veeam

7 Critical Reasons for Microsoft 365 Backup

The case for why organizations need to protect Microsoft 365 data

Introduction

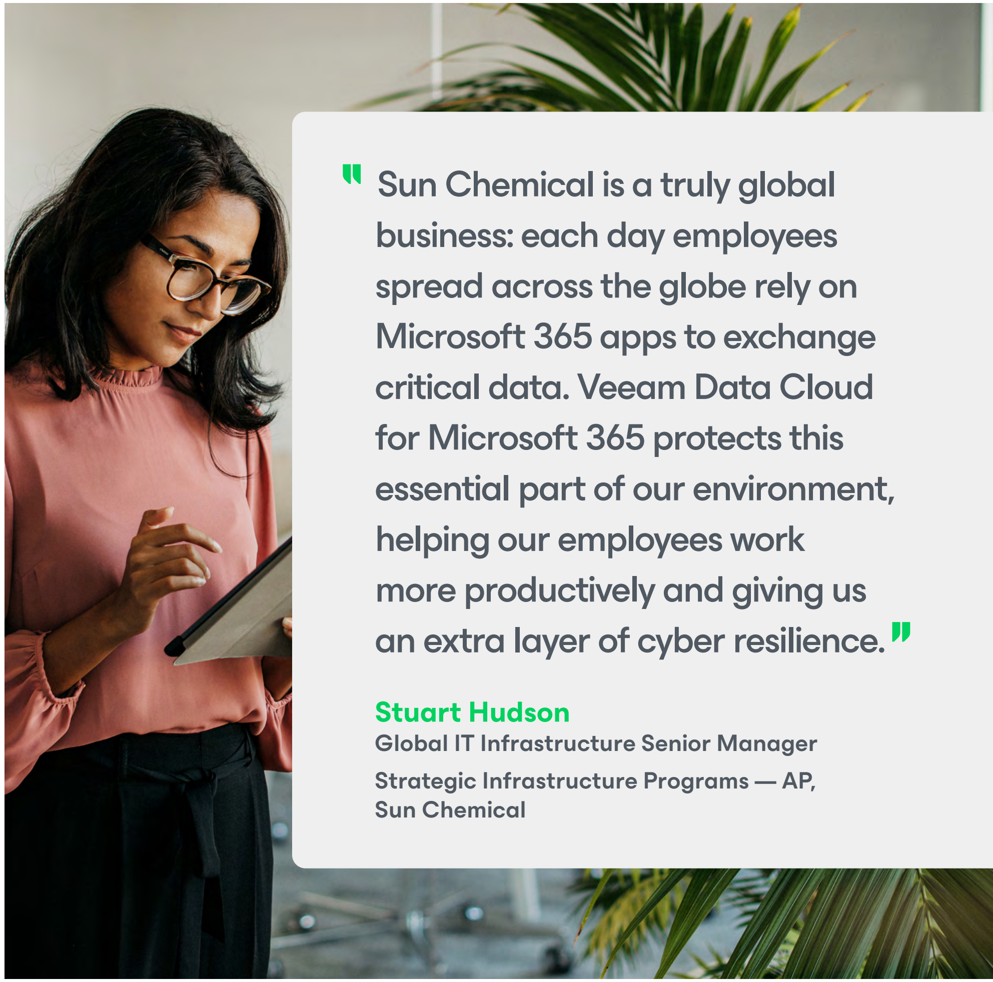
Do you have control of your Microsoft 365 data? The knee-jerk answer is typically, "Of course," or "Microsoft takes care of it." But look closer. Microsoft protects the availability of the service, not the recoverability of your data — and attackers are deliberately targeting that gap between uptime and clean rollback.

Microsoft maintains the infrastructure and keeps the lights on. But the Shared Responsibility Model makes one point unambiguous: the integrity, retention, and recovery of your data sits squarely with you. Comprehensive backup is not included in a standard license. Without a shift in mindset, that blind spot becomes visible only after data is lost.

The stakes have changed. Most serious incidents now involve identity compromise — threat actors targeting Entra ID to impersonate users, escalate privileges, and quietly modify, delete, or exfiltrate data across Exchange, SharePoint, OneDrive, and Teams. Because these actions appear to originate from valid credentials, Microsoft 365 treats them as normal activity, and native retention faithfully preserves the compromised state. Meanwhile, extortion economics are shifting: as payment rates decline, attackers lean harder on data theft and identity abuse to regain leverage. When that happens, you need clean, independent restore points — not just a service that stays online.

This creates two distinct recovery challenges. On one side are everyday "undo" moments: a deleted mailbox, an overwritten file, a misapplied permission. On the other are disaster-scale incidents: tenant-wide tampering, mass deletion, or identity-driven changes that ripple across workloads. A modern strategy must cover both.

This report explores what happens when that safety net is missing — where the real hazards lie, how purpose-built backup closes gaps in retention and resilience, and why independent recovery has become a core requirement for every organization that depends on Microsoft 365.



> "Sun Chemical is a truly global business: each day employees spread across the globe rely on Microsoft 365 apps to exchange critical data. Veeam Data Cloud for Microsoft 365 protects this essential part of our environment, helping our employees work more productively and giving us an extra layer of cyber resilience."
>
> **Stuart Hudson**
> Global IT Infrastructure Senior Manager
> Strategic Infrastructure Programs — AP,
> Sun Chemical

The Big Microsoft 365 Misconception

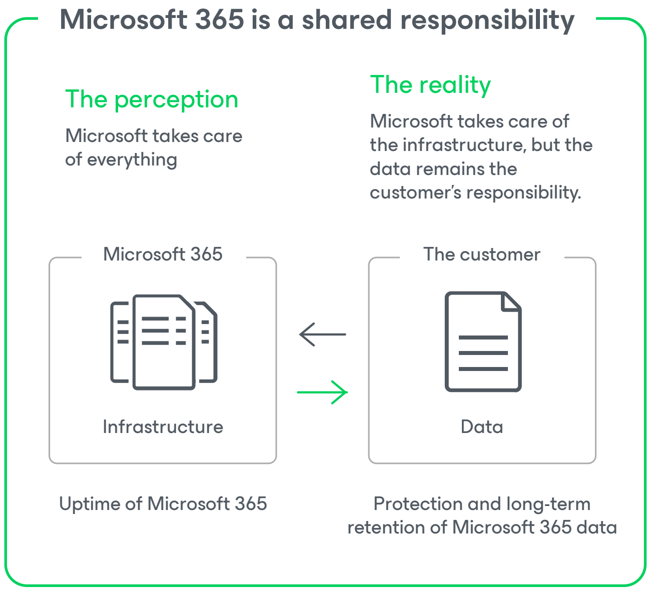
The disconnect between what organizations assume Microsoft protects and what the Shared Responsibility Model actually requires is one of the most persistent risks in Microsoft 365. The resiliency included in a standard license — and the protection users think they're getting — are often very different.

A major source of confusion is geo-redundancy. Many interpret it as backup. It isn't. Geo-redundancy safeguards Microsoft's infrastructure: if a datacenter fails, users stay online. But it does nothing to restore a clean version of your data. If a permission is misapplied, a Team is deleted, or an attacker modifies content under a valid identity, geo-redundancy simply replicates the compromised state across regions.

Native retention behaves the same way — preserving what exists now, including anything that shouldn't be there. None of these mechanisms maintain the history you need to unwind harmful changes, especially when those changes were made under trusted credentials. That gap grows more consequential as Entra ID becomes the control plane for Microsoft 365. User objects, groups, roles, app registrations, and Conditional Access policies all follow the same pattern: if tampered with, the platform preserves the altered state, not the authoritative one.

Backup serves an entirely different purpose. A true Microsoft 365 backup creates historical, point-in-time copies stored outside the tenant — copies that remain intact regardless of what happens inside Microsoft 365. These independent restore points make clean recovery possible: the ability to return to a pre-tampered state of your mail, files, Teams content, SharePoint structures, and identity-linked configurations.

Backups — not geo-redundancy, retention, or version history — are an organization's last line of defense. But that defense only works if the backups are independent, immutable, and recoverable at speed.



Microsoft 365 is a shared responsibility

The perception

Microsoft takes care of everything

The reality

Microsoft takes care of the infrastructure, but the data remains the customer's responsibility.

Uptime of Microsoft 365

Protection and long-term retention of Microsoft 365 data

> "For all cloud deployment types, you own your data and identities."

Source: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

7 Reasons Why a Microsoft 365 Backup Plan is Critical

Microsoft 365 delivers exceptional availability and productivity. It keeps applications online, ensures collaboration continues, and minimizes disruption when infrastructure fails. But availability is not recoverability — and without a dedicated backup strategy, that distinction becomes visible only after data has been altered or lost.

It's common to assume the recycle bin is good enough. It isn't. The average time from compromise to discovery can be around 140 days — far longer than most native retention windows. Identity-based attacks, silent exfiltration, misconfigurations, or unnoticed permission changes can reshape data months before anyone realizes something is wrong. By the time the issue is detected, Microsoft 365 has preserved the tampered state, not the clean version your business needs.

These risks play out across two realities:

- **Day-to-day operational recovery.** Accidental deletions, overwritten files, broken permissions — issues requiring fast, granular, "undo"-style restores.
- **Full-scale disaster recovery.** Identity compromise, tenant-wide corruption, poisoned automations, or destructive actions performed under legitimate credentials — events requiring clean, immutable restore points and the ability to rebuild with precision.

A modern backup strategy must handle both pillars automatically and consistently. And critically, it must operate independently of the tenant that may already be compromised. If backup access depends on Entra ID — the same identity layer attackers now target — recovery can fail precisely when you need it most. True resilience requires an external control plane, isolated credentials, and restore points that remain untouched even when the tenant is compromised.

From conversations with hundreds of IT professionals who have transitioned to Microsoft 365, seven vulnerabilities appear repeatedly — and each exposes why independent, point-in-time backup is no longer optional:

1. Identity-Driven Attacks and External Security Threats
2. Insider and Internal Threats
3. Accidental or Malicious Deletion
4. Retention Policy Gaps and Confusion
5. Teams Data Structure and Collaboration Complexity
6. Legal and Compliance Requirements
7. Hybrid Environments and Consistent Recovery

1. Identity-Driven Attacks and External Security Threats

Malware and ransomware still disrupt organizations worldwide, but the attack path has shifted. Threat actors now target identity, not infrastructure. Once an attacker compromises Entra ID and obtains valid credentials, they stop looking like an intruder and start behaving like a trusted user. Their actions blend into routine activity, yet impact can be strategically destructive.

This convergence of insider-like access, human error, and external intrusion is now the defining risk of Microsoft 365. A departing employee wiping files, a well-intentioned user mishandling sensitive content, or an attacker posing as either — all can trigger destructive changes that cascade instantly across SharePoint, OneDrive, Exchange, and Teams.

Attackers are adapting to economic pressure as well. With ransomware payment rates declining, threat groups increasingly turn to identity compromise and quiet exfiltration to restore leverage. Using valid OAuth tokens, delegated permissions, or abused app registrations, attackers can siphon sensitive data without triggering traditional detection. Often the theft occurs long before encryption or destruction begins.

Entra ID sits at the heart of this exposure. As the identity foundation for Microsoft 365, it governs users, groups, app permissions, roles, and the policies that tie collaboration data together. Compromising Entra ID — through credential theft, malicious OAuth consent, token misuse, or misconfiguration abuse — allows attackers to disable protections, escalate privileges, and corrupt large sections of the environment at once. What begins as an identity intrusion quickly becomes an operational failure.

When identity is the attack vector, clean, external restore points allow you to recover not only your data but the trust structure that makes your environment function. Identity compromise determines the blast radius; independent recovery determines whether it becomes a setback or a crisis.

What begins as an identity intrusion quickly becomes an operational failure.

2. Insider and Internal Threats

The idea of a security threat brings to mind hackers and viruses. But any activity performed under trusted access — whether by an employee, contractor, or attacker operating through a compromised identity — carries the potential to reshape data in ways difficult to detect and harder to unwind.

Internal changes also introduce integrity and compliance risk. A quietly altered record, a permissions change that hides critical content, or a modified workflow can undermine audits, eDiscovery, and regulatory obligations. By the time discrepancies surface, native retention has preserved the altered state — not the trustworthy version required for legal and forensic review.

Hybrid work and broad collaboration deepen this exposure. Users access data from varied devices, automated processes run continuously, and identity-driven policies govern much of the environment. Distinguishing normal behavior from harmful activity grows increasingly difficult. Without visibility into unusual permission changes, anomalous user actions, or unexpected data movement, internal risks remain invisible until they escalate.

When internal actions — accidental or malicious — become the source of disruption, resilience depends on detecting irregularities early and returning both data and configurations to a verifiable, known-good state.

When internal — whether accidental or malicious — become the source of disruption, resilience depends on your ability to detect irregularities early and return both data and configurations to a verifiable, known-good state.

3. Accidental or Malicious Deletion

Deletion events in Microsoft 365 propagate instantly. Removing a user also removes their mailbox, OneDrive content, and the linked objects that underpin collaboration. When these changes originate from trusted identities, Microsoft 365 treats them as legitimate updates and replicates them without hesitation.

Native protections offer narrow guardrails, but understanding deletion pathways matters:

- **Soft deletes** transition items into recoverable folders, but only briefly.
- **Hard deletes** purge content entirely, with no native recovery path.

Microsoft 365's built-in mechanisms were never designed to maintain an isolated, authoritative history. A modern backup solution fills this gap by capturing clean, point-in-time snapshots of mail, files, sites, Teams content, and identity-linked objects — stored independently from the tenant and insulated from policy drift and identity-driven actions. With this foundation, accidental or malicious deletions become recoverable events, not irreversible losses.

When these changes originate from trusted identities, Microsoft 365 treats them as legitimate updates, not anomalies, and replicates them without hesitation.

4. Retention Policy Gaps and Confusion

Retention in Microsoft 365 is often treated as a built-in safety net. In reality, it is a governance feature — designed to keep data for a defined period inside the live tenant, under the same identity and policy framework that manages day-to-day operations. It does not create an independent history, and it does not provide the clean rollback needed when something goes wrong at scale.

As collaboration expands and more policies, labels, and automated rules are introduced, the risk of drift grows. A mis-scoped retention rule, an aggressive deletion policy, or a permissions change applied to the wrong scope can alter or remove critical data across Exchange, SharePoint, OneDrive, and Teams long before anyone notices. The challenge sharpens with identity-aware components: retention does not rebuild group memberships, permissions, Teams structures, Conditional Access policies, or role assignments.

Retention can help in narrow cases — when a misstep is spotted quickly and affected items still fall within a short recovery window. But when identity abuse, policy drift, or automation failures reshape the environment over weeks or months, retention simply preserves the outcome. It cannot reconstruct an earlier, healthy state.

A modern backup approach maintains independent, point-in-time copies of both data and critical configurations outside the tenant — and outside the identity plane attackers target. This history underpins both pillars of Microsoft 365 resilience: fast day-to-day recovery when something small goes wrong, and authoritative disaster recovery when the environment itself has been reshaped.

Retention can help in narrow cases, but when identity abuse, policy drift, or automation failures reshape environments, retention simply preserves the outcome.

5. Complex Teams and Collaboration Data

Microsoft Teams is where work actually happens. Project timelines, approvals, side conversations, handoffs, and decisions all live in a web of channels, files, meetings, and shared workspaces. Under the surface, each Team is backed by a Microsoft 365 Group and tied into Exchange, SharePoint, OneDrive, and Entra ID — with membership, permissions, and app connections driven by those identity relationships.

That design is powerful, but fragile. Removing a Team or channel can also remove the SharePoint site and shared files behind it. A structural change in one place can ripple through tabs, plans, and connected apps elsewhere. When those changes are intentional, Teams feels effortless. When they're accidental, rushed, or carried out under compromised credentials, entire workspaces can vanish in seconds.

Rebuilding that fabric by hand is not realistic at scale. Teams data is far more complicated than chat messages and documents; those assets are organized into complex structures of who can see them, which channels map to which sites, and how that reflects the way your business operates. After a major incident, trying to recreate that context from fragments in native tools is slow, error-prone, and often incomplete — especially when weeks or months have passed.

A dedicated backup solution captures Teams as a whole system rather than scattered artifacts. By preserving point-in-time snapshots of content, memberships, and configuration outside the tenant, it provides quick, targeted restores when a channel or file goes missing — and the ability to reconstitute entire Teams from a clean, known-good version when something breaks at wider scale. The result is not just data back in place, but collaboration restored with its context intact.

When they're accidental, rushed, or carried out under compromised credentials, entire workspaces can vanish or become unusable in seconds.

6. Legal and Compliance Requirements

Legal action, audits, and regulatory inquiries often arrive without warning. When they do, organizations must produce exact versions of emails, files, chats, and records from months or years past. Microsoft 365 includes litigation hold and retention, but these are governance tools — not backup.

That distinction matters because many changes occur under legitimate permissions. A user — or an attacker operating as one — can quietly alter or remove data long before anyone applies a legal hold or realizes a record will be needed. By the time the issue surfaces, native controls may be protecting the compromised state, not the trustworthy version legal and compliance teams require.

Regulators increasingly treat recoverability and integrity as matters of governance, not just security. Emerging mandates — from privacy regimes to sector-specific rules and frameworks like NIS2, DORA, and modern SEC reporting expectations — assume organizations can reconstruct an accurate historical record, even when disruptions originate from within their own identity systems.

A dedicated backup solution closes this gap by maintaining independent, point-in-time copies of mail, files, Teams content, SharePoint data, and identity-linked objects outside the production tenant. These clean, immutable versions provide the defensible history needed for audits, investigations, discovery requests, and regulatory inquiries — even if the live environment has been altered or partially wiped.

And because keeping pace with evolving requirements is its own challenge, a backup service with built-in reporting, monitoring, and retention controls helps translate policy into practice. Instead of stitching together ad hoc exports and holds, organizations gain a structured, auditable approach to preserving evidence — ensuring critical data is not only recoverable, but ready to stand up to scrutiny.

Native controls may be protecting the compromised state, not the trustworthy version legal and compliance teams require.

7. Hybrid Environments and Migration to Microsoft 365

Hybrid Microsoft 365 environments occupy an unusual space: flexible and continuous, yet supported by two fundamentally different systems — on-premises Exchange and Exchange Online — each with its own rules for retention, access, and recovery. For many organizations, this configuration isn't a brief transition but their operational reality for years.

That duality introduces risk the moment something needs to be recovered. On-premises and cloud mailboxes follow separate retention boundaries, permissions behave differently, and directory changes don't always propagate predictably. A mailbox deleted in the cloud may have dependencies that still live on-prem, and vice versa.

When users, groups, and authentication states sync between Active Directory and Entra ID, a single compromised credential or misapplied administrative action can modify mail, contacts, permissions, or shared data on both sides of the hybrid boundary. This is where hybrid recovery diverges into two needs:

- **Operational fixes:** restoring a mailbox, folder, or item quickly, regardless of whether it originated on-prem or in Microsoft 365.
- **Full-environment reconstruction**: reestablishing a known-good state across both systems after destructive changes have propagated through sync.

The right backup service closes these gaps by protecting on-prem and cloud mailboxes through a single, consistent platform — with the same speed and clean recovery capabilities across the entire hybrid footprint. It maintains independent recovery points regardless of where data originated, enabling fast bulk restoration or targeted granular recovery as needed. The backup layer normalizes recovery: cloud workloads benefit from high-throughput, backup-optimized APIs, while on-prem workloads follow a consistent restore workflow — giving hybrid organizations one recovery model instead of two.

A single compromised credential or misapplied administrative action can modify mail, contacts, permissions, or shared data on both sides of the hybrid boundary.

Conclusion

Evaluate your resilience posture. There are likely gaps you didn't realize existed. Protecting Microsoft 365 now requires more than governance policies or confidence in uptime. Most serious incidents begin with identity compromise, and once an attacker operates under a trusted account, they own your data. You made a smart decision deploying Microsoft 365. Now pair it with a backup service that provides an independent, trustworthy record of your environment — one that remains intact even when the tenant does not.

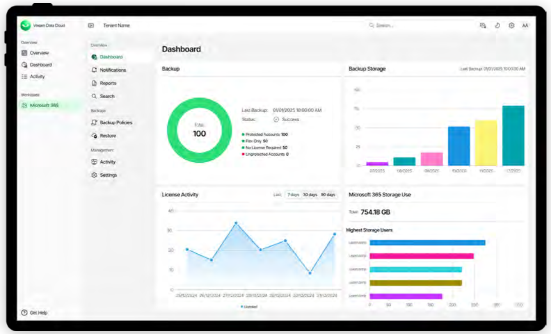
Veeam Data Cloud *for Microsoft 365* unifies these capabilities in a fully managed, cloud-native service built in partnership with Microsoft. Powered by backup-optimized APIs, it provides AI-enhanced visibility, Zero-Trust-aligned protection, immutable restore points, and high-speed recovery across every workload — Exchange, SharePoint, OneDrive, Teams, and identity-linked objects in Entra ID. With unlimited storage and continuous hardening, organizations gain a recovery platform that moves as fast as the environments it protects.

The result is modern data resilience for collaboration and identity: clean recovery, independent control, and confidence that your Microsoft 365 data is always recoverable, always trustworthy, and always under your control.

If you found this report helpful, we encourage you to email it to a colleague: Forward this report.

Veeam Data Cloud *for Microsoft 365*:

Resilient data protection made simple



- Operational and disaster recovery in one solution
- Bounce back from any cyberattack or data loss scenario
- Unified SaaS Platform with unlimited storage included

→ Request Demo

→ Contact us

→ **Interested in Entra ID protection? Read the 6 Reason for Microsoft Entra ID Backup White Paper**