SPANNING
A Kaseya COMPANY

The 7 Deadly Sins of SaaS Backup

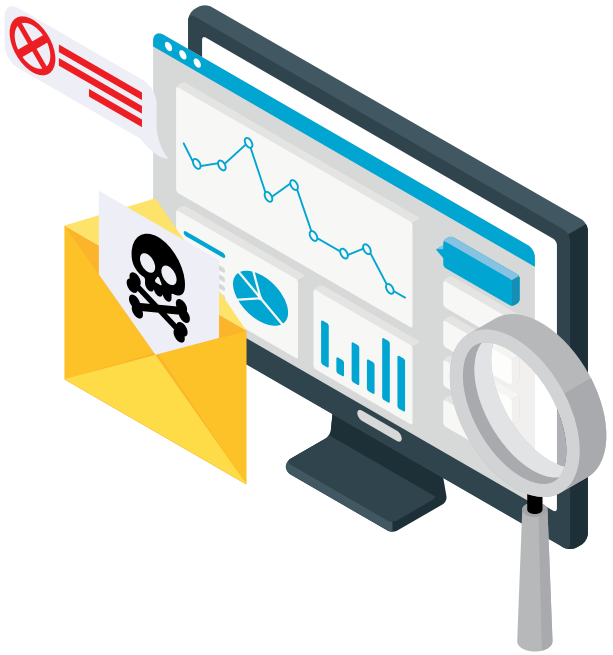
Introduction

Cloud-based Software-as-a-Service (SaaS) applications, such as Google Workspace, Microsoft 365 and Salesforce, have revolutionized how teams collaborate, store data and conduct daily operations. Due to their flexibility, cost-effectiveness, scalability, and integration and automation capabilities, SaaS solutions have become an increasingly popular strategic option for businesses of all sizes.

As reliance on SaaS solutions continues to grow, the amount of critical data stored on these platforms also increases. This invaluable SaaS data is the lifeblood of modern organizations — ranging from customer information, contracts and financial records to sensitive internal communications and intellectual property. As businesses store more data in cloud-based systems, the need for robust data protection becomes more critical than ever.

Without a strong defense strategy, SaaS data can be lost or compromised due to accidental deletions, malicious attacks, misconfigurations or gaps in data retention policies.

In this eBook, we'll explore the seven deadly sins that businesses make when it comes to SaaS backup — oversights that can lead to devastating data loss disasters. From relying solely on built-in SaaS protections to neglecting compliance obligations, we'll walk you through these critical errors so you can ensure your business's mission-critical data remains secure, recoverable and compliant with industry standards.



The 7 deadly sins of SaaS backup

SaaS applications have indeed revolutionized how businesses operate, but they also present unique challenges for data protection. Let's take a closer look at the seven deadly mistakes businesses make when protecting their SaaS data.

1 Relying on built-in SaaS protection? Think again

Sin: Relying solely on the native protection and retention features offered by SaaS providers.

A dangerous misconception among businesses using cloud solutions is that the native protection provided by SaaS vendors is sufficient to safeguard their data. SaaS providers like Google, Microsoft and Salesforce ensure the availability and security of their infrastructure. However, that does not extend to the data itself. While some built-in features, such as recycle bins and retention policies, provide a basic level of data protection, these are often limited in scope and duration.

For instance, a deleted email or document in Google Workspace may remain recoverable for a limited period (up to 30 days), after which it is purged permanently. In SharePoint, deleted data is retained for 93 days. Once this window closes, recovering the data becomes challenging without a dedicated backup solution.

In 2025, organizations took an average of 241 days to detect and contain data breaches — it's all too likely that retention in native tools expired well before the discovery of altered, damaged or deleted data.

Remediation:

Understanding the shared responsibility model is critical for businesses using SaaS applications. According to this model, SaaS providers are responsible for application uptime and infrastructure resilience. Data protection, however, is the customers' responsibility. Your company must take proactive steps to implement a dedicated third-party backup solution that provides comprehensive coverage, including long-term retention, versioning and point-in-time restores.

Spanning Backup simplifies your part of the shared responsibility model. Our industry-leading SaaS backup solution for Google Workspace, Microsoft 365 and Salesforce proactively defends your critical SaaS data with automated backup and unlimited data retention, eliminating the risk of data loss and downtime. Spanning provides advanced recovery capabilities, enabling you to find and restore data when needed seamlessly.

2 Overlooking data after account deactivation — A dangerous gamble

Sin: Deactivating user accounts without backing up or transferring their data. This can lead to permanent data loss when those accounts are purged.

It's common practice for organizations to deactivate SaaS accounts belonging to ex-employees. However, many companies fail to consider what happens to the valuable data associated with these accounts. Whether it's emails, files or CRM records, the data stored in these accounts is often critical to ongoing business operations and historical records. Unfortunately, once an account is deactivated or deleted, the associated data can be lost forever if no backup was taken. In some cases, organizations will opt to keep the user's license active to retain their data, which creates security risks around unmanaged accounts and is not a cost-effective solution.

Remediation:

Your organization must set up automated processes to back up or transfer critical data before deactivating accounts. You must also ensure that important user data is retained as per your organization's data retention policy. Leverage a third-party backup solution with the ability to retain the data of deactivated users. By archiving and backing up this data, your business can preserve essential information while ensuring compliance with data retention regulations.

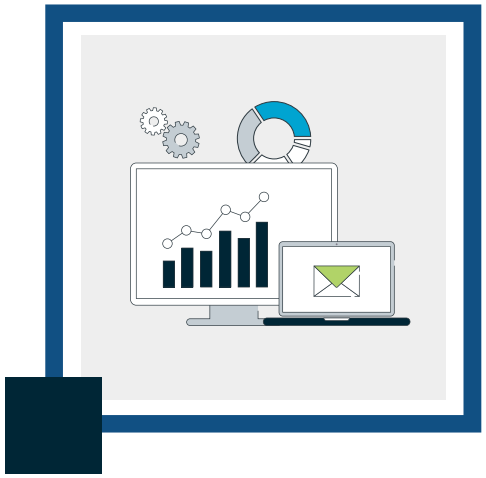
Spanning Backup for Microsoft 365 and Google Workspace allows you to protect and preserve deleted user data on more flexible terms. When a user actively protected by a Spanning Backup Standard license is deleted from your Microsoft 365 tenant or Google Workspace domain, and there is an available Archived license in your tenant, Spanning assigns the user an Archived license automatically. However, if no Archived license is currently available, the deleted user will continue to be protected on Standard license terms. Priced lower than Standard licenses, Archived licenses help you optimize costs while retaining your critical data long-term.

3 End-user data isn't enough — Cover all your bases

Sin: Backing up only user-generated content and neglecting system-level data.

Another common mistake businesses make is focusing solely on backing up end-user data, like emails, documents and chats, while neglecting other critical data sources within the SaaS ecosystem. SaaS applications store far more than just end-user files. Configuration settings, system metadata, permissions and security settings are often equally important yet frequently overlooked.

For instance, in a Salesforce environment, backing up only customer records without preserving configuration settings, workflow rules and automation scripts can lead to a disaster during recovery. Losing these elements could significantly disrupt operations, leading to downtime and data inconsistencies.



Remediation:

Develop a comprehensive SaaS backup strategy that includes both end-user and non-end-user data to ensure you can fully restore all aspects of the application in the event of data loss. Look for a backup solution that includes system configurations, permissions and security settings. Covering these essential components is vital to ensuring quick recovery and preventing costly misconfigurations post-restoration.

Spanning Backup for Google Workspace and Microsoft 365 enables you to back up and restore your data to its full and original state, including document directory structure, nested folders, site structure, metadata and sharing and permissions settings.

For Salesforce, Spanning Backup ensures comprehensive protection, covering everything from user-generated reports, dashboards, custom views and email templates to objects, custom objects, files, attachments and metadata. Upon restore of records, Spanning creates new Salesforce IDs and will repair or update prior Lookup Relationships referencing the record prior to restore. You may optionally choose to overwrite field values during the restore process.

4 Leaving your data exposed to insider threats

Sin: Overlooking the risk of insider threats, such as malicious deletions or alterations by disgruntled employees.

While external threats like ransomware often dominate headlines, insider threats — whether intentional or accidental — can pose an even greater risk to SaaS data. Employees or third parties, like contractors with access to sensitive data, may delete, manipulate or export it without authorization. Even well-meaning employees can cause data loss through accidental deletions or changes. In the absence of a robust backup solution, such incidents can go undetected until it's too late.

Remediation:

Implement backup plans that protect against both malicious and accidental insider threats. Your SaaS data protection strategy should involve regular audits of access logs, setting proper permissions and maintaining immutable backups to ensure data recovery, no matter the cause. Use backup solutions with versioning and audit trails to detect, undo and recover from unauthorized changes. Also, use tools that log and alert you to suspicious activity within the backup system itself.

Spanning Backup's auditable activity logs provide a clear record of all actions, showing who performed specific operations and configuration changes. These logs offer an immutable, detailed history of every action by any user or admin within the system. You can view a list of activities, including what was done, by whom and when. The audit log can be easily exported to a CSV file for analysis or reporting. Every action related to your SaaS backup is tracked to ensure full transparency and accountability.

Spanning Backup also performs non-destructive restores by creating a new folder or site for restored content, allowing you to move it to the desired location afterward.

5 No granular restore? You're leaving data vulnerable

Sin: Having a backup strategy that only supports full restores can lead to extended downtime when you only need to recover specific items.

When disaster strikes, speed and precision in data recovery are critical to getting back up and running again quickly. Many businesses make the mistake of relying on backup solutions that offer only broad, all-or-nothing restore capabilities. While it's great to recover a full system, most data loss scenarios require more granular restores, such as retrieving a single email or restoring a specific version of a document.

Remediation:

Choose a backup solution that offers flexible recovery options, such as cross-user restore and granular search and restore. These options enable you to restore data at a granular level, such as individual files, emails or contacts or transfer data to another user account. This minimizes downtime and provides faster, more targeted recovery. SaaS backup solutions that offer both granular and rapid recovery options are vital to an effective backup strategy.

Spanning Backup provides a range of recovery options, making it quick and easy to find lost data and restore it to its desired state and location. Our point-in-time restore feature enables you to access historical snapshots or versions of your data and restore it to any previous version with 100% accuracy. With the granular search and restore functionality, you can easily find and recover individual items or entire folders. The cross-user restore feature allows administrators to transfer data from one user account to another efficiently. Spanning also offers end-user self-service restore, enabling both IT administrators and employees to recover lost data with ease quickly. Additionally, the non-destructive restore feature ensures that deleted or lost files are recovered without overwriting existing data.

6 Skipping backup tests — Betting your data on luck

Sin: Backups are created but never tested. Unverified backups may fail when restoration is needed most.

No matter how advanced your backup solution may be, its value is only realized if it functions effectively when required. One of the most easily overlooked but dangerous mistakes is failing to test backups regularly. Many businesses use a backup solution and assume that their data is secure without verifying the integrity of the backups or the efficiency of the restore process. However, these assumptions can lead to significant repercussions, such as data loss, business disruption and financial losses.

Remediation:

Schedule periodic test restores to verify that your backups are valid and complete and can be quickly restored when needed. This should be part of your disaster recovery drill.

Regular backup testing ensures that your backup solution is working as expected and that data can be successfully restored in the event of a disaster. Additionally, it helps identify any gaps in the backup and restore processes, allowing you to fix errors before disaster strikes. Make sure to regularly test your backups to prevent any unexpected issues during real recovery situations.

With Spanning, your data is automatically backed up daily in the background, and you can perform additional backups at any time as needed. Take advantage of self-service, on-demand backups to test your backup processes regularly. Verify that backups are recoverable, restore procedures are effective, and your team is aligned with your business's SLAs. For example, you can test-run a 20GB SaaS data restore to check the reliability and duration of the process. All recoveries are non-destructive, so you won't risk overwriting data running restores for testing.

7 Overlooking data ownership and compliance — A costly mistake

Sin: Assuming that data within SaaS applications is fully managed and compliant with regulatory requirements by the provider.

Another mistake that can lead to serious repercussions is overlooking data ownership and compliance obligations. When using cloud-based solutions, it's easy to assume that SaaS providers are responsible for complying with regulatory requirements, such as GDPR and HIPAA. However, the responsibility for data protection and retention rests with you — the organization using the SaaS service. Failure to back up and retain data according to regulatory requirements can result in severe penalties and legal liabilities.

Remediation:

To avoid data loss and ensure legal adherence, you must understand who owns the data and the compliance responsibilities associated with it. You should also review compliance obligations, such as GDPR and HIPAA, and ensure your data retention policies meet these requirements. It's important to remember that you are responsible for ensuring your organization's data is stored, protected and retrievable in accordance with applicable laws. Your SaaS backup solution must comply with industry regulations, enabling secure data retention and easy retrieval within required timeframes.

Spanning adheres to the highest standards of data security and compliance, with an extensive list of certifications and audits, including SSAE16, HIPAA and GDPR. Spanning accesses SaaS systems using the OAuth 2.0 protocol, offering a more secure alternative to service accounts and passwords. Our solutions protect data at rest with 256-bit AES object-level encryption, using unique, randomly generated encryption keys for each object and a rotating master key to secure the individual keys. Data in transit is safeguarded by Transport Layer Security (TLS) encryption.

Our systems continuously monitor for potential threats with log analysis, file integrity checks, policy monitoring, rootkit detection, real-time alerting and active response. Access to production servers is limited to specific Spanning employees with operational needs, and all changes to production environment access controls are tracked and auditable for full transparency.

SPANNING
A Kaseya COMPANY

Overcome the deadly sins of SaaS backup with Spanning

With SaaS applications becoming an integral part of modern business, the risks of SaaS data loss have never been higher. To protect your organization from data loss disasters, you must take proactive steps to avoid the seven deadly sins outlined in this eBook. Whether relying solely on built-in SaaS protections or neglecting compliance obligations, each misstep can lead to significant data loss, operational disruptions and regulatory penalties.

Spanning SaaS backup and recovery solutions are designed to help you overcome these challenges. Our industry-leading security certifications, advanced encryption and continuous threat monitoring ensure your data is always protected. Spanning's robust backup and recovery features, including point-in-time restores, cross-user recovery, and non-destructive restores, allow you to recover data efficiently, securely and with complete accuracy.

Avoid the costly consequences of data loss and downtime.

SCHEDULE A PERSONALIZED DEMO

with our SaaS experts today to discover how Spanning makes SaaS data protection effortless.

COPYRIGHT © 2025 SPANNING CLOUD APPS, LLC. ALL RIGHTS RESERVED.