

EXECUTIVE PAPER · DISASTER RECOVERY

Your SaaS Vendor Does Not Back Up Your Data

Microsoft, Google and Salesforce keep their platforms running. Their own terms leave deleted, corrupted and ransomed customer data with the customer, and most companies have never tested whether they could get it back.

AUTHOR

Chris Watkins

SERVICE

Disaster Recovery

FOR

CEO, CFO, CTO · 12 min read

AT A GLANCE

The problem. Email, files, customer records and increasingly the general ledger now live in software-as-a-service platforms. The providers replicate that data to survive their own hardware failures. Their terms and documentation say the customer is responsible for protecting it against deletion, corruption and attack, and their recycle bins empty within weeks.

Why it persists. Executives hear "the cloud" and assume the provider keeps a copy they can ask for. Replication copies a mass deletion as faithfully as it copies a new invoice. In a 2025 survey, two thirds of IT decision makers believed their SaaS vendors were solely responsible for protecting their data.

The recommendation. List the SaaS platforms that hold records you cannot rebuild. Back each one up to a copy held outside the provider's tenant, under credentials your everyday administrators do not hold. Restore from that copy every quarter, time it, and report the result to leadership with the same weight as any other recovery test.

The Decision in Front of You

Most companies moved their critical records into SaaS over the last decade: Microsoft 365 or Google Workspace for mail and documents, Salesforce or a similar platform for customers, a cloud ERP for orders and finance. The decision is whether to pay for an independent copy of that data and the discipline to restore it, or to rely on whatever the provider keeps.

The providers have answered half of that question in writing. The Microsoft Services Agreement recommends that customers regularly back up the content they store on Microsoft's services, and warns that customers may be unable to retrieve their data during an outage [1]. Microsoft's shared responsibility model assigns customer data, configuration and identities to the customer in every deployment type, SaaS included [2]. Salesforce's own training tells customers they are responsible for protecting the data they put into Salesforce, including against accidental or malicious user actions [3].

The stakes are the records the business runs on. A deleted sales pipeline, a corrupted price book or an encrypted document library is a revenue, legal and regulatory problem the day it happens. The provider's uptime commitment covers none of it.

What's Happening

Native recovery is a short retention window

Every major platform keeps deleted items for a while. SharePoint in Microsoft 365 retains them for 93 days from deletion, and Microsoft keeps backups for 14 more days that an administrator can ask support to restore from [4]. Items can leave the recycle bin earlier if it exceeds its quota or an administrator purges it [4]. Google Workspace lets an administrator restore a user's Drive or Gmail data for up to 25 days after it leaves the user's trash, and a deleted user account for 20 days; after that, Google says, the data cannot be restored even through technical support [5]. Salesforce's recycle bin holds deleted records for a limited time and does nothing for records that were changed or corrupted [3].

These windows handle the employee who deletes the wrong folder. They do not handle corruption discovered after the window closes, a sync tool that overwrote thousands of records last quarter, or an attacker who empties the recycle bin on the way out.

Exhibit 1. Provider recovery windows close in weeks, and what they leave out is the customer's problem

Platform	What the provider keeps for you	What it does not cover
Microsoft 365 (SharePoint, OneDrive)	Deleted items for 93 days, then 14 days of backups restorable through support [4]	Purged recycle bins, corruption found later, full tenant rebuild [4][14]
Google Workspace	Drive and Gmail data for 25 days after trash, deleted users for 20 days [5]	Anything older; Google support cannot restore it [5]
Salesforce	Recycle bin for a limited time [3]	Changed or corrupted records [3]
Any SaaS, any provider	Physical infrastructure and platform operation [2]	Customer data protection, which the customer owns [1][2][3]

Source: provider documentation as cited. Retention periods change; confirm current terms for your contracts.

The providers sell backup as a separate product

Salesforce once offered a last-resort Data Recovery Service. In 2020 it cost a flat $10,000, took six to eight weeks, did not guarantee full recovery, and was retired on July 31, 2020 because, Salesforce said, it did not meet its quality standards [6]. Salesforce now offers its own Backup and Recover product [3]. Microsoft sells Microsoft 365 Backup as a pay-as-you-go service at a list price of $0.15 per GiB of protected content per month, covering SharePoint sites, OneDrive accounts and Exchange mailboxes [7].

Attackers now go after the data and the copies together

Salesforce data theft, 2024 to 2025. The FBI reported in September 2025 that a group it tracks as UNC6040 had, since October 2024, phoned companies' call centers posing as IT support and talked staff into authorizing a modified version of Salesforce's Data Loader tool [8]. The attackers then used API queries to pull large volumes of customer data for extortion [8]. A second group, UNC6395, used stolen OAuth tokens from the Salesloft Drift integration in August 2025 until the tokens were revoked on August 20 [8]. These were thefts, and a backup does nothing to un-steal data. The lesson for this paper is the access involved: an integration trusted to read and write in bulk can delete in bulk.

Storm-0501, 2025. Microsoft Threat Intelligence described in August 2025 a ransomware group that operated entirely inside a victim's Azure environment [9]. After gaining the Owner role, the group exfiltrated data, then deleted snapshots, virtual machine restore points, storage accounts and Recovery Services vault protection containers [9]. Where resource locks and immutability policies blocked deletion, it removed the locks and policies [9]. The environment was Azure, and the pattern carries over to any platform: backups that live under the same administrative identity as the data are deleted with the data.

Microsoft nonprofit subscriptions, 2025 to 2026. Microsoft ended its Business Premium grant for nonprofits after July 1, 2025 and advised affected customers to move plans and export what they wanted to keep [10]. In September 2026 The Register reported that, because of an error, Microsoft had deleted remaining data from expired subscriptions before the retention period ended [10]. Microsoft told one customer the data could not be recovered and that it could not provide a list of what had been deleted, or whether anything had been [10]. The number of organizations affected was not disclosed [10]. Here no attacker and no employee was involved. The provider made the mistake, and the customer had no record of what was lost.

When Google Cloud accidentally deleted the private cloud subscription of the Australian pension fund UniSuper in May 2024, the fund's 647,000 members got their service back largely because UniSuper kept backups with another provider [11]. Another paper in this series covers that case.

Most companies have not closed the gap

HYCU, a vendor of SaaS backup, surveyed 500 IT decision makers in 2025. Treat its figures as the sponsor's: 66% believed their SaaS vendors were solely responsible for protecting their data, 43% said nobody owned SaaS data resilience, 87% admitted at least one SaaS application at risk from inadequate protection, and 75% did not test resilience regularly [12]. Respondents used an average of 139 SaaS applications, and only 56% of them were under IT's control [12].

The standards are plain. NIST's Cybersecurity Framework 2.0 includes subcategory PR.DS-11: backups of data are created, protected, maintained and tested [13]. The CISA #StopRansomware Guide says to keep offline, encrypted backups of critical data, test them regularly, and consider a second cloud for cloud-to-cloud backups so one vendor's compromise cannot reach every copy [15]. Neither document exempts data because a SaaS provider hosts it.

Why the Usual Approach Fails

Uptime gets mistaken for durability. A provider can meet its availability commitment while a customer's data is deleted, because the platform served every request correctly, including the destructive one.

Replication gets mistaken for backup. Providers copy data across disks, zones and regions so their own failures do not lose it. A deletion or a corrupting sync job replicates in seconds. UniSuper's environment was duplicated across two geographies, and the deletion took out both [11].

The backup sits inside the blast radius. Retention policies, litigation holds and the provider's own backup add-ons usually sit in the same tenant and answer to the same global administrator. An attacker who holds that role, as Storm-0501 did in Azure, can remove the protections before removing the data [9].

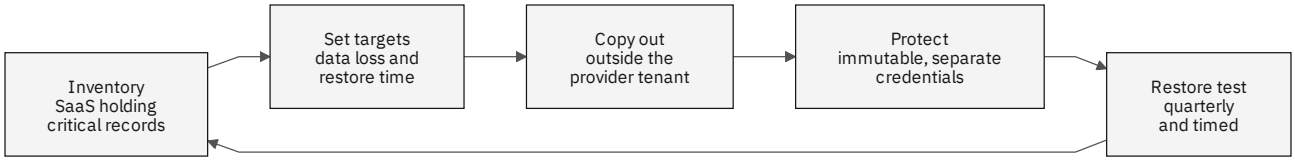
Restore is never tested at scale. Restoring one file proves little. Tony Redmond, a long-time Microsoft 365 commentator, wrote in September 2026 that no product can yet restore a complete Microsoft 365 tenant after a destructive attack [14]. Recovery means rebuilding identities in Entra ID first, then groups, then the sites and mailboxes that depend on them, one workload at a time, over weeks [14]. Teams, Planner and much of the tenant's configuration still lack full backup or export interfaces [14]. A company that has not rehearsed that order will learn it during the outage.

The long tail is ignored. Microsoft 365 gets a backup because it is visible. The CRM, the HR system, the e-signature archive and the ERP often do not, and a large share of SaaS applications are bought outside IT [12].

The Framework: Own the Copy, Prove the Restore

The goal is simple to state. For every SaaS platform that holds records you cannot rebuild, you hold a recent copy the provider and your own administrators cannot delete, and you have proved within the last quarter that you can restore from it in a known time.

Exhibit 2. Own the copy, prove the restore: five steps per platform



Source: author's framework, built on NIST CSF 2.0 PR.DS-11 [13] and the CISA #StopRansomware Guide [15].

Inventory. List every SaaS platform that holds records the business cannot recreate from another system: mail and documents, customer and pipeline data, contracts and signatures, HR, finance and ERP, code repositories. Include configuration as well as data. A Salesforce org without its custom

objects and automation, or a Microsoft 365 tenant without its identities and access policies, will not run even after the records come back.

Set targets. For each platform, the business owner agrees how much data the company can afford to lose and how fast it must be usable again. Those are business decisions, covered in another paper in this series, and they set backup frequency and spend.

Copy out. Back up to storage outside the provider's tenant. That can be a third-party backup service, a second cloud, or your own storage. The copy must not depend on the provider's account remaining open, since account closure and provider error are both causes of loss [1][10].

Protect. Make the copy immutable for a defined period and hold it under credentials that no everyday administrator, integration or AI agent can use. Require a second person to approve any change to retention. Storm-0501 removed immutability policies because the same identity controlled them [9].

Restore test. Every quarter, restore a real sample from each critical platform into a test environment, and once a year rehearse the loss of a whole platform, starting with identities. Record the time taken and what failed. The first rehearsal usually finds something missing, such as permissions, metadata or attachments.

What it costs

Backup is cheap relative to the records it protects. As an illustration, a company with 2,000 employees protecting 20 TiB of Microsoft 365 content at Microsoft's list price would pay about $3,072 a month, or $36,864 a year, roughly $18 per employee [7]. That figure is the author's illustrative estimate. It assumes 20,480 GiB of protected content, no growth, and list price, and it covers one platform. Third-party tools that also cover Salesforce, Google Workspace and ERP data are priced differently, and the larger cost is staff time for the quarterly restore tests.

Costs, Risks, and Tradeoffs

Exhibit 3. Tradeoffs of independent SaaS backup

Area	Cost or risk	Mitigation
Subscription spend	Per-user or per-GiB fees across several platforms	Protect platforms holding unrebuildable records first; set retention by need
A new attack surface	The backup tool holds broad read access to every platform it protects	Scope its credentials, monitor them, and keep them out of everyday administration
Data residency and privacy	A second copy of personal data in a second location	Choose the region deliberately; apply the same deletion and access rules as production
Gaps in coverage	Some platforms expose no full backup interface, notably parts of Microsoft 365 [14]	Document the gap, export what can be exported, and write a manual rebuild procedure
Restore testing time	Quarterly tests take engineering hours	Automate sample restores; rehearse a full platform once a year
When this is wrong	A small company with little in SaaS that cannot be rebuilt from email, invoices and partners' records	Rely on native retention, set a calendar reminder for exports, and revisit as the business grows

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	Inventory SaaS platforms holding critical records, including those bought outside IT. Name a business owner for each. Record current protection: native only, vendor add-on, or independent copy.	CIO with business unit leaders	Inventory signed off; every critical platform has an owner and a protection status
First 30 days	Find every identity and integration that can bulk delete or bulk export in each critical platform.	Security lead	List complete; unused integrations revoked
First 90 days	Agree data loss and restore targets per platform. Put independent backup in place for the top three, with immutability and separate credentials.	CIO with infrastructure lead	Top three platforms backed up outside their tenants; no everyday administrator can delete the copies
First 90 days	Run the first restore test for each of the top three.	Infrastructure lead	Restore time recorded against target for each platform
First 365 days	Extend coverage to every critical platform, including configuration and identities. Rehearse the total loss of one platform end to end. Map evidence to NIST CSF PR.DS-11.	CIO with risk or compliance	All critical platforms covered; one full-platform rehearsal completed; quarterly restore results reported to leadership

Source: author's recommendation.

Questions to Ask Your Team

1. Which SaaS platforms hold records we could not rebuild from any other system?
2. For each, where is our most recent copy, and who can delete it?
3. If our global administrator account were taken over tonight, which backups could the attacker reach?
4. When did we last restore more than a single file from Microsoft 365, Google Workspace or Salesforce, and how long did it take?
5. How would we know if a sync tool or integration had been corrupting customer records for three months?
6. Which integrations and AI agents can delete or export data in bulk, and who approved them?
7. If a provider told us our data was gone, could we say what had been lost?

Closing

The SaaS providers have been clear in their terms: they run the platform, and the customer protects the data. Their recycle bins are a convenience measured in weeks. Provider errors and stolen administrator accounts both reach past them. Keep an independent, immutable copy of every SaaS platform that holds records you cannot rebuild, hold it under separate credentials, and prove each quarter that you can restore it.

Sources

[1] Microsoft. "Microsoft Services Agreement." Sections 4 and 6. Published July 30, 2026, effective September 30, 2026. https://www.microsoft.com/en-us/servicesagreement.

[2] Microsoft. "Shared responsibility in the cloud." Microsoft Learn. 2026. https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility.

[3] Salesforce. "Get Started with Backup and Recover." Trailhead module, Backup and Recover Basics. https://trailhead.salesforce.com/content/learn/modules/backup-recover-basics/get-started-with-backup-recover.

[4] Microsoft. "Restore deleted items from the site collection recycle bin." Microsoft Support. https://support.microsoft.com/office/restore-deleted-items-from-the-site-collection-recycle-bin-5fa924ee-16d7-487b-9a0a-021b9062d14b.

[5] Google. "Data recovery." Google Workspace Security Whitepaper. https://workspace.google.com/learn-more/security/security-whitepaper/data-recovery.

[6] TechTarget. "End of Salesforce Recovery highlights need for SaaS backup." June 30, 2020. https://www.techtarget.com/searchdatabackup/news/252485430/End-of-Salesforce-Recovery-highlights-need-for-SaaS-backup.

[7] Microsoft. "Pricing model for Microsoft 365 Backup." Microsoft Learn. 2026. https://learn.microsoft.com/en-us/microsoft-365/backup/backup-pricing.

[8] Federal Bureau of Investigation. "Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion." FLASH-20250912-001, coordinated with CISA. September 12, 2025. https://www.ic3.gov/CSA/2025/250912.pdf.

[9] Microsoft Threat Intelligence. "Storm-0501's evolving techniques lead to cloud-based ransomware." Microsoft Security Blog. August 27, 2025. https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/.

[10] Page, C. "Microsoft tells nonprofits their deleted M365 data isn't coming back." The Register. September 28, 2026. https://www.theregister.com/saas/2026/09/28/microsoft-tells-nonprofits-their-deleted-m365-data-isnt-coming-back/5299433.

[11] UniSuper and Google Cloud. "A joint statement from UniSuper and Google Cloud." May 2024. https://www.unisuper.com.au/about-us/media-centre/2024/a-joint-statement-from-unisuper-and-google-cloud.

[12] HYCU. "HYCU State of SaaS Resilience Report 2025 Reveals the Hidden Cost of SaaS Growth." Press release; survey of 500 IT decision makers, sponsored by a SaaS backup vendor. September 30, 2025. https://www.hycu.com/company/newsroom/press-release/hycur-state-saas-resilience-report-2025-reveals-hidden-cost-saas.

[13] National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." NIST CSWP 29, subcategory PR.DS-11. 2024. https://doi.org/10.6028/NIST.CSWP.29.

[14] Redmond, T. "Restore a Microsoft 365 Tenant After a Catastrophic Attack." Office 365 for IT Pros. September 22, 2026. https://office365itpros.com/2026/09/22/backup-restore-catastrophic-attack/.

[15] Cybersecurity and Infrastructure Security Agency and MS-ISAC. "#StopRansomware Guide." https://www.cisa.gov/stopransomware/ransomware-guide.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.