

Google Workspace: The Critical Gaps

Addressing the missing layers of data protection

May 2025

H04519

White Paper

Abstract

This document describes the need for third – party solutions for Google Workspace to address data protection gaps, highlighting risks like data loss and legal pitfalls.

Copyright

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2025 Dell Inc. or its subsidiaries. Published in the USA May 2025 H04519.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Executive summary.....4

What’s Missing from Google Workspace that will put your data at a risk?5

Cloud data gets lost.....5

The big takeaways.....10

Executive summary

Overview

While the rapid adoption of SaaS-based applications has been fueled by the unique advantages of cloud-based apps for remote workforces, it is essential to note that increased data sprawl and endpoints have opened the door for cyber criminals to compromise your data.

Revisions

Date	Part number/ revision	Description
May 2025	H04519	Initial release

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by [email](#).

Author: Adeola Adelugba

Note: For links to other documentation for this topic, see [PowerProtect Backup Services InfoHub](#).

What's missing from Google Workspace that will put your data at a risk?

The SaaS market grew to approximately \$145.5 billion in 2021 according to Statista¹, and could be worth more than \$300 billion by 2026 according to Valuates Reports². Overall, the SaaS market is expected to continue growing as organizations look for flexibility, increased functionality, and affordability to support a variety of business functions and workflows. This increase in SaaS usage means a proportional growth in the movement of customer business data from on-premises to cloud instances.

Forrester Research strongly recommends organizations deployed on Google Workspace use third-party solutions to address gaps in its native capabilities, particularly for backup and recovery, ransomware recovery, advanced threat protection, encryption, and business continuity. While Google Workspace includes some capabilities, the productivity suite contains some deficiencies that purpose-built, third-party solutions can address more reliably. And frequently, these solutions come with a better price point than Google offers.

Here are a few key reasons why having third-party data availability and governance in conjunction with Google Workspace provides major benefits and capabilities, such as more comprehensive data protection for reliability and confidence in addition to a reasonable price point for any organization.

Cloud data gets lost

Different business units in your organization probably use Google Workspace and assume that because their data is in the cloud it's safe. But it's not. And, ultimately, IT — not the business units — is responsible for managing and protecting the data successfully and carries the burden of regulatory compliance and legal obligations.

Here are two of the most common ways that cloud data gets lost:

Users make mistakes

Google automatically deletes files 30 days after they're sent to the recycle bin. What's wrong with that? Project status can frequently fluctuate. An intern may try to show initiative and clean up files after a big campaign is canceled. A month later, the campaign is back on. Where's the data?

Malicious users wreak havoc

When an employee feels they've been treated badly and their job is in jeopardy, there's no telling how they'll react. If they are the proactive sort, by the time they pack their things and are "walked out," it's too late. Even within the smallest organizations, it only takes one untrustworthy person to put your data — and your business — at risk.

Data Recovery gaps

Google provides cloud-based solutions that are essential to businesses around the globe. But do major SaaS providers like Google protect their customers' data with backup and recovery? Why would anyone need additional protection for data that's already in the cloud? It turns out that cloud providers such as Google do indeed offer different levels of recovery, largely to ensure data accessibility and save themselves and their clients from data loss. But here's the catch: Such backups are not intended to make all data available

to customers. With most online services, the only backup you have for your organization's data is via the recycle/trash folder, which is automatically purged after a fixed period of time. After that, your data is gone forever.

Once your data is deleted, altered, or corrupted — whether accidentally or intentionally — there is very little an admin can do to recover it.

Drive file stream is not data protection



Recovery Scenario	Google Drive File Stream	PowerProtect Backup Services
Recovering Drive File Stream contents: Drive contents (including team drives) can easily be deleted, corrupted, accidentally overwritten, or encrypted by ransomware. What happens when the organization needs those lost Drive files?	Because Drive File Stream syncs changes across devices, a file that is deleted, corrupted, or infected by a virus on one device will sync to all your devices and could lead to data loss. Moreover, because the trash folder in Drive File Stream only stores files for 30 days, if the error isn't discovered in time, the data is gone for good.	An end user or admin can search for the files or view their Drive exactly how it looked at any point in time. An end user can then restore their files directly back into their Google account, and an admin can restore Drive files into whichever account they prefer.
Legal hold for Drive File Stream contents: What happens when an organization needs to place an employee on legal hold?	<p>In the event of a legal hold, Drive File Stream isn't useful, since it does not preserve data indefinitely to meet legal or preservation obligations.</p> <p>Legal Hold in Google Workspace requires the use of Google Vault, which only captures data in Google Workspace and not on the end user's device.</p>	With a single click, administrators can initiate a legal hold policy, preserving user backup data and avoiding data deletion for Google Workspace files as well as data that resides on end-user devices. PowerProtect Backup Services does not delete the data that the user backs up from any user device.

Recovery Scenario	Google Drive File Stream	PowerProtect Backup Services
Archival to address compliance needs: What happens when the organization needs to archive data to adhere to regulatory obligations and/or to monitor for potential data risks.	Drive File Stream isn't useful for archival purposes as it does not preserve data indefinitely. When a user deletes a file stored in one location, Drive File Stream moves that file to their trash folder, which gets auto purged after 30 days. Archival in Google Workspace requires the use of Google Vault, which only captures emails and chats.	Automated policy-based archival management ensures that all types of information can be easily obtained for a specified period to meet the strict guidelines for compliance with regulations like HIPPA or Sarbanes Oxley.

Google Vault backup and recovery gaps

Another Google product that is often mistaken for backup is Google Vault, which is primarily an archiving and eDiscovery tool which can provide some “backup-like” capabilities, such as the ability to set retention policies that control the availability of Gmail content. Some Google administrators may think that Vault is a “good enough” tool to use for backup and restore, as well as for eDiscovery and archiving. While Vault can be a solution for data retention for legal needs, it doesn't meet the primary use case for backup and restore-business continuity.

Most importantly, Vault isn't purpose-built to enable rapid, granular restores from any point in time. The table below outlines the backup and restore functionality of Google Vault versus PowerProtect Backup Services for Google Workspace.

Recovery Scenario	Google Vault	PowerProtect Backup Services
Global data search capabilities	Only data that resides inside of Google can be searched.	PowerProtect Backup Services enables central data searches across all Google Workspace files as well as all files residing on user endpoints.
Non-active user data retention for litigation	Requires a user to maintain an active Google Workspace license.	PowerProtect Backup Services preserved user license enables archival of non-active end-user data across Google Workspace as well as all files residing on user endpoints.
Third-party eDiscovery tool integration	No integration with third-party eDiscovery tools for exporting search results.	API integration with the leading eDiscovery tools for seamless exporting of search results.
Compliance management	No predefined, customizable, or policy-based templates for regulatory compliance.	Customizable templates have been built within the PowerProtect Backup Services platform to enable

Recovery Scenario	Google Vault	PowerProtect Backup Services
	Compliance management for Gmail messages only.	enterprise compliance with regulations like HIPAA, FINRA, Sarbanes-Oxley, FRCP, and others.
Data residency and access controls	No control of where the data is stored, who can see it and how it is being used.	Data residency and accessibility can easily be applied to users based on the needs of the business.


















Here's how each one addresses various aspects of archiving.


Archiving Functionality	Google Vault	PowerProtect Backup Service
Offers granular Gmail and Drive retention policies	Yes	Yes
Google Workspace data retained	Gmail, Hangouts, chat, Google Talk chat, Groups, and Drive	PowerProtect Backup Services retains all enterprise Google Workspace data including Gmail, Drive, Calendars, Contacts and Sites
Ability to archive data outside of Google Workspace	No	Yes (endpoints and other cloud apps such as Office365, Box and Salesforce)
Cost of archiving accounts for former employees	Vault requires a user to maintain an active Google Workspace license priced at \$120/user/year	PowerProtect Backup Services preserved user license is priced at \$24 user/year

How PowerProtect Backup Services fits in

PowerProtect Backup Services helps some of the world's largest enterprises, in addition to small to mid-sized businesses, protect their investment in Google Workspace from data loss and compliance violations. PowerProtect Backup Services gives users a single pane of glass to monitor and protect data no matter where it resides.

Feature	Google Workspace	PowerProtect Backup Services
Data Protection		
Continuous data protection of endpoints	X	✓ Windows/Linux/Mac
Continuous data protection of cloud applications	X	✓ Google Workspace, Microsoft 365, Salesforce

Feature	Google Workspace	PowerProtect Backup Services
User self-service deploy and restore		 IOS & Android
System and application settings backup		 For OS Migration & Device Refreshes
Data backup for smartphone & tablets		
Data Governance		
Proactive compliance & eDiscovery for endpoints		
Proactive compliance for content compliance policies	Gmail messages only	 Google Workspace (Gmail, Drive), Microsoft 365, Box and Salesforce
Long-term retention for legal eDiscovery purposes	Google Workspace only	 Endpoints & cloud apps (Google Workspace, Microsoft 365, Box & Salesforce)
Direct access for eDiscovery platforms		 AccessData, Recommind, DISCO & Exterro
Anomaly detection for ransomware		 Continuously monitor snapshots for signs of ransomware intrusion such as modified or deleted files, MIME type changes and file encryptions
Network encryption (in flight)	Gmail uses TLS by default, but when a secure connection isn't available Gmail will deliver messages over non-secure connections	 All data is protected in-flight using Transport Layer Security (TLS)
Network encryption (in flight)	Google encrypts data as written to disk using 128-bit or stronger Advanced Encryption Standard (AES)	 When data arrives it's immediately encrypted using AES 256-bit encryption
Encryption key management	Google authorizes access to systems and data repositories containing customer data. This extends to job duties including debugging and maintenance activities that can expose decrypted customer data to employees.	 Unique encryption keys are under customer control. PowerProtect Backup Services has no access to this encryption key or customer data. Key is session-based modeled on envelope encryption and results in

Feature	Google Workspace	PowerProtect Backup Services
		customer key never being stored, transferred or accessible from outside a user's active cloud session
Data loss prevention	Limited to mobile devices: Android, iOS and Windows phone via Google's Mobile Management feature	 Flexible backup and recovery for end user devices, remote device encryption and sanitization, geolocation, geofencing and role-based access controls

The big takeaways

There are two critical issues after reading what is offered by Google Workspace:

1. Hidden data retention gaps

By ignoring the data retention gaps within Google Workspace, you are relinquishing control of your organization's business-critical information and putting it entirely in the hands of the end users. This puts the burden of data retention — and compliance — solely on the shoulders of those who may have no understanding of what is needed to manage company data correctly and who may inadvertently (or intentionally) destroy it.

2. Legal pitfalls

Most litigation takes weeks, if not months, to reach a stage at which custodians are identified, and data is put on legal hold. By the time this happens, all relevant data could be lost under any of the scenarios outlined above.

PowerProtect Backup Services provides the essential layer of data-protection functionality that enterprises need to defensibly archive and discover business-critical information, adding to the core of Google Workspace without sacrificing security or compliance across four crucial areas of exposure:

- Protection of all end-user data
- Data recovery
- Data governance
- Third-party managing archival

Safeguard and centrally manage data across multi-cloud environments, including SaaS applications like Google Workspace, with secure, scalable, cloud-native backup and disaster recovery. Visit the PowerProtect Backup Services website to learn more Dell.com/APEX-Backup