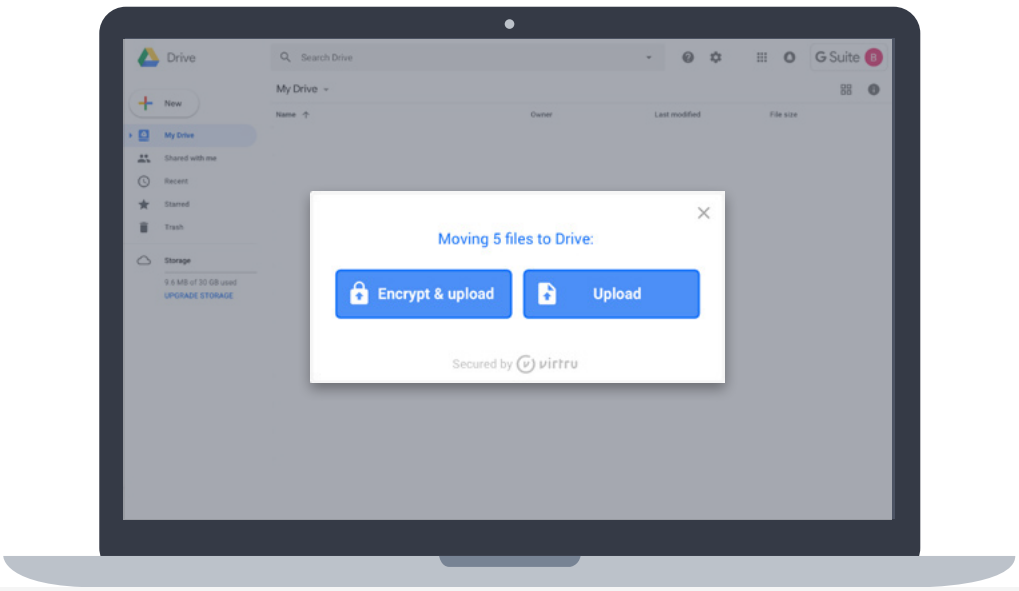
Virtru Google Drive Encryption

End-to-End Drive Encryption, Recommended by Google

Virtru enables secure enterprise cloud collaboration in Google Drive by providing end-to-end encryption, granular access controls, and encryption key management to protect and control Drive files wherever they are shared.



Layered Drive Security

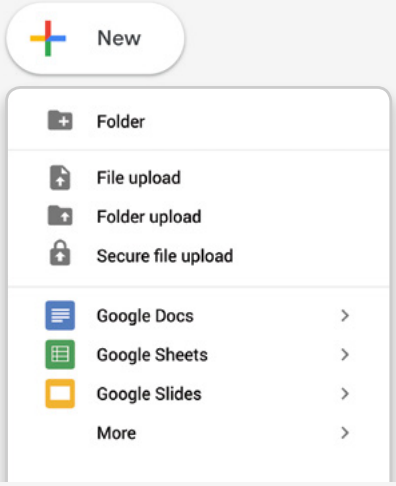
Ensure Corporate Confidentiality
Maintain confidentiality of corporate private data migrated and stored in Google Drive. Leverage Drive without giving Google or any third party access to sensitive content.

Meet Regulatory Requirements
Meet compliance requirements for HIPAA, EAR, CJIS, and other data privacy regulations.

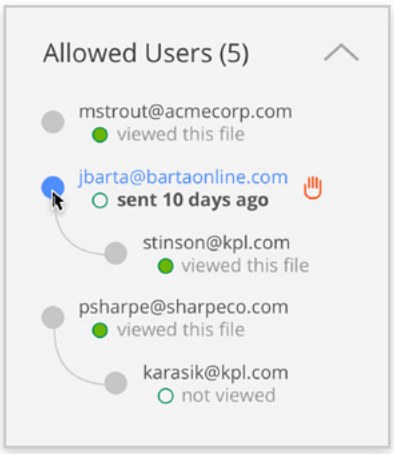
End-to-End Encryption
Files are encrypted before they are uploaded to Google Drive, with persistent data-centric protections that ensure only the creator and authorized recipients have access.

Audit and Control
Collaborate securely with access controls for files and folders. Change permissions at any time. Audit who has accessed and shared encrypted content.

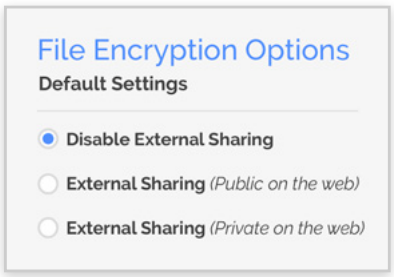
Surprisingly Easy
On-demand and policy-based encryption with a seamless user experience. No new software, applications, or clients. Collaborators don't even need a Google account.



Encrypt files upon upload, before they ever reach Google's servers.



Centrally manage and audit who has accessed encrypted files, with granular visibility into resharing.



Control how users can share Drive files inside and outside your organization.

Feature Overview

Recommended for G Suite

Encryption, Security, and Key Management

- Encrypt Drive files with the click of a button
- Convert and encrypt Drive files before sharing externally
- Attach and encrypt Drive files to Gmail
- Encrypt folders, then mandate encryption for added files
- Host keys on-premise to prevent unauthorized third party access
- Integrate with Hardware Security Modules (HSMs) for heightened enterprise security

Collaboration and Control

- Share encrypted Drive files with anyone - even if they don't have a Google account
- Instantly revoke access to files shared in error, or whose contents have become confidential
- Watermark documents, disable sharing, and set expiration

Administration, Audit, and Incident Response

- Mandate encryption by user, group, or OU
- Meet eDiscovery requirements in Google Vault
- Audit where encrypted files have traveled and who has accessed them
- Stop data leaks via SIEM integrations and threat response workflows
- Search encrypted files with search tagging
- Perform bulk encryption operations, with offline support

"Content collaboration introduces new opportunities for inappropriate behavior that don't exist with traditional computing. Open shares can be an especially pernicious risk."

Research Note: *What You Need to Know About Security in G Suite*, Steve Riley, June 2018

Gartner

More than 8,000 Organizations Trust Virtru Data Protection.

SoftBank · Brown · wework · KPCB Kleiner Perkins Caufield Byers · Maryland · CapitalOne

"G Suite's TLS encryption only goes so far; it doesn't address man-in-the-middle attacks or the actual content itself being encrypted. Virtru fills in that missing piece simply and quickly."

Dennis Dayman, Chief Privacy and Security Officer
Return Path

virtru