Acronis

WHITEPAPER

Six costly G Suite data threats and how to fix them

Get easy, efficient and secure cloud backup for G Suite data with Acronis

TRY NOW

A DATA LOSS DISASTER IS JUST WAITING TO HAPPEN

If your business depends on G Suite, you can expect reliable access to its applications with very high uptime. But many IT professionals are laboring under a dangerous misconception: that Google provides fully-fledged data protection and long-term data retention for G Suite.

The reality is that the emails, attachments, calendar events, contacts, and files stored in G Suite are not protected from the most common and serious data loss issues, ranging from simple accidental deletions to sophisticated malware attacks.

Thus for many organizations, G Suite usage leaves a major data protection gap, an unhappy surprise waiting to happen. Too late, they may learn that Google provides only limited features to help restore lost, destroyed or damaged G Suite data, with nowhere near the backup functionality or robustness with which most businesses protect their other critical applications.

> This paper outlines several easy-to-miss limitations of Google's data protection capabilities, and examines how you can address those shortcomings to ensure that you can quickly recover from the many data loss issues to which G Suite is vulnerable.

TOP 6 DATA SECURITY THREATS YOUR BUSINESS CAN FACE WHILE USING G SUITE.

Google has invested heavily in its data centers' hardware, software, networks, security and operations to ensure high performance, access and uptime for G Suite. Its primary goals are basic infrastructure resilience, the ability to recover from major natural disasters (e.g. floods, earthquakes, hurricanes), and some limited, short-term recovery of lost or corrupted G Suite data.

This means that Google can quickly detect and recover from many of its own cloud data center operational errors, outages, hardware failures and network issues to meet its service-level agreements, which center on application uptime. But these measures do not protect your business from many common G Suite data loss issues, including accidental or malicious data deletion by employees, and external assaults on data integrity like ransomware and other malware attacks. Further, it is easy and fairly common for IT administrators to set overly aggressive (i.e. too short) retention periods for Gmail emails, leading to the swift deletion of messages that might be needed later, at which point Google cannot restore them.

> Google is able to restore most G Suite data resources for a short time after they have been deleted by a user or administrator (by default, 25 days for Gmail messages and Drive files, 20 days for user profiles). You may determine that a long-idle project or a former employee's emails or files are important again, but after a time-consuming search, you discover that Google did not retain a copy that you can recover.

CYBER-THREATS	MALICIOUS INSIDERS
DEPARTING EMPLOYEES	RETENTION POLICY GAPS
ACCIDENTAL DELETION ISSUES	LEGAL / COMPLIANCE ISSUES

G SUITE ADMINISTRATORS NEED TO ADDRESS DATA THREATS IN SIX KEY AREAS

1. Accidental deletion issues

DATA RISK: In the course of their daily work, IT administrators and ordinary employees routinely delete G Suite user profiles, Gmail emails and attachments, Calendar events, Contacts and Google Drive files. These deletions may be accidental in nature, or intentional but later regretted – most of us have suddenly needed to refer to an email that we deleted only yesterday.

GOOGLE WEAKNESS: Such everyday resource deletions are routinely replicated across the network. Of course, the age of the resource exacerbates the problem: older data may be hard-deleted and unrecoverable. More recent deletions of newer resources are slightly less problematic, as soft-deleted files and emails may be recoverable in the short term from the Trash / Recycle Bin or Recoverable Items folder.

2. Malicious insiders

DATA RISK: In addition to routine, non-malicious deletions, G Suite resources need protection from malicious alteration or data destruction by disgruntled or criminal employees, contractors or partners.

GOOGLE WEAKNESS: With the exception of relatively recent resource deletions, Google does not protect against malicious insider destruction or alteration of G Suite data. After all, they have no way of knowing what constitutes a threat or not.

3. Cyber-threats

DATA RISK: G Suite data is vulnerable to destruction or alteration by a variety of malware threats, notably ransomware, which encrypts user data and holds it hostage until an online ransom is paid. These attacks may be mounted by hackers, cybercriminals or hostile state actors.

GOOGLE WEAKNESS: Google offers very limited protections against malware attacks like ransomware, and has a restricted ability to restore malware-encrypted or -altered files to their pre-attack state.

4. Departing employees

DATA RISK: Companies frequently make the error of terminating the G Suite accounts of departing or terminated employees without saving their data.

GOOGLE WEAKNESS: With the exception of recent terminations of G Suite accounts (i.e. in the last 20 days), Google cannot restore a deleted user's G Suite data.

5. Retention policy gaps

DATA RISK: Changing or misaligned priorities in G Suite data retention policies can result in data being hard-deleted before its usefulness has expired. This can be only partially mitigated by regular reviewing and updating of retention policies.

GOOGLE WEAKNESS: G Suite customers have the onus of managing retention policies, but if for whatever reason a hard-deletion occurs due to aging out of the existing retention policy, Google is unable to recover the deleted resource.

6. Legal and compliance issues

DATA RISK: Compliance requirements (e.g. storing tax documents for a mandated period) and legal issues can exacerbate the business costs of the unprotected data losses described above. Unrecoverable G Suite data loss can expose the business to government or industry-specific regulatory fines, legal penalties (e.g. damages or lost lawsuits stemming from failure to meet e-discovery or evidentiary requirements), revenue and stock price losses, loss of customer trust, and damage to the company brand.

GOOGLE WEAKNESS: With all of the associated data loss risks described above, Google can do little to protect organizations using G Suite against a variety of compliance and legal exposures. For example, after a ransomware attack, a business storing its EU-based customers' personal data in G Suite might be unable to honor requests for copies of that data, thereby violating GDPR requirements.

THE BOTTOM LINE

Once you understand the various soft spots in Google's ability to protect G Suite data, you can start looking at data protection solutions that address those gaps. We all know the stakes are high: failure to defend against G Suite data loss can be career-limiting.

ACRONIS BACKUP PROVIDES EASY, EFFICIENT AND SECURE CLOUD BACKUP FOR G SUITE

EASY TO USE CLOUD-TO-CLOUD G SUITE BACKUP

Acronis Backup protects G Suite data with direct, agentless backup from Google data centers to the Acronis global network of data centers. The Acronis Backup agent runs in the secure Acronis Cloud instead of on premises, streamlining and simplifying the process of configuration and maintenance.

HIGHLY GRANULAR RECOVERY FOR G SUITE

Acronis Backup offers a range of enhanced recovery features that make it easy to quickly restore a variety of G Suite items. These highly granular recovery features make it possible to download a required file directly from the backup, to download any of multiple versions of documents (not only the most recent one), or to restore any data element to its original location or to a new destination.

ADVANCED SEARCH CAPABILITIES

With convenient and easy search functionality, it is possible to quickly find data you need, such as a departed employee’s email or a legacy document required to resolve legal issues. For Gmail, customers can evaluate metadata search for mailboxes – searching by email subject, recipient, sender, attachment file name and date, or use full-text search to find data in email body content. For Drive, Contacts and Calendar, customers can search by metadata like file names.

UNIQUE BLOCKCHAIN-BASED NOTARIZATION FOR GOOGLE DRIVE DATA

Businesses backing up their Google Drives via Acronis Backup can take advantage of the built-in Acronis Notary service, which uses blockchain technology to verify that Google Drive backups have not been tampered with. This ability to attest to the integrity of your Google Drive backups is especially useful for legal documents, contracts, media files, surveillance camera footage, medical records, rental or lease agreements, and loan agreements.

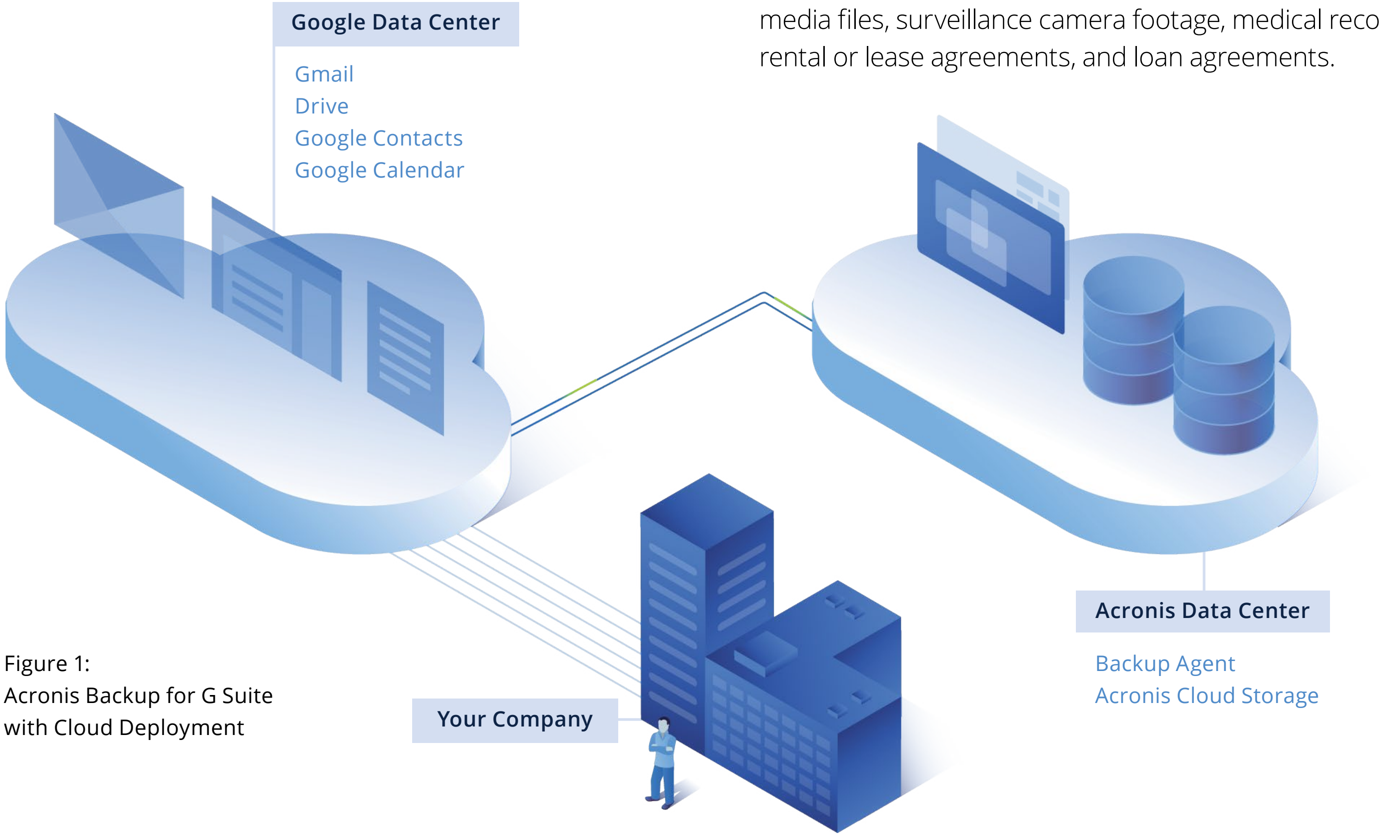

Figure 1:
Acronis Backup for G Suite
with Cloud Deployment

ENHANCED PRIVACY FOR DATA

Acronis Backup protects data against prying eyes with multi-level backup encryption reinforced by data transfers over the network with TLS encryption, data-center storage with high-grade disk-level encryption, and per-archive encryption using AES-256.

AUTO-DISCOVERY OF NEW G SUITE USERS AND TEAM DRIVES

Once an initial group backup plan has been configured and enabled for a G Suite environment, IT staff does not have to worry about having to modify it every time a new G Suite user, or Team Drive is added. Acronis Backup automatically detects when these have been added and updates the backup plan to include them.

SUPPORT FOR GOOGLE MULTI-FACTOR AUTHENTICATION

Acronis supports Google multi-factor authentication (MFA) to enable the use of additional authentication measures, like trusted devices or fingerprints. Without MFA, only a password is required for verification

POWERFUL REPORTING AND STATUS MONITORING

Acronis provides advanced reporting and backup-status monitoring capabilities to help IT staffers improve their efficiency and responsiveness. The Acronis management portal contains compact, easy-to-understand widgets containing all statistics for backup and restoration as well as reports, notifications and alerts for critical events.

HIGHLY SECURE ACRONIS CLOUD

Acronis backs up G Suite data to the Acronis Cloud, a global network of data centers secured via a comprehensive information security and compliance program that includes administrative, physical and technical controls based on ongoing risk assessment.

Our information security policies and processes are based on broadly accepted international security standards such as ISO 27001 and the National Institute of Standards and Technology (NIST), and take into account the requirements of related local regulation frameworks such as Europe's General Data Protection Regulation (GDPR) and the United States' Health Insurance Portability and Accountability Act (HIPAA). Acronis Cloud security features include:

- **Enterprise-wide access control** based on unique user IDs and strong passwords, secure authentication protocols (LDAP, Kerberos, SSH certificates), two-factor authentication, and the use of web application firewalls
- **Multi-layered, zone-based data security** buttressed by real-time data encryption in transit and at rest, secure data transfer over HTTPS (TLS), enterprise-grade AES-256 encryption for customer data, and Acronis Cloud RAID technology for maximum data availability
- **Rigorous, high-fences physical security** with access controlled by biometric hand-geometry scans and proximity key cards, video surveillance backed up by 90-day archiving, and staffed by security personnel 24x7x365
- **Highly available, redundant data center** infrastructure protected by UPS and backup diesel-generators, redundant HVAC, network and UPS, VESDA air sampling and dual zone pre-action (dry pipe) sprinkler systems, plus temperature and humidity monitoring

ACRONIS PROTECTS YOUR G SUITE ENVIRONMENT (AND EVERYTHING ELSE, TOO)

Acronis Backup is a **single data protection solution for your entire IT environment,** whether your workloads are premises-based, or hosted in private or public clouds.

That includes **a broad range of platforms** and applications, including physical, virtual and cloud environments, servers running any of the major operating systems (OSes) and hypervisors, a variety of popular applications and databases, plus desktop OSes (including macOS) and mobile OSes like iOS and Android.

A single data protection platform for your entire IT environment eliminates the mutual incompatibility of standalone premises-only and cloud-only backup solutions. It also reduces the cost of licensing, education and integration. Figure 2 shows the 20+ platforms protected by **Acronis Backup.**

Further, the Acronis Backup user interface is simple enough to be run by IT generalists, allowing you to ramp up new data protection staffers quickly and save on implementation, maintenance and daily operations costs.

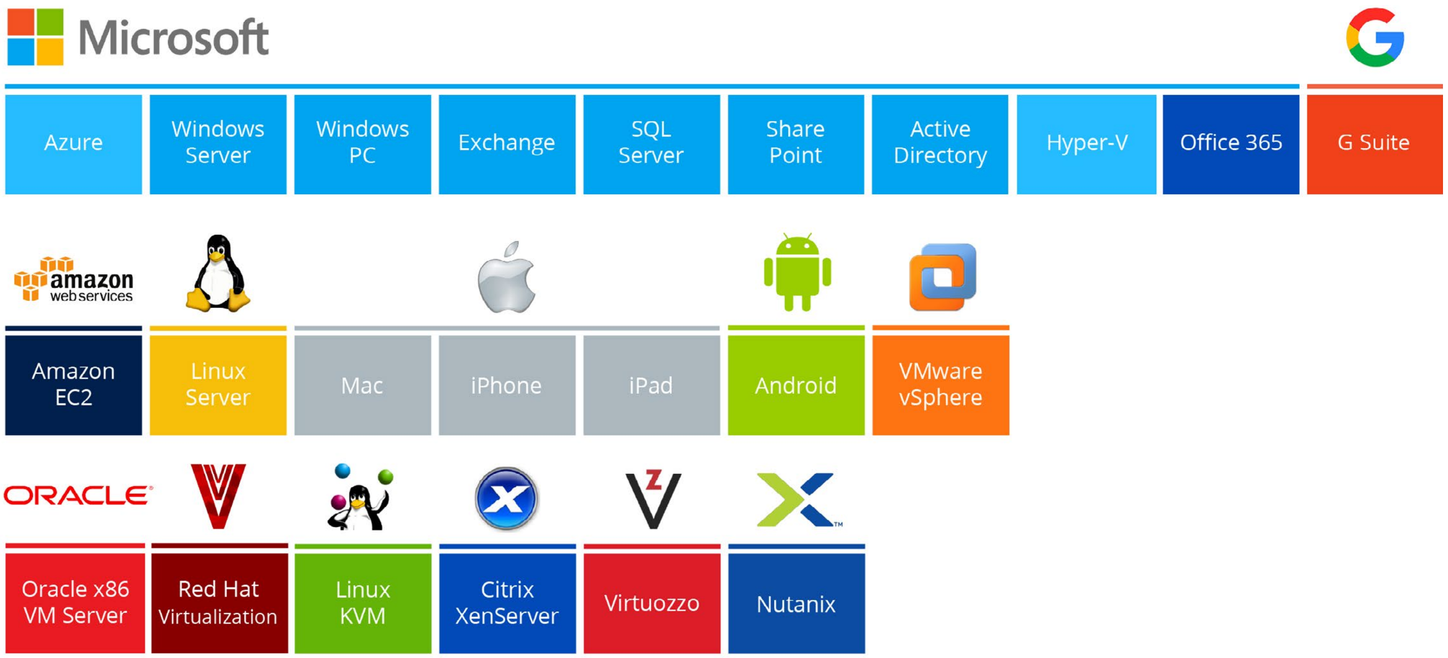

Figure 2. Platforms Protected by Acronis Backup

CONCLUSION

If your business relies on G Suite, you need to complement Google's limited data protection with Acronis Backup, the most reliable and easy-to-use backup for businesses of all sizes.

To learn more about **how Acronis Backup can greatly improve,** simplify and reduce the cost of protecting your G Suite data, get a complimentary 30-day trial here, or find an Acronis reseller here.

Acronis

Learn more at
www.acronis.com