ConversationalGeek

MICROSOFT 365 MULTI-TENANT BACKUP & RECOVERY

Why it's business-critical to look beyond Microsoft 365's built-in data protection capabilities

www.conversationalgeek.com

Sponsored by Quest

Common Misconceptions About Microsoft 365

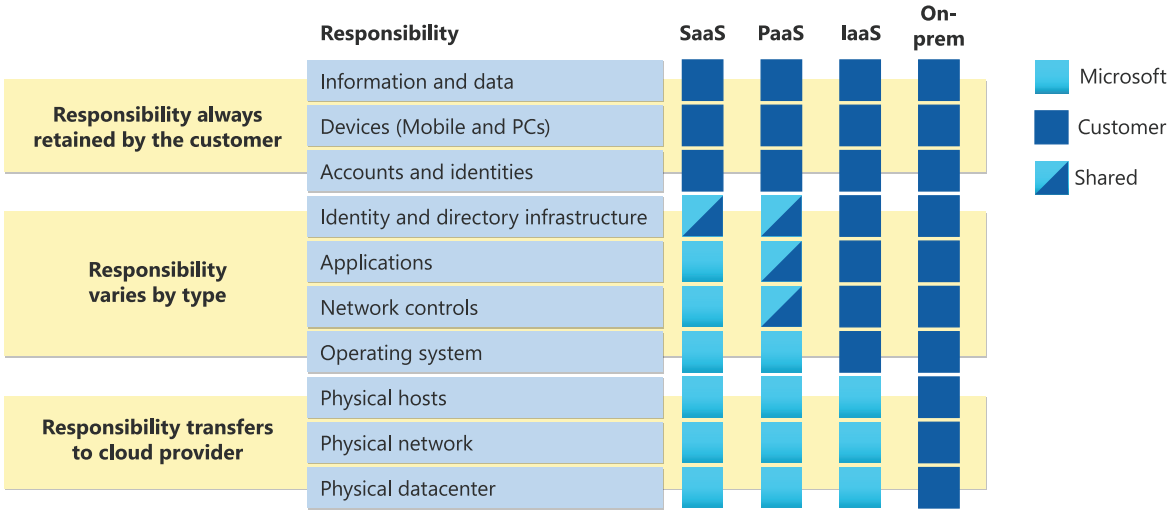
Microsoft 365 is the most popular suite of tools for productivity and collaboration in today's business world. However, relying solely on built-in data protection capabilities can leave your organization with some serious security gaps. Having a flexible and robust backup solution is no longer a "nice-to-have" line on the budget. It's mission-critical in today's ever-changing digital environment.

It's easy to assume that Microsoft 365 has your data covered, but the reality is a different story! Microsoft's built-in features are geared toward document retention, rather than long-term data protection. For instance, if files are accidentally deleted or overwritten, there's usually a short window of time for recovery, depending on your retention policies.

Another misconception is the belief that native tools provide comprehensive backup capabilities against threats such as ransomware or human error. While Microsoft offers some great versioning and retention tools, these are not a true backup!

This is what Microsoft refers to as the Shared Responsibility Model. While Microsoft ensures service uptime and infrastructure security, protecting your data is your responsibility, particularly when multi-tenancy makes this even more difficult – more on this later, so keep reading!

Microsoft 365 Shared Responsibility Model[1]



For all cloud deployment types, you are responsible for your data and identities. It's up to your team to protect the security of your data and identities, on-premises resources, and the cloud components you control.

Regardless of the type of deployment, you always retain the following responsibilities: *Data*, *Endpoints*, *Accounts*, and *Access Management*[2]

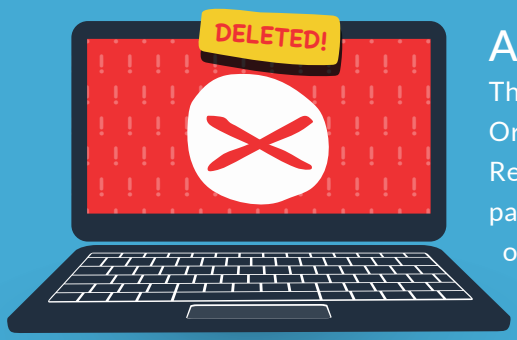
Since Microsoft does not back up your data, you must decide what and how to back it up. Because not having a backup is what is known in the industry as a "bad idea"!

[1]"Shared Responsibility Model

[2]"https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

THE DANGERS OF NOT HAVING A BACKUP

The risks of not having proper backups for Microsoft 365 data are the things that keep IT directors awake at night. What are some specific risks? Let's take a look:



Accidental (?) Data Loss Risk

Think about when an employee accidentally deletes a critical SharePoint file. Or wipes out the files on their OneDrive account before quitting in a fit of rage. Retention policies can act as a safety net, but they are not always perfect, particularly if some time passes before the problem is discovered. Recovery options provided by Microsoft are limited, leaving gaps that can allow critical data to slip through. Without backups, these files may be permanently lost.

Cybersecurity Threats

Ransomware everywhere

Ransomware attacks are becoming increasingly sophisticated and often target backup storage. Recent surveys conducted by the cybersecurity industry highlight the importance of protecting backups with immutability and encryption.

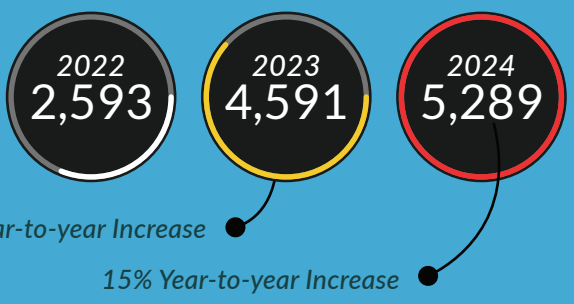
18.6% of respondents reported that their organization had been the victim of a ransomware attack in 2024.

14% of respondents whose organization suffered a ransomware attack reported that their backup storage was also compromised.

Ransomware predominantly attacks small organizations, with **55.8% of incidents** aimed at firms with 1-50 employees.

9.8% of respondents were unaware that Microsoft 365 data could be impacted by ransomware.

Total randomware attacks worldwide per year:



Education is good, but not good enough

Increasingly, companies are training their employees to prevent phishing attacks, with over **80% of organizations providing training to end-users** on how to recognize and avoid ransomware attacks. However, the effectiveness of training is often reduced because employees frequently do not have time to complete it. Over half of the companies surveyed expressed a need for more 'time-friendly' end-user training.[3]

And it's not just end-users that are affected by the lack of time and budget for cybersecurity training – **27.4% of respondents would invest in upskilling their IT department** if given an additional security budget.[3]

Although companies are investing more time and money in education and training, the **results remain less than 100% effective**. Malicious cyber actors are increasingly using zero-day vulnerabilities to launch attacks. By their nature, zero-day attacks are more challenging to prevent with traditional cybersecurity measures.

In 2023, cybercriminals took advantage of more zero-day vulnerabilities than in 2022, enabling them to target higher-priority networks. The majority of the most exploited vulnerabilities in 2023 were used as zero-days, marking an increase from 2022, when fewer than half of the top vulnerabilities were zero-day exploits.[4]

This is where prevention gives way to recovery in the form of solid, well-protected backups.

Compliance Risks

In addition to the risk from cybercriminals, many companies are required to adhere to strict regulations and face penalties if proper data retention measures aren't in place.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires healthcare organizations to implement a backup plan that ensures protected health information (PHI) isn't lost or destroyed in the event of a disaster. [5]

The Gramm-Leach-Bliley Act's safeguards rule requires that financial organizations provide a written information security plan that outlines the processes they've implemented to secure customer information. The Federal Trade Commission recommends maintaining secure backup records that are written out to an encrypted server. [6]

The Sarbanes-Oxley Act's Section 404 requires companies to provide an annual evaluation of their internal controls related to financial reporting. This encompasses controls designed to prevent and identify cyber threats that may impact financial reporting, as well as to apply controls to mitigate these risks. Additionally, these controls should undergo regular testing and evaluation, with any shortcomings reported to the company's audit committee and external auditor. [7]

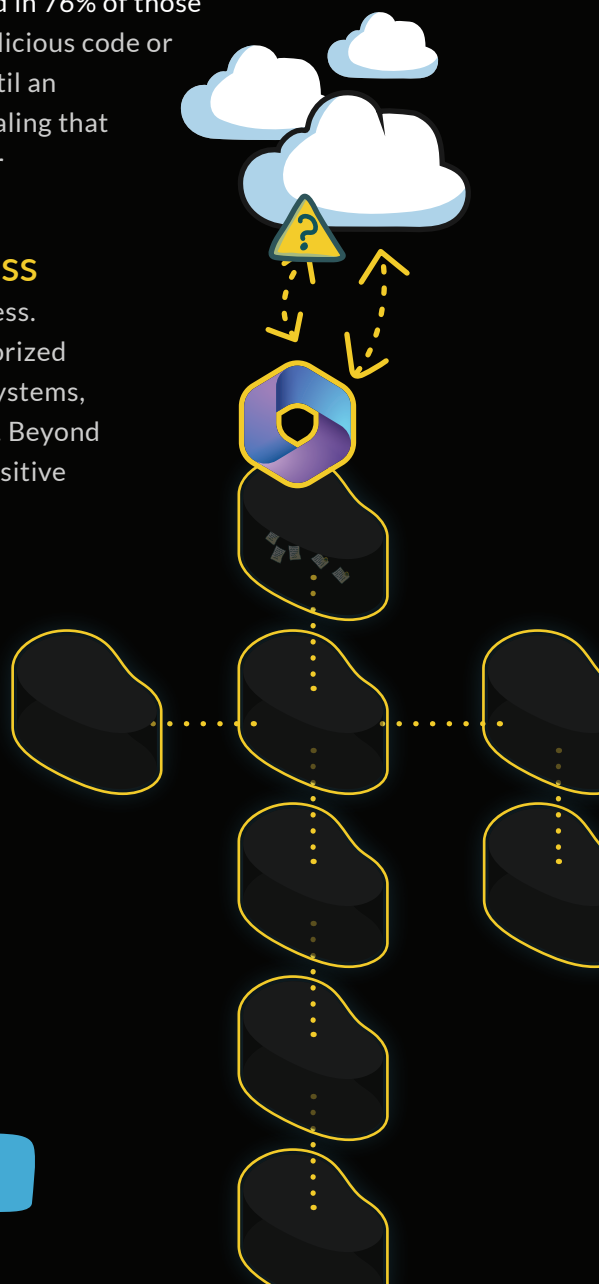
[3] Hornet Security Ransomware Attack Survey Q3 2024
[4] CSA-2023-TOP-ROUTINELY-EXPLOITED-VULNERABILITIES.PDF
[5] HIPAA's Administrative Safeguard 45 CFR § 164.308(a)(7)(ii)(A)
[6] GBLA's Safeguards Rule
[7] SOX Section 404: Management Assessment of Internal Controls

CHALLENGES IN BACKING UP MICROSOFT 365 DATA

Backing up Microsoft 365 data presents its own set of challenges, often stemming from the complexity of cloud environments and the need for customized solutions.

Securing Backups

As we've mentioned, just having a backup isn't enough. Cybercriminals employ various techniques to target and compromise secure data backup systems, which can be on network-attached storage (NAS), external drives, cloud backups, and even shadow copies. **Backup repositories are targeted in 96% of attacks**, with backup repositories **successfully affected in 76% of those cases.**[8] In some instances, attackers may damage backups by injecting malicious code or modifying the data structure. This corruption might remain unnoticed until an organization attempts to restore from these compromised backups, revealing that the data is unusable. Understanding these types of attacks is essential for organizations to strengthen their defenses.



Credential Compromise and Unauthorized Access

Data backup systems typically require administrative credentials for access. Cybercriminals can steal or brute-force these credentials to gain unauthorized access to backup servers or cloud repositories. Once they breach these systems, attackers have the capability to exfiltrate, delete, or encrypt backup data. Beyond simply encrypting or destroying backup files, attackers may also steal sensitive backup data for use in extortion. This stolen information can pressure organizations into paying ransoms, as attackers threaten to disclose confidential or proprietary information publicly.

Man-in-the-middle (MITM) attacks on backup transfers

During data transfers to and from cloud-based systems, attackers may intercept and tamper with backup data using man-in-the-middle techniques. This can lead to data corruption, exfiltration, or unauthorized modifications to backups.

In all these cases, by rendering backups useless, attackers ensure that victims have no choice but to pay the ransom. However, organizations can take proactive steps to understand these attack vectors and secure their backup systems against potential threats.

[8] Microsoft 365 Backup and Recovery Buyers Guide, Expert Insights

MULTI-TENANT ENVIRONMENTS INCREASE COMPLEXITY

Navigating the complexities of backup and restoration is a challenge in itself, but adding multi-tenant Microsoft 365 environments to the mix takes it to an entirely new level. While these environments offer scalability and centralized management, they also introduce unique obstacles, especially when it comes to cross-tenant backups and restorations.

Cross-Tenant Restoration: Why It Matters

Cross-tenant restoration is not just a technical exercise, but an absolute necessity for organizations that operate across multiple tenants. Why might a business need this functionality?

Mergers and Acquisitions

In the increasingly common case of two companies merging, each has its own Microsoft 365 environment. Consolidating these systems isn't just about efficiency. It's about ensuring employees have uninterrupted access to critical data. Cross-tenant restoration enables the seamless transfer of all content, including emails and Teams conversations.

Regulatory and Legal Requirements

Compliance can sometimes mandate moving or restoring data across tenants. For instance, specific regulations might require separating sensitive data into dedicated environments or restoring archived content for legal reviews.

Disaster Recovery

Imagine a catastrophic event compromises one tenant's environment. In this case, cross-tenant restoration serves as a safety net, enabling businesses to recover and transfer critical data to an unaffected tenant, thereby maintaining smooth operations.

The Challenges of Cross-Tenant Restoration

As valuable as cross-tenant restoration is, it's far from simple. The process involves several layers of complexity:

Security and Data Isolation

Moving data between tenants can introduce security risks, especially when handling sensitive information. Without proper protection, such as encryption during transfer and robust access controls, your data may be vulnerable to interception or unauthorized access.

Resource Dependencies

Multi-tenant setups often rely on shared resources, which can complicate restoration. For example, if you're restoring data tied to shared Teams channels or SharePoint sites, you'll need to account for overlapping dependencies to avoid creating inconsistencies.

Ensuring Data Consistency and Integrity

Cross-tenant restoration isn't just about moving data. It's about ensuring that the information remains intact, accessible, and functional in its new environment. Imagine restoring a SharePoint document library only to discover that its permissions and folder structures are corrupted. It's a logistical headache that can disrupt workflows.

For businesses operating in multi-tenant environments, investing in a robust, tailored backup solution isn't optional. It's essential for ensuring smooth operations, maintaining compliance, and preparing for the unexpected.

GRANULAR CONTROL OF BACKUP

Selective Data Backup

Selective backups are vital for businesses with specific data priorities. Think of critical documents or sensitive emails. They need to be safeguarded without wasting resources on redundant information. Granular control empowers organizations to focus backup efforts on essential data sets, streamlining storage usage and recovery processes.

Customizable Retention Policies

Compliance requirements can vary significantly across different industries. Some businesses are required to retain data for several years to comply with regulations such as Sarbanes-Oxley, while others may have shorter retention periods. Solutions offering customizable retention policies enable the alignment of data management strategies with these unique demands.

Storage Cost and Optimization

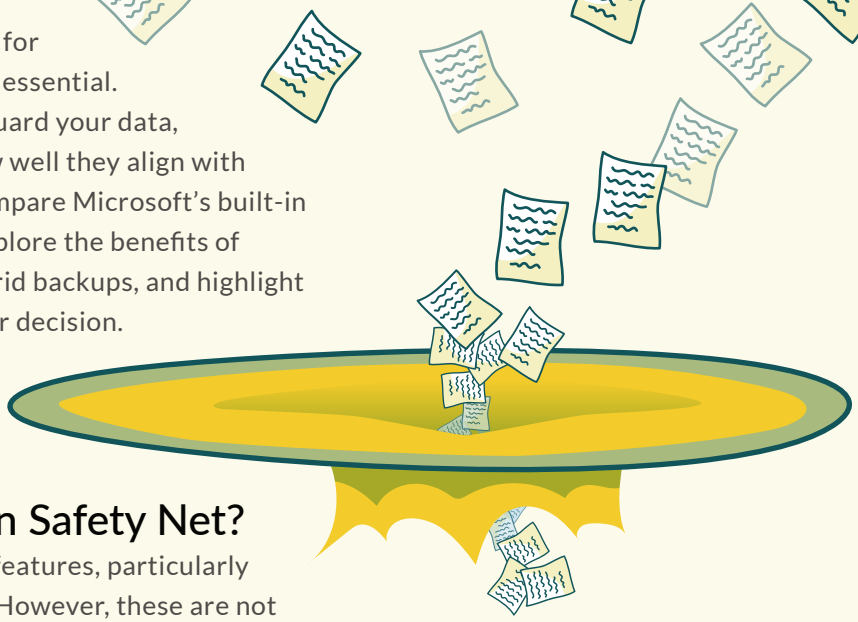
Many enterprises migrate to SaaS offerings, such as Microsoft 365, to reduce or eliminate the need for on-premises infrastructure. However, additional cloud storage for backup can be expensive for businesses with extensive data volumes. By identifying scalable options, implementing deduplication, and adopting predictive analytics, organizations can optimize expenses while ensuring sufficient capacity for their backup needs.

Continuous Data Protection

Continuous Data Protection (CDP) ensures that every change is backed up as it happens. This eliminates the limitations of traditional backup windows, allowing for the instant restoration of lost or overwritten data. By capturing every version of your data, CDP provides a comprehensive safety net against cyber threats or accidental errors. For example, ransomware attacks that encrypt files in real-time can be countered effectively with CDP, allowing organizations to recover clean copies of the affected data.

SELECTING THE BEST BACKUP SOLUTION

Choosing the right backup solution for your Microsoft 365 environment is essential. While all backup tools aim to safeguard your data, their effectiveness depends on how well they align with your organization's needs. Let's compare Microsoft's built-in tools with third-party solutions, explore the benefits of cloud-based, on-premises, and hybrid backups, and highlight critical considerations to guide your decision.



Microsoft Backup: A Built-in Safety Net?

Microsoft 365 does offer built-in backup features, particularly for SharePoint, OneDrive, and Exchange. However, these are not 100% included in your M365 licenses. You still need to create a storage account in Azure to store the backup data and incur the associated storage costs. While Microsoft Backup gives you the basics, it also comes with some notable limitations:

Short Retention Periods

The length of time retaining your backup depends on the service being backed up.

After that year? Sorry, there is no option for extended storage.

NAME	BACKUP FREQUENCY	SHORT-TERM RETENTION	LONG-TERM RETENTION
SharePoint	Every 10 minutes	10-minute snapshots are retained for 14 days	One snapshot per week for one year
Teams			
OneDrive			
Exchange		10-minute snapshots are retained for one year	

Limited Granularity & Scope

SharePoint and Teams data can only be restored as an entire site at a time, with no other way to restore a single file or set of files. Likewise, OneDrive is an all-or-nothing proposition. However, Exchange mail can be restored at the mail item level via a rather tedious search procedure. Looking to back up your Entra ID data? No option at this time.

So, while Microsoft 365 Backup is better than no backup at all, it often falls short of meeting the rigorous demands of modern businesses.

The Case for Third-Party Solutions

Third-party backup tools provide advanced features that complement and enhance Microsoft's built-in capabilities. These tools can allow for a granular, immutable, and customizable solution for your backup needs. For businesses that prioritize flexibility, long-term data protection, and peace of mind, third-party solutions are a must-have.

Any backup solution for your Microsoft 365 tenant should check the following boxes, or at least the majority of them:

Immutable storage

Also known as "Write Once-Read Many" in the old days of tape and optical storage. The bad guys can't hurt your data if they can't write or alter it.

Granularity

This is achieved through three key aspects: the selection of data to back up, the retention period, and the selection of data to restore. Ideally, you should have the ability to choose what is backed up, implement a tiered retention policy, and restore individual items.

Flexibility

Backups can and should last a very long time. However, the medium storing the data has evolved over the years, from punch cards to tapes to spinning disks to optical drives, to solid-state storage, and the cloud. Ensure your solution allows for flexibility to handle future changes.

Multi-Tenant capability

You need to be able to back up multiple tenants and perform cross-tenant restorations as well.

Multi-Cloud (where applicable)

If you are keeping your backups cloud-based, you should be able to back up your Microsoft 365 data to Azure and another cloud service, such as AWS or Google.

However, in the third-party market, it's not one size fits all. There are essentially three categories of backup that you should investigate to determine which one best suits your organization's needs. Let's look at the strengths and weaknesses of each one...

#1 Cloud-Based Backup Services

Cloud-based solutions are a favorite among modern businesses, and for many of the same reasons as using a SaaS product like Microsoft 365 in the first place.

These advantages make cloud backups a practical choice for organizations prioritizing flexibility and resilience.

Scalability

As your organization grows, so does your need for storage. Cloud solutions can quickly scale to match your data requirements, helping you avoid the costs of overprovisioning.

Accessibility

Whether you're working from the office, home, or halfway across the world, cloud backups ensure your data is always accessible.

Off-Site Protection

By storing data in secure, off-site locations, cloud backups safeguard against localized disasters, such as fires or hardware failures.

Key Features to Look For

However, not all cloud-based services are created equal! It's essential to evaluate your options carefully. Prioritize solutions that offer:

Strong Encryption

Look for services that encrypt data during transit and at rest to prevent breaches.

Compliance Certifications

Certifications like GDPR, HIPAA, or ISO 27001 ensure the solution meets industry standards.

Automation

Automated backup scheduling reduces administrative workloads and minimizes the risk of human error.

Cost-Efficiency

Flexible pricing models allow you to pay only for the storage you use, making cloud backups a budget-friendly option.

#2 On-Premises Backup Solutions

While cloud backups are gaining popularity, on-premises solutions remain a strong contender for organizations seeking complete control over their data. With on-premises backups, businesses can:

Maintain data sovereignty, ensuring sensitive information stays within the organization's infrastructure.

Customize their backup strategies based on specific operational needs.

Avoid potential connectivity issues that can occasionally hinder access to the cloud.

These benefits make on-premises solutions especially appealing to industries like government, finance, and healthcare, where data control is paramount.

Challenges of On-Premises Solutions

That said, on-premises backups come with their own set of challenges:

High Cost

Setting up and maintaining on-premises infrastructure can require significant investment in hardware and IT expertise.

Limited Scalability

Expanding storage capacity often means purchasing additional equipment, which can be costly and time-consuming.

Disaster Vulnerability

On-premises backups stored in a single location may be at risk during localized events, such as fires or floods.

Despite these challenges, on-premises solutions remain a viable option for organizations that prioritize security and control.

#3 Hybrid Backup Solutions

Why choose between cloud and on-premises when you can have both? Hybrid backup solutions offer the best of both worlds by combining the flexibility of cloud storage with the control of on-premises systems. Key advantages include:

Redundancy

By storing data in multiple locations, hybrid solutions provide an extra layer of protection against disasters.

Flexibility

Critical data can be stored on-premises for quick access, while less sensitive information is backed up to the cloud.

Scalability

Organizations can scale their cloud usage up or down without disrupting their on-premises infrastructure.

Hybrid solutions are ideal for businesses with diverse needs, offering the adaptability to meet ever-changing requirements.

Crafting a Hybrid Strategy

Implementing a hybrid strategy doesn't have to be complex. To get started:

Identify which data is most critical and should be stored on-premises.

Utilize cloud backups for large-scale or infrequently accessed data to reduce storage costs.

Ensure both systems are integrated seamlessly to streamline recovery processes and minimize downtime.

By leveraging the strengths of both approaches, hybrid solutions provide unmatched resilience and flexibility, making them an increasingly popular choice for forward-thinking organizations.

Selecting the best backup solution ultimately depends on your organization's specific needs, priorities, and available resources. Whether you opt for Microsoft's built-in tools, a cloud-based service, an on-premises system, or a hybrid solution, the key is to ensure your backup strategy provides the security, flexibility, and scalability your business needs to thrive.

Quest®

Quest® creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest solutions.

Quest NetVault® Plus for Microsoft 365 Backup:

- Complete Protection – Back up Exchange Online, SharePoint, OneDrive, Teams, and more in one unified solution.
- Fast, Granular Recovery – Restore everything from a single email to full mailboxes in seconds.
- Ransomware-Ready – Immutable, encrypted backups block unauthorized changes and ensure data integrity.
- Storage Flexibility – Store backups on-prem, in the cloud, or across hybrid environments.
- Multi-Tenant Support – Backup and restore multiple Microsoft 365 tenants from a single interface.

NetVault Plus simplifies Microsoft 365 backup, so your data stays safe, compliant, and recoverable.

For more information, visit:
https://www.quest.com/products/netvault-plus/Microsoft-365-data-backup-and-recovery.aspx