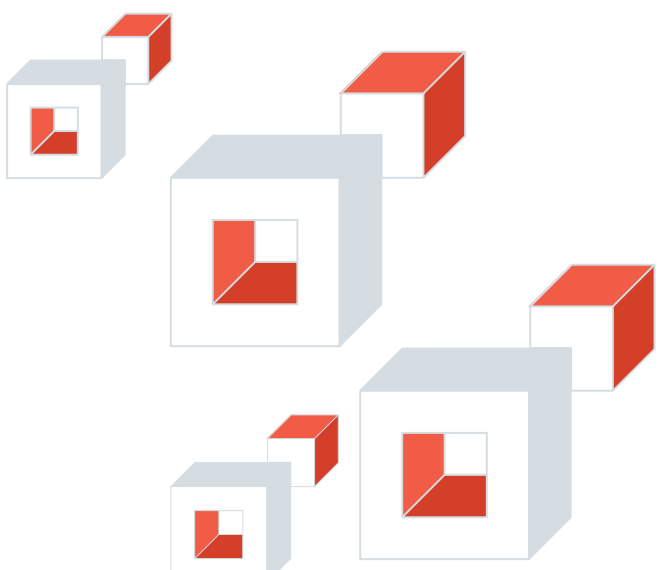
SPANNING
A Kaseya COMPANY

EBOOK

THE ROI OF GOOGLE WORKSPACE BACKUP

HOW WILL A GOOGLE WORKSPACE BACKUP SOLUTION IMPROVE BUSINESS?

TABLE OF CONTENTS



INTRODUCTION

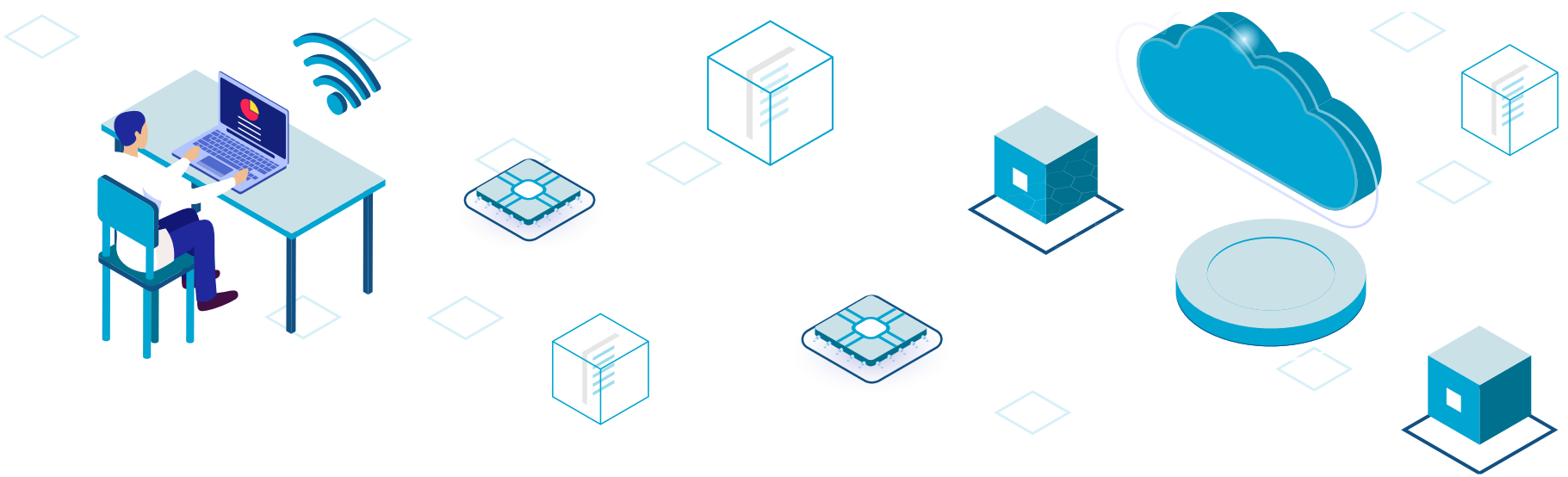
"How will a Google Workspace backup solution improve business?"

This is a common — and valid — question from decision-makers. Unfortunately, IT professionals often struggle to answer it in business terms. While IT teams understand the risks of data loss, they often struggle to translate that technical urgency into business value that resonates with stakeholders.

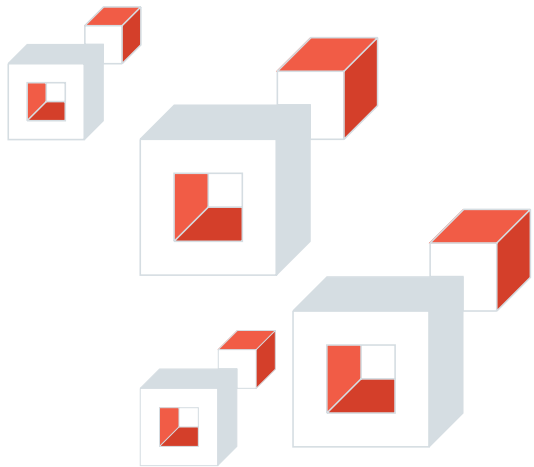
That's why we created this guide to empower IT professionals with the right tools and insights to effectively communicate the importance of a Google Workspace backup solution.

We'll explore the risks of relying solely on Google's native protection and highlight real-world scenarios to frame data protection as a strategic investment, not just an IT concern.

To help strengthen your case even further, we've included access to Spanning Backup's ROI Calculator. This tool lets you quantify the value of a Google Workspace backup, allowing you to justify costs with confidence and improve your chances of getting budget approval.



GOOGLE WORKSPACE SECURITY: TACKLING FALSE PERCEPTIONS



Perception is NOT reality

“Perception is reality” is a phrase often used to validate one’s beliefs as a universal truth. However, in business, especially when it comes to data protection, **perception and reality are not the same**. Decision-makers frequently fall into the trap of treating assumptions as facts, which can lead to costly oversights.

This is particularly true when it comes to safeguarding data in the cloud. Many decision-makers assume that cloud platforms like **Google Workspace** don’t require a backup solution. This assumption stems from a critical misunderstanding of Google’s actual responsibilities in data protection. In the absence of clear knowledge, these gaps are filled with misconceptions, often false and deeply ingrained. Decision-makers frequently lean on Google’s strong brand reputation as a safety net, reinforcing their flawed beliefs.

Why does it matter if perception diverges from reality?

Perception is the lens through which leaders evaluate risks, make decisions and act. But when that lens is distorted, so is their view of reality. The result? Organizations are left vulnerable, caught between **illusion and delusion**, with no awareness of the risks they face. And that means your **Google Workspace** data could be in danger without you even realizing it.

It’s time to shatter the myths, replace assumptions with clarity and make informed decisions that ensure your **Google Workspace** environment is truly protected.

Perception no. 1:
My Google Workspace is *really, really* secure

Google Workspace has best-in-class security: disaster recovery capabilities against infrastructure threats like hardware and software failure, power outages and natural disasters.

Reality No. 1:
Google cannot protect you from attacks at your end

Human error: Accidental deletion or human error was responsible for over 30% of SaaS data loss incidents in 2024.[1]

Sync error: Third-party apps in Google Workspace can ruin valuable data with no option to undo.

Ransomware: Shared drives and folders that make up the best part of Google Workspace also allow ransomware to proliferate easily.

Insider threat: Even Google Workspace's sophisticated security infrastructure cannot predict employees' intentions, making such employees an effective cyberattack vector.

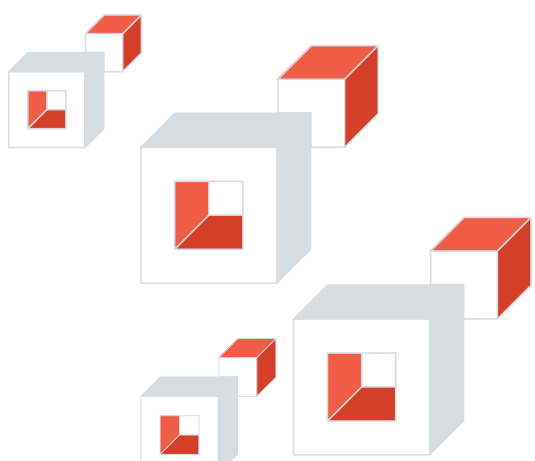
Perception No. 2:
Google is responsible for my data

Google Workspace holds my business data, so Google is responsible for keeping my data safe.

Reality No. 2:
Google Workspace is not responsible for your data

Remember the terms of service you signed (probably without reading)? Here's a disclaimer you missed:

"When permitted by law, Google, and Google's suppliers and distributors, **will not be responsible** for lost profits, revenues, or data, financial losses or indirect, special, consequential, exemplary or punitive damages."



Perception No. 3:
My Google Workspace has a built-in backup

Google Workspace has built-in features like Recycle Bin and Vaults to store deleted data.

Reality No. 3:
They are temporary archival solutions, not backup solutions

That means deleted data is stored for a limited period, the backup is not as comprehensive as one would hope and restoring data can be a nightmare.

In Google Workspace, deleted emails and files remain in the trash for 30 days before they are permanently removed. However, administrators can still recover deleted items within 25 days after they've been removed from the trash. Once this recovery period ends, the data is permanently deleted and cannot be restored using Google Workspace's native tools.

In Google Vault, admins can set custom rules or holds to retain data in Gmail, Drive and other services for a specific period or indefinitely. However, it is important to note that Google Vault is built for archiving and eDiscovery, not backup. It lacks critical features like automated restores, point-in-time recovery and efficient, large-scale data restoration with original structure and permissions.

THE BUSINESS VALUE OF USING A GOOGLE WORKSPACE BACKUP SOLUTION

Relying solely on Google Workspace for data protection leaves your business exposed, period. To truly safeguard your emails, files and user data, you need a dedicated backup and recovery solution that adds a critical layer of security.

But here's the challenge: getting decision-makers to invest in one isn't easy.

Many are hesitant to allocate a budget for backup solutions, often questioning their necessity or reliability. This skepticism isn't without reason. Over the years, some vendors have undermined trust by using inflated claims and marketing hype instead of real value. As a result, decision-makers are wary, unsure if backup solutions deliver on their promises or if a Google Workspace backup is even worth the investment.

The following insights will highlight the value a robust backup and recovery solution brings to a business.

DIRECT COSTS OF CYBERATTACKS

After a cyberattack, businesses often shift into investigative mode – scrambling to uncover the what, how and why behind the breach. For organizations still relying on a reactive, trial-and-error approach, these investigations typically result in one of three outcomes: almost accurate, inaccurate or a swirl of conflicting theories with high variability. The result? **Dozens of hours wasted on investigations that produce more confusion than clarity.**

Yet, these flawed conclusions are frequently used as the foundation for future security decisions — decisions that ultimately fail to prevent similar incidents.

Here's how direct costs typically add up:

TOTAL DIRECT COST =

Loss from the attack (e.g., ransomware, hardware failure) + *Working hours spent investigating the attack* + *Loss from potential attacks*

A Google Workspace Backup solution enables you to adopt a proactive approach when dealing with cyberattacks.

With Spanning Backup, you can:

- **Monitor the most recent backup activity** across your Google Workspace environment.
- **View the backup health of every Google Workspace user** in their domain and drill down into issues before they escalate.
- **Opt to receive automated email notifications** — daily, weekly or monthly — to ensure you're always up to date on your Google Workspace backup status.

Instead of spending hours on post-attack investigations, you'll have the confidence and visibility to protect your business before threats become disasters.

HIDDEN COSTS OF CYBERATTACKS

Ever wonder why data breach headlines often come with multimillion-dollar price tags? In 2024, the global average cost of a data breach surged to $4.88 million, a 10% jump from the previous year.[2] And it's not just about the obvious expenses. That figure includes both direct and hidden costs: loss of business, operational disruptions and diminished productivity, to name a few.

Loss of business: Whether you're a small ad agency that has lost its latest creative work or a large retailer that has lost a month's worth of orders, an unexpected data loss can bring any business to a standstill, regardless of its size. On average, each compromised record costs a business $173.[2] As recovery expenses climb and revenue stalls, what starts as a data incident can quickly escalate into a full-blown crisis, sometimes even leading to permanent business closure.

Business disruption: Financial losses are only part of the story. The real cost of data loss lies in what you can't get back — *time*. Recovery efforts can take hours, halting progress and throwing day-to-day operations into disarray. The impact doesn't stop there. It cascades across teams and departments, causing delays, missed deadlines and lost momentum throughout the business.

Lost productivity: Workplace productivity is often the first casualty when data is lost. IT teams are forced to drop everything, working overtime to recover what was lost. Whether or not the recovery is successful, the business still pays the price — extra hours, extra costs and zero contribution to the bottom line. It's time and money spent fighting fires instead of driving growth.

COST OF INSIDER THREATS

One bad apple can cost your business BIG! Here's how:

Impacts market value

When Harold Martin, a former contractor for Booz Allen Hamilton, was arrested, the consulting firm's shares saw an immediate dip of 5%.[3]

Risks the company's future

When sensitive data is too easy to access, stealing intellectual property becomes effortless. As a result, you lose your competitive advantage, and with it, the confidence in your company's long-term viability.

Increased overheads

Security incidents lead to costly overheads — restructuring, retraining and hiring new employees drive up operational expenses significantly.

Gives way to bad culture

Breached trust erodes morale, fostering a toxic culture that drives up employee turnover and recruitment costs.

Insider threats (malicious or accidental) are harder to detect and recover from. However, a good backup solution like Spanning Backup can mitigate it.

Backup creates an independent copy of data that users can't alter or delete. Spanning Backup provides transparency and accountability by recording every Google Workspace backup activity. Get detailed insights on every action done by the user and report suspicious activities that can possibly compromise your data.

COST OF DOWNTIME

To quantify the impact of downtime on your business, it's essential to understand two key metrics: recovery time objective (RTO) and recovery point objective (RPO).

RTO refers to the maximum amount of time your business can tolerate a disruption before normal operations must be restored.

RPO defines the maximum amount of data your business can afford to lose without disrupting operations or impacting performance.

Without clearly defined RTO and RPO goals, recovery will be delayed, increasing downtime costs. Defined objectives enable faster, more efficient restoration of systems, minimizing business disruption during a disaster.

Here's an overview of a typical RTO/RPO plan.

COMPONENT	WHAT IT IS	EXAMPLE GOAL
Recovery Time Objective	Maximum allowable time to restore systems and resume operations after a disruption.	Recover critical systems within two hours.
Recovery point objective	Maximum acceptable amount of data loss measured in time before the disruption occurred.	Restore data to the state it was 30 minutes before the incident.

Figure 1: RTO/RPO overview

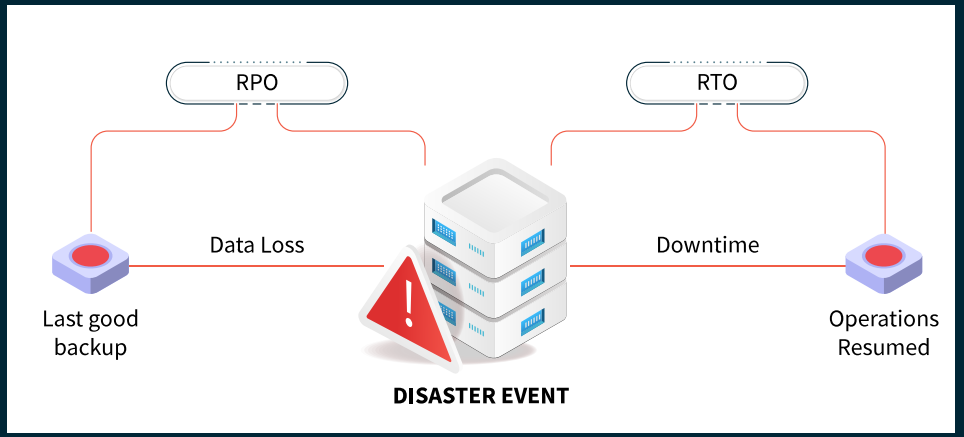


Figure 2: RTO/RPO concept

RECOVERY VS. RESTORE

When it comes to Google Workspace backup, data recovery is not the same as data restoration.

Recovery may bring your data back, but not always in its original format or location. This often leads to extended downtime, lost productivity and extra hours spent locating files, rebuilding folder structures and manually reimporting content back into Google Workspace.

Restoration**,** on the other hand, returns your data exactly as it was — in its original format, structure and location — automatically and seamlessly.

That's where Spanning Backup for Google Workspace makes all the difference. Spanning's powerful, reliable restoration capability has earned the trust of thousands of organizations and millions of users worldwide because it enables business continuity even during a disaster.

REPUTATION COSTS

Would you associate yourself with a business that's been breached? Can you overcome the disappointment of having your confidential data exposed? Would you be okay with no explanation as to why your data went missing? Probably not.

Why should you expect any other treatment when your business is under the data breach spotlight?

Fixing the reputation of your business after a data loss is a tough nut to crack. In fact, reputation management can have a huge impact on your margins. Not only do you lose out on current customers, but with poor credibility and bad publicity, potential customers will never come knocking on your door. It's no surprise that 41% of businesses lose out on revenue due to a negative reputation.[4]

COST OF NON-COMPLIANCE

Compliance has always been a prerequisite for regulated industries like healthcare and finance. However, with GDPR and CCPA, the need for compliance is extending to non-regulated industries as well.

The cost of non-compliance is nearly three times higher than the cost of staying compliant, and it comes with unpredictable risks that businesses simply can't afford to ignore.[5]

Compliance legislation	Penalties
HIPAA	Fines up to $250k and 10 years of imprisonment.
GDPR	20 million euros or 4% of the total global turnover of the previous fiscal year, whichever is higher.
CCPA	Civil penalties of up to $7,988 for each violation and the maximum fine for other violations is $2,663 per violation.

Figure 3: Cost of non-compliance

Legal fees

Fighting penalties means dealing with a pile of legal paperwork and courts, not to mention potential civil lawsuits. For instance, let's say a European citizen whose data was leaked decides to sue your business. This can lead to a mountain of legal fees that can exceed the penalty itself.

Recertification costs

A non-compliant business is expected to recertify employees in compliance training. This can be an overwhelming expense for a business that's already dealing with penalties and legal costs.

SPANNING BACKUP ROI CALCULATOR: FIND THE REAL VALUE OF GOOGLE WORKSPACE BACKUP

Use Spanning's Google Workspace Backup ROI Calculator to uncover the real dollar value of protecting your data. Calculate in real time the amount of money you'll save on employees and overall IT productivity, along with knowing potential returns. The insights will help you make decisions that are rooted in reality, not perceptions. Ready to make smart decisions?

GET ROI ON MY GOOGLE WORKSPACE

SPANNING
A Kaseya COMPANY

Spanning Cloud Apps, a Kaseya company, is the leading provider of backup and recovery for SaaS applications, helping organizations around the globe protect their information in the cloud. Spanning provides powerful, enterprise-class data protection for Microsoft 365, Google Workspace and Salesforce. With data centers located in North America, the EU, UK, Australia and South Africa, Spanning Backup is the most trusted cloud-to-cloud backup solution for thousands of organizations and millions of users around the world.

1. https://www.spanning.com/resources/the-state-of-saas-backup-and-recovery-report-2025/
2. https://www.ibm.com/reports/data-breach
3. https://www.federaltimes.com/2016/10/05/fbi-arrested-contractor-for-theft-of-nsa-code-docs/
4. https://electroiq.com/stats/reputation-management-statistics/
5. https://www.cornerstoneondemand.com/resources/article/the-cost-of-non-compliance/