The Complete Guide to **Email Encryption for G Suite Administrators**

virtru

Google Cloud Partner

The Complete Guide to **Email Encryption for G Suite Administrators**

Alarming increases in security breaches and data leaks, new and expanded regulatory regimes and a growing public awareness of digital privacy have all contributed to a burgeoning need to protect sensitive information.

Email is at the center of how people communicate in the business world. Professionals send more than 108 billion emails each year, and that number is likely to grow to 139 billion by 2018, according to research conducted by The Radicati Group. Many of the emails poses potential security and regulatory compliance risks. Email is still the most important collaboration tool and represents the greatest security and compliance risk for businesses today.

From invaluable intellectual property to sensitive employee data, the corporate inbox is a veritable treasure trove for hackers and a rich opportunity for costly user error (has anyone hit "reply all" or "forward" by mistake? These simple mistakes can cost literally millions). That's why your security strategy must include comprehensive email security, including client-side encryption.

Perhaps an equally significant enterprise risk is regulatory compliance. Along with increases in data breaches, government regulators have increased oversight of data privacy and security measures. In the United States, for example, HIPAA, CJIS, FERPA, PCI, ITAR and many other regulations require specific steps, including encryption, to protect sensitive information.

Taken together, security and regulatory risk make email encryption a priority for enterprise security teams. Add in the increasing need to share sensitive information, the proliferation of devices, and the move to cloud-based systems like G Suite (formerly known as Google Apps), and it's clear that IT and security professionals need new email protection plans.

This guide will explain the factors driving the need for email encryption, walk you through the options available to organizations using G Suite

and provide a practical security checklist for your organization. It will also provide a brief overview of Virtru, a practical client-side encryption solution for G Suite.

Your Data Is Your Business. And It's In Your Email.

According to Symantec's Internet Threat Security Report, email malware creation was up 26% year over year in 2014, with hackers creating 317 million new pieces of malware. That brings the total overall count to 1.7 billion individual pieces of malware, each of which can lead to data leaks, personal identity theft or costly compliance violations. To put this into perspective, this means that there's an individual piece of malware for every four people on earth.

What are all these cybercriminals going after? What makes your organization's email so enticing? As it turns out, your servers and emails contain plenty of data that hackers (and even unwitting users) can expose to unintended eyes.

"There's an individual piece of malware for every four people on earth."

Legal Data. There's a reason why the American Bar Association has an entire page on its website dedicated to encryption. A breach of sensitive legal data, whether a simple case of user error or a malicious attack, can rack up costly fines and fees, as well as damage your company's reputation and your clients' sense of trust.

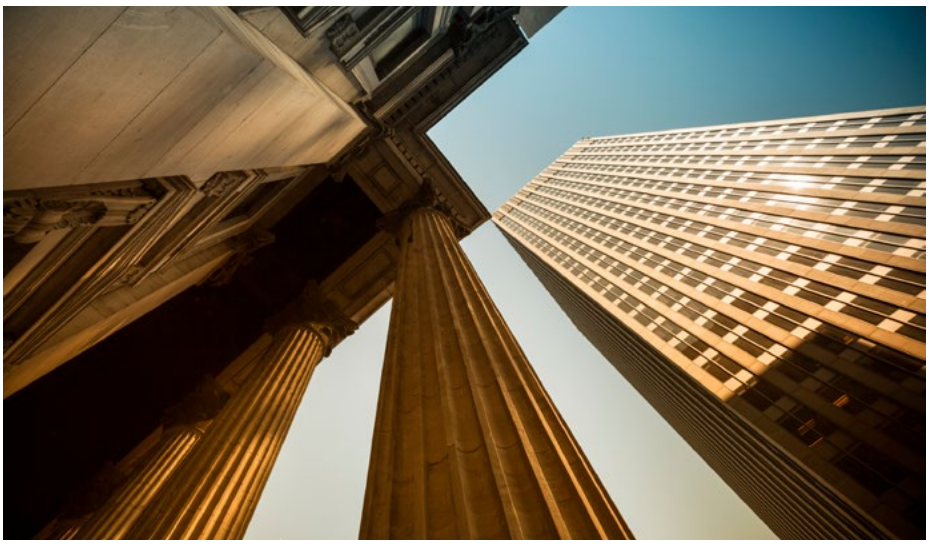
Financial Data. This can include your own internal accounting information, company credit cards and other sensitive financial documents, or customer financial data. If you process credit card transactions for customers, for example, those credit card numbers can be batch sold on the black market. Hackers are wise to the possibility that banks are proactive about detecting fishy transactions, so they need massive quantities of those credit card numbers to make it worth their time.

Human Resources Data. Any business that houses sensitive personal data, like social security numbers, is a major draw to criminals looking to steal someone's identity. All those tax documents your new hires have to fill out? Those are potential cash grabs for someone with bad intentions and some hacking know-how.

Intellectual Property. Though harder to put a number on than physical goods, your IP is one of your business's most valuable assets — and one that your competitors might love to get their hands on. Your patents, your published documents and your trade secrets make your business tick. Don't let them fall into the hands of corporate spies.

Regulation and Compliance

If your business uses a cloud email solution, it's crucial that you're aware of any compliance protocols your company must adhere to, as well as their email security and privacy requirements. Let's take a look at five common compliance protocols, and why email encryption is important to each.



HIPAA (The Health Insurance Portability and Accountability Act)
Doctors, nurses, hospital administrators, insurance professionals and healthcare clearinghouses all worry about HIPAA compliance on a daily basis. However, any organization that deals with protected health information (PHI), from HR departments to universities to government agencies and any other organization that provides support to covered entities, must take special care to protect health data.

"Any patient data transmitted by email, whether it's a brief overview of a recent appointment or a patient's most recent lab report, should be encrypted."

Key to maintaining HIPAA compliance — and avoiding costly penalties for slip-ups — is keeping PHI secure and private. That means that any patient data transmitted by email, whether a brief overview of a recent appointment or a patient's most recent lab reports, should be encrypted.

CJIS (Criminal Justice Information Services)
Law enforcement and government agencies on the federal, state and local levels are responsible for maintaining CJIS compliance in order to access federal databases of deeply sensitive criminal justice data. This data, which includes everything from fingerprints to background checks, can often make or break a case. Agencies who lose compliance are stymied in their ability to enforce laws and protect the public.

CJIS compliance requires not only data protection, but also access control and an auditable chain of custody for all criminal justice information. A vast amount of criminal justice data is transmitted by email, so using strong email encryption is a vital component of staying CJIS compliant.

PCI (Payment Card Industry)
Any business that deals with credit card data, including most online merchants, needs to meet the requirements set out by the PCI Security Standards Council. One of the most important aspects of PCI

compliance is protecting cardholder data. That means avoiding storing a customer's credit card data anywhere on your servers if possible. If you must store this data, it needs to be encrypted. And if any credit card information even crosses your network in transit, it better be secure.

Other sensitive customer information, like dates of birth or home addresses, should also be encrypted to protect customer privacy and prevent data leaks or identity theft.

FERPA (The Family Educational Rights and Privacy Act)
FERPA gives students (or, if they're below the age of 18, their parents) the right to review, challenge, and consent to any disclosure of educational records, provided they go to an educational institution that receives federal funding. This includes grades, standardized test scores, behavior reports, health data and more. As students and teachers make increasing use of email to communicate and turn in work, and as teachers email parents to check in on students, the vulnerability of unencrypted email becomes a threat to FERPA compliance.

If you use G Suite for your email, there are several measures you can take to lock down your messages, but knowing is half the battle. As security, privacy, and meeting regulatory requirements become top priorities for enterprise IT, it's critical to understand how Google protects you, and when additional layers of security might be beneficial.

Moving to the Cloud

If you're switching from an on-premise hosting system to a cloud solution, like G Suite, you know that the flexibility, scalability and collaboration promised by the cloud can help your business save money and time. But what about security?

For instance, how can you achieve compliance by housing personal health information (PHI) in cloud-based systems? To what extent can you store copies of sensitive content on Google servers? Do you have data residency requirements that mandate storage of sensitive data only in certain geographic regions?

G Suite (formerly known as Google for Work) provides many built-in data security protections, particularly for information shared within the Google ecosystem. To maximize security and ensure regulatory compliance, there are certain questions your organization should consider.

Google offers some of the industry's best security and compliance capabilities for data shared within the Google ecosystem. But, depending on your regulatory and data privacy requirements, you might need additional security capabilities to protect your info no matter where it travels.

How Does Gmail's Native Encryption Protect Your Data?

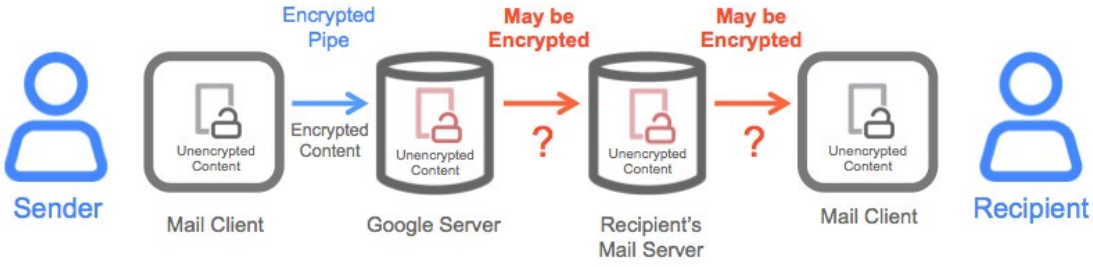
Google mandates secure server connections for all email sent from or received by Gmail users. By providing transport layer security (TLS), G Suite adds a critical layer of security that on-premise solutions lack, and ensures that communications sent to or from your mail server will remain encrypted–assuming the other servers that they travel through also support TLS. In addition, Google has made significant efforts to convince other service providers to use TLS.

TLS provides a solid foundation for email security, particularly for communications that remain inside the Google ecosystem. But since no cloud provider has control over servers outside of their ecosystem, you ultimately have no control over how many servers your emails pass through, and no way to predict the security measures that these servers provide.

In other words, as soon as your email leaves Google's server, it's vulnerable, and that vulnerability doesn't just end with your recipient. Every person your recipient forwards your email to creates another vector of attack and risk of a data leak.

Given these circumstances, and the fact that most on-prem email platforms do not support TLS like Google does, you might consider adding a client-side encryption tool like Virtru to your G Suite domain. As the name implies, client-side encryption protects your data from the time it is created until it is consumed by your recipients, or anyone else to whom they send it.

This additional layer of protection ensures security regardless of where you or your recipients share your data.



Without client-side encryption, your data is open to several points of vulnerability.

Types of Encryption

TLS

When we say that Gmail encrypts your email using TLS, what do we mean? You're probably at least a little bit familiar with TLS, because it's what encrypts secured connections you make using your Internet browser. If you look at your address bar and see "https" instead of "http," you know that your connection is encrypted by TLS.

To begin an encrypted connection, your computer initiates a handshake by sending a packet of information to the server it is trying to connect to, asking it to verify its identity. The server sends back a digital certificate, a piece of code that contains both a public key and an encrypted signature that proves that the server isn't an imposter.

"While using TLS encryption is better than nothing, it can't guarantee data security."

The public key attached to the certificate can then be used to send encrypted messages to the server, but it can't be used to decrypt those same messages — in order to do that, you need the private key, which only the server has.

While using TLS based email encryption solutions are better than nothing, they can't guarantee that your data is being transmitted between servers securely. While your data might be secure when it leaves your computer, there's no guarantee that it will remain that way on its journey to the intended recipient's computer.

Portal Systems

Many organizations, particularly covered entities that must comply with HIPAA, choose to use all-in-one portal systems to manage their sensitive data and encrypt email. However, these solutions don't provide true client-side email encryption. While data on the organization's server and messages sent via the portal are secure, that data has to reach the server before it can actually be encrypted.

With portals, messages and data aren't encrypted on the device you're using. Additionally, they are often decrypted on the server, before reaching the endpoint device. This leaves multiple opportunities for data breaches. All it would take to gain unauthorized access to that data would be to gain access to a specific device (for example, by stealing a laptop). Likewise, data can be stolen while it's in transit.

The other major shortfall of portal systems is that they're painful to use. User friendliness and interface design do not usually provide enjoyable experiences for employees, customers, or patients, who have to remember new sets of credentials to access their data. This leads to workflow disruption, lost productivity and countless calls to your IT help desk.

In the Google world, the most common portal application is called Google Apps Message Encryption, or GAME. Despite the name, this isn't a native G Suite feature, but a portal-based email encryption solution offered by a third party. It suffers from all of the security and usability limitations of other portal based solutions. In addition, it is not client-side, which means it will not meet many regulatory and privacy requirements.

Client-Side Email Encryption

Client-side encryption ensures your message remains encrypted from the time you send it to the time it is received. Any server your email touches won't be able to read it, as it will have no way to decrypt the email — only the intended recipient will be able to use their key to decrypt your message. Not only are you giving cybercriminals fewer opportunities to access your email, but you're also keeping your email private from the servers it lives on. Neither Google nor Virtru has access to your content, and your recipient's provider doesn't have access to your content. Only you and your recipient have access to the content.

Think of it as a language that you make up with a friend: you can drop messages in each other's mailboxes, and nobody else will be able to intercept and understand that message. Without client-side encryption,

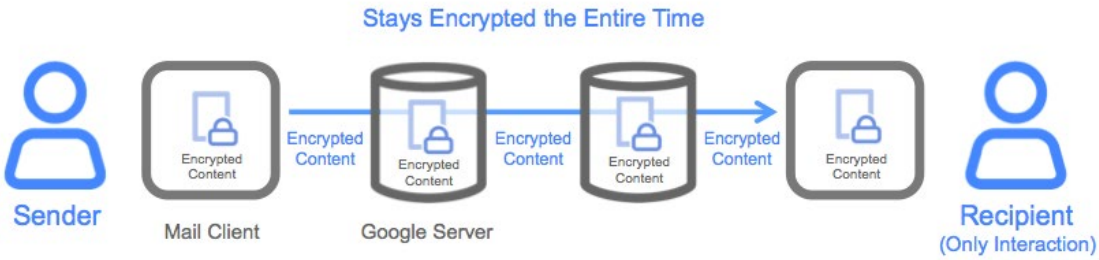
you'd have to create a dictionary explaining the language and trust it with a third party. If you're looking for the most secure, private way to send email or transmit data, client-side encryption is the answer.

Requirements for the Cloud Era

Email encryption is particularly important in the cloud era, now that organizations don't have as much ownership of — or visibility into — the infrastructure and applications that make their businesses tick. Any viable email encryption solution for cloud-hosted email requires three basic things: client-side protection, ease of use and key management and control.

Client-Side Protection

The only truly secure encryption solutions for enterprise email must include client-side protection. Your business can't afford a major loss of data because an email was compromised on the recipient end. Unlike TLS and portal-based solutions, client-side encryption protects email the moment you create a draft, and that content stays protected even after your recipient receives it. Additionally, some regulation and compliance regimes require client-side encryption. So if you need to stay CJIS compliant, TLS isn't going to cut it.



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

Key Management and Control

The whole point of using encryption, beyond protecting against data theft and leaks, is to own your own data. When you use the TLS encryption 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.

"The whole point of using encryption is to own your own data."

Only with a true client-side encryption solution do you have complete, granular control over encryption keys, and therefore who can unlock and access your content.

Ease of Use

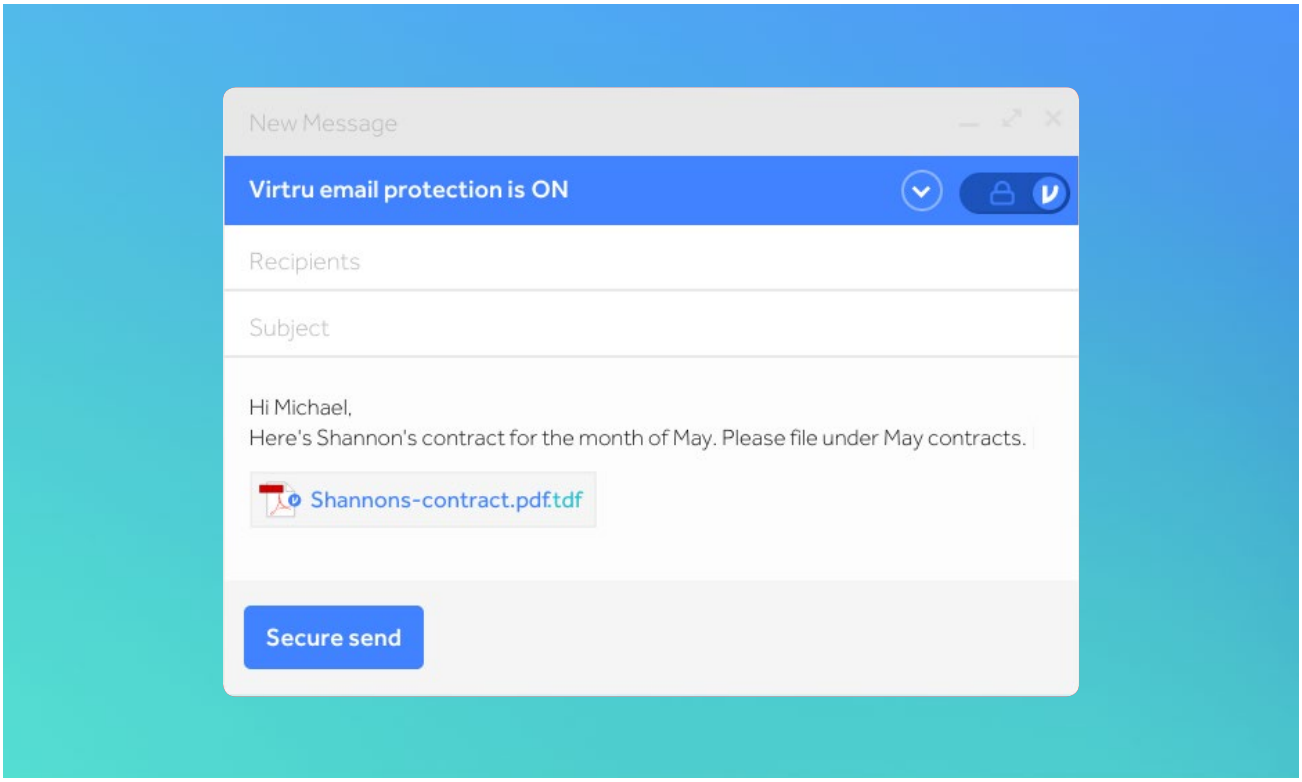
One issue businesses commonly encounter with client-side encryption is that legacy solutions like Pretty Good Privacy (PGP) and S/MIME are a pain to use. PGP will give you control over your keys, but key management is a painstaking manual process best undertaken by someone with significant technical know-how (and plenty of time on their hands). S/MIME requires you to purchase a separate digital certificate for each person using your encrypted email solution, and isn't compatible with many email clients.

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 dealing with the volume of incoming and outgoing emails an enterprise receives on a daily basis. Organizations moving to Google expect ease of use and simplicity, and legacy approaches to client-side encryption just don't follow suit.

Introducing Virtru

Compared with legacy approaches, Virtru provides the best of both security and ease of use. Public key-based technologies provide client-side 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. This unnecessarily exposes the content to eavesdroppers and can lead to a data breach or other compromise of confidentiality.

With Virtru, you don't just get better Gmail security — you get total control over your secure email, a seamless Gmail experience and convenience not only for users, but also for admins. In addition to client-side encryption, Virtru allows company admins to control forwarding and recall emails, so your organization's data is protected at every step of the email's journey.



Unlike portal solutions, Virtru doesn't just encrypt your data in transit. Your message is encrypted from the moment you strike up a new draft, so Virtru never has access to your email content. Because Virtru uses true client-side encryption, there are fewer points of vulnerability along your email's path to your recipient's inbox. Your message stays safe from beginning to end, and no third parties can access your data, including Virtru. Your business maintains full control over your keys and your content.

Also, with Virtru, you can monitor data going in and out of your domain from a centralized dashboard. It just takes a minute to add to your domain, and your users only have to download a simple browser plug-in. You can track emails and attachments sent to or from anyone in your organization, as well as control forwarding and revoke messages at any time. You can also trace where outgoing emails have been forwarded.

The best part? Virtru is convenient both for senders and recipients. You never have to leave Gmail to send and receive encrypted email. There are no extra credentials to remember. You don't have to manually exchange keys with your recipient. To send an encrypted email, you simply click a switch, compose and send your email as normal.

Protect Your Business with Virtru for G Suite Today

Whether you need to meet regulatory requirements for HIPAA or CJIS, or you need to protect sensitive legal, financial or HR information, encryption is a critical component of enterprise security. Virtru's email encryption is the easiest, most secure way to protect your business on G Suite.

To see if Virtru is right for your business, you can:

- Download Virtru for free now and start sending securely
- Integrate your domain for free and access admin controls within minutes
- Contact us and request a demo

Email Encryption Needs Assessment Checklist

The following checklist will help you to evaluate your organization's need for email encryption and determine appropriate solutions to meet your requirements.

Requirement	Needed in My Organization (Y/N)	Google Alone	Vendor A	Vendor B	Vendor C
Privacy Requirements					
Do you need to protect HR information?					
Do you need to protect legal information?					
Do you need to protect financial information?					
Do you need to protect intellectual property information?					
Regulatory Requirements					
Do you share personal health information (PHI) via email?					
Is your organization subject to CJIS regulation for criminal justice information?					
Is your organization subject to FERPA regulation for student information?					

Requirement	Needed in My Organization (Y/N)	Google Alone	Vendor A	Vendor B	Vendor C
Is your organization subject to ITAR regulation for defense information?					
Does your organization have data residency requirements?					
Functional Requirements					
Does your organization require client-side encryption?					
Does your organization need to be able to revoke or expire emails?					
Does your organization require data loss prevention to detect and automatically protect sensitive information?					
Do you want to require recipients to establish credentials on a separate portal system, requiring the administrator to manage passwords?					

About Virtru

By combining military grade encryption, cloud-based access and controls and seamless integration with applications like G Suite (formerly known as Google Apps for Work), Virtru enables security without getting in your way. Whether for regulatory compliance, security or corporate privacy, Virtru is the easiest way to protect sensitive information.

Try Virtru for G Suite at
www.virtru.com/google-apps-encryption.

Need to Encrypt Google Drive?

In addition to Gmail encryption, Virtru now offers client-side file encryption in the cloud. Contact us if you're interested in gaining early access for your business.