Gmail confidential mode offers basic access controls for Gmail users sending email messages and attachments—including the ability to set an expiration date, revoke access at any time, and prevent email recipients from forwarding, copying, printing or downloading message contents or attachments.

Although Gmail users get some added control with confidential mode, it’s important to understand where this feature falls short—and what to do about it.

**With Gmail confidential mode:**

1. **Admins must place their trust in end users.**
   Currently, confidential mode cannot be enforced as a protection policy as part of G Suite’s DLP Rules. This means that admins must rely on end users to proactively apply confidential mode, introducing security risks.

2. **Sharing and controls are limited.**
   Confidential mode forces senders to apply all access controls at once, making collaboration unnecessarily rigid. For example, you can’t set an expiration date but then allow forwarding. Attachments can’t be shared beyond the initial email, and confidential mode doesn’t support watermarking attachments, so there is nothing stopping recipients from leaking photos or screenshots of sensitive files.

3. **Non-Gmail recipients have a less seamless, less secure experience.**
   Non-Gmail recipients must authenticate themselves via an additional email with a verification code, introducing friction to collaboration workflows. They can’t use confidential mode themselves, preventing them from sending secure responses and adding risk to external collaboration workflows.

4. **Visibility is limited.**
   Senders can’t see who has accessed messages sent in confidential mode. Neither Google Vault nor the Google Workspace Admin Console supports direct reporting on confidential mode activity, restricting audit workflows.

5. **Google is in control of your sensitive data.**
   Even when using confidential mode, Google has access to plaintext content. It’s not truly confidential. Plus, Google controls the keys protecting your data, meaning you can’t prevent government surveillance via blind subpoenas.
Additional Protection You Need to Maintain Data Privacy and Security

As Google's recommended encryption solution, Virtru ensures privacy for email messages and attachments while fostering secure collaboration with persistent protection, access controls, and key management options that give organizations superior control over and visibility into data access.

In order to ensure messages and their attachments remain secure, Virtru:

- Offers protections that give customers complete control over who can access sensitive content.
- Enables the secure sharing of attachments with persistent protections and watermarking that offer superior control to prevent data leaks.
- Supports more seamless and secure collaboration workflows for recipients, helping mitigate compliance and privacy risks.
- Provides admins with DLP rules that automatically enforce protection, so admins don’t have to rely on end users to proactively do so.
- Provides fine-grained audit capabilities—including SIEM integrations—for enhanced threat response.

Learn more about Virtru’s ability to offer persistent protection for Gmail messages and attachments. [virtru.com/contact-us](http://virtru.com/contact-us)

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it’s stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 20,000 organizations trust Virtru for data security and privacy protection.