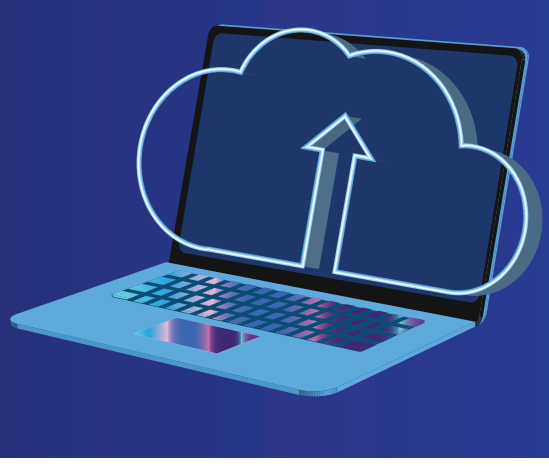
backupify
A Kaseya COMPANY

HOW SAFE IS YOUR DATA IN THE CLOUD?



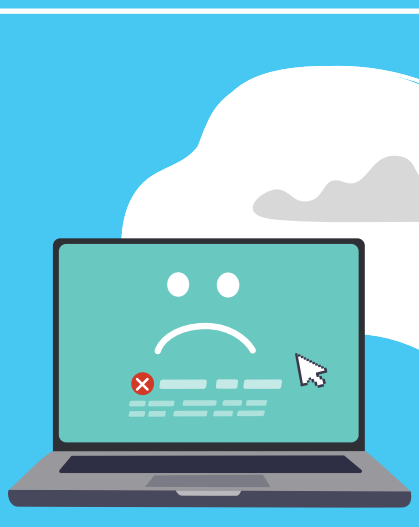
Google Workspace has emerged as the collaboration suite of choice for thousands of organizations worldwide. While cloud-based solutions offer numerous benefits, such as scalability and flexibility, SaaS providers like Google do not provide data protection against every loss scenario. Unfortunately, many organizations make dangerous assumptions about who is actually responsible for backing up data in their SaaS apps.

Ultimately, you need to ensure you have access to and control over Google Workspace data. This infographic explores the common blind spots when it comes to SaaS data loss and the threats that could bring disastrous consequences if overlooked.

HUMAN ERROR

Human errors, such as accidental deletions, overwrites and unintentional data corruption, are some of the most common risks in Google Workspace.

Almost 70% of breaches were attributed to unintentional human actions, including individuals falling prey to social engineering attacks or making mistakes.[1]



MALICIOUS ACTIVITY

Malicious activities, including insider threats and cyberattacks, pose a significant threat to data stored in cloud environments, such as Google Workspace.

More than 20% of organizations experienced data loss caused by employees intentionally deleting data.[2]

In 2023, over half of businesses (59%) across the globe experienced ransomware attacks.[3]

COMPLIANCE AND LEGAL RISKS

Compliance and legal risks are critical for organizations handling sensitive information. While Google Workspace's native retention policies help with compliance and regulatory requirements, they might not meet all regulatory requirements, especially for industries with stringent data preservation rules.

THIRD-PARTY APP INTEGRATIONS

Integrating third-party applications with Google Workspace enhances functionality but also introduces risks. Granting these apps access to your organization's data can lead to file encryption, data theft or exposure of confidential information.

APIs linking apps may unintentionally expose your data, making it vulnerable to unauthorized access and loss. Ensuring third-party integrations follow security best practices is essential for maintaining data integrity.

The average organization has 157,000 sensitive records exposed to everyone on the internet.[4]

SERVICE OUTAGES AND DOWNTIME

Even with Google's robust infrastructure, service outages and downtime can still happen.

In May 2024, a major Google outage disrupted services for thousands of users globally. [5]

According to the Data Protection for SaaS report, the leading cause of data loss was the SaaS service itself. [6]

ELIMINATE BLIND SPOTS WITH BACKUPIFY

Seal every data protection blind spot and take full control of your Google Workspace data with Backupify. Our cloud-to-cloud backup solution simplifies Google Workspace data through:

IMMUTABLE, PRIVATE CLOUD STORAGE

Backupify stores your critical Google Workspace data in an immutable, private cloud separate from SaaS infrastructure. This means your data cannot be altered or deleted, providing robust protection against accidental or malicious changes.

MULTILAYERED SECURITY

Backupify ensures top-notch security with two-factor authentication, allowing only authorized personnel to access your business-critical data. We also use OAuth-based authentication for enhanced security and convenience, safeguarding user data privacy without compromise.

THREE DAILY BACKUPS

Our industry-leading solution automatically backs up your data three times a day, keeping it secure, accessible and always ready for recovery.

GRANULAR RESTORE OPTIONS

Granular restore features in Backupify make data recovery seamless. Find and restore exactly what you need quickly and efficiently.

24/7 BEST-IN-CLASS SUPPORT

Our expert support team is available around the clock. Reach out via chat or phone anytime for immediate assistance.

***Take a quick tour** to discover how Backupify empowers you to protect your Google Workspace data without breaking a sweat.*

Sources:

1 https://www.verizon.com/business/en-gb/resources/reports/dbir/

2 https://www.techtarget.com/searchdatabackup/opinion/Caution-There-are-many-ways-to-lose-SaaS-data

3 https://www.sophos.com/en-us/content/state-of-ransomware

4 https://info.varonis.com/hubfs/Files/docs/research_reports/Varonis-The-Great-SaaS-Data-Exposure.pdf?hsLang=en&_gl=1*geo1iv*_gcl_au*MTcyNzgxNjk0NC4xNzI0NDlyOTI3

5 https://fox59.com/news/national-world/google-outage-impacting-users-worldwide-reports/

6 https://www.techtarget.com/esg-global/research-report/research-report-data-protection-for-saas