virtru

The Complete Guide to Zero Trust Security Across the Google Ecosystem

Cloud Security Best Practices for Business Leaders

The world is increasingly embracing Google's cloud-based collaboration tools — for good reason:

- They're simple and easy to use.
- They are cost-effective while providing world-class functionality.
- They facilitate fast collaboration and data sharing.
- They are easily scalable.

But many organizations have hesitated to move all their workflows to Google Cloud because, historically, it was not secure enough to protect the sensitive information shared by enterprise or government users.

But this has now changed: It's safer than ever to move to the cloud.

Notably, Google announced its rollout of Google Workspace Client-side encryption in 2021 which includes protection for Google Docs, Sheets, and Slides; the cloud and desktop versions of Google Drive; and calls and video messages in Google Meet. This enables enterprises to completely shield their data, so that not even Google can access it.

But there are still several facets of data protection that IT and security leaders need to consider in order to effectively protect the data they store and share across the Google ecosystem. This guide aims to provide context on the layers of Zero Trust data protection that make up a secure cloud strategy across Google Workspace, Google Cloud Platform (GCP), and beyond.

Table of Contents

Taking Control of Your Data in the Cloud

Organizations may be hesitant to store sensitive data in the cloud, for fear that it won't be secure enough, or that they won't have full control over it. Historically, this was true. Until recently, many highly regulated industries (such as manufacturing and government) simply haven't been allowed to use cloud-based solutions.

Many global organizations have also hesitated to host their data on Google because they need to maintain data residency, sovereignty and control. With most major cloud providers being based in the U.S., there has been concern that these organizations would be unable to maintain data residency and sovereignty while storing data on a server outside their own country or region — putting their customers' private information at risk.

The good news is that Google is continually expanding customers' ability to encrypt and shield their data, maintaining full data ownership and sovereignty. From Gmail across Google Workspace and the Google Cloud Platform, customers have the option to layer in additional encryption, as well as manage encryption keys externally, in a way that blinds Google to the data it stores.

> Having a unified data protection framework for Google Cloud helps organizations save money, reduce complexity, and gain speed.

This gives you the best of both worlds: The efficiencies and collaboration capabilities of the cloud, as well as the assurance that your data remains fully under your control at all times, preventing third parties — including Google — from gaining access to your data.

To make this level of security a reality, organizations need to select an encryption partner. Because the Google ecosystem is expansive, organizations need to consider a partner whose capabilities span across Google Workspace and the Google Cloud Platform — giving them a single, holistic framework for protecting their data according to Zero Trust standards. Having a unified data protection framework for Google Cloud helps organizations save money, reduce complexity, and gain speed.

Google Cloud
Partner

Data Protection and Key Management, Recommended by Google
Virtru is the only third-party, Google-recommended security partner that provides encryption across the Google ecosystem, from Gmail throughout Google Workspace and Google Cloud Platform.

Bringing End-to-End Encryption to Gmail

From invaluable intellectual property to sensitive employee and customer data, the corporate inbox is a veritable treasure trove for hackers. A mistakenly forwarded message, or an absentminded click on a phishing email, can be incredibly damaging: IBM estimates the average cost of a data breach to be US$3.86 million. For executives with especially sensitive, strategic, and valuable information stored in their inboxes, the stakes can be even higher.

Equally significant enterprise risks include regulatory compliance and government penalties. As data breaches have become increasingly commonplace, government regulators have increased oversight of data privacy and security. U.S. regulations like HIPAA, CJIS, FERPA, ITAR, CMMC, and many others require specific steps, including encryption, to protect sensitive information. In 2021, a White House cybersecurity executive order emphasized the importance of encryption to safeguard government data — particularly as cyber attacks continue to increase in scale, sophistication, and severity.

Meanwhile, the EU's General Data Privacy Regulation (GDPR) requires broad security precautions, with steep penalties for non-compliance that have made it top of mind for security leaders across the globe. In addition to facing noncompliance fines, executives at the helm of breached companies draw the ire of government officials and are often obligated to testify in hearings, amplifying the damage to their brands' reputations.

Taken together with the increasing need to share sensitive information, the proliferation of mobile devices and remote work, and the pace of migration to cloud platforms, security and regulatory risks make email encryption an imperative for enterprise leaders.

Executives need to make comprehensive email security with end-to-end encryption a strategic priority for the entire organization. Equipping your teams to encrypt Gmail messages and attachments can make the difference between a close call and a costly, damaging breach.

> "We want everyone to have the ability to protect the files they're sending. At some point, everybody in the company will need to share something sensitive—maybe not daily, maybe not weekly—but eventually, they'll need to."
>
> **-Ram Avrahami, Head of Global IT and IS, NEXT**
>
> NeXT
>
> Read the Case Study

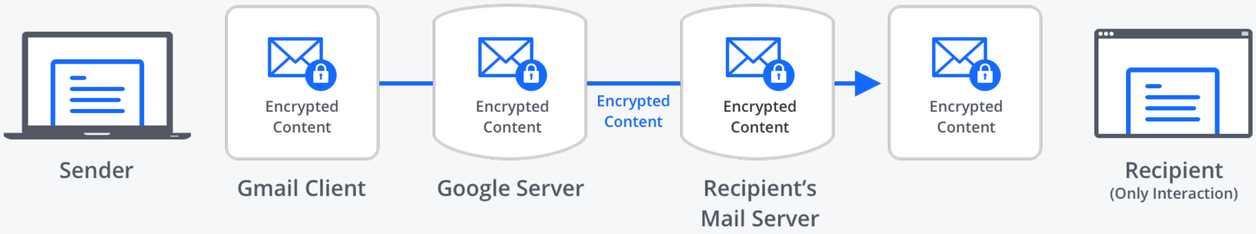
Any viable Gmail encryption solution has three basic requirements: end-to-end protection, key management and control, and ease of use.

End-to-End Encryption

Truly secure encryption solutions for enterprise email protection employ end-to-end protection. Your business can't afford a major loss of data because an email was compromised on the recipient end. Unlike Google's native, default transport layer security (TLS) and third-party portal-based solutions, end-to-end encryption protects data from the moment it's created, and that secure content stays protected even after it's been shared and recipients have accessed it.

Additionally, some regulation and compliance frameworks require end-to-end, client-side encryption. So, if you need to meet compliance regulations — or maintain data sovereignty — native TLS email and file security in the cloud isn't going to cut it.

End-to-end Encryption Protects Content Through Its Entire Lifecycle



Client-side encryption ensures your message remains secure from the time you send it to the time it is received.

Key Management and Control

The whole point of using encryption, beyond protecting against data theft and leaks, is to maintain full control of your own data. When you use the TLS encryption natively built into Gmail, Google owns the keys to your content and must access that data in order to enable searching and malware scans. When you use a portal system, the provider of that portal owns your keys and has access to your content. Only with a true end-to-end, client-side encryption solution do you get complete ownership of your own encryption keys and granular control over who can unlock and access your content.

Ease of Use

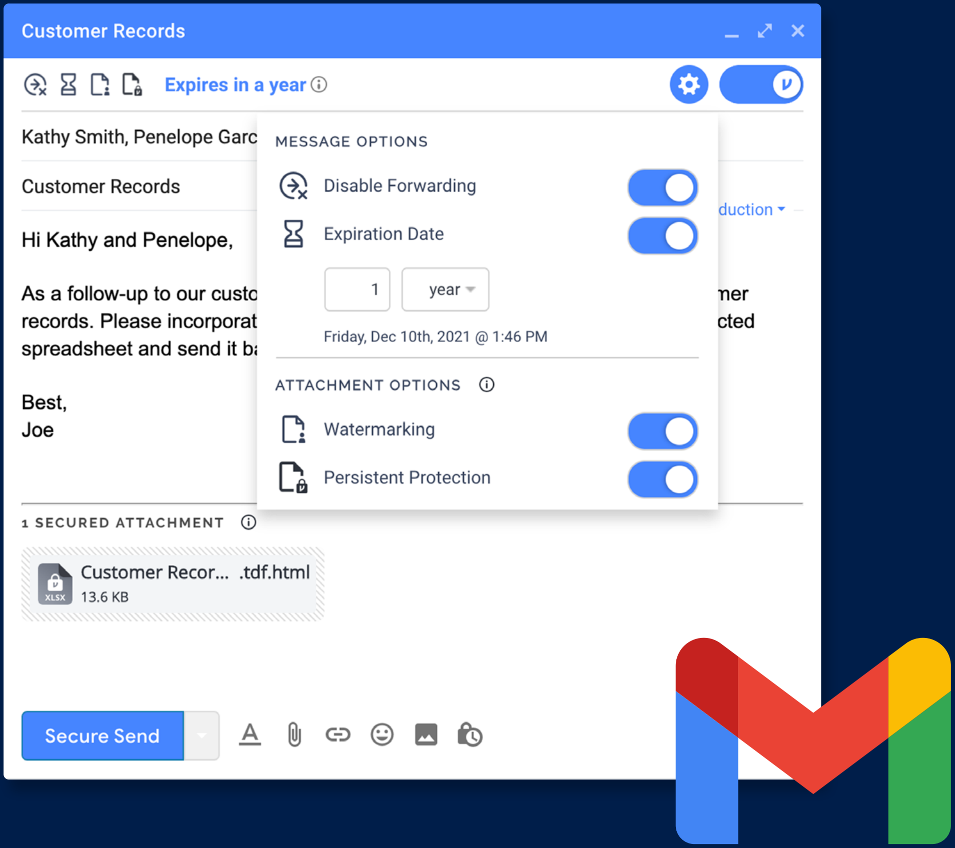
One issue businesses commonly encounter with end-to-end encryption is that legacy solutions like Pretty Good Privacy (PGP) and S/MIME are a pain to use. Additionally, Google's Hosted S/MIME does not prevent third party access to data. Google has access to unencrypted content, as well as the encryption keys that control who can view this content.

For enterprise email encryption to be a viable solution, it doesn't just require the best in security and control — it also requires convenience, especially given the volume of incoming and outgoing emails enterprises receive on a daily basis. Organizations moving to Google expect ease of use and simplicity, and legacy approaches to end-to-end encryption just don't deliver on the needs of security-conscious leaders.

Empower Users with Virtru for Gmail

When it comes to protecting data shared via email, security leaders need to accomplish two key things: Foster strong end-user security behaviors, and create a safety net that catches sensitive information that may have slipped through the cracks.

Virtru equips you to do both. Users are empowered to protect their own data and set access parameters with a single click of the Virtru blue button, directly within their Gmail interface. Users and administrators can maintain visibility into their data at all times, and they can choose to revoke access any time they choose — even after the data has been shared or viewed. Administrators can also set customized DLP rules to create a “safety net” that automatically encrypts messages containing certain types of sensitive data. Administrators can also automatically turn on encryption by default for users that typically handle highly regulated data, ensuring that information is protected the moment a user starts drafting a message.


Customer Records

Expires in a year

Kathy Smith, Penelope Garc

Customer Records

Hi Kathy and Penelope,

As a follow-up to our custo ... mer
records. Please incorporat ... cted
spreadsheet and send it ba

Best,
Joe

MESSAGE OPTIONS

Disable Forwarding: on

Expiration Date: on

1 year

Friday, Dec 10th, 2021 @ 1:46 PM

ATTACHMENT OPTIONS

Watermarking: on

Persistent Protection: on

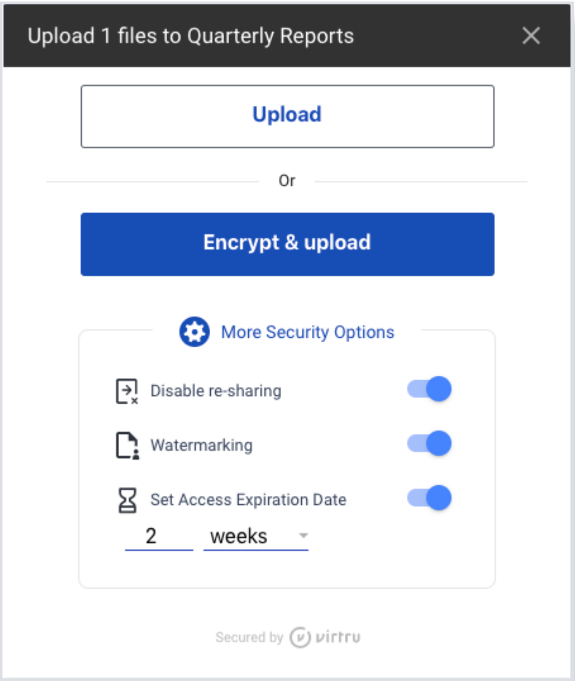
1 SECURED ATTACHMENT

Customer Recor... .tdf.html
13.6 KB

Accelerating Secure Collaboration in Google Workspace

Teams around the world already love to use Google's collaboration apps. With the 2021 announcement of Google's Client-side encryption for Workspace, enterprises can use Google Docs, Sheets, and Slides with the confidence that they're secure and no third party can access their data. Google also expanded these encryption capabilities to Google Meet calls and video messages. Organizations can also add a layer of encryption to their documents stored and shared in Google Drive, similar to the encryption used to protect Gmail messages and attachments.

A key component of this layer of security is independent key management: Ensuring that the encryption keys to unlock sensitive data are stored and managed independently of Google. To do this, organizations are required to select a Google-authorized key management partner, such as Virtru.


Upload 1 files to Quarterly Reports

Disable re-sharing ●
Watermarking ●
Set Access Expiration Date ●
2 weeks

Share with Confidence Using Virtru for Google Workspace

Virtru provides end-to-end file encryption for Google Drive, which complements its end-to-end encryption for Gmail. This protects files outside of the Google ecosystem uploaded to Drive, including PDFs, images, videos, CAD and Adobe files, and more.

Virtru is also a Google-recommended key management provider for its Client-side encryption for Google Workspace — including Google Docs, Sheets, and Slides, as well as calls and video messages in Google Meet. In this capacity, Virtru serves as a trusted, third-party key manager to secure the keys to your cloud-hosted data. With this approach, neither Virtru nor Google can access your protected data.

A key benefit of using Virtru across the Google ecosystem is that you gain a single, comprehensive framework for securely protecting your data, everywhere it lives and moves throughout Gmail, Google Drive, and Google Workspace.

When evaluating your encryption partner, you'll want to consider their full suite of capabilities, and whether those capabilities extend throughout the Google ecosystem. The chart below compares Virtru to other third-party encryption key partners. For a more detailed breakdown, check out Virtru's Data Sheet, Choosing Your Encryption Key Management Partner for Google Workspace Client Side Encryption.

Compare Partner Solutions for Google Workspace

	Data Protection Capabilities	Other Third-Party Providers	Virtru
Google Workspace	Secure Google cloud-native files (Docs, Sheets, and Slides) within Google Workspace	1 2 3 Provider 1 Provider 2 Provider 3	v
	Encrypt and upload static files into Google Drive (e.g. PDF, Word, Excel, PowerPoint, and image files)	1 2 3	v
	Use a Hardware Security Module (HSM) for maximum security	1 3	v
	Extend data protection to Gmail messages and file attachments	2	v
	Use a cloud-based solution to improve deployment, management, and ease of use across your organization	1	v

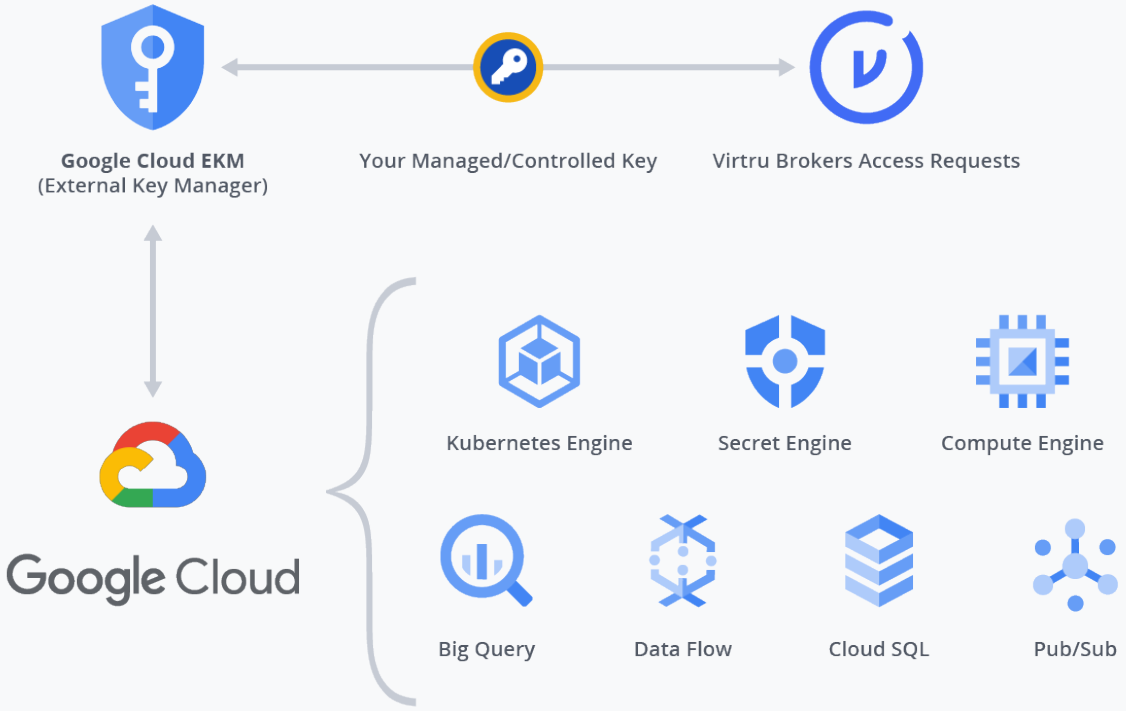
Ensuring Complete Data Privacy for Google Cloud Platform (GCP)

With so many enterprises undergoing digital transformations, many are leveraging Google Cloud Platform to modernize their tech stacks. Google Cloud Platform provides organizations with a versatile, scalable landscape to build and host their system architectures.

Like Client-side encryption for Workspace, Google enables enterprises to encrypt their data on Google Cloud Platform. As with Workspace, this requires an External Key Management (EKM) partner.

Starting in 2021, organizations can leverage Virtru as their EKM partner to securely manage their encryption keys separately from their data in the Google Cloud Platform, strengthening data privacy and sovereignty across the entirety of Google Workspace, GCP, and other cloud applications. This Zero Trust approach to data protection can be used to safeguard data lakes, databases, and information that flows through Google's cloud computing and AI capabilities.

With Virtru's key management solution in place for Google Cloud, enterprises can have a single, global framework and policy language to protect all data across the Google Cloud ecosystem — whether generated by users, devices, or systems.



Data Sovereignty in the Cloud

For global organizations, end-to-end encryption solves an important problem: Data sovereignty and residency. Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner.

Given the market dominance of U.S. cloud and software solution providers, most companies competing in the EU that leverage cloud technologies and collect consumer data must face the issue of U.S. vs. EU regulations head-on as they operate day to day.

Fortunately, there is a solution for those businesses— one that enables full participation in the global economy, maintains the benefits of the public cloud, and provides complete control over data access. In November 2020, the European Data Protection Board (EDPB) adopted guidance clarifying that end-to-end encryption is an effective measure to enable both cloud adoption and EU data sovereignty requirements, which are often viewed as the global privacy gold standard.

In essence, companies competing in the EU can pair stringent security controls offered through encryption technology with SCCs, ensuring compliance with European law post-Schrems II while offering a managed path to authorized access for U.S. government agencies and other entities. This is where Virtru can help. Virtru has adopted an approach to data security that prioritizes privacy and control that is fully managed by customers. The Virtru platform ensures your data — and your customers' data — remains encrypted and unreadable, even in the event of the U.S. CLOUD Act being activated.

How? Virtru's solution is cloud infrastructure- and provider-agnostic, crypto-agile and implemented end-to-end as a default. Encrypted key management options ensure that no entity—including cloud vendors—is able to access the data without obtaining consent from the data owner, who has the sole ability to grant access through decryption. In a nutshell, Virtru supports global collaboration through compliant, cross-border data flows by ensuring:

1. Data can be stored on any cloud solution, including those offered by U.S.-based providers including commercial off-the-shelf solutions from Google, Microsoft, and Amazon.

2. Data is wrapped in a layer of protection (encryption) that can only be unlocked by the designated customer or recipient. While the data is still accessible, it remains encrypted and unreadable.

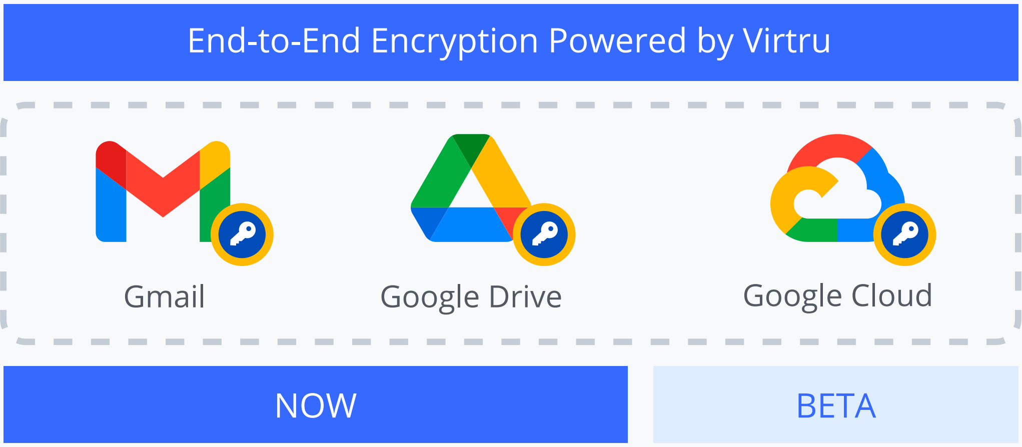
3. The keys that unlock that protective layer are managed outside of the cloud solution. Virtru offers the capability to store the encryption keys—the core of the encryption mechanism—on premise or in a private cloud that is solely owned and managed by the customer, thereby achieving data sovereignty.

For more details on maintaining data sovereignty in the cloud, read our guide, ***Who Holds the Keys to Your Data?***

Virtru Secures Data Across Your Google Ecosystem

Virtru provides the best of both security and ease of use, across the entirety of Google's ecosystem.

- ✓ No Software to Install
- ✓ Use Existing Identity
- ✓ Zero Trust Key Management
- ✓ Easy to Use for All
- ✓ Data Privacy, Sovereignty, Residency and Control



End-to-End Encryption Powered by Virtru

Gmail

Google Drive

Google Cloud

NOW

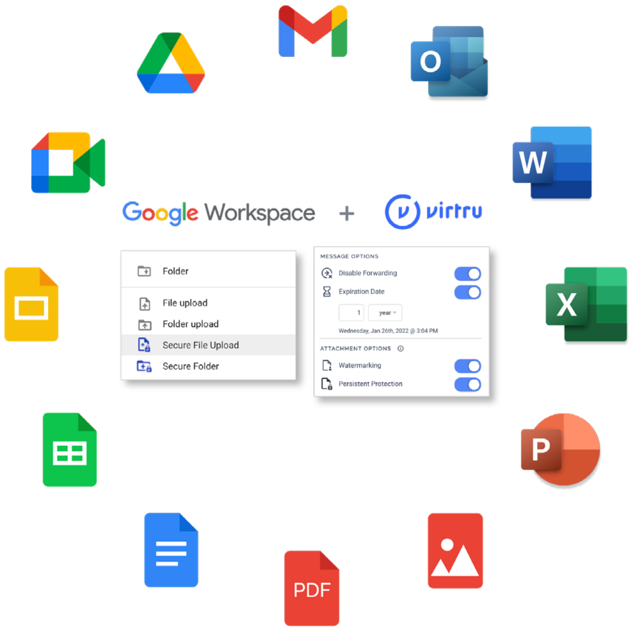
BETA

Most recent collaboration with Google Workspace Client-side encryption

Public, key-based technologies provide end-to-end encryption; however, they do so at the expense of usability. Portal-based encryption technologies don't encrypt the full path between the content's sender and recipient, and they also introduce a lot of complexity, often requiring users to create credentials or download additional software. With Virtru, you don't just get better Google security — you get total control and visibility; a seamless experience; and convenience for users, recipients, and administrators.

Unlike TLS and portal-based solutions, Virtru doesn't just encrypt your data in transit. Your message is encrypted from the moment you strike up a new draft. Because Virtru uses true end-to-end, client-side encryption, there are fewer points of vulnerability along your email's path to your recipient's inbox. Your message stays safe, and no third parties can access your data, including Virtru. Your business maintains full control over your keys and your content.

Beyond encryption, Virtru also adds granular access control. Users and administrators can control who has access to sensitive content with features like message revocation, expiration, forwarding control, and file watermarking. Virtru also adds powerful audit capabilities via the Control Center. You can track emails and attachments sent to or from anyone in your organization and trace where outgoing emails have been forwarded.



MESSAGE OPTIONS

Disable Forwarding ●

Expiration Date ●

1 year

Wednesday, Jan 26th, 2022 @ 3:04 PM

ATTACHMENT OPTIONS

Watermarking ●

Persistent Protection ●

Finally — but importantly — Virtru is exceptionally easy to use, for everyone involved. You can deploy across your organization in minutes, and because it's integrated directly within the Google interface, your users simply have to click a button to encrypt a file or email. There are no extra credentials to remember. You don't have to exchange keys manually with your recipient.

Whether you need to meet regulatory requirements or you need to protect sensitive legal, financial or HR information, encryption is a critical component of strategic enterprise security. Virtru provides the easiest, most secure, and holistic framework to protect your data across Google Workspace, Google Cloud, and beyond.

Want to explore how Virtru can add a layer of security to your Google ecosystem? Contact us to start the conversation.

virtru

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 6,000 customers trust Virtru for data security and privacy protection.