Whitepaper

Why Need for On-Premises Backup of Google Workspace & The Role of Third-Party Solution!

As of 2024, 67.7% of businesses experience significant data loss, with only 32.3% of organizations reporting minimal impact. Google works on a shared responsibility principle, where they protect the data infrastructure, and the responsibility of data loss prevention lies upon users.

Migrating data to cloud storage platforms isn't the one-stop solution you think it is. As per IBM's 2024 Cost of Data Breach report, around 82% of reported data breach incidents happened with data stored in cloud platforms. On the contrary, on-premises storage accounted for a merely 14.4% of data breach incidents. This puts forth a remarkable statistic, highlighting that on-premises environments are still the better choice in terms of control over data and privacy.

Myths of Google Workspace Backup and how it can affect you

Assuming Google provides complete data protection can be disastrous for your organization in case of data loss. We've cleared three most common myths related to Google Workspace Backup below:

How Kernel Google Workspace Backup and Restore saved a business?

Recently, a marketing company lost a sizable amount of its data due to a misconfigured retention policy. Not only did this mishap cost them a lot of money, but this put their business functions to a complete halt.

After one of our regular clients suggested our tool, a representative from this marketing company reached out to our expert team and stated their problem.

The main issue

- Lost 6 months of crucial client files stored on Google Drive.
- Noticed the data loss after the 30-day retention period of Google.

Myth 1: Google offers complete data backup

In reality, Google protects the infrastructure, while users are responsible for protecting data. It introduces timely updates and bug fixes but doesn't protect data against accidental deletions, malicious attacks, sync errors, etc.

Myth 2: Google Vault is enough

Google Vault is a tool designed by Google primarily for retention and compliance purposes. Even though it can retain data, this in-built tool doesn't offer complete data backup and recovery. Apart from that, it not only skips Shared Drive items, but you also can't recover specific emails using this tool.

Myth 3: Cloud Storage is foolproof

Cyber attacks and insider threats are some of the threats that even Google's top-class security can't prevent. A large-scale data breach can essentially wipe out your entire organization's data, with no recovery option.

The suggested solution:

Used Kernel Google Workspace Backup and Restore to backup all the data locally.

Recovered almost all the lost data with original structure and metadata.

The bottom line?

Businesses relying primarily on Google's native tools face these risks regularly:

Permanent data loss due to retention policy gaps.

No protection against cyberthreats and accidental deletions.

If the retention policies aren't configured correctly, it can lead to legal issues for businesses.

Why is Google Workspace backup necessary?

If you don't wish to lose your crucial data permanently, it's extremely necessary to take periodic backups of your data. Go through some common reasons why we believe Google Workspace backup is essential.

- **Cyber-threats:** Risks like malware/virus attacks or a phishing attack put your data in a vulnerable position.

- **Legal and regulatory compliance:** Organizations bound to regulations like GDPR, HIPAA, CCPA, etc., need to comply with rigid standards for legal requirements. These regulations require organizations to retain their data for an extended period of time for legal or regulatory reasons.

- **Accidental deletion:** Users might delete crucial emails intentionally or by accident, leading to significant data loss.

Benefits of shifting to On-Premises storage

Even though cloud-based platforms are convenient, many organizations still prefer traditional on-premises storage for data privacy and security control.

Better security features

- Cloud-based platforms are vulnerable to data breaches and ransomware attacks. Storing data on on-premises servers isolates the data to the local system.

- Unlike cloud platforms, when you store your data on on-premises platforms, the sole ownership of encryption keys stays with you.

- Certain industries require their data backups to be stored on local servers for legal and regulatory purposes.

Quicker data recovery and minimal downtime

- Recovering backups from cloud platforms may take time, especially if the data is in large volume. Compared to that, you can restore data from on-premises storage almost instantly.
- You can perform granular recovery from on-premises backups.
- On-premises backups are still accessible even when there's an internet outage or if Google experiences downtime.

Bridging the Gap: Google's Native Tools with a Backup Strategy

Let's talk about two native tools offered by Google; Google Vault and Google Takeout.

Google Vault

Google Vault is a data retention and eDiscovery tool developed by Google for compliance purposes. It preserves crucial data with set retention policies to help organizations meet legal and regulatory requirements.

What Google Vault can do?

- **Retention policies:** Can set specific rules to preserve mailbox data, like emails, documents, and chat messages, for a set period of time.
- **Legal compliance:** Can preserve data for a long time for compliance purposes.
- **Regulatory compliance:** Meets regulatory requirements of standards like GDPR, HIPAA, CCPA, etc. for record keeping.

What Google Vault can't do?

- **Point-in-Time recovery isn't possible:** Vault cannot restore a corrupted mailbox item to its previous state. Also, recovering a single specific email or file isn't possible with Google Vault.

- **Loss of data due to retention failure:** There's no way to recover lost data once a retention policy expires. Furthermore, you might accidentally clear up all your data while improperly configuring retention policies.

- **Can't restore accidentally deleted data:** Google Vault can't restore data that got lost due to accidental deletion or sync errors.

When is Google Vault useful?

- Setting up retention policies and basic compliance needs.

- Enhancing a strong backup strategy.

Google Takeout

Google Takeout is a widely known data export tool developed by Google that helps users back up their Google Workspace data, including emails, media files, documents, calendars, etc.

What Google Takeout can do?

- **Easy backup of data:** Backup Google data like emails, documents, calendars, contacts, etc., to the location of your choice.

- **Schedule backup process:** Either choose to export data once or schedule the export process for a set period.

- **Create personal backups/archives:** Google Takeout easily exports data to the location of choice while migrating data or creating backups.

What Google Takeout can’t do?

- **Incremental backup isn’t possible:** Users can’t skip already-backed items and backup specific required mailbox items. Every export process creates a copy of the entire data, leading to data duplicity.

- **Granular recovery isn’t possible:** It’s not possible to backup an individual file or an email with Google Takeout. Moreover, this in-built tool only exports healthy files and emails.

When should you opt for a comprehensive backup solution?

You should opt for a complete backup solution if these are your backup goals:

- Granular data recovery.

- Recovering accidentally deleted or lost data.

- Retaining data for an extended period of time

- Backup large-sized mailboxes easily