Evaluating Email Encryption Products

A Comparison of Virtru© and Proofpoint Email Encryption©

Importance of Email Encryption

Most modern email providers, such as Google and Microsoft, offer excellent default security options, but many customers require additional encryption and data protection capabilities to meet regulatory, compliance, or privacy needs. Email remains the most common method of business communication. It's where companies create, house, and share their most valuable information, which means it is also where unauthorized third parties look when trying to access corporate data.

By entrusting large technology companies like Google and Microsoft with their email, businesses and governments solve key infrastructure and collaboration problems, but they often rely on third party vendors for help with other encryption-related issues:

- External sharing and control
- Object-level protection
- Data loss prevention (DLP)
- Cloud provider access levels
- Corporate governance
- Data residency
- Encryption key management
- Regulatory compliance (HIPAA, CJIS, EAR, PCI, etc.)

Given the growing number of privacy and security concerns in today's corporate ecosystems, compounded by the emerging complexities of the cloud, it's essential that organizations understand the additional encryption options available to them, how these solutions work, and when it makes sense to deploy them.

> This analysis was completed by an experienced deployment engineer who has implemented both Virtru and Proofpoint at multiple large enterprises.

Objectives of this Evaluation

As security specialists, our customers rely on us to evaluate many email encryption solutions. In recent years, two companies have garnered the majority of interest in the market: Virtru© and Proofpoint©. This analysis was completed by an experienced deployment engineer who has implemented both Virtru and Proofpoint at multiple large enterprises.

The purpose of this document is to provide a head-to-head comparison of Virtru and Proofpoint, which calls its solution Proofpoint Essentials (PPE for short). We intend to compare these products objectively based on available functionality and overall user experience.

We list out the full functionality of each product in the "Feature Comparison Matrix" section, which assesses capabilities across the following areas:

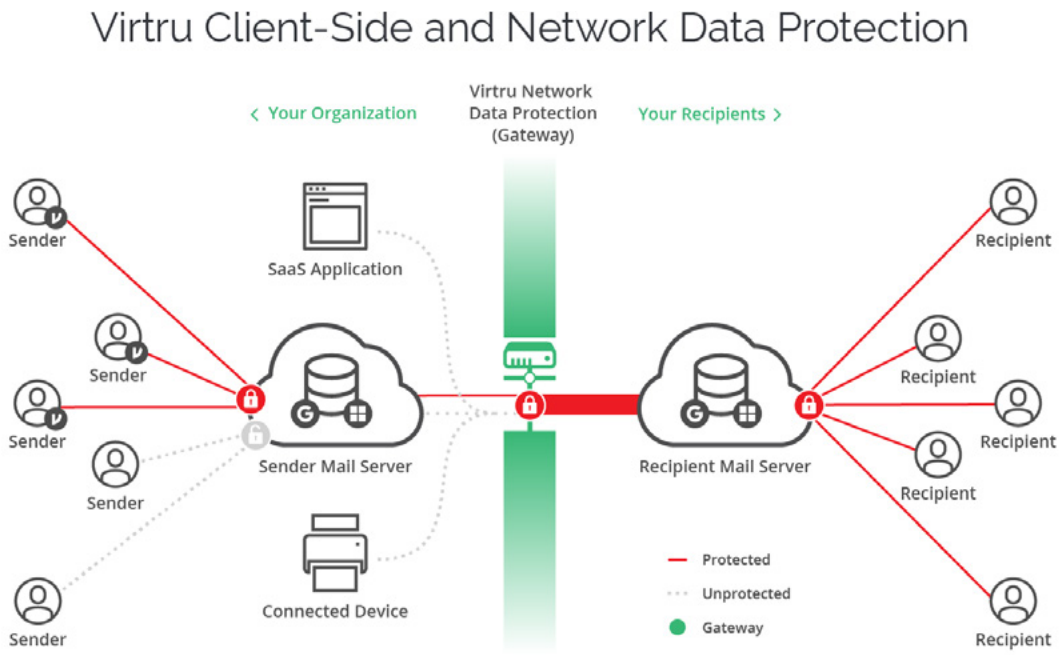
1. Sender UX
2. Recipient UX
3. Same Service Auto-decrypt UX
4. Mobile UX
5. Administrator UX
6. Control Features
7. Encryption
8. e-discovery
9. DLP Types
10. DLP Options

When evaluating any data protection solution, our team prioritizes three qualities, which we have highlighted here for Virtru and PPE in the "Key Findings" section of this document:

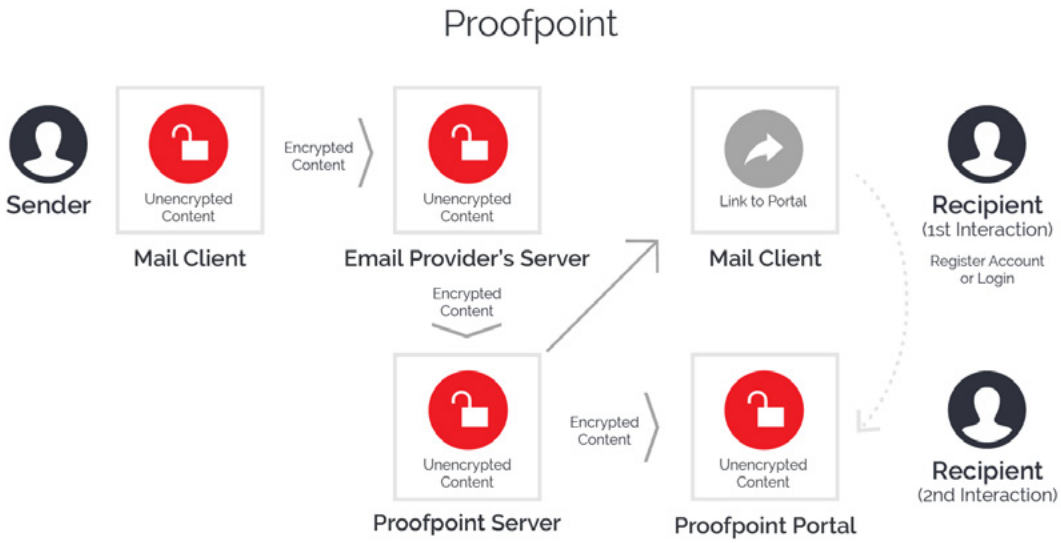
1. Ease of Use
2. Security
3. Control

To perform our evaluation, Wursta security experts deployed both Virtru and PPE within the same domain, using the same default settings that most email solutions provide for their customers. In certain instances, we had to adjust these settings in order to best compare functionality across products.

Architecture Comparison



- Choose to encrypt and decrypt content on the client-side, at the network level, or both to ensure protection from the time of creation no matter where data travels.
- No provider, including Virtru, Microsoft, and Google, has access to unencrypted content.
- Senders and receivers can use their native email clients or device; no portal, passwords, or other service is required.
- Customers manage access to encryption keys.



- Unencrypted plain text is sent via TLS connection.
- Email provider and Proofpoint have access to the customer's unencrypted content.
- Recipients must register a portal to read content, unless they are already registered PPE customers, in which case messages appear transparently in their inbox.

Feature Comparison Matrix

Category	Functionality	Virtru	Proofpoint Essentials
Sender UX	Max Attachment Size	100 MB	Email Provider's Max
	Read Receipt / Audit	✓	✗
	Sent Label Encrypted	✓	✗
	Encrypted Inbox Discovery	✓	✗
	Encrypt Notification	✓	Email Notification Only
	Above Line Plain Text	✓	✗
	Delegated Inbox (View Access)	✓	Not Encrypted (Plain Text Delivery via TLS)
	(Mobile) Send Encrypted in Native	✓	✓
Recipient UX	No New Password Required	✓	✗
	Branded Recipient Email Template	Logo + Text	Logo + Custom From
	Customized Recipient UX	Secure Web Reader	Portal (Logo & Color Scheme)
	Reply Encrypted	✓	✓
	Send to Anyone	✓	✗
	View Encrypted in Native	Secure Web Reader	Web Portal
	Max Attachment Size	150 MB	25 MB
Same Service Auto-decrypt UX	Receive	✓	Plaintext TLS delivery
	Send	✓	Plaintext TLS delivery
	(Mobile Client) Receive	Secure Web Reader or Virtru App	Plaintext TLS delivery
	(Mobile Client) Send	Secure Web Reader or Virtru App	Plaintext TLS delivery
Mobile UX	Browser Access	✓	✓
	Dedicated Mobile App	✓	✗

Category	Functionality	Virtru	Proofpoint Essentials
Admin UX	Roles	✓	✓
	Revoke	✓	✗
	Expiration	Per message / per recipient	Fixed Domain Default
	Admin Console	✓	✓
	Licensing Reports	✓	✓
	Customizable Portal	Secure Web Reader	Portal (Header & Footer Only)
	Siloed e-Discovery Role	✓	✗
	SIEM API	✗	✓
	Admin Reporting / Auditing	✓	✓
	Anti-Phishing	✗	✓
	Anti-Virus / Anti-Spam	✗	✓
Persistent Control Features	End User Revoke	✓	✗
	End User Forwarding Control	✓	✗
	End User Message Expiration	✓	✗
	End User PDF Watermarking	✓	✗
	End User Read Receipt	✓	✗
	Admin Read Receipt	✓	✗
	Admin User Revoke	✓	✗
	Admin User Forwarding Control	✓	✗
	Admin User Message Expiration	✓	✗
	Admin User PDF Watermarking	✓	✗
Encryption	Client-Side (Required for CJIS, EAR, and GDPR)	✓	✗
	Server Side	✓	✓
	Customer Can Host Encryption Keys	✓	✗

Category	Functionality	Virtru	Proofpoint Essentials
Encryption	Customer can Choose Key Location	✓	✗
	In-Transit Encryption	✓	✓
	No 3rd Party Access to Plain Text	✓	✗
	Object-Level Protection*	✓	✗
	Google Drive Encryption	BETA	✗
E-Discovery	End user Encrypted Search	✓	✗
DLP Types	Client-Side Scanning	✓	✗
	Server-Side Scanning	✓	✓
	Inbound Encryption Options	✓	✗
	Message Scanning	✓	✓
	Attachment Scanning	.PDF and .TXT files	✓
DLP Options	IP Address	Out of the box	Out of the box
	Credit Card Number	Out of the box	Out of the box
	Federal EIN Number	Out of the box	Out of the box
	Possibly Sensitive	Out of the box	Out of the box
	Social Security Number	Out of the box	Out of the box
	Account Number	Out of the box	Out of the box
	Confidential	Out of the box	Out of the box
	PII	Out of the box	Custom Lexicon/ Expression
	IP Address	Out of the box	Custom Lexicon/ Expression
	Non Disclosure Agreement	Out of the box	Custom Lexicon/ Expression
	Off the Record	Out of the box	Custom Lexicon/ Expression
	Password	Out of the box	Custom Lexicon/ Expression
	FINRA	Out of the box	Custom Lexicon/ Expression

* Data is encrypted the moment it is created and remains encrypted no matter where it travels.

Key Findings

Virtru and PPE enable email and attachment file encryption for communications, but they do so using very different approaches.

PPE processes email security policies at the network level, after messages have left the sender's browser/mail client, received by the sender's email provider, and then sent through an email gateway, which is hosted by Proofpoint.

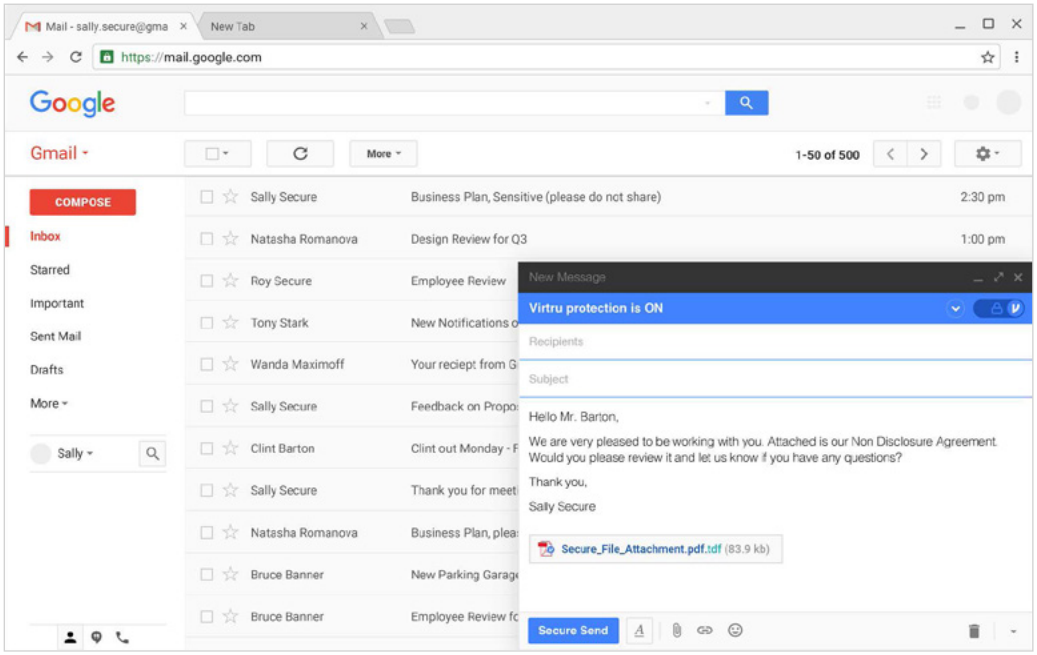
In addition to its Network Data Protection feature, which encrypts data at the server-side no matter where it's shared from, Virtru provides client-side encryption that protects emails from the moment they are created and keeps them secure at all times, wherever they travel.

This distinction means that Google, Microsoft, and other cloud providers can access PPE customer content, whereas only senders and receivers ever have access to Virtru customer content.

Virtru will soon release a product that adds encryption, access control, and DLP to documents stored and shared via Google Drive. This offering is currently in Beta. Proofpoint has no plans to support protection of file sharing platforms.

Ease of Use: End Users

Virtru integrates encryption directly into the sender experience in major browsers, email clients and devices with minimal disruption or change to the way users work. With a simple toggle, senders can decide on-demand which messages and files to encrypt. In addition, Virtru's DLP allows administrators to set policies that automatically encrypt certain messages.

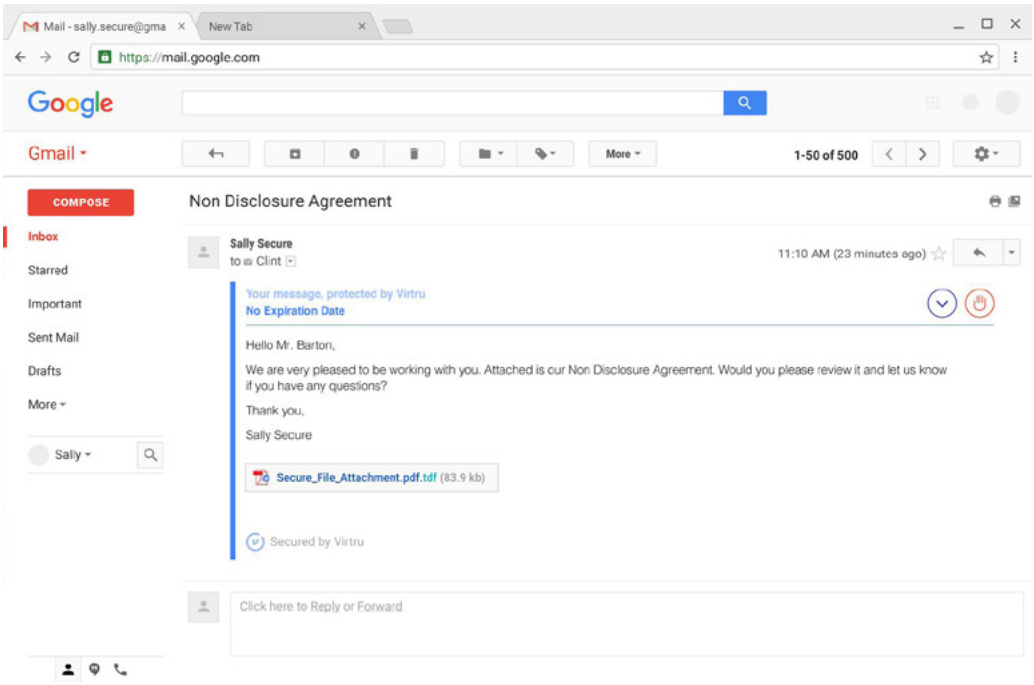


Virtru Integrates Directly into Gmail, Outlook, OWA, and Other Tools

Sending with PPE relies on customer administrators to define filters in order to trigger encryption, such as including the string “encrypt” in the subject line. If users forget to utilize these filter keywords, their emails may be sent without encryption, unless a filter is set to encrypt all mail from a given domain. Additionally, users can create separate filters to scan email with PPE’s “Smart Identifiers” or “Dictionary” features, but these capabilities are only available if PPE is configured as the outbound email gateway for the domain.

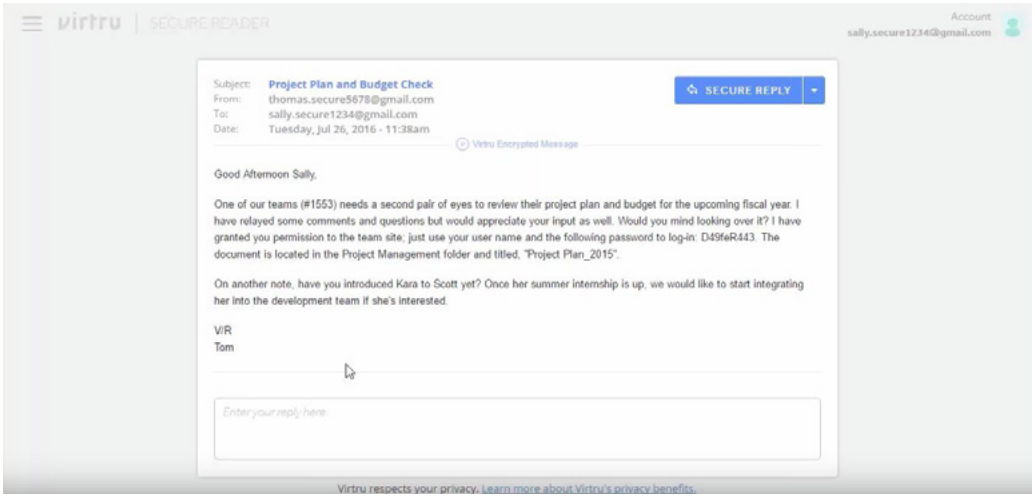
Virtru uses existing platform credentials to enable recipients to decrypt and consume messages and content. Virtru provides recipients with two authentication options:

- Users can activate an extension that enables them to read their messages, as well as send their own encrypted messages, directly from Gmail, Outlook, or mobile.



Virtru Gmail Recipient Experience

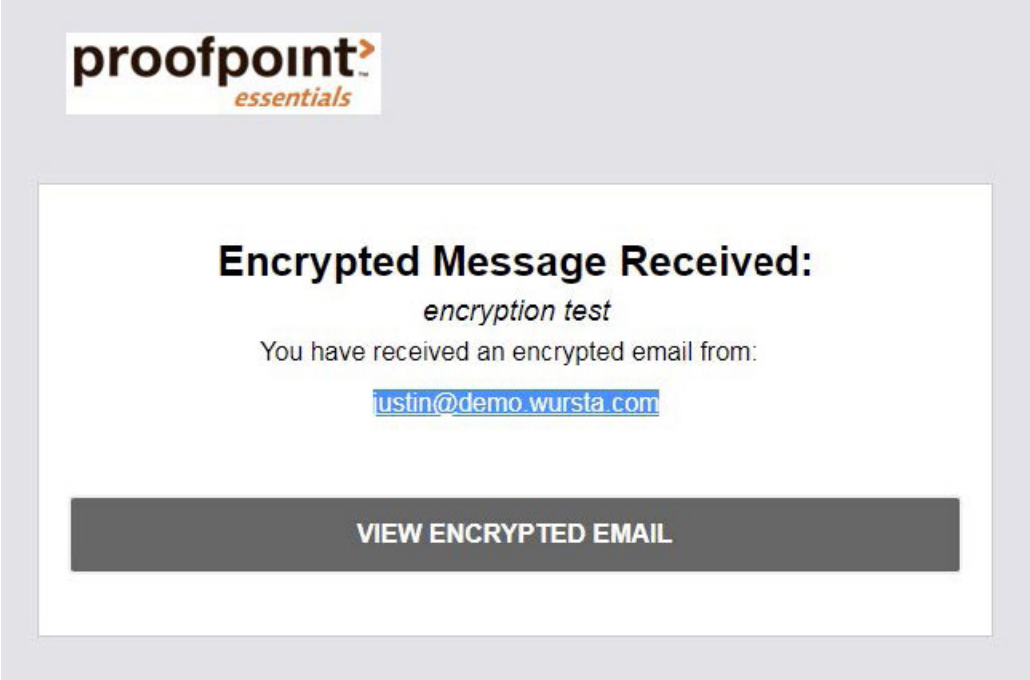
- Users can read via a secure web reader that opens in the browser.



Virtru In-Browser Recipient Experience

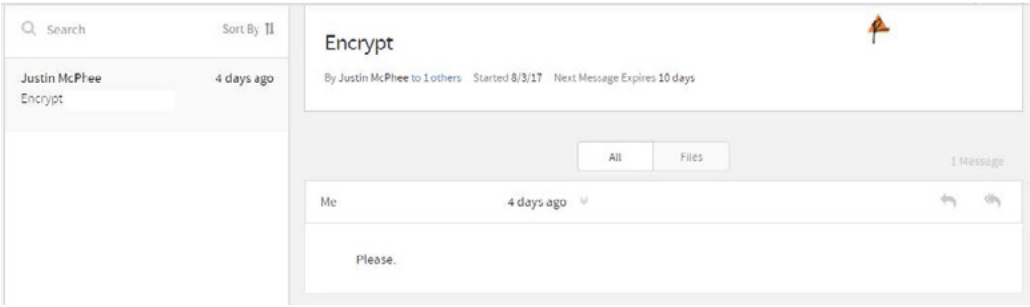
In both cases, Virtru enables authentication with existing platform credentials. No new software, accounts, or passwords are required.

Recipients who have already configured PPE onto their email servers can read PPE messages transparently. If recipients do not have PPE configured, they must create a password-protected account to access encrypted messages from the Proofpoint secure email portal.



Proofpoint Message Seen by External Recipient

After account creation, their secure messages will be available only via this portal; they will not be visible in the recipient's standard inbox.



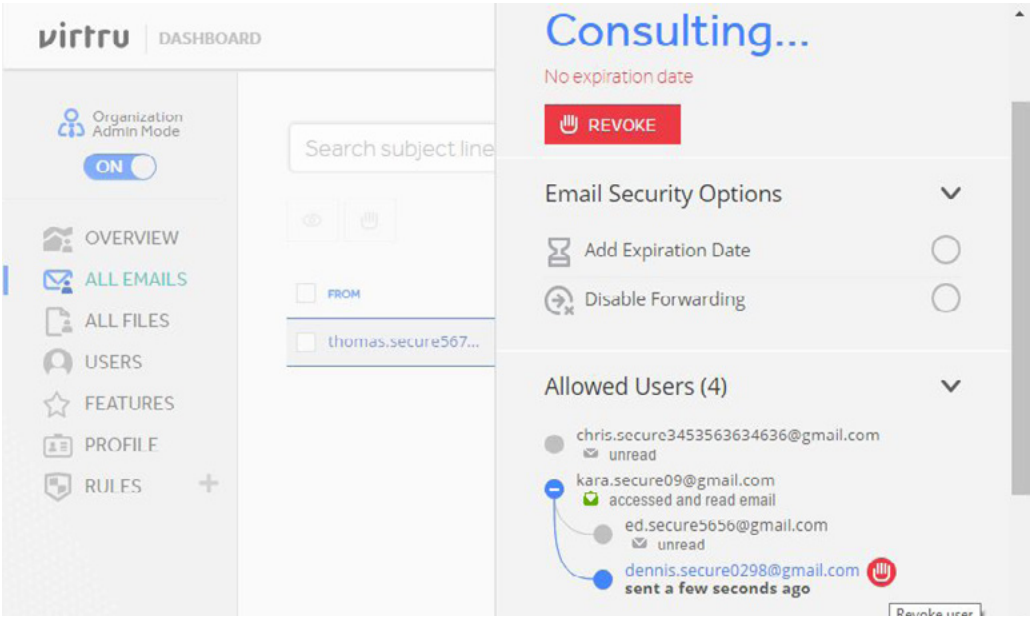
Proofpoint-Hosted Recipient Portal

A common complaint from PPE users is that receivers often forget passwords and cannot access the portal and their messages, which admins report is frustrating to recipients and creates additional support burdens for IT.

Ease of Use: Administrators

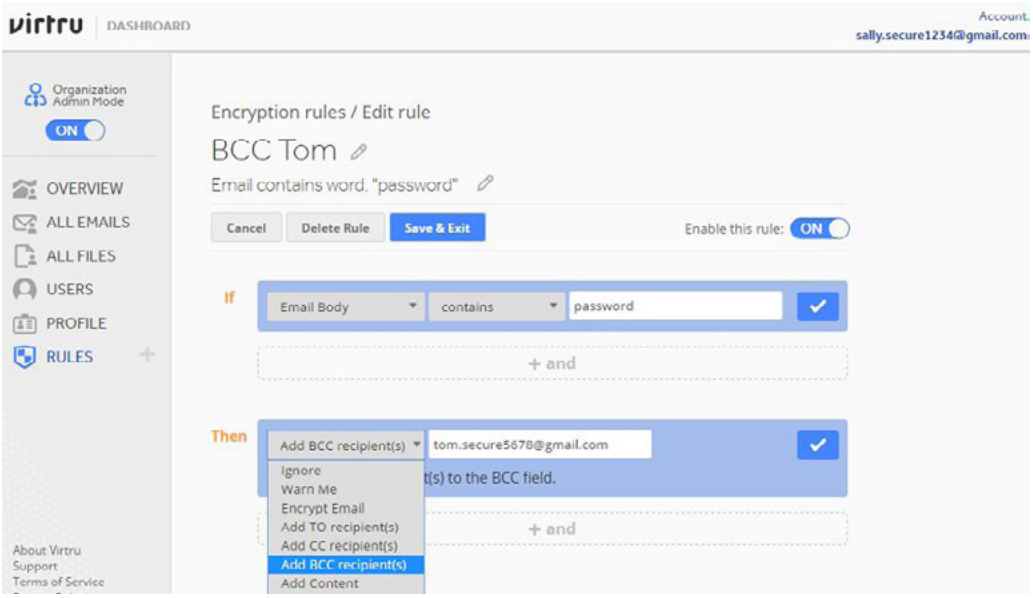
Virtru offers a centralized dashboard from which administrators can:

- View active Virtru users
- Track where end-user emails travel and control access
- Configure DLP rules — for the entire domain or for specific OUs and groups



Virtru Forwarding Tree for Administrators

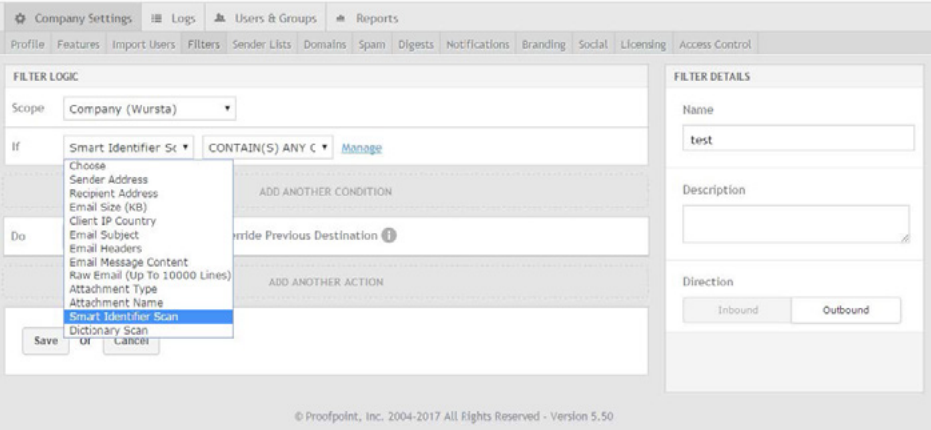
Compared to Google and Microsoft's DLP options, Virtru's dashboard provides a flexible and straightforward interface:



Virtru's DLP Rule Builder

In addition to message bodies and metadata, Virtru's DLP can scan the content of .PDF and .TXT attachments, where PPE DLP can scan a wider variety of attachment types. However, Virtru customers looking for enhanced attachment scanning capabilities can use Virtru with existing third party DLP solutions that support these and other features.

Like Virtru, PPE administrators can configure DLP rules via an administrative console. These rules can only scan content after it has already left the sender's device, so customers must give Proofpoint access to unencrypted content in order to utilize its DLP capabilities.



Proofpoint DLP Rule Console

Security

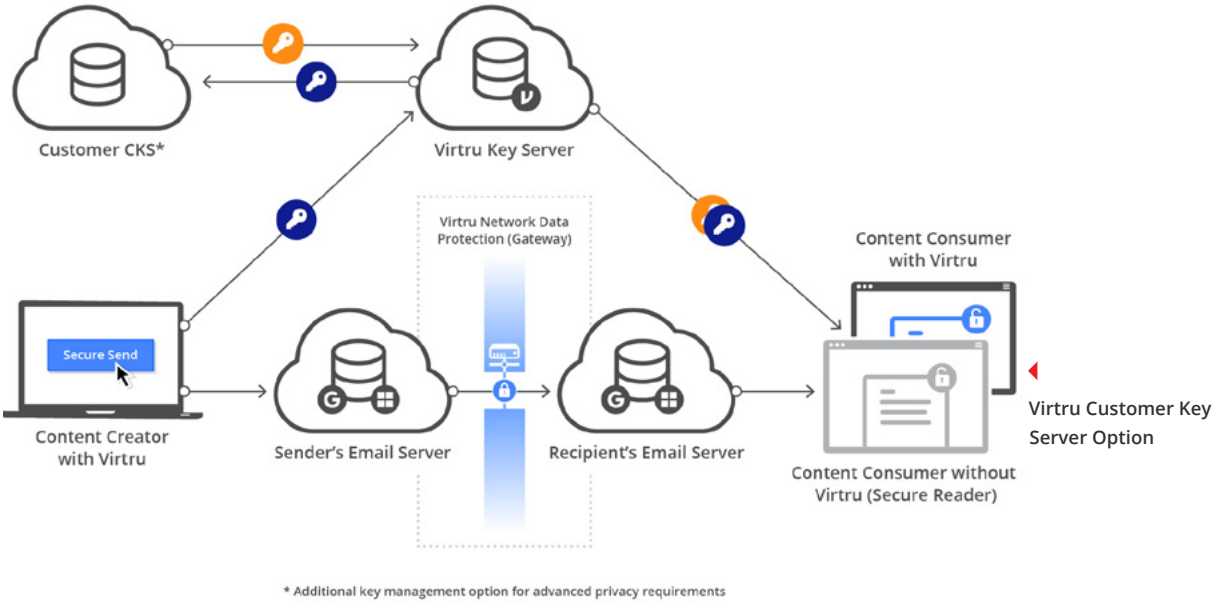
Virtru protects emails and attachments using object-level, or data-centric, encryption. This means that data is encrypted the moment it is created, and it remains encrypted no matter where it travels. Like regular Gmail and Outlook messages, content is transmitted and stored on Google or Microsoft's (or any recipient's mail provider's) servers, but in encrypted form. The encryption keys that protect these emails are stored on Virtru's servers, and access to them is always managed by the customer.

Since protected content and encryption keys are stored separately, neither Google, Microsoft, nor Virtru — nor any other cloud provider — can access unencrypted customer content.

PPE protects emails and attachments after they have left the sender's device. Messages are encrypted in transit via Transport Layer Security (TLS) until they reach the sender's email provider's servers, at which point the email provider has access to the customer's unencrypted content. Unencrypted content is then sent via TLS to Proofpoint's servers, where it is hosted.

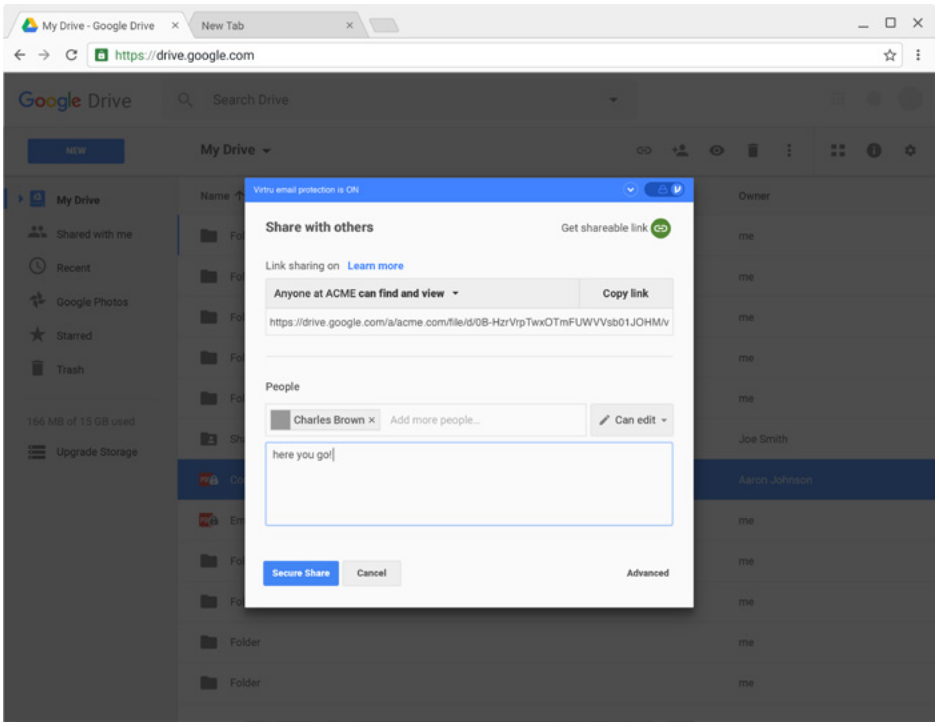
Unlike Virtru, both email providers (i.e., Google and Microsoft) and Proofpoint can access the unencrypted content shared by their customers, which prevents PPE from meeting certain data residency, privacy, and compliance (CJIS, EAR, GDPR, etc.) requirements that Virtru can satisfy.

Virtru also offers a Customer Key Server (CKS) feature that enables organizations to maintain complete and exclusive access to the encryption keys that protect their data. The CKS adds public key encryption to Virtru's standard SaaS product, so that the encryption keys hosted on Virtru's servers are encrypted by additional keys that only the customer can access.



As a result, Virtru customers can choose where their encryption keys are stored, either in the cloud or on a physical device. Proofpoint does not allow customers to manage or host their own encryption keys or choose where they are located.

Virtu also supports encryption and control of documents stored and shared via Google Drive. As of August 2017, the product is in Beta. Proofpoint has no plans to support encryption of file sharing platforms.

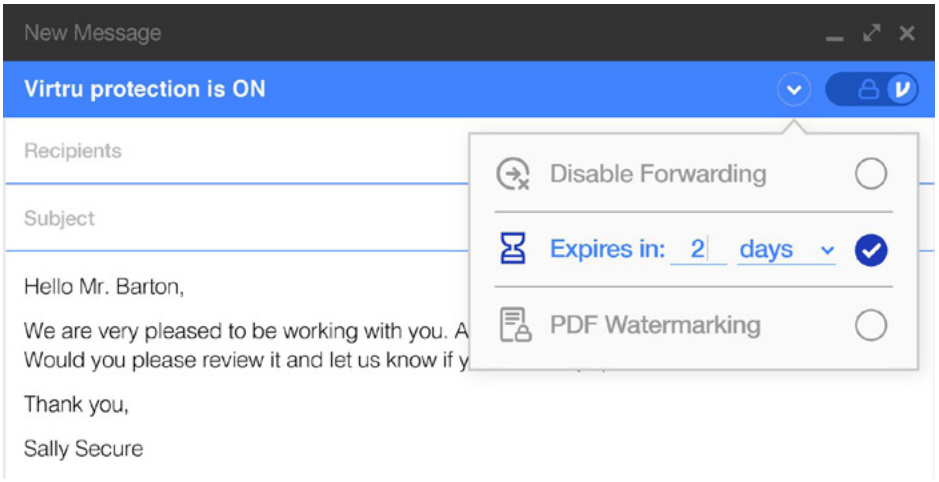


Virtru's Google Drive Protection

Control

While PPE leverages a traditional portal-based approach to email protection, Virtru offers a more modern, object-level architecture, which affords users and administrators the opportunity to exercise granular, persistent control of emails and files. Since content is not protected at the object-level, PPE does not offer any control capabilities.

Virtru allows both senders and administrators to manage access to encryption keys. Users can control their encrypted emails and files in several ways — even after they've been read.



Virtru Sender Control Capabilities

Senders can use these features for the emails that they send, while administrators can use them on behalf of any of the encrypted emails sent by users in their organization:

- Revoke message access
- Expire message access
- Disable message forwarding
- Track where messages have been forwarded
- See when messages have been read
- Watermark PDF attachments with recipient email addresses

Summary

PPE provides a seamless experience for recipients whose organizations are Proofpoint customers. It meets some security use cases, but does not offer client-side encryption or control, so many privacy and regulatory requirements will not be covered.

Virtru's integration directly into existing email platforms provides a user experience that mirrors Gmail, Outlook, and OWA. The combination of client-side encryption with customer-managed keys provides enhanced levels of privacy and control that enable organizations to protect data even after it has left their domain. Since there is no third party or provider access to unencrypted content, Virtru's encryption meets most privacy and regulatory requirements.

For organizations that communicate primarily with other Proofpoint customers, PPE is a good fit.

For other organizations evaluating encryption, we recommend Virtru for three reasons:

1. Direct integration to Gmail, Outlook, and OWA and lack of recipient portal provide excellent ease of use.
2. Client-side encryption prevents third parties from viewing customer content — a security requirement for many organizations with regulatory or privacy requirements.
3. Message control capabilities allow customers to manage access to emails and files even after they have been shared outside the sender's domain.

Additionally, organizations interested in protecting all of their data — beyond just emails — will be better suited with Virtru, since they will soon release a product that protects Google Drive documents. Proofpoint has no public plans to move beyond email protection.

About Wursta

At Wursta, we are shaping the way our customers use technology to grow their businesses. Our organization represents a new breed of consultancy — one that combines a depth of Cloud experience that is unparalleled in traditional consulting firms, with a focus on imaginative efficacy. This model incentivizes the inception and development of effective processes through new technologies. Our approach is centered on generating value for our customers; it is our commitment to measure everything that we do for our customers with business value creation. In many ways, we are helping organizations invent the way they will do business for years to come.

About The Author

Phil Behmer has been deploying collaboration tools for enterprises and state governments since 2010. These deployments often require additional email encryption for meeting regulatory compliance and business privacy. Some of his former clients used either only Virtru or Proofpoint services, while some used a combination of both. Through his experience with these deployments, Phil has become one of the industry's foremost experts on encryption solutions, in addition to DLP configuration, provisioning, user management, e-discovery, authentication, and bulk data migrations.