CrashPlan™

# 2025 Guide to SaaS Backup

CrashPlan™

# 2025 Guide to SaaS Backup

**The cloud has transformed the way businesses operate.**

Organizations from small startups to Fortune 500 companies rely on Software-as-a-Service (SaaS) applications like Microsoft 365, Google Workspace, and Slack for their daily operations. However, there's a widespread misconception that SaaS providers automatically back up and protect business data.

**Short answer: They don't.**

Most SaaS platforms offer limited, short-term data retention policies that fail to protect against threats like accidental deletion, cyberattacks, insider threats, and compliance breaches. According to a 2024 IDC report, 76% of organizations that use SaaS applications have experienced data loss due to user errors, malicious deletions, or SaaS provider outages.

This guide will help you prevent disasters and build a resilient SaaS backup strategy.

## What happens without a proper SaaS backup?

Let's consider that your HR department uses Microsoft 365 to store confidential employee records. One day, an employee mistakenly deletes an entire folder containing tax documents. Microsoft 365's built-in recovery window is only 30 days, and no one realizes the mistake until 45 days later. The data is now permanently gone.

Or worse—your finance team uses Salesforce, and a rogue admin, angry over a denied promotion, intentionally deletes key financial reports before resigning. Without an independent SaaS backup solution, there is no way to restore them.

These are not hypothetical situations—they happen every day. And this guide is here to help you prevent these disasters and build a resilient SaaS backup strategy.

## What is SaaS backup?

SaaS backup is the process of creating independent, restorable copies of data stored in cloud-based applications. Unlike traditional backups (which focus on on-premises systems), SaaS backup solutions are designed to protect cloud-stored data from loss, corruption, or unauthorized deletion.

## How SaaS backup works

SaaS backup solutions operate behind the scenes, continuously protecting your critical data from loss. Here's how they function:

### Automated Data Capture

SaaS backup solutions automatically pull data from cloud applications at regular intervals. Some solutions offer continuous backup, while others back up data daily or hourly.

### Data encryption and storage

The backed-up data is encrypted and stored securely in an independent cloud location, separate from the original SaaS platform.

### Versioning and retention policies

Unlike SaaS providers with limited recovery windows (30-90 days), third-party SaaS backup solutions store multiple file versions, allowing businesses to restore past versions and mitigate unintended changes.

### Granular restore capabilities

Need to recover a single email, an entire user account, or a specific file? Granular restore enables precision-level recovery, preventing unnecessary downtime.

# Why SaaS backup is essential today

As businesses increasingly rely on cloud applications, data loss risks are growing. Many assume their SaaS provider fully protects their data, but the reality is actually quite different.

Here's why SaaS backup is essential:

## SaaS providers do not fully back up your data

SaaS vendors like Microsoft and Google operate on a Shared Responsibility Model—meaning they ensure platform uptime but NOT full data protection.

Microsoft 365's service agreement states:

> **"We recommend that customers regularly back up their content and data using third-party services."**

This means that while Microsoft ensures their servers don't fail, they won't recover data lost due to:

- → Accidental or intentional deletion
- → Ransomware attacks
- → Insider threats
- → SaaS application glitches

## Rising cybersecurity threats (ransomware, insider attacks, and data breaches)

Ransomware attacks targeting SaaS applications **increased by 62% in 2024** (source).

Attackers now specifically target SaaS applications, encrypting files and demanding ransom payments for recovery. Without an independent backup, businesses must either pay the ransom or lose their data permanently.

Insider threats are equally alarming. Employees or ex-admins with elevated permissions can delete entire datasets out of spite or for financial gain. Without a backup, there's no undo button.

## Compliance and legal requirements

Data protection laws like GDPR, HIPAA, and CCPA require businesses to maintain recoverable copies of sensitive data for regulatory compliance.

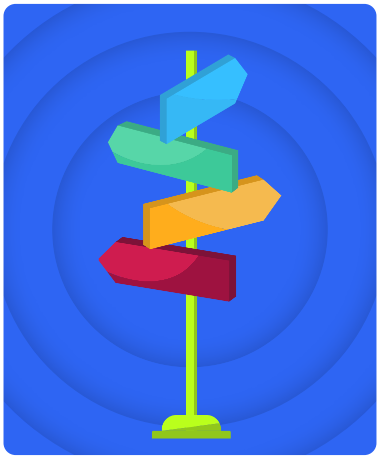
For example, under GDPR Article 32, businesses must:

> **"Ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services."**

Failure to implement proper backup solutions can result in hefty fines and legal actions.

# SaaS backup vs. traditional backup

SaaS backup and traditional backup serve fundamentally different purposes. Understanding their differences helps businesses make informed decisions about protecting mission-critical data.



Traditional backup solutions were designed for on-premises environments, where businesses controlled their infrastructure, storage, and disaster recovery processes. However, as organizations shift to SaaS platforms, relying on traditional backups is no longer effective because:

- SaaS providers control data storage locations, limiting access to infrastructure-level backups.
- Most SaaS platforms have limited retention policies, meaning deleted data is often unrecoverable after a short period.
- Threats like accidental deletions, cyberattacks, and SaaS service outages require specialized backup strategies that traditional methods cannot support.

Here is a detailed comparison of SaaS backup versus traditional backup:

| Feature | SaaS Backup | Traditional Backup |
|---|---|---|
| Data location | Cloud-based (e.g., Microsoft 365, Google Workspace) | Physical storage devices like on-premises servers and endpoints |
| Threats covered | Ransomware, insider threats, accidental deletion, SaaS outages | Hardware failures, system crashes, physical damage |
| Backup frequency | Automated & continuous backup based on policies | Typically scheduled (daily, weekly, or monthly) |
| Recovery time | Minutes to hours with granular recovery | Hours to days, depending on backup size & method |
| Accessibility | Anywhere, anytime from the cloud | Requires on-premises infrastructure or VPN access |
| Retention policies | Configurable long-term retention, versioning available | Typically fixed retention periods based on storage constraints |

# Who needs SaaS backup?

Businesses of all sizes, industries, and compliance levels are vulnerable to data loss, accidental deletions, cyberattacks, and insider threats. Without a solid SaaS backup plan, an unexpected incident could bring an organization to its knees, resulting in financial losses, compliance violations, and operational downtime.

## Small businesses

For small businesses, one major data loss event can mean closing doors permanently. Unlike large corporations with dedicated IT teams and cybersecurity budgets, small businesses often lack the internal expertise to handle security breaches, accidental deletions, or SaaS failures.

**60% of small businesses shut down within six months of suffering a major data loss event** (source).

As an example: You run a small law firm that relies on Microsoft 365 to store client contracts, legal documents, and confidential case notes. One day, a junior associate accidentally deletes an important client folder. By the time you realize it, Microsoft's built-in 30-day retention policy has expired, and the data is permanently lost. Now, you're facing a compliance nightmare and potential lawsuits for losing client-sensitive information.

With a reliable SaaS backup system, businesses can restore data within minutes, ensuring that no accidental deletion or cyberattack can harm them.

## Enterprises

Large organizations generate massive amounts of data daily, spread across different SaaS platforms. With multiple departments and thousands of employees accessing cloud-based applications, the risk of human errors, insider threats, or ransomware attacks multiplies exponentially.

Take an example of an enterprise retail company managing supply chain operations through Google Workspace. A rogue employee, frustrated over a denied promotion, intentionally deletes critical financial reports and inventory logs before resigning.

Here's where things get even worse:

- → The company realized the data loss 45 days later, beyond Google's default 30-day retention period.
- → Google Workspace's native recovery options can't restore permanently deleted files, leaving the company with no way to recover lost data.
- → Without backups, the business loses months of financial records, leading to revenue loss, regulatory fines, and internal chaos.

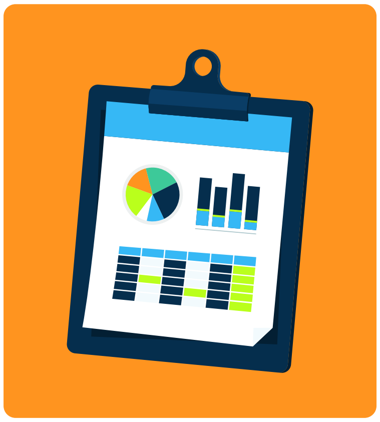
For enterprises, SaaS backup is about business continuity. A well-structured backup system ensures that no human mistake, IT failure, or malicious insider action disrupts operations.

## IT Teams

IT teams are often held accountable for data security, yet they don't control the SaaS environments they manage. Most SaaS providers operate under a Shared Responsibility Model, which means:

- → The SaaS provider ensures platform uptime and infrastructure security.
- → The customer (your IT team) is responsible for securing and backing up the data inside the platform.

This gap leaves IT teams in a dangerous position. If data is deleted—whether due to an employee mistake, a failed software integration, or a cyberattack—the responsibility for recovery falls on them.



## Regulated industries

SaaS backup is also about staying compliant with legal and industry regulations. Businesses in healthcare, finance, government, and legal sectors must adhere to strict data retention, security, and privacy laws.

For example:

- → **HIPAA (Health Insurance Portability and Accountability Act)** mandates secure, long-term storage of patient data. Losing medical records due to a SaaS failure violates HIPAA regulations and can result in heavy fines.
- → **GDPR (General Data Protection Regulation)** requires businesses to secure and retain customer data. Failure to do so can lead to fines of up to €20 million or 4% of annual revenue.
- → Financial institutions must store transactional records for 5+ years under regulations like **SOX (Sarbanes-Oxley Act)** and **FINRA (Financial Industry Regulatory Authority)**. A lack of independent backups could mean legal action or revoked licenses.

For industries bound by strict compliance laws, SaaS backup is not optional—it's a legal requirement.

# How does SaaS backup work?

SaaS backup acts as a protective shield, ensuring that your business-critical data remains secure, retrievable, and resilient against unexpected events. Unlike traditional backups that often require user intervention intervention, SaaS backup solutions work autonomously, safeguarding data in real-time.

Here's how modern SaaS backup works in five critical steps:

## Continuous data capture

Data inside SaaS applications changes constantly. Employees edit, delete, and create new files daily, making traditional scheduled backups ineffective for cloud-based environments.

Modern SaaS backup tools integrate directly with platforms like Microsoft 365 and Google Workspace, automatically capturing every file, document, and record as they are modified. This means that:

- If an employee mistakenly deletes a customer contract, a backup version is instantly available.
- If an integration malfunctions, causing mass data corruption, the last clean version can be restored in minutes.
- If files are encrypted by ransomware, backup snapshots can revert the system back to a pre-attack state.

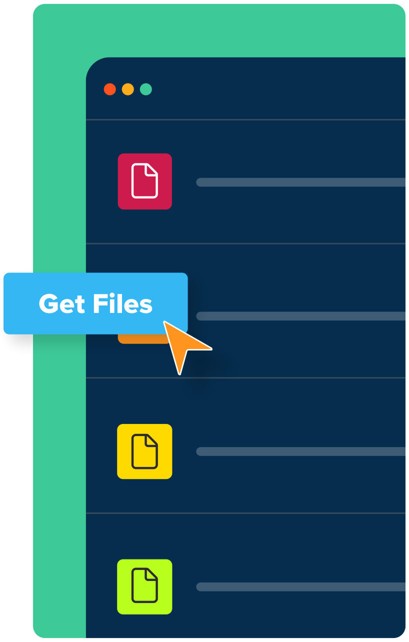
Without continuous data capture, businesses risk losing critical updates, especially in fast-paced environments where decisions are data-driven and real-time accuracy is essential.

## Secure and encrypted storage

Once data is backed up, it must be stored securely not just anywhere, but in an isolated, encrypted cloud environment. Unlike SaaS providers that store live data within the same infrastructure, independent SaaS backup solutions ensure:

- AES-256 encryption secures backups, preventing unauthorized access.
- Immutable storage ensures that once data is backed up, it cannot be altered, overwritten, or deleted—even by administrators.
- Geo-distributed storage protects against regional outages and disasters, ensuring data redundancy.

This level of security is critical because cybercriminals have evolved beyond direct attacks. Modern ransomware now targets SaaS applications, infiltrating cloud environments and encrypting valuable business data. Having an independent, tamper-proof backup ensures that even if an attack compromises the primary SaaS environment, the backup remains intact and fully restorable.



## Customizable retention and versioning

Many SaaS providers operate under short retention windows. Microsoft 365, for example, permanently deletes emails after 30 days. If a company realizes data loss too late, it cannot recover past versions without a backup.

A modern SaaS backup solution stores multiple versions of every file, email, and record, allowing businesses to:

- Recover past versions of documents, even if they were edited or deleted weeks ago.
- Restore individual records within applications without affecting the rest of the database.
- Customize retention policies based on business needs, whether 30 days, 1 year, or indefinitely.

This flexibility ensures that businesses are not at the mercy of SaaS providers' limited retention policies, and can retrieve data whenever needed.

## Granular and instant recovery

In the past, recovering lost data meant restoring an entire system backup. It is a time-consuming process that often overwrote newer data in the process.

With modern SaaS backup, businesses no longer need to roll back an entire system just to retrieve one missing file. Granular recovery allows for:

- **Single-file restoration:** Retrieve one email, one contract, or one customer record without disrupting everything else.
- **Instant search and recovery:** Need to restore a deleted report? Simply search by name, date, or user, and restore within minutes.
- **Selective user recovery:** If a former employee's account was deleted, recover their files without restoring unnecessary data.

Granular recovery means that a single mistake, whether accidental or intentional, doesn't have to cause massive disruptions.

## Audit logs and reporting

For businesses operating in regulated industries like healthcare, finance, and legal services, compliance is just as important as security. Regulations like GDPR, HIPAA, and FINRA require businesses to:

- **Retain records for specific timeframes:** Healthcare providers must store patient records for years, and financial institutions must preserve transactional data for audits.
- **Provide complete audit logs:** Businesses must prove they have a record of every file modification, deletion, and restoration.
- **Ensure data security and accessibility:** Failure to protect customer data can lead to massive fines, legal action, and reputational damage.

SaaS backup solutions come with built-in compliance features, ensuring that:

- Data retention policies align with industry regulations.
- All user actions are logged to prevent insider fraud.
- Audit-ready reports are available for regulatory inspections.

This means businesses can focus on growth and operations, rather than worrying about compliance penalties or lawsuits due to lost data.

# How to choose the right SaaS backup solution

The effectiveness of your backup strategy depends on the features, security standards, and recovery capabilities of the solution you choose. Many organizations assume that all backup solutions function the same way—but that's far from reality. Below, we break down the most crucial factors businesses should consider before investing in a SaaS backup solution.

## Identify your backup needs

Before diving into options, define what you need from a backup solution:

- **Which SaaS applications do you use?** Ensure the solution supports them.
- **What type of data needs protection?** Emails, files, databases, or customer records?
- **How frequently do you need backups?** Daily, hourly, or in real-time?
- **What compliance requirements do you have?** Industries like finance and healthcare have strict regulations.

## Evaluate security and compliance features

Your backup solution must prioritize security. Look for:

- **End-to-end encryption:** Data should be encrypted both in transit and at rest.
- **Zero Trust Architecture:** Ensure only authorized users can access backup data.
- **Data Residency Compliance:** If regulations require data to be stored in specific locations, check for that capability.
- **Ransomware Protection:** Advanced solutions offer anomaly detection to prevent cyber threats.

## Check backup and recovery performance

Speed and efficiency matter when disaster strikes. Ask:

- **How fast can you restore data?** A slow recovery process can lead to downtime and revenue loss.
- **Does it support granular recovery?** Can you restore individual emails, files, or messages instead of an entire dataset?
- **Is versioning available?** The ability to recover previous file versions prevents data overwrites and corruption.

## Assess storage and retention policies

Storage policies determine how long data is retained. Consider:

- **Retention period options:** Some solutions offer flexible retention periods, while others have limits.
- **Storage scalability:** Will the solution grow with your business needs?
- **Data deduplication:** This feature helps optimize storage costs.

## Understand pricing models

Backup pricing varies widely. Some key points to check:

- **Flat-rate vs. pay-per-use:** Flat-rate models offer predictable pricing, while pay-per-use might be cost-efficient for smaller businesses.
- **Hidden fees:** Ensure there are no extra costs for restores, bandwidth usage, or long-term retention.
- **Trial periods:** Does the provider offer a free trial to test functionality?

## Look for easy management and automation

A good backup solution should simplify your life, not complicate it. Features to look for:

- Centralized dashboard: A single pane of glass for managing backups across applications.
- Automated backup scheduling: Set it and forget it—backups should run without manual intervention.
- Alerts and monitoring: Get notified of backup failures or unusual activities.

## Evaluate vendor reliability and support

Not all backup vendors are created equal. Investigate:

- **Customer support availability:** 24/7 support is ideal for global businesses.
- **Customer reviews and case studies:** Learn from other businesses' experiences.
- **Uptime guarantees:** Look for at least 99.9% uptime commitments.

**A well-structured backup solution ensures uninterrupted operations, fast recovery, and confidence.**

The question isn't whether you need SaaS backup; it's whether your business can afford to go without it. The right backup strategy keeps you in control, resilient, and prepared for whatever the future holds.

CrashPlan™

CrashPlan provides cyber resilience and data protection through a unified platform trusted by organizations worldwide. With secure, scalable backup and recovery for servers, endpoints, and SaaS applications, CrashPlan safeguards critical data against threats such as accidental deletion, ransomware, and system failure. Built with proactive threat detection and automated governance, CrashPlan ensures continuous access, compliance, and peace of mind–without disrupting your business.

**Contact us to learn more at** [crashplan.com/contact-sales]

| | |
|---|---|
| in crashplan | f crashplan |
| X crashplan | www.crashplan.com |