druva

White paper

G Suite: The critical gaps

Addressing the missing layers of data protection

Q420-20092

What's missing from G Suite?

While the rapid adoption of SaaS-based applications has been fueled by the unique advantages of the cloud, it is essential to note that no offering—cloud-based or otherwise—can be all things to all customers.

In fact, Forrester Research strongly recommends organizations deployed on G Suite use third-party offerings to address gaps in its native capabilities. These third-party features include those that fill gaps for backup and recovery, ransomware recovery, advanced threat protection, encryption, and business continuity. While G Suite includes a number of these capabilities, the platform cannot do everything, so it contains some deficiencies that purpose-built, third-party offerings can more adequately address. Oftentimes, these offerings come with a better price point than Google offers.

> *The SaaS market will grow to $157 billion in 2020; some providers have more than $1 billion in revenue and are growing strongly. This rapid increase in SaaS usage means a proportional growth in the movement of customer business data from on-premises to cloud instances.*
>
> — Forrester Research

Here are few key reasons why having a third-party data availability and governance offering in conjunction with G Suite is critical and provides major benefits in capabilities and price point for any organization.

Cloud data gets lost

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

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

1. Users make mistakes.

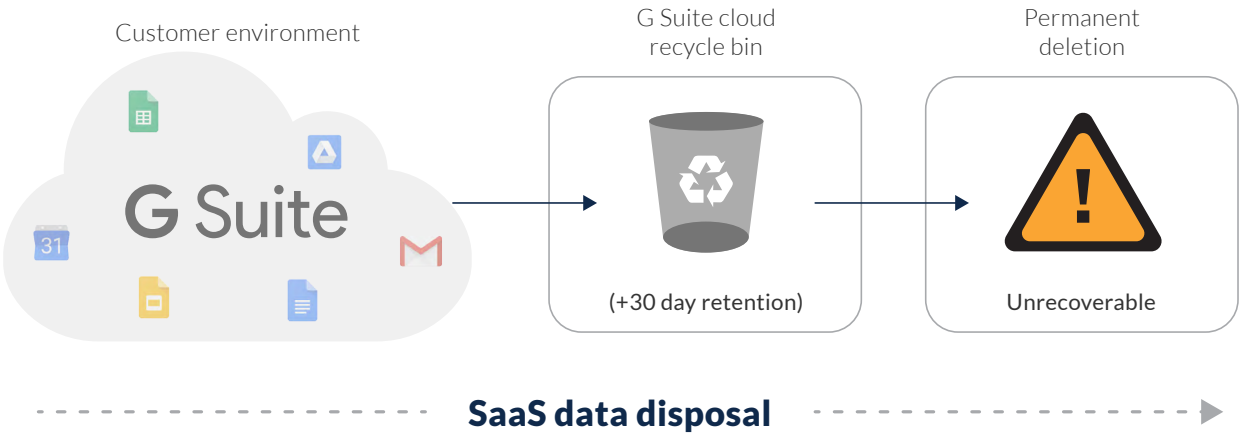
Google automatically deletes files 30 days after they're sent to the recycle bin. What's wrong with that? Project statuses fluctuate. An intern may try to show initiative and clean up files after a big campaign is canceled. A month later, the campaign is back on. Where's the data?

2. 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 are "walked out" it's too late. Even within the smallest organizations, untrustworthy people are a reality

Data recovery gaps

Leading online service providers such as Google offer cloud-based information solutions that are essential to business operations around the globe. But do these major SaaS providers protect their customers' data with backup and recovery? Why would anyone want 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. Generally speaking, in 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.



The truth is that 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	Druva inSync
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 of 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?	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. Legal Hold in G Suite requires the use of Google Vault, which only captures data in G Suite and not on the end user's device.	With a single click, administrators can initiate a legal hold policy, preserving user backup data and avoiding data deletion for G Suite files as well as data that resides on end user devices. inSync does not delete the data that the user backs up from any user device.
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 G Suite 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 of time in order 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. Google Vault is now part of G Suite Enterprise edition. For a detailed comparison of Google Vault and Druva, please see the table below. **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 Druva inSync backup for G Suite.**

Recovery scenario	Google Vault	Druva inSync
Recovering emails: A malicious insider deleted emails and then emptied the trash folder in an attempt to harm the organization.	The end user must contact an admin to find the emails. Once the emails are located, the admin can export them to an .mbox or .pst file format and then manually upload them back into the user's Google account using a tool like Thunderbird. Any labels that were previously attached will be lost.	The end user uses the search function to find the emails, then simply clicks to restore them directly to Gmail, with all labels intact.
Recovering Drive 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?	In the event of a ransomware attack, Vault isn't useful, since it doesn't include previous versions of non-native Google files like Microsoft Word, Powerpoint and Excel—the last-known-good version before the attack. In the case of simple loss or data corruption, a user must contact an admin, who must then search for the specific Drive contents in order to find the file. Note that Vault only searches the latest version of the Drive files, and does not include deleted files. An admin would then download the file, and manually import them back into Drive. These files do not retain any sharing settings.	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.

Google Vault litigation and archiving gaps

Vault is designed for archiving and data retention, but not for data backup and restore. On the other hand, Druva inSync was designed to backup and restore data, but it can also handle archiving and data retention—even for data outside of G Suite. In many cases, Druva inSync can do it in a more cost-effective manner as Druva does not require users to maintain an active user license in the case of a departing employee.

The table below outlines the legal and compliance functionality of Google Vault versus Druva inSync backup for G Suite.

Legal and compliance functionality	Google Vault	Druva inSync
Global data search capabilities	Only data that resides inside of Google can be searched.	Druva enables central data searches across all G Suite files as well as all files residing on user endpoints.
Non-active user data retention for litigation	Requires a user to maintain an active G Suite license.	Druva's preserved user license enables archival of non-active end user data across G Suite 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. Compliance management for Gmail messages only.	Customizable templates have been built within the Druva platform to enable 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 might be 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	Druva inSync
Offers granular Gmail and Drive retention policies	Yes.	Yes.
G Suite data retained	Gmail, Hangouts chat, Google Talk chat, Groups, and Drive.	Druva retains all G Suite data including Gmail, Drive, Calendars, Contacts, and Sites.
Ability to archive data outside of G Suite	No.	Yes (endpoints, and other cloud apps such as Office 365, Box, and Salesforce).
Cost of archiving accounts for former employees	Vault requires a user to maintain an active G Suite license priced at $120/ user/year.	Druva's preserved user license is priced at $24 user/year.

How Druva fits in

Druva helps some of the world's largest organizations protect their investment in G Suite from data loss and compliance violations. Druva's industry-leading solutions give users a single pane of glass to monitor and protect data no matter where it resides.

Druva is the essential layer of data-protection functionality companies need to defensibly archive and discover business-critical information, adding to the core of G Suite 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

Feature comparison

Feature	Google G Suite	Druva inSync
Data protection		
Continuous data protection of endpoints	✗	✓ Windows/Linux/Mac
Continuous data protection of cloud applications	✗	✓ G Suite, Office 365, Box & Salesforce
User self-service deploy and restore	✗	✓ iOS and Android
System and application settings backup	✗	✓ For OS migration and device refreshes
Data backup for smartphones & tablets	✗	✓
Data governance		
Proactive compliance & eDiscovery for endpoints	✗	✓
Proactive compliance for content compliance policies	⚠ Gmail messages only	✓ G Suite (Gmail, Drive), Office 365, Box & Salesforce
Long-term retention for legal eDiscovery purposes	✓ G Suite only	✓ Endpoints & Cloud Apps (G Suite, Office 365, Box & Salesforce)
Direct access for eDiscovery platforms	✗	✓ Direct access for eDiscovery platforms (e.g. AccessData, Recommind, DISCO, Exterro)

Security		
Anomaly detection for ransomware	✗	✓ Continuously monitor snapshots for signs of a ransomware intrusion such as modified or deleted files, MIME type changes and file encryptions.
Network encryption (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 that Druva sends to the cloud is protected while in flight using industry-standard Transport Layer Security (TLS).
Storage encryption (encryption at rest)	✓ Google encrypts data as it is written to disk using 128-bit or stronger Advanced Encryption Standard (AES).	✓ Once the data arrives in the Druva Cloud Platform, it's immediately encrypted using AES 256-bit encryption.
Encryption key management	⚠ Google authorizes certain individuals to have access to systems and data repositories containing customer data. This authorization extends to job duties including debugging and maintenance activities that can expose decrypted customer data to an employee.	✓ The encryption keys are unique to, and completely controlled by the customer. Druva has no access to this encryption keys or customer data. This customer encryption key is a session-only based key algorithm modeled on digital envelope encryption and results in the customer key never being stored, transferred or accessible fromoutside a user's active cloud-side session.
Data loss prevention	⚠ Limited to mobile devices such as 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

Consider these two critical issues after reading what is offered by G Suite:

Hidden gaps

By ignoring the data retention gaps within G Suite, 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 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.

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.

Learn how to address the critical gaps in your G Suite data protection capabilities at our SaaS applications solution page.

druva

Sales: +1 800-375-0160 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.