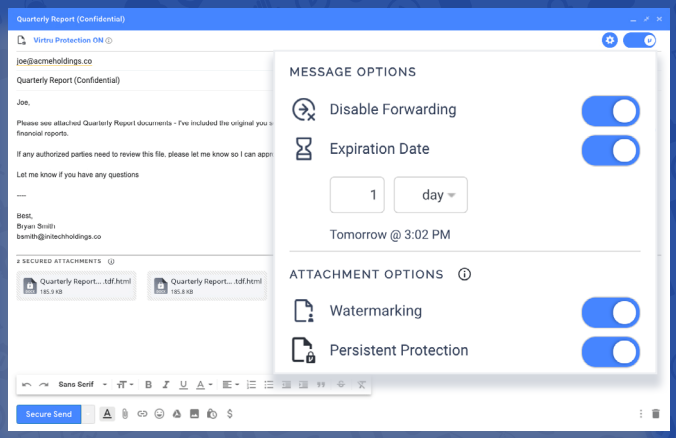
Virtru vs. Egress

Comparing Email Encryption Products



In today's fast-paced business world, email remains the most pervasive form of business communication. It's where companies create, store, and share their most valuable information, causing attackers and unauthorized parties to target inboxes when trying to access sensitive corporate data and regulated private personal information.

When developing your secure email strategy, you must first understand that email platforms are not perfect—breaches and hacks do occur and even the most modern email platforms (Google and Microsoft) aren't secure by default, so adding an additional layer of security with encryption is oftentimes mission-critical. Many customers require additional encryption and data protection capabilities to meet regulatory, compliance, or privacy needs, such as:

- 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, FERPA, CJIS, PCI, NIST, ITAR, GDPR, CCPA, GLBA, CFPB, etc.)

As organizations navigate the growing number of privacy regulations, security concerns in today's corporate ecosystems, and the emerging complexities of the cloud, it's critical that they understand the additional encryption options available to them and how these solutions work.

Two prominent email encryption solutions, Virtru and Egress, enable email and attachment file encryption for increased security and privacy, but they do so using very different approaches. What follows is a head-to-head comparison guide of Virtru Email Encryption vs. Egress's email encryption product, Egress Protect, evaluated in four key areas:

1. Sender protections and UX
2. Recipient access and UX
3. Administration
4. Security and privacy

Capability of Offered Solution to Support Feature Need:

○ No solution ◔ Minimal solution ◑ Partial solution ◕ Good solution ● Complete solution

Detailed Comparison

Sender Protections and UX

Feature	Virtru	Egress Protect
Email Encryption	◕ Client-side, end-to-end encryption supported for Gmail browser extension and Outlook add-on. Gateway-level encryption options available.	◑ Client-side, end-to-end encryption supported for Outlook-to-Outlook workflows between paid customers. If recipient does not have Egress, decryption reveals plaintext within the browser session. Gateway-level encryption only for Gmail browser extension and mobile.
Attachment Encryption	◕ Supports up to 150MB total per email.	◕ Supports up to 5GB per email for paid accounts. Unpaid users have 50MB file size limit within Egress Web Access.
Persistent Protection (Beyond Email) for File Attachments	● Supported via .tdf.html file extension, with seamless decryption and access via Secure Reader.	◑ Supported via .switch file extension, but decryption and access require manual steps for recipients.
On-Demand, In-App Encryption and Controls	●	◔

Sender Protections and UX - cont.

Feature	Virtru	Egress Protect
Revoke Access / Recall Message	Revoke directly from your Sent folder or Vitru Control Center.	Revoke from separate application.
Set Expiration	Available directly from the Compose window.	Available via hidden submenu.
Disable Forwarding		Not available to end users; only via admin-defined classification rules.
Attachment Watermarking (and Pairing with Disable Print, Copy, Save, and Download)		Not available to end users, only via admin-defined classification rules.
Read Receipt Visibility for Audit		
Encrypted Search	Encrypted search included within email encryption offering.	Encrypted search supported via separate product (and cost), Egress Investigate.
Above Line Plaintext Intro to Improve Recipient Experience/ Access		
Mobile Support	Mobile app supports end-to-end encryption and granular controls.	Mobile app only supports gateway-level encryption. iOS app does not support Gmail environments.

Sender Protections and UX Summary:

The key point of differentiation is that Virtru encryption occurs directly within the Gmail and Outlook email clients, encrypting the email message and attachments at the object level. Egress also encrypts email messages at the object level, but whether it is end-to-end encrypted depends on the use case. For Outlook, end-to-end encryption is supported when the recipient also has Egress for Outlook, but when the recipient does not, the decryption process for the Egress Web Access portal reveals plaintext within the browser session, not meeting requirements of true end-to-end encryption. For Egress for Outlook or Mobile, encryption happens at the gateway, also failing to meet the definition of true end-to-end encryption. With Virtru, only the sender and authorized recipients have access to unencrypted content for true end-to-end encryption: third parties (including Virtru) cannot access protected content throughout the data lifecycle.

With easy-to-use controls, Virtru senders can apply more granular and on-demand access controls with an intuitive UX, right within the compose window. Egress senders are limited in the controls they can apply based on the classification rules and policies that administrators have configured, within a more cumbersome user experience. Virtru access control can be applied in any combination, directly within the Compose window, for more flexibility.

Both services include the ability to disable forwarding and set expiration. With Egress, expiration is the only option for end users (and it's only accessible via a separate menu from the compose window). Disable forwarding controls are only available to end users if the Egress admin has included it in a classification rule. Virtru streamlines revocation, allowing end users to revoke access directly from their sent folder, while Egress's revocation forces users to revoke access from "Sent Packages," a separate, redundant application workflow.

Further, Virtru offers watermarking for attachments, placing the authorized recipient's email address on the file to deter them from leaking screenshots or photos. Virtru's watermarking feature also prevents the recipient from printing, saving, copying, or downloading the file. While Egress supports these controls, they are not immediately accessible to senders as they're generally tied to admin-defined classification rules. This makes it difficult for the sender to prevent their recipients leaking sensitive, regulated content via screenshot or photo.

Virtru enables persistent protection for attachments leveraging the tdf.html file extension. This allows recipients to download protected files beyond the initial email for storage on their desktop, shared network drive, cloud collaboration platform (CCP), or anywhere else files are stored. Recipients simply authenticate and click on the file, and it opens automatically via Secure Reader. Egress offers a similar capability but without Virtru's patented ease of use. Egress creates a .switch file extension, but decryption and access require manual steps for recipients, forcing them to upload the file into a separate application workflow, adding friction to secure collaboration use cases.

Egress creates a .switch file extension, but decryption and access require manual steps for recipients to upload the file into a separate application workflow, adding unwanted and unnecessary friction to secure collaboration use cases.

Recipient Access and UX

Feature	Virtru	Egress Protect
Seamless Authentication for External Recipients	● Recipients access protected data by authenticating their existing account via federated identities.	○ Recipients must create and manage a new portal account ID and password to access protected data.
Branded Recipient Email Template	●	●
Branded Read / Consumption Experience	● Custom logos and graphics supported.	○ No customization available.
Recipient Send / Reply Encrypted Support	◕	◕
Seamless Attachment Download (Where Permitted) for External Collaborators	●	○ Requires download of Egress client software.
Mobile Access	●	◑
No Intrusive Personal Security Questions Required	●	○ Account sign-up requires personal questions for validation, forcing recipient to reveal unnecessary personal information.

Recipient Access and UX Summary:

Virtru offers modern, seamless recipient access and secure collaboration workflows either directly in the email client or using Secure Reader. Egress forces external recipients into a portal experience that requires extra steps to access the email and attachments.

Virtru pioneered the use of federated identities to enable seamless, secure access for recipients, without requiring new accounts and passwords or straining helpdesk queues. Egress requires recipients who don't have Egress installed to create, manage, and maintain a new account ID and password to access protected email via the Egress Web Access portal application. This experience adds unnecessary friction to external collaboration workflows, frustrating customers, partners, and other external parties. It also burdens IT administrators with support issues that aren't related to users within paying customer accounts.

Egress account sign-up requires submitting intrusive personal information for password recovery questions. This forces the recipient to unnecessarily reveal private details, even if the recipient only uses Egress once. Virtru never forces recipients to reveal this kind of personal information, since it uses existing credentials for the external recipient's authorized account

Downloading Egress attachments requires a complex process where external collaborators are forced to install Egress client software onto their machine, download the ".switch" file associated with the message, select the relevant attachment, and finally download it. With Virtru, authorized recipients can seamlessly download attachments to their device without requiring any additional software. If the sender has applied watermarking or persistent protection, download is prevented by design, and the file remains easily accessible via the Secure Reader.

BROWN

"We had experience with a traditional, portal-based email encryption product, but our users found this mechanism far too cumbersome for our users and their recipients. With Virtru, we found a solution that met our security and compliance requirements, was easy enough to ensure widespread adoption, and gave us the audit and control features we wanted."

- Mark Dietrich, Director of IT and Security, Brown University

Administration

Feature	Virtru	Egress Protect
Users Administration	● Centralized admin console via Virtru Control Center.	○ Google Workspace / Active Directory domain syncs not supported.
Data Loss Prevention and Classification	◕ Integrated DLP with preconfigured rules and ability to create custom rules. Classification workflows supported via Titus partnership.	◔ Built-in DLP rules and trigger warnings tied to classification rules, but administration UX is not intuitive. Rules cannot be tied to specific users or groups.
Deployment and Installation	● Automated org-wide deployments via managed Chrome or Microsoft Installer.	○ No support for automated org-wide deployments. End-user self-service only.
Revocation / Recall on Behalf of Senders	●	○
Change Expiration Date on Behalf of Senders	●	○
Disable Forwarding on Behalf of Senders	● Per-message disable forwarding.	◔ Only via classification rules, not per-message.
Audit Reporting and Event Logs	◑ Detailed event logs are accessible to admins via log export.	◑ Detailed logs are accessible to admins.
SIEM Integration	●	○

Administration Summary:

The main point of differentiation is regarding administrative ease of use. Administrators and IT teams at medium-sized organizations and large enterprises expect the ability to deploy across their entire organization with automated processes that sync their existing user repositories and install the software on behalf of end users.

Virtru supports both domain syncs and automated installation for seamless enterprise-wide deployments that can be completed in minutes via the Virtru Control Center. Egress supports neither. Without the ability to sync the customer's domain, Egress users must be added one-by-one or by uploading a CSV file with a list of users. This means every time new employees are added to the organization, admins must update those users manually. And without support for automated installation processes via managed Chrome or Microsoft Installer, end users must install Egress software themselves, inevitably placing a heavy burden on the customer's IT team and administrators with support questions. When combined with the recipient user experience difficulties, Egress customers can expect helpdesk teams to be strained even more than usual.

Similarly, Egress's classification and data loss prevention (DLP) rules are not always intuitive for the administrator to configure themselves, so they tend to rely on Egress support personnel to guide them through the process. And since Egress cannot be synced to the customer's domain, DLP rules and classifications cannot be scoped to subsets of users who handle sensitive data most often. This forces admins into configuring protection rules for the entire organization (including groups of users who don't actually need it), exacerbating tradeoffs between security and ease of use. Virtru's support for domain syncs allows DLP rules and classification (via Titus partnership) to be scoped to specific groups, enforcing protections only for users who need it most. Preconfigured rules and a custom rules builder makes Virtru DLP configuration seamless.

Egress administrators lack the ability to adapt access controls on behalf of end users. If an email becomes confidential, administrators have to rely on end users to restrict forwarding, reset the expiration date, or revoke access. This opens the door to unauthorized access, data breaches, and potential noncompliance fines. Virtru offers administrators intuitive search capabilities to find individual emails or a collection of emails and modify access controls easily within the Virtru Control Center.

For audit reporting, both Virtru and Egress offer detailed event logs of protection, control, and access activity. Virtru also makes it possible to feed event logs directly into a Security Information and Event Management (SIEM) system for more advanced threat remediation and forensic analysis workflows.

Security and Privacy

Feature	Virtru	Egress Protect
No Third-Party Access to Plaintext Email Content	●	◑ Only for Outlook-to-Outlook workflows when both parties have Egress.
Customer-Hosted Keys	●	○
HSM Integration	●	○
GDPR Compliant	●	●
FERPA Compliant	●	●
HIPAA Compliant	●	●
CJIS Compliant	●	○
ITAR Compliant	●	○
EAR Compliant	●	○
FedRAMP Certified	●	○
SOC 2 TYPE 2 Certified	●	○
Cloud Security Alliance (CSA) Certified Vendor	●	○
ANSSI CSPN First Level Security Certified	●	○

Security and Privacy Summary:

Virtru deployments leverage client-side, object-level encryption for Gmail and Outlook, providing end-to-end encryption that prevents third-party access. As discussed in the Sender Protections section, Egress also encrypts email messages at the object level, but whether it is end-to-end encrypted depends on the use case: only Outlook to Outlook workflows where both parties have Egress installed. When recipients don't have Egress, unencrypted plaintext may be revealed to third-party users or services throughout collaboration workflows, failing to keep sensitive data truly private and putting compliance at risk.

For enhanced security, the Virtru Customer Key Server gives customers the option to host and manage the encryption keys protecting their data for absolute control, with HSM integration support. Egress doesn't offer any customer-hosted key options or HSM integrations, failing to meet the needs of enterprise security teams. Virtru customers can fulfill compliance requirements for GDPR, HIPAA, as well as more stringent regulations like ITAR, EAR, and CJIS that require end-to-end encryption. While Egress meets GDPR requirements, it will come up short for other regulations since many use cases are not end-to-end encrypted.

Virtru adheres to the most rigorous industry accreditations to demonstrate the security of our cloud infrastructure. Virtru has a certified Authorization to Operate (ATO) at the moderate level under FedRAMP, implementing the security controls defined in the NIST 800-53 and 800-171 publications to ensure integrity of federal information systems. Virtru has also achieved SOC 2 Type 2 Certification, is a certified vendor for the Cloud Security Alliance, and is certified by The French National Cybersecurity Agency (ANSSI) with the CSPN First Level Security Certification for cyber security.

omada

"We quickly settled on Virtru as a partner - they had the key functionality we were looking for, which was end-to-end encryption and seamless integration with Google Workspace."

- Bill Dougherty, Chief Information Security Officer, Omada Health

Conclusion

In a modern world where innovation is driven by collaboration, organizations must ensure not only that their email encryption solution doesn't slow them down, but that it protects their most sensitive data at all times.

Egress's encryption doesn't meet modern needs. Where it fails, Virtru succeeds with ease of use for end users and admins, and end-to-end protection that provides unmatched visibility and control. Virtru's end-to-end encryption and persistent access controls better support protected sharing workflows to give senders and admins greater assurances that email stays private, wherever it's created or shared.

Where Egress falls short, Virtru provides:

- True end-to-end encryption for Outlook and Gmail.
- Seamless user experiences, providing senders more intuitive protections and granular controls and recipients an easy way to access protected content.
- Easy administrative experiences with easy installation and user management and intuitive DLP rules.
- The option for organizations to host their own keys and integrate with HSMs for the highest levels of security and control.

The best way to secure your data is with data-centric protection. Data-centric security focuses on protecting the data itself regardless of where it is hosted, from applications to the body of an email.

To truly eliminate risks and develop a strategy for complete email protection, reinforce native Gmail and Microsoft encryption with a third-party solution that provides strong, data-centric encryption. This ensures that unauthorized users—such as hackers, your email provider, or even your third-party encryption provider—are not able to access your content.

Virtru's end-to-end encryption ensures that all data is encrypted at all times—not just in transit and at rest—and that only the sender and recipient can view the contents of an email, providing the highest level of confidentiality and protection to your organization's emails.