

# Virtru Data Protection for Gmail



Easily protect Gmail messages and attachments, 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, unlocking the power of your data to help achieve your organization's goals. Virtru for Gmail is FIPS validated, helping you support advanced security requirements mandated by certain regulatory obligations, including CMMC and ITAR.

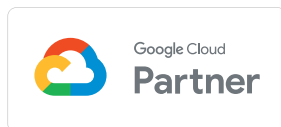
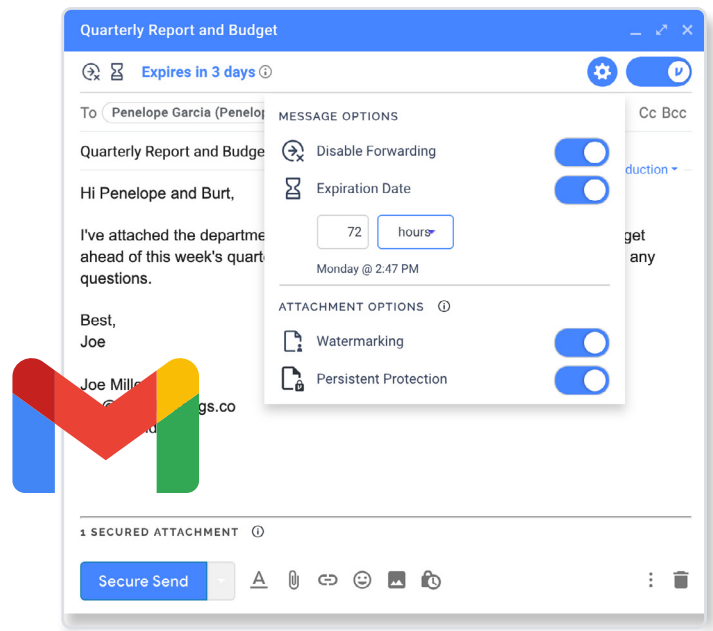
## Google's Only Recommended Encryption Partner

### End-to-End Encryption

Encrypt email messages & attachments directly within the Gmail client with a simple Chrome extension that prevents unauthorized access, everywhere they're shared.

### Persistent Protection & Control

Set expiration, disable forwarding, and watermark attachments to prevent data leaks. Revoke access at any time. Maintain control of attachments beyond Gmail to desktops, network folders, Google Drive, or anywhere else files are stored.

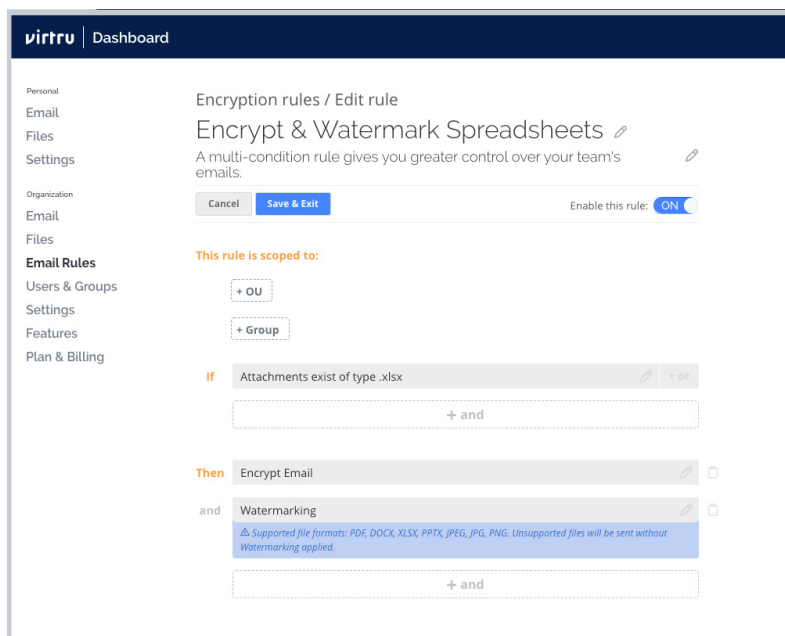
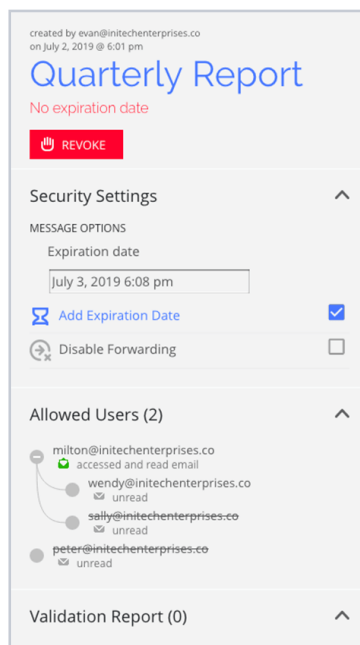


BROWN

*"Virtru is extremely easy to install and use, and it works seamlessly with our Gmail. Compared with legacy email encryption products, it's a breeze."*

- Mark Dieterich  
Director of IT and Security, Brown University

# A Closer Look at Virtru Data Protection for Gmail



## Granular Audit

Maintain visibility of who has accessed or forwarded messages and attachments throughout their lifecycle. Integrate with your SIEM to strengthen threat response and compliance workflows.



## Industry-Leading Ease of Use

Deploy organization-wide in minutes. Support your users without changing the way they work today, and enable seamless access for recipients via existing accounts.

## Data Loss Prevention

Automatically enforce Gmail encryption with DLP rules that detect, protect, and control sensitive data. Reinforce security awareness with proactive alerts that warn users to protect sensitive email.



## Trusted Data Format

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



## Customer Hosted Keys

Integrate with your existing key management processes and HSMs. Host your own keys for full control, manage policies and key exchanges.



See how Virtru can enable privacy and compliance for your Gmail at:  
[virtru.com/lp/get-demo](https://virtru.com/lp/get-demo)