Enhancing Data Protection and Secure Collaboration for Google Workspace and Beyond

The Power of Google Workspace Client-side encryption + Virtru

Use Virtru as your key management partner for Google's new Client-side encryption to support heightened privacy in Docs, Sheets, Slides, and the Google Drive File Stream desktop app, as well as encrypted calls (media stream) and video messages in Google Meet.

Google Cloud Partner

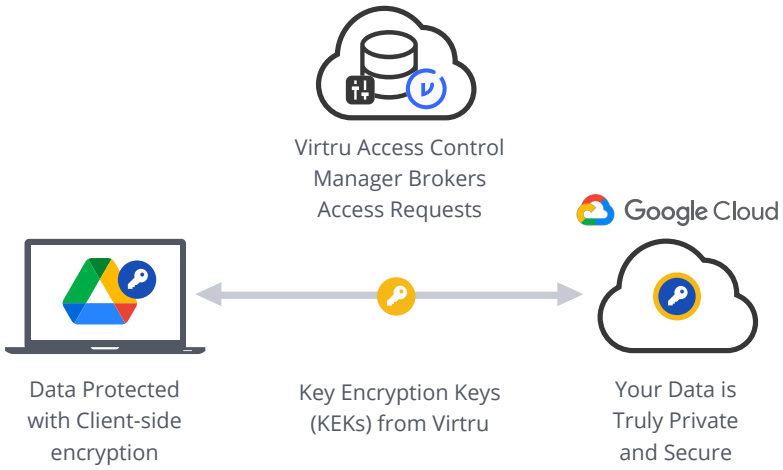
Virtru is a recommended Google Workspace Client-side encryption partner to prevent unauthorized or third-party (including Google) access to data and meet global protection standards such as data sovereignty.

Protection That's Better Together - Partnership with Virtru

Your data requires protection throughout each stage in your collaboration workflow - from confidential collaboration in a Google Doc to downloading as a PDF for external sharing to protecting communication via Google Meet.

Here's how it works:

Once your browser client encrypts the content with Google Client-side encryption, those keys are then wrapped with an additional key that's provided by Virtru. These Key Encryption Keys (KEKs) and their associated access control policies are managed by Virtru to determine who can and cannot access your data. This keeps your cloud data private, even from Google, since they won't have the keys to decrypt your data. Virtru cannot access your protected data at any time.



In Addition to Encryption Key Management, Virtru Offers Data Protection for the Applications You Use Every Day

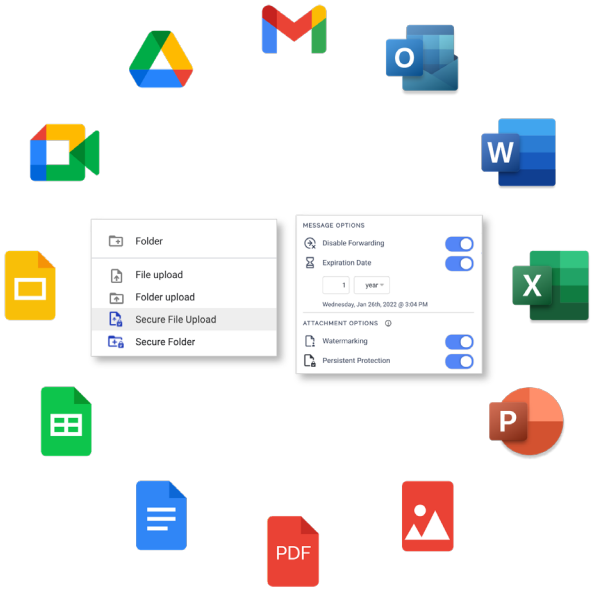
Virtru can take you beyond the capabilities of Google Workspace Client-side encryption. Our Trusted Data Format supports the confidentiality of your data no matter where it lives (including beyond Google Cloud) or who it's shared with. Our services are built to streamline installation and ease of use across your organization.

Secure Send, Upload, and Sharing for Gmail and Drive

- Encrypt and decrypt messages and apply access controls directly within Gmail.
- Securely upload files into Drive (including PDF, Word, Excel, PowerPoint, JPEG, PNG, and CAD) and download to share externally.

Message and File Access Controls

- Expire messages, control forwarding, view read receipts, and add watermarks to files.
- Immediately revoke access at any time.
- Retain access control even after someone downloads a file locally to their desktop.



Protect Additional SaaS Apps

- Extend data protection and control to other SaaS applications — like CRM (e.g. Salesforce) and analytics tools — for organization-wide protection.

Additional Benefits of Virtru

Support Compliance

Have full control over the encryption of files in Google Workspace or shared via other workflows. Host your own encryption keys to help support your compliance with ITAR, EAR, CJIS, IRS 1075, HIPAA, GDPR, etc.

Key Management for GCP

Virtru is now an External Key Manager (EKM) for Google Cloud applications. Apply your own encryption keys to GCP services (including BigQuery and Compute Engine) to encrypt your data in the cloud and ensure true privacy.

Maintain Persistent Visibility

Maintain visibility into all protected data in one place to see what you're protecting, where it's going, and who it's been shared with, even as it's shared externally. Integrate with your SIEM to strengthen threat response and compliance reporting.

virtru

Learn more about Virtru **virtru.com/contact-us**