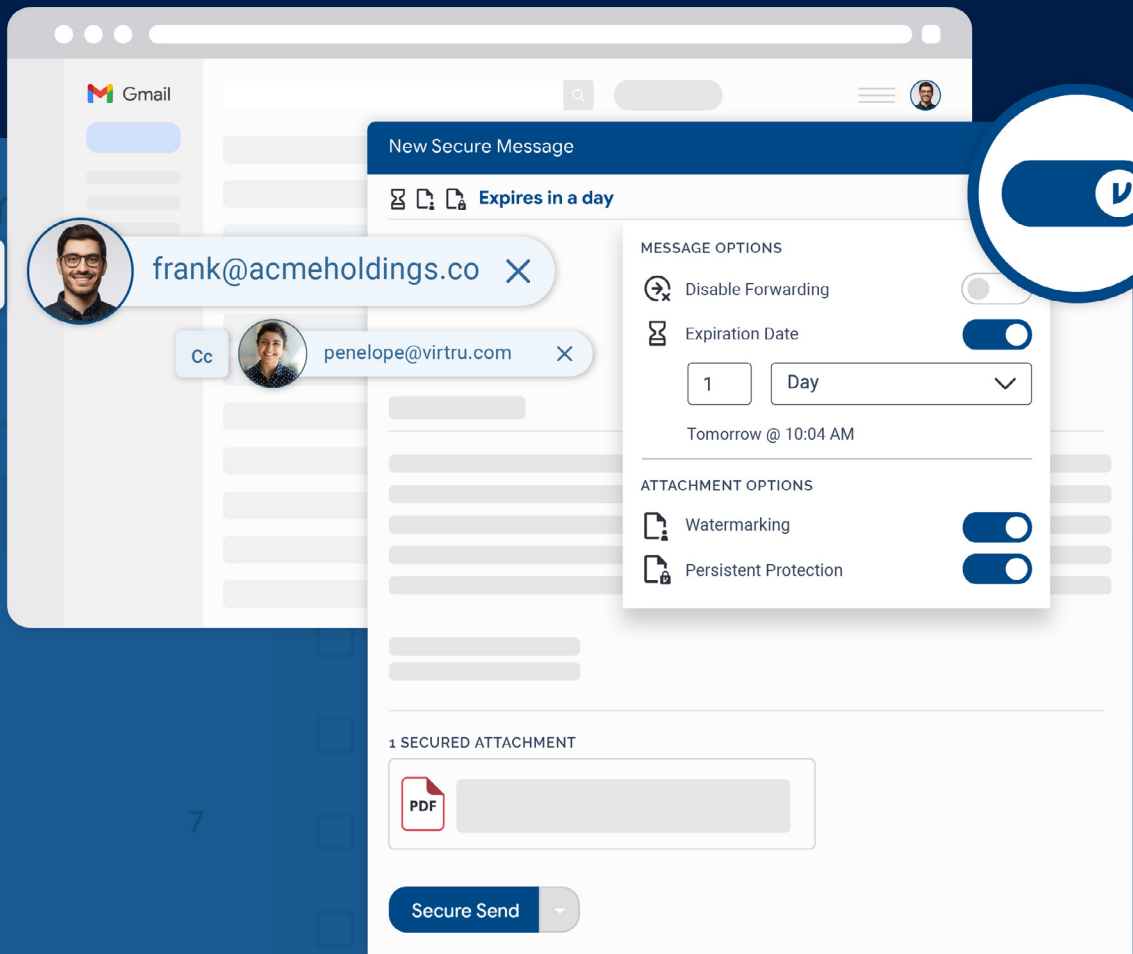# virtru

Guide to Gmail Protection:

How to Encrypt Messages and Attachments
for Enhanced Control and Privacy

The Need for Enhanced Gmail Security

As the digital transformation continues to reshape the modern workplace, Google Workspace has become a dominant force. Google Workspace's flagship product, Gmail, is one of the most widely used email client in the world. And for good reason—Gmail is a powerful, intuitive email platform that supports rapid collaboration and information sharing.

Sharing data via Gmail is a necessity, but it also exacerbates security risks: emails often contain intellectual property (IP), personally identifiable information (PII), protected health information (PHI), and other sensitive data. In fact, email represents a large chunk of all sensitive data in the cloud, and while moving email to the cloud reduces IT infrastructure burdens, it also reduces visibility for IT teams. This makes Gmail protection, access control, and visibility a crucial priority for IT, security, privacy, and compliance teams.

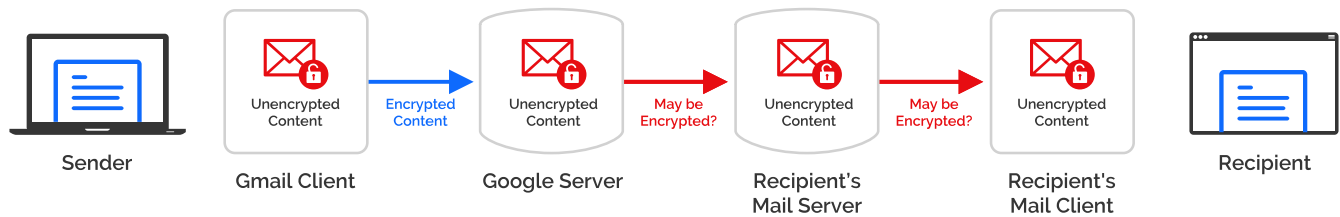**Escalating Privacy Regulations and Public Awareness**

Increasing compliance requirements and public awareness of privacy issues are raising the stakes for Gmail protection even higher. The EU's General Data Protection Regulation (GDPR) set the stage in May 2018 with a binding set of laws designed to protect the privacy of EU citizens' personal data. The United States then followed suit, starting at the state level—the California Consumer Privacy Act (CCPA) was passed in June 2018 to establish similar consumer privacy rights. Since then, dozens of other states are either actively debating or already implementing privacy bills, with a sweeping U.S. federal privacy law becoming more likely.

Most organizations store sensitive personal information under the purview of these laws, so mishandling it could put security teams under regulators' scrutiny. Sharing personal information via email is, in many cases, a force of habit as it's such an easy way to send information critical to getting the job done, so escalating privacy regulations reinforce the importance of Gmail safeguards. And as the layperson becomes more privacy-minded, a leading-edge data protection strategy can become a key business differentiator.

As your organization develops and refines strategies to keep Gmail data private and compliant while maintaining competitiveness, this guide will walk you through native protections for your Gmail messages and attachments, discuss scenarios where additional measures are needed, and review advanced approaches to ensure your Gmail remains secure.

Gmail's Native Protections and Controls

Transport Layer Security (TLS)

| Sender | Gmail Client | Google Server | Recipient's Mail Server | Recipient's Mail Client | Recipient |

When you access Gmail to send and read messages and attachments (or use any other Google Workspace application for that matter), Google encrypts the connection between your web browser and Google's servers by enforcing Transport Layer Security (TLS).

TLS uses asymmetric encryption to ensure both ends of the connection are legitimate and haven't been hijacked by an imposter. At the beginning of a session, your web browser initiates a handshake with a Google server by asking for a digital certificate to verify its identity, then uses the public key from the certificate to encrypt the connection. This process ultimately secures the communication pathway that allows you to draft, send, and access Gmail messages from your browser.

TLS protects your messages and attachments in transit but stops at the network level. The content itself is not encrypted, so once the network perimeter is breached, sensitive data in Gmail is vulnerable.

Gmail Confidential Mode

In 2019, Google introduced confidential mode, providing senders with basic access controls for Gmail messages and attachments. Gmail confidential mode gives senders the ability to prevent recipients from forwarding, copying, printing, or downloading message content or attachments. It sets an expiration date and allows senders to revoke access after messages are sent.

While confidential mode provides some management capabilities, they are limited. Administrators cannot enforce confidential mode as part of Gmail's Data Loss Prevention (DLP) and compliance rules, so admins have to rely on end users to proactively apply it, introducing security and privacy risks. Visibility is limited as well. Neither Google Vault nor the Google Workspace Admin Console supports direct reporting on confidential mode activity, restricting audit workflows.

For senders, expiration and disabled forwarding, copying, printing, and download must be applied all 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.

Recipients with Gmail accounts access the message transparently within their inbox, but non-Gmail recipients (e.g. Microsoft users) must authenticate themselves with a verification code from an additional email, and there is no way for

them to respond securely with confidential mode. For example, if a healthcare organization's IT staff used confidential mode to request a report from a new patient, patients without Gmail are likely to send their PHI in a separate, unprotected email, introducing HIPAA compliance risks.

Finally, your messages aren't truly "confidential." Confidential mode simply sends email and attachments to a TLS-protected subnetwork. Google still has access to the unprotected plaintext (even after recipient access has expired) which fails to meet data sovereignty, privacy, and compliance requirements of organizations concerned about third-party access to their data.

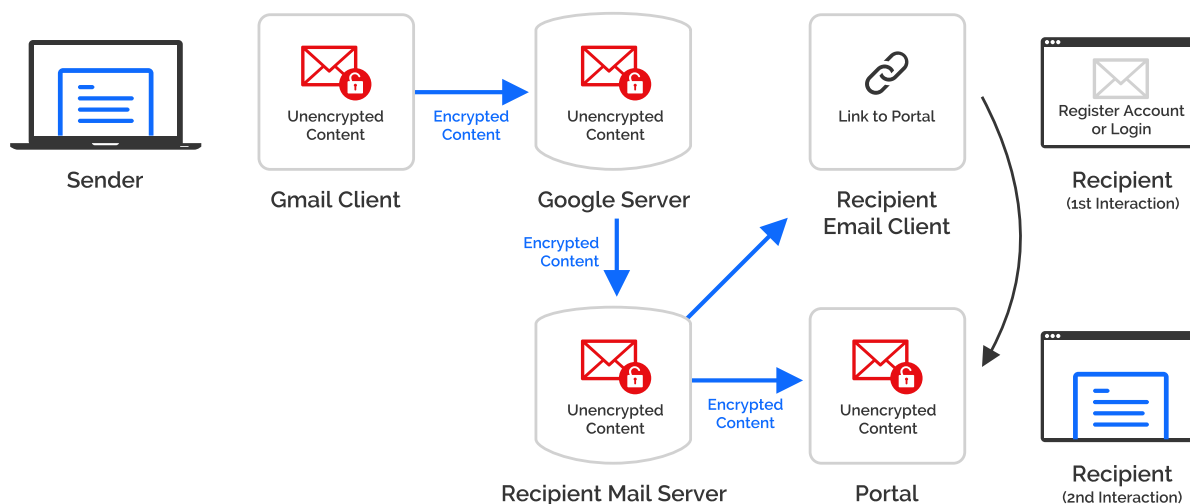## Traditional Approaches to Layered Protection and Control for Gmail

While Google's native protections for Gmail provide a helpful baseline, many organizations determine that additional protection and control measures are needed to ensure privacy and compliance, especially as increasing volumes of sensitive data are stored and shared via Gmail.

Data Loss Prevention (DLP)
Google Workspace administrators can configure rules that automate processes to help safeguard your inbox. Google Workspace calls these "compliance rules," and they work like DLP solutions: by scanning messages and attachments to detect sensitive data—such as credit card, Social Security, or Passport numbers—then triggering an action such as quarantining, blocking, or modifying the message (e.g. removing attachments, changing recipients, adding headers or changing the mail route to support third-party security scanning tools).

Google's compliance rules can improve security workflows, but like many security solutions, they add friction and impede collaboration. Quarantined and blocked messages often leave senders in the dark and reliant on support, and modifying messages adds to administrative complexity. Also, Google's compliance controls are only available for Google Workspace Enterprise, the most costly platform edition.

Email Encryption Portals

Sender — Gmail Client — Unencrypted Content — Encrypted Content — Google Server — Unencrypted Content — Encrypted Content — Recipient Email Client — Link to Portal — Register Account or Login — Recipient (1st Interaction) — Recipient Mail Server — Unencrypted Content — Encrypted Content — Portal — Unencrypted Content — Recipient (2nd Interaction)

Third-party email encryption portal solutions are a prevalent legacy approach to Gmail protection, but with critical limitations. These solutions encrypt Gmail messages at the gateway-level, and recipients have to access the content within a separate portal. They also tend to rely on DLP, which increases maintenance burdens as administrators must configure comprehensive rules.

In a portal workflow, sensitive messages are diverted to a TLS-protected subnetwork in the portal vendor's environment. Just like with Google's native TLS protections, the channel is protected but the messages and attachments themselves are not encrypted, leaving your data susceptible to unauthorized access.

Portal-based solutions limit the protection and controls available to senders; often they're defined by administrators only, creating black-box scenarios where senders don't know whether data is protected or even sent. If senders do have the ability to apply protections, they have to insert specific keywords in the email, risking data leaks when they inevitably forget to use these keywords. The lack of simple functionality to turn on encryption reduces security awareness.

Finally, recipients must access and manage these emails in a new, separate application, generally requiring a new account username and password to authenticate themselves, adding unnecessary friction to collaboration.

S/MIME Encryption

Google offers enhanced message security via Secure/Multipurpose Internet Mail Extensions (S/MIME) as part of the Google Workspace Enterprise edition. Administrators can require the use of S/MIME for outgoing messages, for example, to ensure the content is protected.

S/MIME encryption goes further than TLS and encrypts the message payload, but critical obstacles prevent successful S/MIME deployments in practice. In general, both the sender and the recipient need to have S/MIME configured the same way for it to function properly. If the recipient doesn't have S/MIME or it is misconfigured, they won't be able to access encrypted messages (unless they have extensive knowledge of how to securely exchange encryption keys—a nonstarter for the majority of users).

While S/MIME's advanced encryption would ensure messages stay private and compliant throughout their lifecycle, complexities with its user experience prevent widespread adoption.

A Modern Approach to Data-Centric Protection: End-to-End Encryption from Virtru
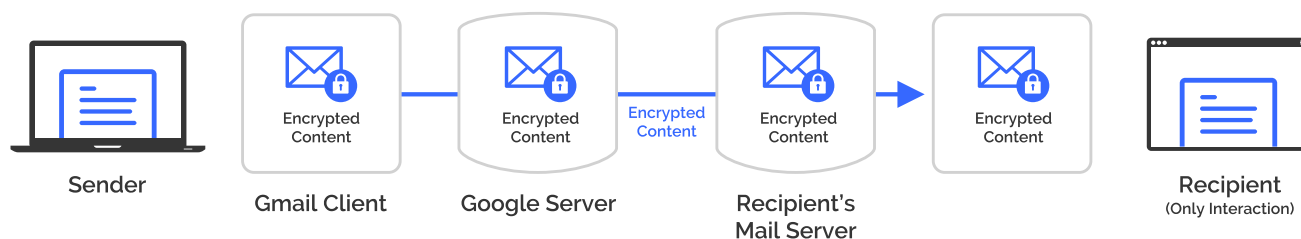
Data-centric protection for Gmail is considered a best security practice for organizations looking to get the most out of Gmail's rapid collaboration and productivity features while keeping messages and attachments protected, wherever they're shared. This approach protects Gmail messages and attachments down to the object level and enables secure sharing and mobility, while the owner maintains control and visibility.

Virtru provides data-centric protection that keeps Gmail messages and attachments private and compliant while fostering secure collaboration. Virtru is embedded directly within the native Gmail user interface via a Google Chrome browser extension, enabling end-to-end encryption, directly within the client. By simply toggling a switch, Virtru encrypts the message body and any attachments before it reaches Google's servers—preventing access by Google and other unauthorized parties—to ensure privacy throughout collaboration workflows.

Virtru's granular access controls give senders a variety of options for secure sharing, with the ability to set an expiration date, disable forwarding, and revoke access at any time. For attachments, watermarks of the recipient's email address can be applied to help deter file-based data leaks. Persistent File Protection can also be added to attachments, applying a protective HTML wrapper that lets recipients download and share attachments beyond email—to desktops, network drives, Google Drive, and other cloud platforms— while the sender maintains control. This opens up more dynamic, secure sharing scenarios.

Meanwhile, Virtru's ease of use reduces support costs for overburdened IT teams. Security features are embedded into Gmail, making data protection seamless for senders. Plus, external recipients don't need to create new portal accounts or manage another password to access secure emails. They simply authenticate themselves with their existing accounts.

Administrators can leverage Virtru's Security Rules that automatically enforce data-centric protections and access controls to emails and attachments, so you don't have to just hope that end users do the right thing. Visibility of protected messages and attachments persists wherever they're shared, allowing admins and senders to adapt access controls as needed. Plus, logs of all

For enterprise email encryption to be a viable solution, it doesn't just require the best in security and control—it also requires convenience.

Virtru provides Gmail users with:

- Seamless ease of use
- Granular access controls
- Custom security rules
- Visibility and control
- Flexible key management options

protection and sharing activity can be integrated with SIEM tools for enhanced threat response.

Virtru is a key management partner for Google Workspace's Client-Side Encryption (CSE) and Gmail S/MIME, providing organizations with a comprehensive solution to safeguard their most sensitive data while maintaining full control. By leveraging Virtru's Private Keystore for CSE, organizations can take ownership of the encryption keys that secure their data, ensuring it remains unreadable by Google, Virtru, or any unauthorized third party. This approach not only supports compliance with regulatory standards but also enhances data sovereignty, as organizations can choose where to store their encryption keys, aligning with geographic and security obligations.

Virtru's solution seamlessly integrates with Gmail S/MIME and Google Workspace CSE, enabling granular access control and ensuring robust privacy and compliance in today's data-centric environments.

Virtru's data-centric approach to protection gives organizations using Gmail the highest assurances that data within Gmail will remain private and compliant throughout the entire email lifecycle. To learn more about how Virtru can support your organization's compliance and privacy programs, visit the link below to talk to a data protection expert.

Learn more about using Virtru for added protection and control over Gmail messages and attachments. **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 data-centric security solutions —built on our open Data Security Platform—governs and protects data throughout its lifecycle. More than 7,000 organizations trust Virtru for data security and privacy protection.