTO/RPO requirements with appropriate security controls by storing backup data in the cloud or at another location. Your backup data will be available during an M365 outage and be resistant to tampering from cybercriminals as it is stored in an immutable snapshot.

3. Adopt fast, flexible protection and recovery

Whether your organization needs to recover from a ransomware attack or find files archived for years (well beyond the standard retention periods of M365), you need a modern backup solution that can recover data from any point in time—and fast. With a newer management backup as a service (BaaS) solution, you get automated backups along with full and granular restores together with on-demand access and ease of use.

Rapid recovery at scale

The right BaaS solution can quickly recover hundreds, even thousands, of mailboxes or files in case of a large-scale attack, natural disaster, or human error. And recovery at scale shouldn't just be limited to M365, but also allow you to rapidly restore hundreds of VMs, large databases, or large volumes of unstructured data to any point in time and target location.

Point-in-time recovery

Within M365, an employee can bring up a different version of a single document or presentation to quickly recover it. Yet with versioning in M365, your organization cannot pick a specific point in time to get a snapshot of the last clean copy of all of your data before it was compromised. That's included in a modern backup solution. With BaaS, you can quickly and easily recover large volumes of data at scale after an attack or disruption, helping ensure you meet your RTOs and RPOs.

Clean recovery where you need it

To have confidence in a full restore, a machine-learning (ML) engine built into a modern BaaS solution can recommend the last known clean copy. That way, you can be assured when you perform a restore that the snapshot data is free from anomalies and ransomware. Ensure your solution also allows you to recover data directly to the original location or to a new location in the event of an M365 service outage or if your accounts have been compromised.

Microsoft 365 backup and ransomware protection checklist

Capabilities		Vendor 1	Vendor 2	Vendor 3
Meet SLAs and simplify hybrid cloud operations	Single Management Plane	□	□	□
	Unified Backup (M365 Plus Other Data Sources)	□	□	□
	Flexible Retention	□	□	□
	Pricing Flexibility	□	□	□
Secure backups	Immutable Snapshots	□	□	□
	Write Once, Read Many (WORM)	□	□	□
	Access Controls	□	□	□
	Separate Backup Data from Production	□	□	□
Adopt fast, flexible protection and recovery	Rapid Recovery at Scale	□	□	□
	Point-in-Time Recovery	□	□	□
	Clean Recovery Where You Need It	□	□	□

Cohesity boosts Microsoft 365 protection from ransomware and more

Cybercriminals continue to set their sights on data sources with the potential to yield large ransom payments. Cohesity empowers your organization to defend all of your data no matter where it resides.

Cohesity DataProtect delivered as a Service provides comprehensive backup as a service for M365 services including Exchange Online and other Office 365 productivity apps, OneDrive, SharePoint, and Teams as well as other cloud and on-premises data sources (such as VMs, files, and databases). With it, your organization has an immutable snapshot that is stored separately from Microsoft that protects your backup data from malicious tampering or deletion. It allows you to recover quickly in the event of a ransomware attack or outage, and provides you with flexible data retention so you can best meet your business and compliance requirements. Cohesity also seamlessly integrates with Microsoft 365 Backup Storage to further enhance the protection of data backed up by providing an additional layer of resilience against cyber threats.

Sign-up today for a 30-day free trial of DataProtect delivered as a Service and start backing up your Microsoft 365 data in minutes.

Learn more at **Cohesity.com**.

COHESITY

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and © is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.