Whitepaper

Secure

Your Google Workspace Data

Backup is key!!

Google Workspace data loss is a nightmare for online businesses as it interrupts workflow. The valuable data stored within emails, contacts, calendars, attachments, etc., are essential for smooth operations. The G Suite environment has stringent security policies such as Gmail spam, Two-Step Authentication, and DLP. Still, Google Workspace is prone to get a variety of errors, including virus attacks, server crashes, internal breaches or deletion that might lead to complete data loss.

Businesses often want to export G Suite data to avoid severe downtime scenarios or even permanent damage. That's why Google Workspace backup plays an important role in data protection as well as other business practices.

Need for Backing Up Google Workspace Data!

- **Virus Threat:** Google Workspace can suffer from virus attacks through emails or firewall breaches. It can lead to data inaccessibility or even permanent loss. Data backup helps you to recover data & regain workflow.

- **Accidental deletion:** Deletion of Google Workspace data is possible intentionally or by accident. Data backup assists you to recover data under such situations.

How Our Tool Saved a Company?

The Crisis:

A video production firm lost 3 months of project files due to a silent sync error.

Their old backup tool reported "100% success" but stored corrupted renders.

Kernel Google Workspace Backup's Intervention:

Detected the corruption pattern in daily scans.

Alerted IT before the next backup overwrote good data.

Restored from an uncorrupted version automatically.

The Result:

Zero lost work.

Got a detailed backup report for data analysis.

Code Red: 3 Companies That Nearly Died Due to Data Loss

Organizations that lack data prevention practices have paid a very high price. There are various examples that can help you to learn the importance of Google Workspace data backup.

Example 1. National Public Data (2024)

National Public Data was a US-based background verification and fraud prevention organization. In 2024, the company announced a data loss massacre that resulted in a data breach of about 2.9 billion records. These records have claimed to carry sensitive information of approximately 170 million users from UK, US and Canada. They later announced bankruptcy and were shut down due to the financial impact of the breach. Lack of data backup led to the complete business collapse.

Example 2. Discord.io hack (2023)

Globally renowned organization Discord.io also shut down operations in August 2023 due to a hacking of their main database. It was presumed that this data breach exposed about 0.76 million user information. After that, Discord announced to shut down its operations. This incident highlights the negligence of proper data backups; otherwise, the business would have survived.

Example 3. TravelEx Ransomware Attack (2020)

TravelEX is a UK-based foreign exchange organization that caters to users across the globe with prepaid travel & manages user banknotes. But in 2020, the company was struck by a ransomware attack and lost all the data to intruders. They demanded $6 million, but after $2.3 million payment post negotiation, the company failed to recover complete data. However, if TravelEX had followed a proper backup & disaster recovery plan, they would have easily recovered 100 % of the data.

Why "Just Back It Up" Fails?

The evaluation of the backup failure scenarios is essential for successful export. There are several blind spots in data backup that any user can miss out on.

Blind Spot 1. Moderation of Permission Changes in Shared Drives

- **The Scenario:** An admin modifies folder access from "Anyone in the organization" to "Specific people".
- **The Risk:** It will not affect the automated backups but can impact data file access. Once the update is completed, files become inaccessible to authorized users.
- **The Aftermath:** A financial audit reveals that right people lose data file access due to wrong permission settings.

Blind Spot 2. Incomplete Data Files in Backup Logs

- **The Scenario:** The initiated backup process is displayed as "Success" in the tool report.
- **The Reality:** Output is different as:

    1. Corrupted files are also backed up.
    2. Empty folders are backed up and show as "completed."

- **The Aftermath:** If a ransomware attack hits your Google Workspace environment, failed backups will only restore useless or corrupt files.

Kernel’s Smart Backup Services

Integration of advanced Kernel Google Workspace Backup & Restore solution is the best choice. This automated utility will help you with specific or entire data backups. It offers quality features for error-free results and convenient filters for specific backup. The tool is based on a simple interface which even beginners can use without prior training. Explore the key features & services of this tool:

- Complete data backup from Google Drive, Shared Drive, Google Groups, and Gmail.
- Multiple options to save backups, such as PST, MSG, EML, PDF, DOC, etc.
- Bulk migration features with CSV file import.
- Preserves data integrity and folder hierarchy post backup.
- Easy to run multiple backup processes at one time.