

# Comparing Virtru with Gmail Confidential Mode



Gmail confidential mode offers baseline access controls for messages and attachments, but many organizations face pain points because those controls are limited, the features restrict common sharing workflows, and their messages aren't truly "confidential." Virtru ensures data privacy with persistent protection and granular access controls that give you complete control over your data so you can collaborate with confidence.

## Why Virtru

### True Privacy

- End-to-end encryption for messages and attachments
- Customer-hosted encryption keys to prevent blind government subpoenas
- No access by Google or other unauthorized third parties



### Secure Collaboration

- Secure responses for all recipients, even if they don't use Gmail
- Seamless, secure access for non-Gmail recipients, without extra verification steps
- Persistent protection for attachments, even after download

### Control and Visibility

- Automatic protection and control via DLP rules and policy enforcement
- Document watermarking
- Granular access controls (e.g. allow forward, disable download)
- Persistent visibility into recipient access and sharing
- Granular audit logs and SIEM integrations

## Side-by-Side Comparison

Capabilities		
Access Revocation & Expiration	✓	✓
Disable Forwarding	✓	✓
Attachment Download for Recipients	✓	✗
Attachment Watermarks	✓	✗
Persistent Protection for Attachments	✓	✗
End-to-End Encryption for Email & Attachments	✓	✗
Automatic Protection via DLP Enforcement	✓	✗
No Third Party Access	✓	✗
CJIS & PCI Compliant	✓	✗
Visibility into Access & Forwarding for Senders & Admins	✓	✗
Customer-Hosted Encryption Keys	✓	✗