THE DEFINITIVE GUIDE TO BACKUP FOR G SUITE

—

HOW TO FIND EXACTLY WHAT YOU NEED TO KEEP YOUR DATA SAFE

TABLE OF CONTENTS

INTRODUCTION

Congratulations!

You've found the perfect cloud-based productivity suite in G Suite. Now you just need to find a way to keep your data safe from loss.

Wait. What? Doesn't Google have data protection covered?

Well, yes and no. Google is just like all the other SaaS providers. They're focused on availability, reliability, and security, and they're able to protect your data in the cloud from problems on their side of the equation—say, a Google disk failure or natural disaster.

But what happens when ransomware locks up all the contents in a shared folder—and then spreads to every other shared folder on you and your customers' Drives? Or when an executive loses critical Calendar data while syncing with their new phone? Or your team is missing contacts because a disgruntled employee deleted them before quitting? Or an employee "tidies up" their email—mistakenly deleting some with critical data—on their last day at your organization?

You may be surprised to find out what can happen when the problem is on your side.

> You may be surprised to find out what can happen when the problem is on your side.

To avoid unwelcome surprises, you need a SaaS data protection solution that's designed to protect your G Suite data by keeping a second copy that's always available to you and then making it easy to restore the data in case of a loss.

Researching and evaluating a truly valuable solution—one that can do both of those things equally well—isn't easy. If you don't know what to look for and where to look for it, you could find yourself on quite a challenging expedition, facing plenty of obstacles along the way.

This guide is designed to provide the information you need to make the best choice for G Suite backup. With the information in these pages, you'll be able to quickly navigate past the false leads, stumbling blocks and dead ends on your search—and uncover exactly the right backup solution for your organization .

WHY YOU NEED TO GO IN SEARCH OF A BACKUP SOLUTION FOR G SUITE

The latest EMC Global Data Protection Index report found that 64% of enterprises experienced data loss or downtime in the 12 months covered by the report. Organizations are also experiencing more data losses than ever—400% more on average, or the equivalent of about 24 million emails each. The cost of all this data loss? Dell EMC pegs it at about $1.7 trillion.[1]

If you think your G Suite data is somehow immune to this growing problem because it's in the cloud, think again. Data in the cloud is vulnerable to loss, just like data anywhere else. In fact, IDG reports that 58% of companies that use SaaS applications suffered a data loss incident over a 12-month period.[2]

Or, as Storage Strategies NOW puts it, "...the dirty little secret of the SaaS industry is that companies lose company SaaS data on a regular basis and most SaaS providers do not offer on demand data restore capabilities that can be initiated by their customer companies."[3]

Basically, if you have data in the cloud, you're at risk for losing it. Of course, risk isn't the same thing as reality; if you want a good dose of that, read on for the stories of real-life losses some companies have suffered.

58%

—

of companies that use SaaS applications suffered a data loss incident over a 12-month period.

[1] EMC Global Data Protection Index
[2] Report: IDG Quick Pulse Survey
[3] Report: Backing Up Software-as-a-Service Applications

The dirty little secret of the SaaS industry is that companies lose company SaaS data on a regular basis.

Cautionary tales: Learning from others' losses

No matter what business you're in or what size your company, the risk of losing data is very real—as the following stories make very clear.

CASE IN POINT: LONG-LOST GOOGLE DRIVE FOLDER

An employee at a pharmaceutical company deleted a shared folder within Google Drive—and then left the company. So when an administrator went looking for the data set months later, it couldn't be found. No one even knew the exact file names to look for, but an administrator eventually found the file by searching on date stamps and keywords. However, the path was concatenated, making it impossible to clarify the location.

CASE IN POINT: MYSTERIOUSLY MISSING EMAILS

Not one, not two, not three, but all of an employee's emails in Gmail inexplicably vanished at one of the largest and most respected construction companies in the US. Not only did this wreak havoc with the employee's ability to do his job, it also threatened to damage the company's reputation for being able to keep confidential client data safe and secure.

Fortunately, both of these cases had happy endings—but only because the companies had third-party backup tools in place that enabled them to uneventfully restore the lost data. We'll talk more about third-party tools later in this guide. (We'll also talk in an **upcoming chapter** about the tools Google itself offers for data protection, including what they do and don't cover, and what they can and can't do.)

What's at Risk?

- PRODUCTIVITY
- DATA LOSS
- NON-COMPLIANCE

DON'T COUNT ON GOOGLE TO SAVE YOU

It's not that Google doesn't have robust technology in place for protecting data in the cloud; it's just that the technology, like that of most SaaS application vendors, is designed to protect against losses originating on Google's side. As Forrester reports:

"Data is replicated multiple times across Google's clustered active servers, so, in the case of a machine failure, data will still be accessible through another system. They also replicate data to secondary data centers to ensure safety from data center failures."[4]

That's fine if Google suffers a data center failure—but doesn't help much if the failure is instead yours. Should a G Suite end user or G Suite administrator delete data, Google will also delete it, in accordance with the terms of its customer agreement and privacy policy.

Google does offer their customers some options for recovering data that's been lost, but they are somewhat limited, as explained in an **upcoming section**. Furthermore, as Forrester also mentions, "data is irretrievable once an administrator deletes a user account."

[4] Rachel A. Dines, "Back Up Your Critical Cloud Data Before It's Too Late," Forrester

> MOST SAAS PROVIDERS DO NOT OFFER ON-DEMAND DATA RESTORE CAPABILITIES THAT CAN BE INITIATED BY THEIR CUSTOMER COMPANIES.
>
> —
>
> Storage Strategies NOW

THE TOP 5 REASONS YOU NEED BACKUP FOR G SUITE

01

HUMAN ERROR

Whether it’s an end user error, such as deleting important email by mistake, or admin error, such as deleting a user by mistake—and losing all that user’s associated email and data—human error is the leading cause of data loss in SaaS applications. It accounts for a whopping 64% of data loss incidents, according to Aberdeen Research.

02

SYNC ERROR

It’s not uncommon for data loss to occur due to sync errors. When integrating with another application, deploying new devices, or simply working within G Suite, sync errors can be a significant source of risk to business continuity.

03

INSIDER THREAT

Data breaches caused by people working inside companies, rather than by outside hackers, make up 27% of all electronic crime events, according to the CERT Insider Threat Center at Carnegie Mellon University’s Software Engineering Institute.[5]

[5] CERT Insider Threat Center at Carnegie Mellon University’s Software Engineering Institute

THE TOP 5 REASONS YOU NEED BACKUP FOR G SUITE

30%

of decision-makers consider insider attack as their greatest concern among risk factors for data loss. second only to hacking.

04

RANSOMWARE AND HACKING

Ransomware and other attacks can be more damaging in SaaS productivity suites than they are in traditional tech environments. They can easily proliferate through shared folders and Drives—the very thing that makes G Suite a powerful collaboration tool is also what makes it even more vulnerable.

05

COMPLIANCE

Loss of data can lead to non-compliance with regulations across a number of industries. For example, regulations governing data privacy—for instance, HIPAA in the healthcare field—may be violated if data is compromised by hackers. Your compliance with regulations related to data availability may also be at risk.

HOW GOOGLE CAN (AND CAN'T) AID IN YOUR QUEST

If you lose data in G Suite, Google does offer ways to recover it. Here's a look at the capabilities and limitations of each method.

Built-in restore for Google Drive

Google has a built-in capability for restoring Drive data after a user deletes it from the Trash. The capability is, however, limited in several ways.

- **Only 25 days.** The restore capability is only available for 25 days after the loss, so if you don't realize until later that something important was deleted, you won't be be able to get it back.
- **All-or-nothing restore.** There's no way to view or select which files will be restored before the process is initiated, there is no list of what was actually restored, and the restored files are not marked or flagged in any way. The process could result in files being restored that didn't need to be, cluttering up the Drive, taking up valuable space, and potentially requiring a significant amount of time to sort through.
- **No sharing settings.** Sharing settings are not restored and must be manually reassigned by the user, which could be a problem if they don't remember with whom the data was originally shared.
- **Administrator assistance required.** There's no way for a user to perform this operation on their own; they must contact their G Suite administrator for assistance. This could result in lost productivity, time delays, and unnecessary burdens on the IT staff.

Google's built-in restore for Google Drive can be useful if you're dealing with a recent data loss incident and if there aren't too many other files in the Trash besides the one you need.

Google Vault export/import

Google Vault was designed for legal eDiscovery, not for data restoration, but it can be an option for recovering at least some lost data. Like the built-in restore capability for Google Drive, though, it has its limitations.

- **Current file versions only.** Prior versions of non-native Google files are not recoverable with Vault.
- **Administrator assistance required.** There's no end user interface in Vault, so admin time will always be required to manage the process of attempting to restore data.
- **Export/import only.** There is no direct restore capability with Google Vault; the only way to restore data is to export it and then import it back manually.
- **No sharing settings.** In the export/import process, all of your sharing settings will be lost. As with the built-in restore capability for Google Drive, that can be a problem if you don't remember the previous sharing settings for every lost document.
- **Requires an active account.** If a user's account is accidentally deleted from G Suite, all of their data is also deleted from Vault.
- **Limited app coverage.** Google Vault does not cover all G Suite apps—leaving your organization's critical data vulnerable to data loss.

While Vault can provide the ability to recover some data, it was not designed for rapid recovery. For those who use Vault to back up all data, your Legal team may likely advise against that, since whatever is in Vault can be used in legal action. And it certainly misses the mark if what you're trying to achieve is quickly getting your lost data back to its original location intact; that's simply not what it was designed to do.

Is that all there is?

If you're looking for help to get your lost data back, the options above are all you'll find from Google. But don't stop looking, because there is another way—third-party cloud-to-cloud backup. Head to the **next section** to learn more.

Here's a quick look at what Google offers you in terms of their built-in restore capabilities.

AFRAID OF LOSING DATA? GOOGLE HELP AT A GLANCE

CAPABILITIES	BUILT-IN RESTORE FOR GOOGLE DRIVE	GOOGLE VAULT
RESTORE ABILITY	25 days after Trash is emptied	As long as G Suite account still exists
RESTORE TYPE	All or nothing	Granular, but tedious
RESTORE LOCATOR	Somewhere in user's Drive	Export only
RESTORE INITIATOR	Administrator	Administrator
SHARING SETTINGS	Not restored	Not restored
APPS COVERED	Gmail and Google Drive	Gmail, Drive, Groups and Hangouts Chat

WHAT YOU NEED TO UNDERSTAND ABOUT CLOUD-TO-CLOUD BACKUP

Key concepts

Looking to Google for the cloud data backup you need will only take you so far. Fortunately, there's another path to data loss protection. A third-party cloud-to-cloud backup solution gives you the ability to keep a copy of your G Suite data in a separate cloud in case the original data is destroyed, damaged, or deleted. By moving your data to the cloud, and taking advantage of the vast network of servers and replication that the cloud provides, you raise the certainty that it will be available when you need it and that it will always be accessible.

Before defining your criteria for evaluating third-party cloud-to-cloud backup, you may need to educate others involved in the evaluation and approval process. The following information will help.

Backup & archive are two different things

Know what you're looking for: a solution for backing up data—not archiving it. A backup copy is something that exists for the express purpose of making data available and recoverable in the event that it's no longer accessible in its original form. An archive addresses a completely different need; it exists to meet compliance needs or internal policies, and simply isn't designed for data recovery. Unlike a backup copy, an archive is generally the only form in which the data exists. And that's fine, since its purpose isn't to replace data that's lost, but to preserve data that needs to be kept to meet compliance policy requirements. But it does make an archive solution the absolutely wrong choice for data backup.

Backup is one thing, restore is everything

The most important thing to understand about backup solutions is that backup is only half of the equation. Being able to restore the data you've been backing up is the other half. So while you need a solution that makes backup quick and easy, you also need a solution that makes restoring the data equally effortless. Otherwise, there's not much point in having it. In your quest for a solution, you'll run across some that may offer a relatively simple way to do backup—but then require you to go through a cumbersome, time-consuming process to get back the data you lost.

Data recovery isn't the same as data restore

Recovery simply means you get your data back—not that you get it back exactly the way it was. Recovery can refer to recovering and exporting all the versions of your backed-up cloud data, requiring you to spend a lot of time and effort finding the specific previous version of what you lost, or to rebuild your file structure, or to manually import data back into G Suite apps. Restore means accurately and automatically returning data back into G Suite apps exactly as it was before you lost it. Backup solutions that merely retrieve all your backed-up data, leaving you to sort through it all, are of limited value.

Keeping these concepts in mind, you're ready to evaluate the third-party cloud-to-cloud backup solution that will work for your organization. Turn to the **next section** to learn more about how to determine what G Suite data protection solution will best meet your needs. Use the provided **checklist** to easily evaluate your chosen backup solution.

Cloud-to-cloud backup gives you the ability to keep a copy of your G Suite data in case the original is destroyed, damaged, or deleted.

4 THINGS TO LOOK FOR IN A CLOUD-TO-CLOUD BACKUP SOLUTION

These are some suggested requirements for a cloud-to-cloud backup solution for G Suite. They're followed by a simple checklist that you can use to evaluate solutions.

01 RESTORE CAPABILITIES

02 COMPREHENSIVE, TRANSPARENT BACKUP

03 USABILITY

04 SECURITY AND COMPLIANCE

01 RESTORE CAPABILITIES

GRANULAR DATA RECOVERY OPTIONS

Be sure you have the option to restore everything from a single document to every bit of data you've got. And check to see that older file versions don't overwrite new ones during the restore process, so that you have full control over what gets restored and how.

SIMPLE, STRAIGHTFORWARD RESTORE PROCESS

Look for an interface that works the way the G Suite apps interface works, so no one has to waste time learning to navigate a new and unfamiliar interface.

LITTLE TO NO ADMIN ASSISTANCE NEEDED

Find a solution with a simple process that uses just a few clicks and doesn't require end users to ask for special assistance, to avoid backlogs and bottlenecks caused by IT having to step in every time someone needs to restore lost data.

ACCURATE RESTORE OF POINT-IN-TIME DATA BACK INTO G SUITE

A good backup solution should be able to retrieve data from any specific point in time and then automatically restore it directly back into G Suite with no manual effort. It should be able to store the most recent or any previous point-in-time version with 100% accuracy and also restore metadata such as labels, file structures, and sharing settings.

RAPID RESTORE TIMES TO MEET FAST RTOS

To avoid downtime after a data loss, you need to achieve the fastest recovery time objectives (RTOs) possible. This requires a backup solution with restore processes that involve a minimal number of steps and that can be done by someone with no special training.

02 COMPREHENSIVE, TRANSPARENT BACKUP

CONFIGURABLE DATA PROTECTION

Some users need all their data protected, some just need portions, and some need no data protection at all. Backup solutions should be configurable to support different policies for different users.

INDIVIDUAL FILE PROTECTION

Every object should be protected individually, so that single errors don’t cause an entire backup to be corrupted and lost. Make sure that your backup solution treats every object as a unique entity and not just part of a larger batch file.

BACKUP STATUS REPORTING

Knowing the status of your G Suite backup process can help you identify any issues with your backups and improve the overall quality of your G Suite apps data. A backup provider that enables you to see whether there were any problems with your backups demonstrates a commitment to ensuring the high quality of your data.

64%

—

OF DATA LOSS INCIDENTS ARE CAUSED BY HUMAN ERROR.

ABERDEEN RESEARCH

03 USABILITY

EASY TO USE

A backup solution should require minimal to no training to use. It should be so intuitive in design, that on the rare occasions that you need to use it, you don't have to spend time hunting for a manual and trying to remember how it works.

AUTOMATED

Some backup software requires a significant amount of manual intervention. You should seek a solution that automates both backup and restore. Ideally, whenever you add a new user to your domain, their email, documents, contacts, and calendars will be protected automatically, making less work for everyone involved.

NO STORAGE LIMITS

When you're backing up data, you shouldn't have to worry about whether more backup storage will increase your costs—or worse, that you don't have enough storage for everything you need to back up. Avoid these risks by avoiding solutions that charge for storage.

04 SECURITY AND COMPLIANCE

SECURITY CERTIFICATIONS

An external security certification indicates that a neutral third party has conducted a thorough evaluation of the solution provider's business and coding practices. Look to see that:

- The backup solution you're considering has a widely recognized security certification such as Skyhigh Cloud Trust to indicate it meets stringent, externally established data security requirements.
- The backup provider has completed an SSAE 16 Type II audit, which indicates meeting rigorous security standards for infrastructure, software, employees, procedures, and data handling.

ALIGNMENT WITH COMPLIANCE REQUIREMENTS

The regulatory and compliance mandates that govern data availability don't necessarily mandate backup and restore capabilities, but they do require organizations to keep information available—and that makes the ability to restore data critical. A solution that operates within the COBIT framework of standards for compliance will help ensure compliance.

DATA PRIVACY PROTECTION

To protect data privacy, a backup solution needs to have have measures in place to ensure that users only see the data they are authorized to edit. Look for a solution that:

- Encrypts data using SSL and 256-bit AES object-level encryption technology.
- Retains document security metadata so that restored documents have the same level of protection as the original.
- Permits an IT admin to restore a user's data without gaining access to it.
- Has earned BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus Privacy Certification.
- Is certified under the US-EU and Swiss-US Privacy Shield, and is GDPR-compliant.

CHECKLIST FOR EVALUATING CLOUD-TO-CLOUD BACKUP SOLUTIONS

Before you get on board with a particular backup solution for G Suite, be sure it gives you the ability to do everything on this list.

RESTORE

- ✓ Restore any previous point-in-time version of a single Drive or Team Drive file directly into a G Suite account.
- ✓ Restore multiple Drives, Team Drives, files and folders from any previous point-in-time directly into a G Suite account.
- ✓ Restore Drive or Team Drive files and folders with sharing settings.
- ✓ Navigate, view and restore emails by label.
- ✓ Customizable label name for email restores.
- ✓ Option to restore emails without original labels.
- ✓ Restore an entire site or selected pages with dependent files from any point-in-time version.

EXPORT

- ✓ Export entire accounts or specific services.
- ✓ Export multiple items from any point-in-time backup version.
- ✓ API access for exporting and downloading data.

BACKUP

- ✓ True point-in-time backup and restore of your G Suite data.
- ✓ View the granular results of every backup with file level details.
- ✓ Review backup details and actionable guidance for each problem or identified corrupted file in Google.
- ✓ Unlimited storage.
- ✓ Unlimited versions for all data.

ADVANCED ADMINISTRATION

- ✓ Assign administrative controls to specific users.
- ✓ Quickly assign Spanning Backup to individual accounts, OUs or the whole domain.
- ✓ Automatically assign backup licenses to new users of G Suite.
- ✓ Automatically purchase backup licenses for new users of G Suite.
- ✓ Multiple Administrative Roles.

END USER EXEPIENCE

- ✓ Similar look-and-feel to Gmail and Drive.
- ✓ Enables quick review of the status and details of backups.
- ✓ Search all backups or a specific point-in-time backup for one or more Drive files.

SECURITY

- ✓ All data at rest is encrypted with 256-bit AES encryptions with unique keys generated for every object.
- ✓ Detailed audit log for all security and setting changes.
- ✓ Complete activity log including all user and admin exports and restores with file-level details.
- ✓ Supports HIPAA & GDPR Compliance.

SPANNING BACKUP: IT'S EVERYTHING YOU'VE BEEN LOOKING FOR

The more you rely on G Suite for your everyday business, the more critical it is to find a way to protect your G Suite data. Don't risk your organization with the minimal, time-consuming native options offered by Google. Don't waste time with other solutions that don't focus on restore. Follow the guidance here, and evaluate those solutions that protect your data, enable perfect and rapid restores, and ensure business continuity.

SPANNING
A Kaseya COMPANY

Spanning Cloud Apps, a Kaseya company, is the leader in SaaS Cloud-to-Cloud Backup, proven and trusted by more than 10,000 organizations across the globe to provide enterprise-class data protection. Spanning's cloud-native, purpose-built solutions for Office 365, G Suite, and Salesforce provide easy-to-use yet powerful capabilities for end-users and administrators and meet the rigorous requirements for listing on Microsoft AppSource, Salesforce AppExchange and G Suite Marketplace.

START A FREE 14-DAY TRIAL AT
SPANNING.COM/START-FREE-TRIAL

@SPANNINGBACKUP

FOLLOW US ON LINKEDIN

READ OUR BLOG

WWW.SPANNING.COM

+1 (512) 236-1277