Virtru Data Protection for Google Drive

Easily protect files uploaded to Google Drive, and maintain control everywhere they're shared to unlock the power of your data.

Virtru Keeps Your Gmail Private & Compliant, so You Can Focus on Growing Your Business

Virtru protects and governs access to Gmail messages and attachments throughout their full lifecycle. With seamless encryption and controls, Virtru ensures sensitive data stored and shared in Gmail stays private and compliant with industry regulations like HIPAA, CJIS, ITAR, CCPA, and more, unlocking the power of your data to help achieve your organization's goals.
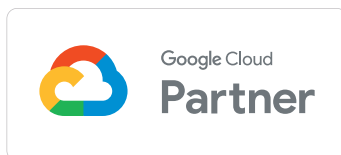
Google's Only Recommended Encryption Partner
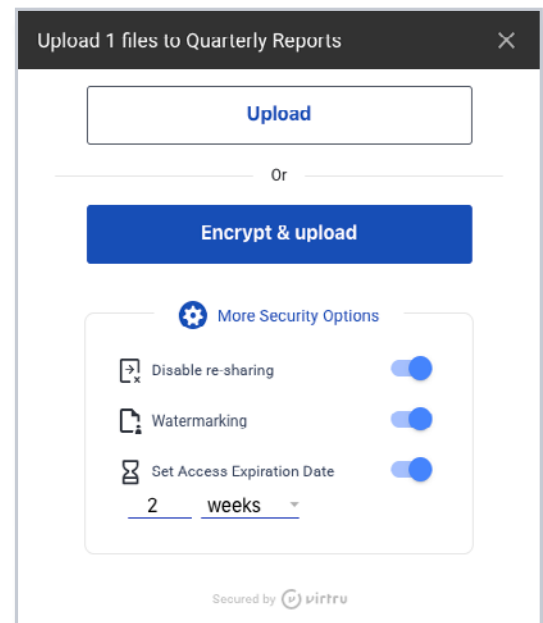
End-to-End Encryption
Encrypt PDF, PowerPoint, Excel, Word, PNG, and JPG files upon upload. Virtru's simple Chrome extension protects files directly in the client to prevent access by Google and unauthorized parties, wherever files are shared.

Granular Access Controls
Set expiration, disable sharing, and revoke access at any time. Watermark files uploaded to Drive with recipients' names to prevent data leaks.

Google Cloud
Partner

Upload 1 files to Quarterly Reports ✕

Upload

Or

Encrypt & upload

⚙ More Security Options

Disable re-sharing

Watermarking

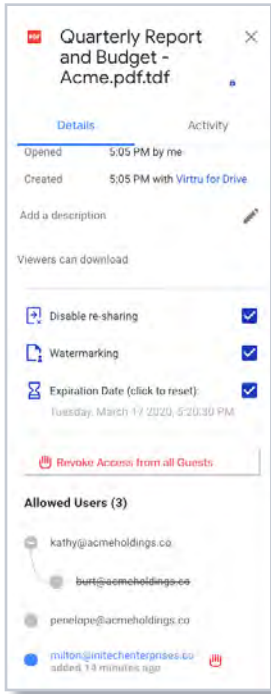Set Access Expiration Date
2 weeks

Secured by virtru

"Virtru's end-to-end protection and ease-of-use empowers us to share sensitive information without worrying about whether the data is secure."
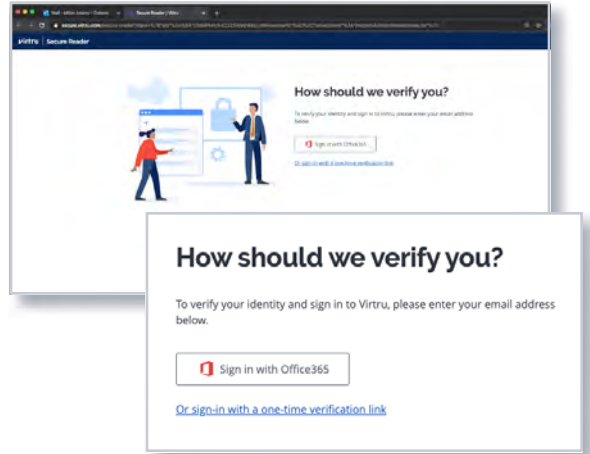
- Bill Dougherty, Vice President of IT and Security, Omada Health

◯ omada

A Closer Look at Virtru Data Protection for Google Drive

Persistent Visibility

Maintain visibility over who has accessed Drive files, even as they're shared externally, and streamline audit workflows. Integrate with your SIEM to strengthen threat response and compliance reporting.

Seamless, Secure Access

Give external recipients secure access to files shared via Drive, without forcing them to create Google accounts or relying on risky open share links.

Automatic Protection

Enforce file protection automatically by designating specific folders to only store encrypted documents, or by requiring certain groups or OUs to encrypt all files they upload.

Trusted Data Format

Open data protection standard for object-level encryption that binds protected files to policies and metadata to prevent unauthorized access.

Key Management

Integrate with your existing key management processes and HSMs. Host your own keys for full control, or let Virtru host them for you and manage policies and key exchanges.

More than 20,000 organizations trust Virtru for data security and privacy protection.

Learn how to maintain privacy and compliance for files stored in Google Drive by requesting a demo at **virtru.com/lp/get-demo**