Druva for Google Workspace Data Protection

Druva provides a comprehensive, scalable, and cost-effective 100% SaaS-based platform to protect Google Workspace data, including Gmail, Google Drive, Contacts, Calendars, and Shared Drives. It protects customer data from common risks like accidental deletion, file corruption, insider attacks, ransomware, non-compliance with immutable, air-gapped backups, long term data retention, legal hold, and eDiscovery. Druva's data protection platform seamlessly supports other cloud applications and endpoints to provide comprehensive data resiliency across the entire IT environment.

The challenge

The rapid adoption of SaaS applications such as Google Workspace is fueled by the scalability and flexibility of the cloud. However, under the shared responsibility model, while Google secures the underlying infrastructure, organizations remain responsible for protecting their own data, access policies, and configurations.

- **Shared responsibility gaps**: Google Workspace ensures service availability, but customers must protect their data, requiring third-party backup solutions for true recovery and long-term retention.
- **Cloud data loss risks**: User errors, malicious insiders, and external attacks (ransomware/malware) can cause significant data loss despite cloud storage.
- **Data recovery limits**: Google's native tools like trash recovery and Vault have time and scope limits, lacking comprehensive backup against deletion, corruption, or overwrites.

The solution

Native Google Workspace capabilities can leave critical data protection gaps, which is why SaaS providers themselves recommend third-party protection solutions. Druva Data Security Cloud simplifies the monitoring, management, protection, and recovery of Google Workspace data — no matter where it resides.

Data backup and retention, 100% in the cloud

Google Workspace files are backed up directly from Google Cloud Platform to the Druva Data Security Cloud. As a 100% SaaS platform, Druva customers are freed from additional cloud storage or hardware costs. Agentless architecture improves recovery performance and avoids taxing your WAN bandwidth or latency. Druva offers customizable data retention for Google Workspace to meet all your data retention and compliance needs.

Data recovery for the strictest RPO/RTOs

An end user or admin can search for files or view their Drive exactly how it looked at any point in time. End users can then restore files directly back into their Google account, and an admin can restore Drive files into whichever account they prefer.

Zero-trust data security and privacy

Druva is compliant with SOC 1, ISAE 3402, SOC 2, SOC 3, ISO 27001, PCI DSSLevel 1 (Cloud), and HIPAA regulations. If you are a contractor of the U.S. federal government, Druva is FedRAMP compliant and can protect your Google Workspace GCC environment.

Druva-managed keys use enterprise-grade digital envelope encryption in-transit (256-bit TLS) and at-rest (AES 256-bit) for the highest levels of data security and privacy for your Google Workspace backup data. Alternatively, customers have the option to use their own AWS Keys to secure backup sets.

Global or Profile admins can be set up to support delegation of backup and restore responsibilities to different groups to prevent data loss attributed to disgruntled employees/rogue admins.

© Copyright 2026 | Druva Inc. | druva.com

Multi-layered ransomware defense

To recover from data corruption of customers' Google Workspace environment, Druva provides immutable, air-gapped backups that ensures true isolation of backup data from customer-controlled storage environments. In addition, unlimited retention for Google Workspace enables ransomware recovery from a clean snapshot, even if the malware has been present in your environment and infecting data for months.

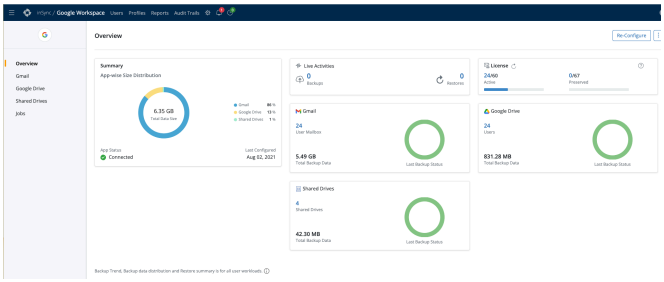
Proactive and automated compliance monitoring

Proactively monitor with out-of-box, predefined, customizable compliance templates for potential violations of key global regulations like GDPR, HIPAA, and CCPA, and receive alerts to quickly remediate violations. Easily customize pre-built compliance templates for global regulation, sensitive data sprawl(PII, PCI, or PHI), or create your own templates for governance policies, including regulation or internal data governance policies.

Key features

Data backup and retention

- User provisioning using AD integration to reduce administrative overhead and improve efficiency.
- Easy-to-use centralized console
- Flexible retention across regions
- Agentless cloud to cloud backup of Gmail, Calendars, Contacts, Google Drive, Shared Drive with zero infrastructure
- Forever incremental backups with flexibility of backup scheduling
- Backup for in-use, open, or large files without limits



Comprehensive support for cloud applications

Integrated eDiscovery legal hold

Unified legal hold management enables the proactive collection and preservation of Google Workspace and endpoint data and its electronic chain of custody until it is extracted, processed, and analyzed in an eDiscovery platform. Druva integrates with market-leading, cloud-native eDiscovery tools to seamlessly collect, preserve, and upload data relevant to legal matters into eDiscovery platforms for review, analysis, and production.

Pre-cull eDiscovery data by dimensions such as time-range and keywords, so that only the most relevant, minimized data set is provided for downstream analysis by the legal team.

Accelerated recovery

- Self-serve restore support, no IT expertise needed
- Automated, AI-driven culling finds most recent clean version of all files
- Granular point-in-time restore across file types
- Restore in same or different use account

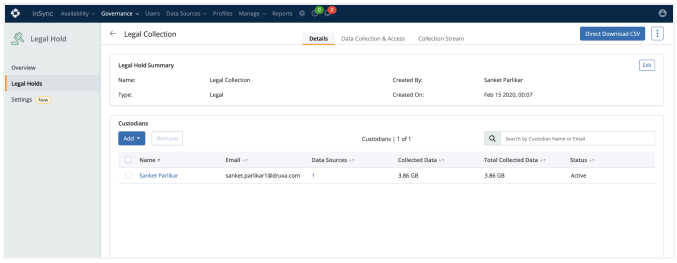
Enhanced security and privacy

- Digital envelope encryption at 256-bit TLS in transit and AES 256-bit at rest
- Compliance with with SOC 1, ISAE 3402, SOC 2, SOC 3, ISO 27001, PCI DSSLevel 1 (Cloud), HIPAA, and FedRAMP
- Data, metadata, and encryption keys stored separate from the environment
- View and download user and admin level audit trails to review activity log

© Copyright 2026 | Druva Inc. | druva.com

Ransomware protection and recovery

- Immutable, air-gapped backups to protect data from ransomware
- Unlimited retention ensures recovery from a clean snapshot
- Quickly rollback deleted data to save from data loss
- Zero-trust security architecture



Centrally manage and automate legal hold across workloads

eDiscovery and legal hold

- Unified legal hold enables electronic chain of custody
- Simple, automated integration with market-leading, cloud-native eDiscovery tools
- Pre-culling for minimized, relevant data-sets

Compliance and sensitive data governance

- Scans and classify information using predefined or custom regulatory templates (GDPR, CCPA, and HIPAA)
- Identify sensitive data sprawl and quarantine or delete the non-compliant files or data

What our customers are saying

"We've already given our users the tools to collaborate through Microsoft 365 and Google Workspace. Now, we can guarantee that their hard work is safe in the cloud."

CityU 香港城市大學 City University of Hong Kong

Chris Fung,
Sr. IT Manager
Learn more in the case study

"Before Druva, we always paid for more backup capacity than we used. Now, we get billed on what we're actually using, and we don't have to manage any hardware."

Chris Brode,
ISO, Network and System Administrator
Learn more in the case study

Read our white paper, Google Workspace: The critical gaps, to learn more about how Druva's leading SaaS-based data resiliency platform addresses Google Workspace's backup and data protection challenges.

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

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the industry's leading SaaS platform for data security, and the only vendor to ensure data protection across the most common data risks backed by a $10 million guarantee. Druva's innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Security Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.

© Copyright 2026 | Druva Inc. | druva.com