Enterprise Information Protection with the Trusted Data Format and the Virtru Trusted Data Platform

Seamless, Cross-Platform Data Protection and Access Control

Table of Contents

1. The Rising Need for a New Approach to Data Protection

With the growth of cloud applications and an increasingly mobile workforce, most enterprises struggle to protect, share, and control sensitive information. Existing solutions require too much effort from both content creators and consumers, and they cannot ensure persistent protections once information leaves the originating domain.

> **Persistent Data-Centric Protections:** Protections that travel with individual data objects (email bodies, files, database cells), rather than being bound to applications or networks are finally solving these longstanding data security challenges. These protections, which can be applied by way of client-side, object-level encryption, have taken center stage because of their ability to travel with the data itself, regardless of which servers or cloud ecosystems it traverses, and provide enterprises with the seamless control, visibility, and encryption that they've long desired.

While this type of data protection is widely recognized as a necessary component of solutions to these and other enterprise security challenges, technical complexity and a lack of control capabilities have inhibited widespread adoption of data-centric protections and closely related client-side encryption approaches. Until recently, it has been widely assumed that these types of powerful data protection technologies were too complicated for ubiquitous use and adoption.

For example, advanced client-side, end-to-end email encryption approaches like Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) require deep technical knowledge and limit where data can be easily shared. Data rights management (DRM) tools for document protection can make it difficult to share content across different cloud environments, making them, too, largely unusable for most enterprise use cases. This gap has left enterprises overly reliant on insufficient approaches to data protection — perimeter security tools and siloed rights management offerings.

2. Data Protection Requirements for the Modern Enterprise

Existing data protection technologies were not designed to meet the modern enterprise's most important requirements:

Easy for Content Creators & Consumers

Cloud collaboration has enhanced usability expectations for modern security tools. If data protection disrupts existing end-user workflows, users will work around the technology—plain and simple—even if it means sharing unprotected data. What's more, today's enterprise shares data with many different organizations, service providers, and cloud applications. Effective protections must persist with the data no matter where it travels, and the user experience must remain consistent across platforms. Even the slightest complexities can limit adoption of the most secure technologies.

Cross-Platform Audit & Control

Full data protection requires more than just securing the data. Most data ends up leaving the organization at some point, whether shared voluntarily with partners, customers, or other stakeholders by the data owner, or shared by a collaborator, without the data owner's knowledge. It's critical that businesses have the ability to monitor where this data travels and manage access to it even after it's been shared and consumed. Otherwise, it becomes difficult for security and collaboration to coexist.

Flexible Security

Between regulatory compliance, data residency requirements, and corporate privacy policies, it's difficult to find organizations that share the exact same security obligations. As a result, data protection approaches must offer flexible configuration options to match the privacy requirements and risk appetites of different enterprises and collaboration use cases.

Specifically, the method of encryption must be tailored to customer needs. In order to eliminate the tradeoff between security and ease of use, organizations must be able to choose where their encryption keys are stored, who can access them, and how they are managed.

Virtru was founded to combine these qualities for enterprises under one seamless and pervasive data sharing platform. Virtru's mission is to unlock the power of data by creating a world where it's always under the control of the data owner. Implicit in this mission is eliminating the tradeoff between data protection and ease of use by making data-centric protection the new norm for businesses.

As most enterprises look to keep pace with emerging data protection and privacy requirements, Virtru's novel approach fills many of the usability, control, and security gaps inherent in legacy technologies.

3. Virtru's Foundation: The Trusted Data Format (TDF)

Many of today's data protection solutions enforce security controls on a per-platform (at-rest) or per-connection (in-transit) basis. As a result, data owners often have to trust that each system or vendor that can store or transmit their content has implemented appropriate security controls and data access policies. If and when they rely on these third parties to protect their content, enterprises have to give up control over their data the moment it is shared or otherwise transmitted and stored.

The Trusted Data Format (TDF) was born out of a requirement for an open, interoperable approach that allows protections to travel with data, but doesn't force collaborators and recipients to enroll in any particular system ahead of time. This can be thought of as per-data object protection.

TDF

The **Trusted Data Format (TDF)** is an open standard XML based file format used by the United States Intelligence Community for the purposes of enabling file level tagging and security features. These features include assertion of data properties or tags, cryptographic binding, and data encryption. The TDF is an open standard and requires no use of proprietary or patented technology and is thus free for anyone to use.

Originally developed by Virtru CTO and Co-Founder, Will Ackerly, to secure sensitive data for the U.S. Intelligence Community, the TDF is an open standard format for placing a secure wrapper around any type of content and its accompanying metadata, including metadata assertions.

These assertions are policy-related requirements that allow a content creator to set and enforce a wide variety of policies on the content being provided to the recipient. Examples include expiring the recipient's access to the content at a certain date and time; enforcing key escrow requirements; allowing or disallowing forwarding of content by recipients; and tracking forwarding of content. TDF also supports integrity through tamper-proof binding of these metadata assertions. By providing both confidentiality and integrity, TDF prevents content from being accessed or altered by eavesdroppers or malicious intermediaries.

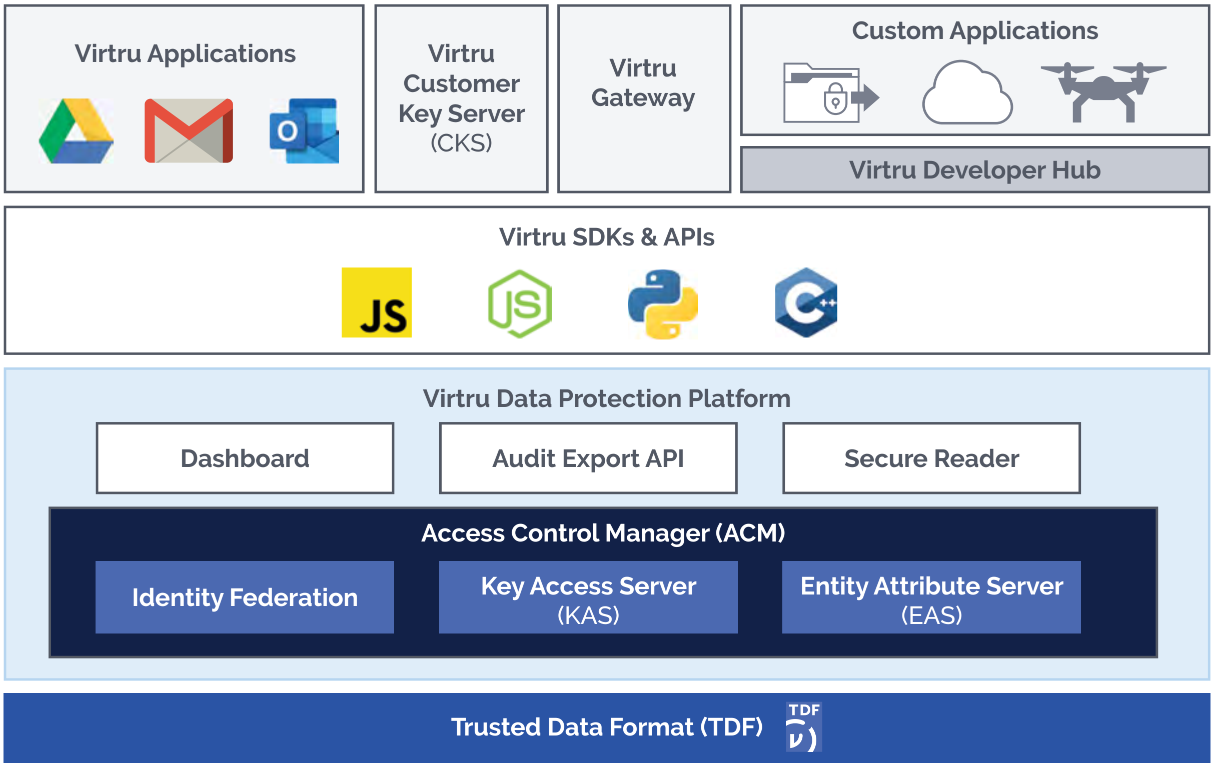
In 2013, the U.S. Intelligence Community formally adopted a government-specific version of the TDF, which includes standardized classification and control markings, as its interagency standard for cross-platform data protection.

4. Leveraging the TDF: The Virtru Trusted Data Platform (TDP)

The TDF enables Virtru to be a much more comprehensive data protection solution than those that simply encrypt content in transit without providing persistent audit and control. While legacy approaches are limited to email, the Virtru Trusted Data Platform (TDP) allows enterprises to seamlessly protect any type of content shared via email, file sharing services, and different business applications.

Virtru leverages the TDF to provide a Software as a Service (SaaS) platform for access control, policy enforcement, and key management. Data protection policies are enforced through seamless integrations with common productivity applications including Google G Suite, Microsoft Office 365 and Exchange, and other SaaS applications, such as Salesforce, WorkDay, and NetSuite. Third party developers can leverage Virtru SDKs to integrate TDF into Google Cloud Platform (GCP) and Amazon Web Services (AWS), embedding persistent, object-level data protection into their applications and custom workflows

Data protection policies are configured and enforced centrally, with optional warnings and on-demand controls for end users. Virtru offers flexible controls, including the ability to audit access, revoke or expire access, and restrict sharing for all protected content—even when content is shared outside of the enterprise. Customers maintain full control of the keys used to protect their information.



The Virtru Trusted Data Platform (TDP) Architecture

The Virtru TDP leaves behind the limitations of legacy approaches to meet the data protection needs of the modern, cloud-based enterprise:

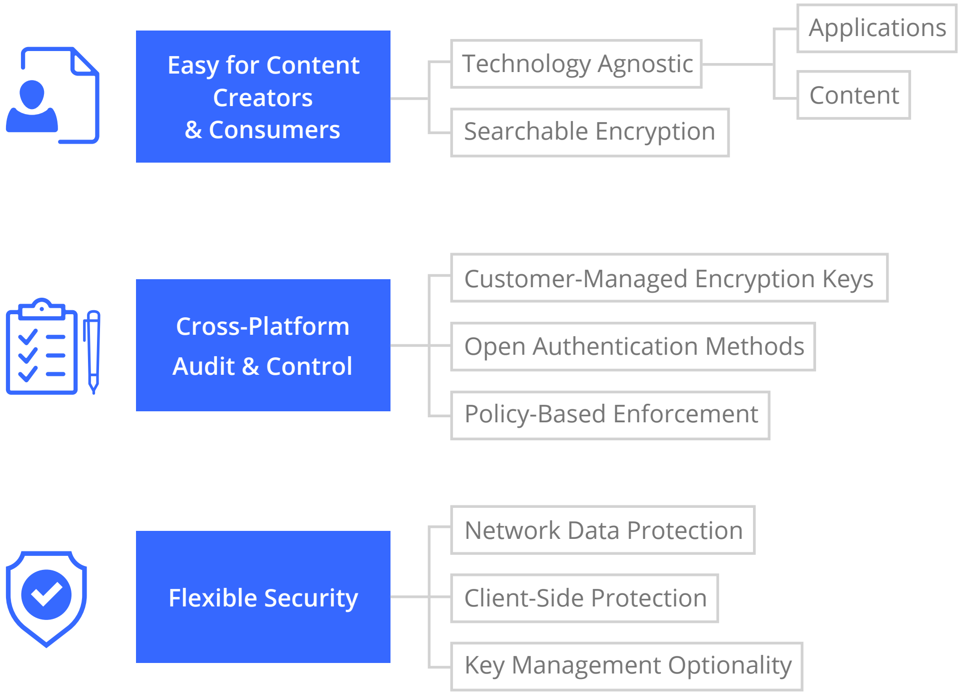
Persistent Protection: The Virtru TDP allows the enterprise to protect all content types from the time of creation, throughout its full lifecycle.

Designed for Easy Sharing: The Virtru TDP allows users to share secure content with anyone inside or outside of the enterprise, without the need for complicated key exchange or other technical complexity.

Transparent Integration with Existing Workflows: The Virtru TDP is designed to integrate easily with existing applications and workflows so that it adds security without impeding user productivity.

To meet these needs, the Virtru TDP focuses on the three core requirements for enterprise data protection:

- Easy for content creators and consumers
- Cross-platform audit and control
- Flexible security


Easy for Content Creators & Consumers
Technology Agnostic
Applications
Content
Searchable Encryption
Cross-Platform Audit & Control
Customer-Managed Encryption Keys
Open Authentication Methods
Policy-Based Enforcement
Flexible Security
Network Data Protection
Client-Side Protection
Key Management Optionality

Three core requirements for enterprise data protection

Originally designed to meet the rigorous requirements of the American Intelligence Community, the Virtru TDP offers high levels of data security and access control, while simultaneously ensuring high levels of user adoption.

The remainder of this paper provides a detailed overview of these requirements and the Virtru TDP implementation as well as functional architecture.

4.1 Easy for Content Creators & Consumers

The modern enterprise uses a wide variety of on-premises and cloud applications and multiple cloud storage platforms, and its users must exchange content in many different formats. To effectively secure enterprise data, the Virtru TDP has been designed to maintain application, cloud, and content heterogeneity in a manner that's seamless for content creators, content consumers, and IT administrators. This openness, coupled with Virtru's patented search technology, enables the Virtru TDP to integrate with your existing security and IT infrastructure without disrupting existing workflows.

4.1.1 Technology Agnostic Applications

To ensure widespread adoption and acceptance, data protection technologies must be tightly integrated with everyday applications for email, cloud storage, and other business tools. This integration ensures ease of use, removes impediments to adoption, and removes any requirements for special technical knowledge or expertise.

The Virtru TDP architecture is designed for easy integration with virtually any type of application. When integrated with an existing application, Virtru libraries perform three functions:

- Enable client-side, end-to-end encryption OR server-side protection at the time of creation.
- Communicate with the Virtru Access Control Manager (ACM) and Dashboard for access control, key management, and policy enforcement.
- Enable decryption when the application receives protected content and the content consumer is authenticated and authorized.

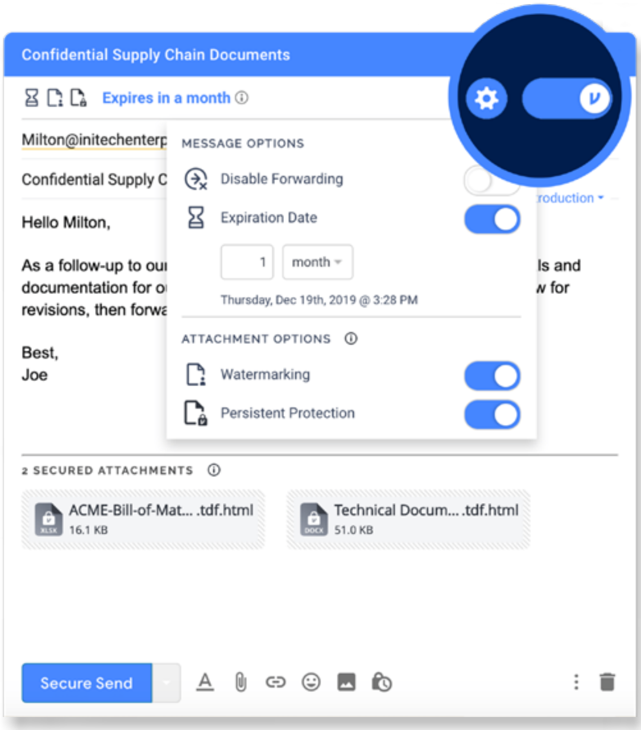
Virtru's Secure User-First Technology

Virtru's unique ease of use and cross-platform access control are based on patented technology that allows:

- Recipients to securely decrypt and consume encrypted content in their browsers without additional software installations or downloads.
- Recipients to authenticate and consume encrypted content using their existing identities. No new usernames or passwords are required.
- Senders and administrators to search encrypted content as easily as they search unencrypted content.

Once Virtru has been deployed, protection is built into native interfaces of end-user applications, while encryption and decryption occurs transparently.

By way of example, Virtru has tightly integrated its client-side data protection with widely used email services, such as Google's Gmail web application and Microsoft's Outlook desktop application. Users simply see a button to encrypt and new menu items for access controls like revoke and expiration. All of these capabilities are provided while preserving the native user interface design of the client application.



Confidential Supply Chain Documents

Expires in a month

Milton@initechenterp

Confidential Supply C

Hello Milton,

As a follow-up to our
documentation for o
revisions, then forwa

ls and
w for

Best,
Joe

MESSAGE OPTIONS

Disable Forwarding ○

Expiration Date ●

1 month

Thursday, Dec 19th, 2019 @ 3:28 PM

ATTACHMENT OPTIONS

Watermarking ●

Persistent Protection ●

2 SECURED ATTACHMENTS

ACME-Bill-of-Mat... .tdf.html 16.1 KB

Technical Docum... .tdf.html 51.0 KB

Virtru's easy end-to-end encryption is embedded directly within Gmail.

Content

Sensitive content can take many forms: emails, Microsoft Office documents, videos, pictures, audio files, and proprietary file formats. To ensure maximum control and security without the need to procure and manage multiple platforms, data protection services must support all content types.

The Virtru TDP leverages the TDF to provide consistently easy-to-use protection of all content types, including emails, documents and other data formats and elements. By providing both confidentiality and integrity, TDF prevents content from being accessed or altered by eavesdroppers or malicious intermediaries. The TDF's fluidity across content types ensures that this added privacy does not come at the expense of usability.

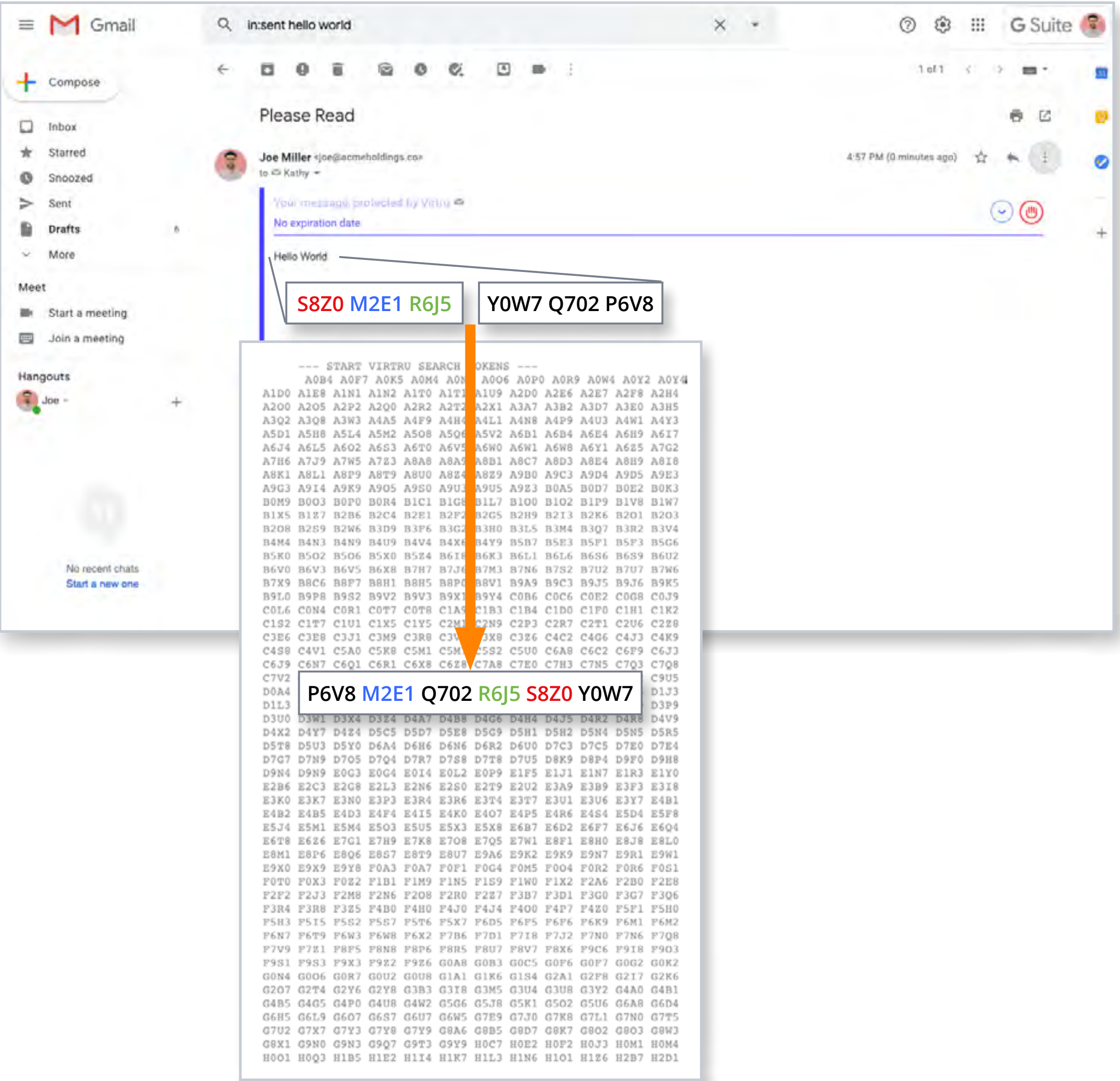
4.1.2 Searchable Encryption

When it comes to search and e-discovery, the tradeoff between usability and security is particularly relevant. Client-side encryption is seen as the most powerful level of protection for enterprise data, but traditional client-side approaches, like PGP and S/MIME, prevent end users and administrators from searching protected content. This limitation forces enterprises to sacrifice security in order to preserve search capabilities, which they need to perform audits, legal holds, and other e-discovery activities.

Via its patented Searchable Encryption, the Virtru TDP offers the only approach to client-side protection that also enables easy searching of encrypted content. Virtru's Searchable Encryption adds tokens to protected content that enable users to run client-side searches of that content without revealing the search criteria to Virtru's servers or any other third parties.

Every customer on the Virtru TDP automatically receives a search key that is shared between users in that organization. In the case of Virtru email clients, that Search Key is used to generate 4-character alphanumeric tokens (i.e., a0b1 x9u3 b4u8) for every word appearing in the email body. These tokens are then inserted into the actual email message, along with a number of random tokens that are added to prevent brute force correlation attacks.

When a user searches for a message from either the inbox or an email archival solution, tokens are generated for each search term and added to the search query. As a result, that user's native email client is able to retrieve and display the search results without getting access to either the original search term or underlying content. Virtru's servers never gain access either, thus ensuring that both existing user workflows and data security remain intact.



in:sent hello world

Please Read

Joe Miller <joe@acmeholdings.co>
to Kathy

4:57 PM (0 minutes ago)

Your message protected by Virtru
No expiration date

Hello World

S8Z0 M2E1 R6J5

Y0W7 Q702 P6V8

```
     --- START VIRTRU SEARCH  OKENS ---
      A0B4 A0F7 A0K5 A0M4 A0N  A0O6 A0P0 A0R9 A0W4 A0Y2 A0Y4
 A1D0 A1E8 A1N1 A1N2 A1T0 A1T1 A1U9 A2D0 A2E6 A2E7 A2F8 A2H4
 A2O0 A2O5 A2P2 A2Q0 A2R2 A2T2 A2X1 A3A7 A3B2 A3D7 A3E0 A3H5
 A3Q2 A3Q8 A3W3 A4A5 A4F9 A4H4 A4L1 A4N8 A4P9 A4U3 A4W1 A4Y3
 A5D1 A5H8 A5L4 A5M2 A5O8 A5Q6 A5V2 A6B1 A6B4 A6E4 A6H9 A6I7
 A6J4 A6L5 A6O2 A6S3 A6T0 A6V5 A6W0 A6W1 A6W8 A6Y1 A6Z5 A7G2
 A7H6 A7J9 A7W5 A7Z3 A8A8 A8A9 A8B1 A8C7 A8D3 A8E4 A8H9 A8I8
 A8K1 A8L1 A8P9 A8T9 A8U0 A8Z4 A8Z9 A9B0 A9C3 A9D4 A9D5 A9E3
 A9G3 A9I4 A9K9 A9O5 A9S0 A9U3 A9U5 A9Z3 B0A5 B0D7 B0E2 B0K3
 B0M9 B0O3 B0P0 B0R4 B1C1 B1G8 B1L7 B1O0 B1O2 B1P9 B1V8 B1W7
 B1X5 B1Z7 B2B6 B2C4 B2E1 B2F2 B2G5 B2H9 B2I3 B2K6 B2O1 B2O3
 B2O8 B2S9 B2W6 B3D9 B3F6 B3G2 B3H0 B3L5 B3M4 B3Q7 B3R2 B3V4
 B4M4 B4N3 B4N9 B4U9 B4V4 B4X6 B4Y9 B5B7 B5E3 B5F1 B5F3 B5G6
 B5K0 B5O2 B5O6 B5X0 B5Z4 B6I8 B6K3 B6L1 B6L6 B6S6 B6S9 B6U2
 B6V0 B6V3 B6V5 B6X8 B7H7 B7J6 B7M3 B7N6 B7S2 B7U2 B7U7 B7W6
 B7X9 B8C6 B8F7 B8H1 B8H5 B8P0 B8V1 B9A9 B9C3 B9J5 B9J6 B9K5
 B9L0 B9P8 B9S2 B9V2 B9V3 B9X1 B9Y4 C0B6 C0C6 C0E2 C0G8 C0J9
 C0L6 C0N4 C0R1 C0T7 C0T8 C1A9 C1B3 C1B4 C1D0 C1F0 C1H1 C1K2
 C1S2 C1T7 C1U1 C1X5 C1Y5 C2M1 C2N9 C2P3 C2R7 C2T1 C2U6 C2Z8
 C3E6 C3E8 C3J1 C3M9 C3R8 C3V  3X8 C3Z6 C4C2 C4G6 C4J3 C4K9
 C4S8 C4V1 C5A0 C5K8 C5M1 C5M  5S2 C5U0 C6A8 C6C2 C6F9 C6J3
 C6J9 C6N7 C6Q1 C6R1 C6X8 C6Z8 C7A8 C7E0 C7H3 C7N5 C7Q3 C7Q8
 C7V2                                                   C9U5
 D0A4                                                   D1J3
 D1L3                                                   D3P9
 D3U0 D3W1 D3X4 D3Z4 D4A7 D4B8 D4G6 D4H4 D4J5 D4R2 D4R8 D4V9
 D4X2 D4Y7 D4Z4 D5C5 D5D7 D5E8 D5G9 D5H1 D5H2 D5N4 D5N5 D5R5
 D5T8 D5U3 D5Y0 D6A4 D6H6 D6N6 D6R2 D6U0 D7C3 D7C5 D7E0 D7E4
 D7G7 D7N9 D7O5 D7Q4 D7R7 D7S8 D7T8 D7U5 D8K9 D8P4 D9F0 D9H8
 D9N4 D9N9 E0G3 E0G4 E0I4 E0L2 E0P9 E1F5 E1J1 E1N7 E1R3 E1Y0
 E2B6 E2C3 E2G8 E2L3 E2N6 E2S0 E2T9 E2U2 E3A9 E3B9 E3F3 E3I8
 E3K0 E3K7 E3N0 E3P3 E3R4 E3R6 E3T4 E3T7 E3U1 E3U6 E3Y7 E4B1
 E4B2 E4B5 E4D3 E4F4 E4I5 E4K0 E4O7 E4P5 E4R6 E4S4 E5D4 E5F8
 E5J4 E5M1 E5M4 E5O3 E5U5 E5X3 E5X8 E6B7 E6D2 E6F7 E6J6 E6Q4
 E6T8 E6Z6 E7G1 E7H9 E7K8 E7O8 E7Q5 E7W1 E8F1 E8H0 E8J8 E8L0
 E8M1 E8P6 E8Q6 E8S7 E8T9 E8U7 E9A6 E9K2 E9K9 E9N7 E9R1 E9W1
 E9X0 E9X9 E9Y8 F0A3 F0A7 F0F1 F0G4 F0M5 F0O4 F0R2 F0R6 F0S1
 F0T0 F0X3 F0Z2 F1B1 F1M9 F1N5 F1S9 F1W0 F1X2 F2A6 F2B0 F2E8
 F2F2 F2J3 F2M8 F2N6 F2O8 F2R0 F2Z7 F3B7 F3D1 F3G0 F3G7 F3Q6
 F3R4 F3R8 F3Z5 F4B0 F4H0 F4J0 F4J4 F4O0 F4P7 F4Z0 F5F1 F5H0
 F5H3 F5I5 F5S2 F5S7 F5T6 F5X7 F6D5 F6F5 F6F6 F6K9 F6M1 F6M2
 F6N7 F6T9 F6W3 F6W8 F6X2 F7B6 F7D1 F7I8 F7J2 F7N0 F7N6 F7Q8
 F7V9 F7Z1 F8F5 F8N8 F8P6 F8R5 F8U7 F8V7 F8X6 F9C6 F9I8 F9O3
 F9S1 F9S3 F9X3 F9Z2 F9Z6 G0A8 G0B3 G0C5 G0F6 G0F7 G0G2 G0K2
 G0N4 G0O6 G0R7 G0U2 G0U8 G1A1 G1K6 G1S4 G2A1 G2F8 G2I7 G2K6
 G2O7 G2T4 G2Y6 G2Y8 G3B3 G3I8 G3M5 G3U4 G3U8 G3Y2 G4A0 G4B1
 G4B5 G4G5 G4P0 G4U8 G4W2 G5G6 G5J8 G5K1 G5O2 G5U6 G6A8 G6D4
 G6H5 G6L9 G6O7 G6S7 G6U7 G6W5 G7E9 G7J0 G7K8 G7L1 G7N0 G7T5
 G7U2 G7X7 G7Y3 G7Y8 G7Y9 G8A6 G8B5 G8D7 G8K7 G8O2 G8O3 G8W3
 G8X1 G9N0 G9N3 G9Q7 G9T3 G9Y9 H0C7 H0E2 H0F2 H0J3 H0M1 H0M4
 H0O1 H0Q3 H1B5 H1E2 H1I4 H1K7 H1L3 H1N6 H1O1 H1Z6 H2B7 H2D1
```

P6V8 M2E1 Q702 R6J5 S8Z0 Y0W7

By using tokens for search terms, Virtru enables encrypted search without revealing plaintext email search to the email provider.

4.2 Cross-Platform Audit & Control

Key management, distribution, and recipient authentication have historically been significant pain points for users of legacy data protection technologies. To address the need to share broadly without relinquishing access control, modern approaches must allow content creators to manage access to their data easily, while enabling automatic enforcement of controls by administrators and seamless authentication by recipients, using their existing credentials and workflows.

Additionally, technologies must be able to protect data traveling across different servers or systems and provide persistent visibility for streamlined audit—an area where DRM solutions have historically failed. While many of these products provide access control capabilities for data exchanged within the organization, they lack the persistent, object-level protections required by modern enterprises looking to share sensitive data with a variety of external recipients.

4.2.1 Encryption Key Management and Access Control

One of the main advantages of the Virtru TDP architecture is that it allows content owners to manage encryption keys to assert granular control over who has access to sensitive materials and for how long. Individual keys are created for each content item and authorized consumer, allowing content creators to manage access at a very granular level.

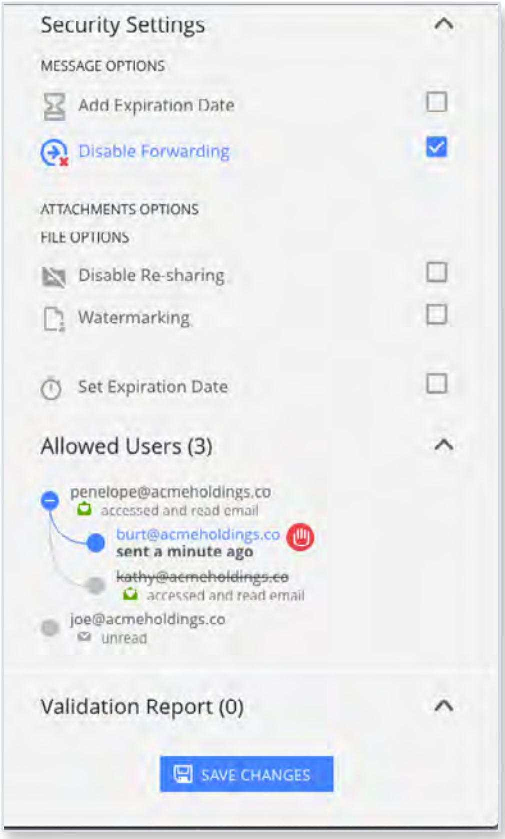
Either through a Virtru-enabled client or a web-based dashboard, users and administrators can revoke access to content, control forwarding, set expiration dates, view read receipts and audit trails, watermark files, and disable downloading of attachments. These controls are available for the life of the content, regardless of whether it has been opened or shared.

Suppose that a sender accidentally emails a sensitive file attachment to a list of recipients, including an external party who should not see the content. When the mistake is realized, the content creator can simply revoke access to the message for the accidental recipient. No other authorized consumers will be affected. Revocation is immediate and can only be reversed by the content owner.

4.2.2 Open Authentication Methods

As the need to collaborate increases, so does the need to share protected content. End users will have a very low tolerance for data protection technologies that only persist when shared with certain users.

One of the largest problems with legacy data protection and rights management technologies is their inability to maintain data protections when communicating with arbitrary recipients using different technologies or cloud networks.



Security Settings

MESSAGE OPTIONS

Add Expiration Date □

Disable Forwarding ☑

ATTACHMENTS OPTIONS

FILE OPTIONS

Disable Re-sharing □

Watermarking □

Set Expiration Date □

Allowed Users (3)

penelope@acmeholdings.co
accessed and read email

burt@acmeholdings.co
sent a minute ago

~~kathy@acmeholdings.co~~
accessed and read email

joe@acmeholdings.co
unread

Validation Report (0)

SAVE CHANGES

Audit and access control capabilities in the Virtru Dashboard

In the case of public key-based email encryption, the sender and the recipient must both have the same technology implemented before initiating any exchange. If the recipient doesn't have a public key, then there is no way to authenticate parties and use these technologies to exchange protected emails.

Legacy rights management technologies also place significant accessibility limitations on senders and recipients. Although these technologies can be used to apply usage permissions to data, authorized recipients can only access this data if they are part of the same network as the original content creator. These conditions force senders and recipients into an awkward negotiation: either the recipient changes their existing workflows and adopts new technology that allows them to properly authenticate, or the sender must share their data unprotected.

Virtru eliminates this tradeoff by avoiding dependencies on both the availability of a public key from the recipient and separate cloud directories or portal systems. Instead, the Virtru TDP verifies identity and authorizes access using either existing identity services like OAuth, OpenID, or SAML, or through simple email-based authentication via verification codes.

As a result, recipients can access protected data no matter what platform or cloud provider they are using. Senders can place usage restrictions on their data without having to worry whether or not authorized recipients will be able to gain access.

For additional flexibility and security, a recipient's existing authentication methods, including public keys and two-factor authentication, can be leveraged to ensure the recipient's identity without creating additional authentication complexities. This approach is possible because of the highly flexible nature of key management within the Virtru TDP.

4.2.3 Policy-Based Enforcement

Enterprise data protection products must extend control capabilities both to content creators and the administrators who manage their IT services. This requirement makes it difficult to balance visibility and security, as data must remain protected from third parties, while still being accessible to internal admins and compatible with any domain-wide policies that they wish to enforce.

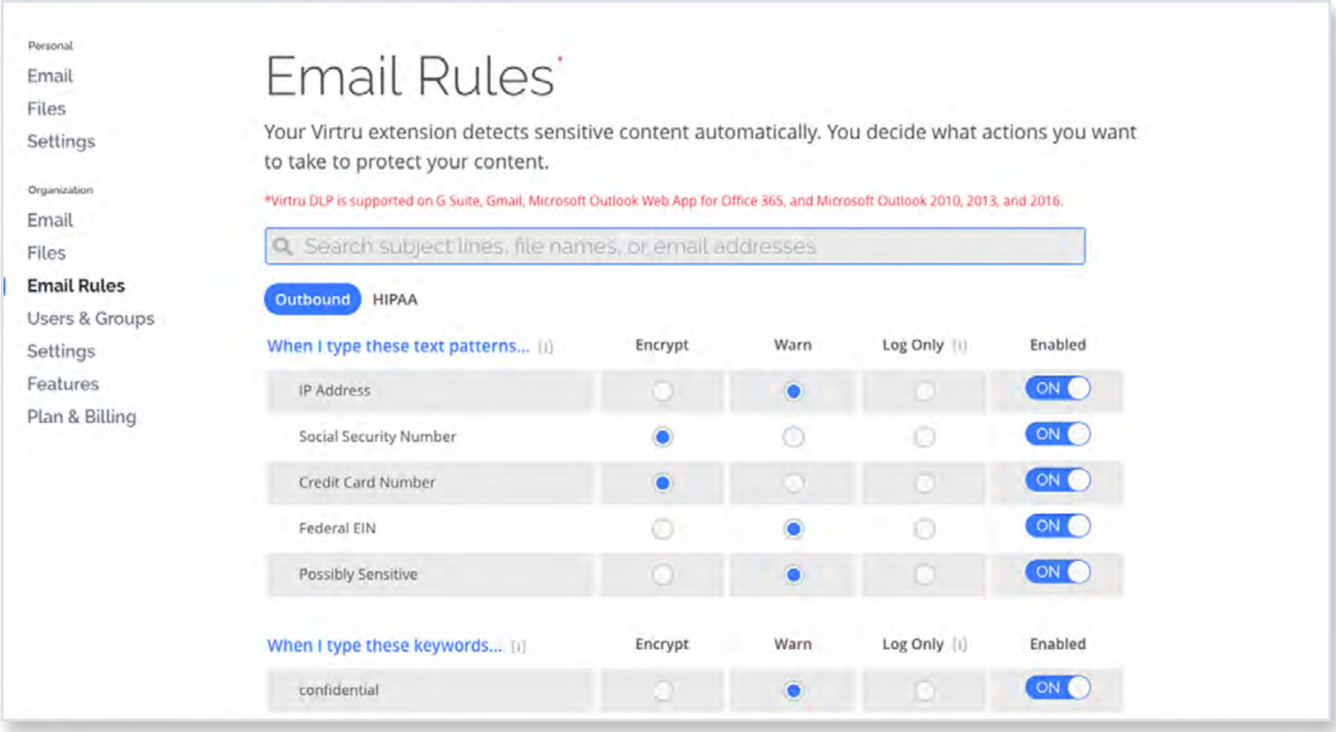
Most data protection technologies give admins the ability to configure rules that automatically perform encryption, rerouting, and other actions on the content leaving their organization, but they often require that customers relinquish access to their data in order to do so.

Virtru's policy-based enforcement, on the other hand, delivers organization-wide control for admins without sacrificing security or convenience. From the Virtru Dashboard, enterprise leaders and administrators can build policies that scan their end users' content on either the client-side or network level before they leave the organization.

Rules can be set to encrypt content, warn end users, add recipients, strip attachments, and take other actions based on whether or not emails and files meet certain predefined criteria, such as containing specific key phrases or text patterns.

To enforce rules on all data leaving the domain, even data that wasn't created on Virtru-enabled clients, the Virtru TDP offers Network Data Protection that scans content at the server level before it reaches any intended recipients. These capabilities can be configured for the entire enterprise, or for individual users, organizational units (OUs), or other groups already configured on the domain.

Policies can be applied to data both leaving and entering the domain, and companies can even build them in ways that integrate existing data loss prevention (DLP) and email archival solutions into the Virtru TDP.



Email Rules*

Your Virtru extension detects sensitive content automatically. You decide what actions you want to take to protect your content.

*Virtru DLP is supported on G Suite, Gmail, Microsoft Outlook Web App for Office 365, and Microsoft Outlook 2010, 2013, and 2016.

When I type these text patterns... (i)	Encrypt	Warn	Log Only (i)	Enabled
IP Address	○	●	○	ON
Social Security Number	●	○	○	ON
Credit Card Number	●	○	○	ON
Federal EIN	○	●	○	ON
Possibly Sensitive	○	●	○	ON

When I type these keywords... (i)	Encrypt	Warn	Log Only (i)	Enabled
confidential	○	●	○	ON

Email rules can be configured within the Virtru Dashboard for DLP that automatically detects sensitive data and enforces admin-defined protection and control.

The Virtru TDP also provides something that legacy data protection solutions have been unable to achieve: client-side policy enforcement. Once an administrator configures policies across the enterprise, those rules can be automatically downloaded onto each Virtru browser extension, mobile app, and desktop plugin being run on an end-user device.

Since these rules operate inside of individual sender machines, and not on Virtru's servers, Virtru does not need access to customer content in order to perform its client-side policy enforcement. Administrators can use these client-side capabilities to educate employees by configuring rules to warn users on their devices before they share certain sensitive data.

4.3 Flexible Security

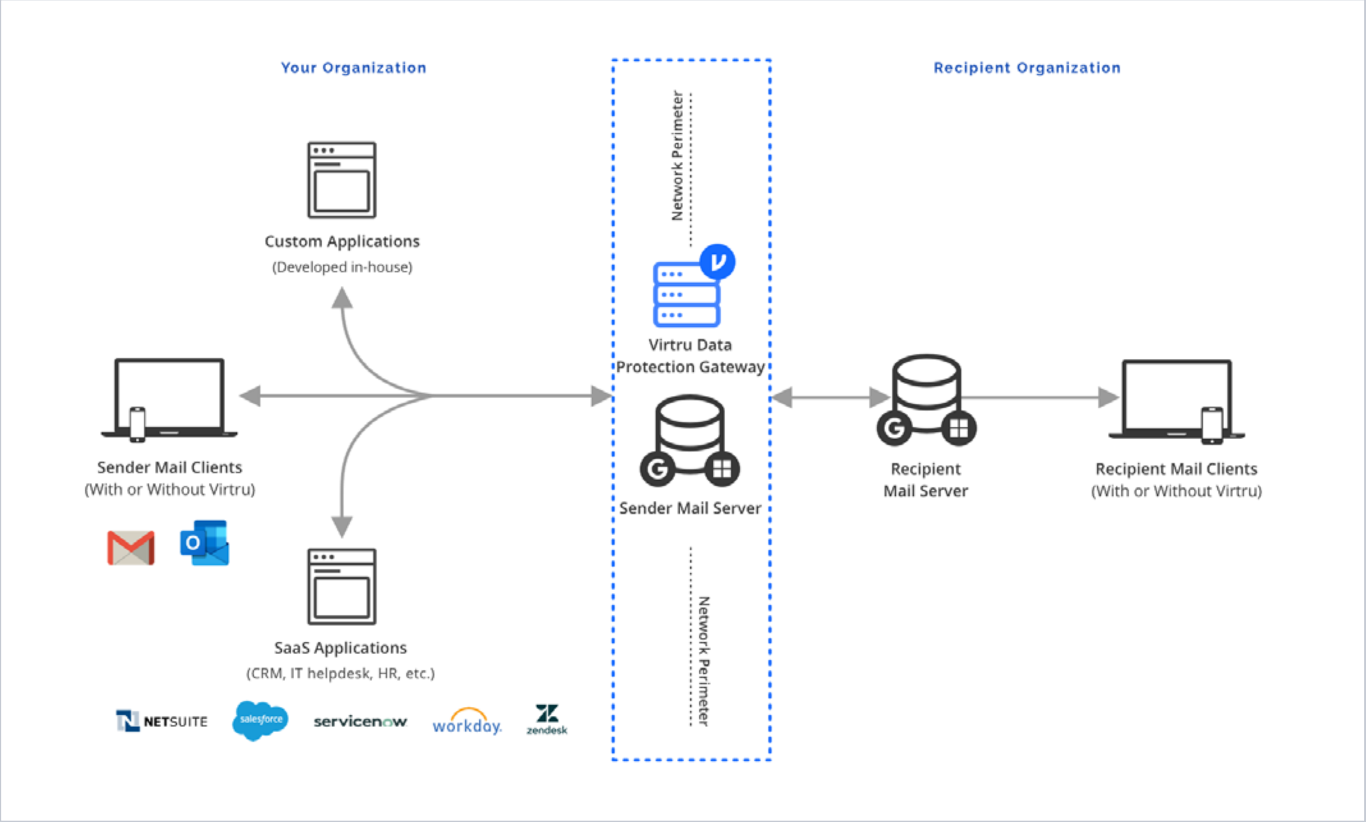
Compared with legacy approaches, Virtru offers a much broader range of data protection, encryption, and privacy options. Public key-based technologies provide client-side encryption; however, they do so at the expense of usability and choice. Portal-based encryption technologies don't protect data at the object-level, which unnecessarily exposes the content to eavesdroppers and can lead to breaches or other losses of privacy. By leveraging the TDF's object-level protection, Virtru delivers the most user-friendly solution for maintaining powerful data protection in perpetuity.

4.3.1 Network-Level Protection via Virtru Data Protection Gateway

In order for security to be pervasive, data protection policies must be enforceable regardless of where the data originates. Administrators need to know that their enterprise's data will be shared securely even when content creators or applications do not enable protection themselves. That's why the Virtru TDP supports network-level data protection via the Virtru Data Protection Gateway, automatically securing data shared by any user, device, or application (whether it's hosted in the cloud or on-premises).

The Virtru Data Protection Gateway allows organizations to enforce Virtru data protection policies for inbound and outbound data entering or leaving a particular email, file sharing, or other cloud application. This complements Virtru's client-side plugins by providing a mechanism for content to be protected even when it is shared from a device that does not have Virtru installed.

The Virtru Data Protection Gateway can be deployed in existing on-premises infrastructure or inside Infrastructure as a Service (IaaS) providers, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure IaaS. Although it can be added to any application workflow, it is most commonly integrated into Microsoft Office 365 or Exchange, G Suite, or automated messaging workflows initiated by enterprise SaaS applications like Salesforce and Workday.



The Virtru Data Protection Gateway protects emails sent from email clients that do not have Virtru installed and secures automated messaging workflows from SaaS and custom applications.

In the instance of email, the Gateway can be deployed anywhere along an enterprise's mail flow path, giving it the ability to relay or perform final delivery of messages. In addition to Virtru's object-level protection, the Gateway also supports industry standard email security and validation technologies, such as Transport Layer Security (TLS), Sender Policy Framework (SPF), Domain Keys Identified Email (DKIM), and Domain Message Authentication Reporting & Conformance (DMARC).

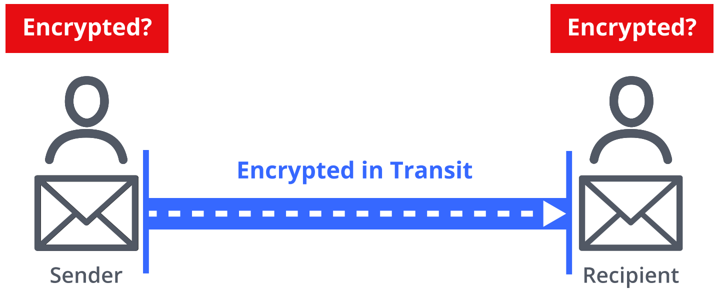
The Virtru Data Protection Gateway is deployed via Docker containers in order to enable flexible and horizontally scalable deployments across different infrastructures. It uses a standards-compliant mail transfer agent (MTA), so all communication occurs via the Simple Mail Transport Protocol (SMTP). It is configured to accept email providers' direct SMTP traffic to and from the gateway.

For every protected email, the Gateway generates a new set of encryption keys. Just like Virtru's client side plugins, it communicates with the Virtru Control Center to manage access to protected data and provide visibility to end users and administrators.

4.3.2 Client-Side, End-to-End Encryption via Endpoint Protection

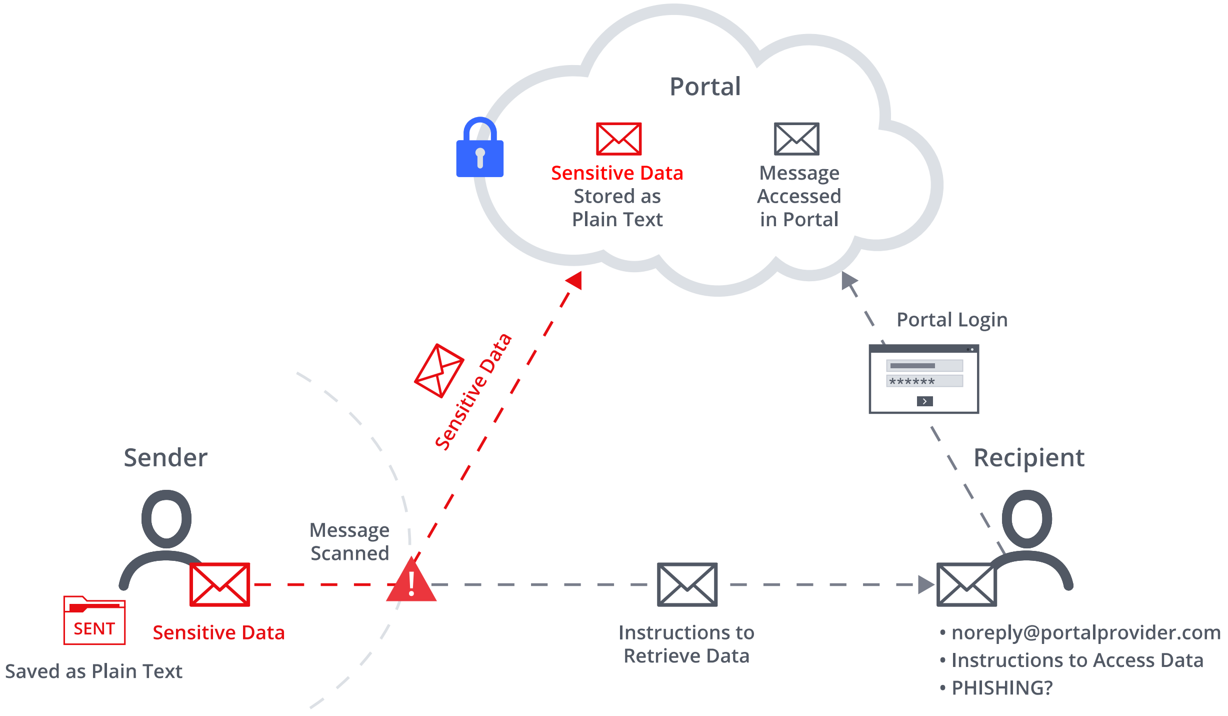
Concerns related to regulatory compliance, data residency, and corporate privacy may require content to be encrypted at the time of creation at the user endpoint, and not decrypted until an authorized party requests access. This client-side protection guards against unauthorized access and ensures that cloud providers do not have access to unencrypted content, making end-to-end encryption inherently more secure than portal-based approaches, such as TLS. In many cases, end-to-end, client-side encryption is a requirement for compliance with CJIS, ITAR, and EAR and other stringent data privacy regulations.

Transport Layer Security (TLS) Based Solutions



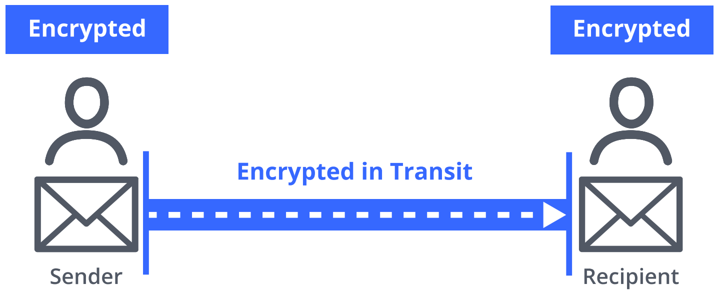
- Only encrypted in transit
- Content may/not be encrypted when stored
- May not meet compliance regulations
- No visibility or control
- Built in with most email providers
- Recipient must support TLS encryption

Portal Based Solutions



- Content may be stored unencrypted
- Less control and visibility over your data
- Heavily reliant on rules
- Recipient must create user name and password

End-to-End With Virtru



- Encrypted at all times
- Data stays protected, wherever it travels
- Zero trust / split knowledge key architecture
- Use existing accounts
- No user names or passwords

End-to-end encryption can also be used to meet data residency requirements. Many organizations are required to store content only in certain geographic regions, yet want to use multinational cloud platform vendors. By using the Virtru TDP for client-side encryption and storing encryption keys in their required geographic region, they are able to satisfy data residency requirements while continuing to use the cloud vendor of their choice.

Independent of regulatory or data residency requirements, end-to-end encryption is the preferred method for ensuring corporate privacy and security. With portal-based encryption technologies and security methods that rely on TLS, plaintext content may be transmitted or stored in the clear and potentially accessible by unauthorized third parties such as engineer employees of the cloud platform vendor. Client-side technologies ensure that only creators and authorized consumers ever have access to unencrypted content.

Traditionally, end-to-end encryption has been achieved using legacy approaches that leverage public key infrastructure, such as PGP or S/MIME for email. These technologies, while highly secure, are hard to implement and manage, and require complex, manual key exchanges to utilize. They also do not provide a way for content creators to maintain control (i.e., revoke, expire access, track forwarding) over data once it has been shared. As a result, adoption has been limited to the technologically sophisticated, while IT departments have often fallen back to perimeter security approaches.

The Virtru TDP addresses these shortcomings by providing true end-to-end, client-side encryption that can be used by virtually anyone. Content is encrypted at the time of creation on the owner's device and before it is shared. Content is not decrypted until the consuming device requests that decryption occur, and the recipient is authenticated and authorized to view the content. With this architecture, content is protected from the time of creation until the time of consumption, and is never available in unencrypted form to any service provider or intermediate storage system.

Common Use Cases for Client-Side, End-to-End Protection on the Virtru TDP

Government Surveillance Prevention	Prevent unauthorized and unknown government surveillance of cloud data by managing access to and storage of encryption keys.
Data Residency Requirements	Choose where encryption keys are stored and accessed in order to prevent decryption of sensitive data outside of specified regions.
GDPR Compliance	Satisfy the European Union's GDPR requirements via "state of the art" encryption, as defined in Article 32 of the regulation.
CJIS Compliance	Share criminal justice information in the cloud by protecting it before it ever leaves the end user's device.
ITAR and EAR Compliance	Meet requirements for compliant cloud sharing of regulated technical data related to military, defense, telecom, and other highly sensitive applications and initiatives.

4.3.3 Key Management Optionality

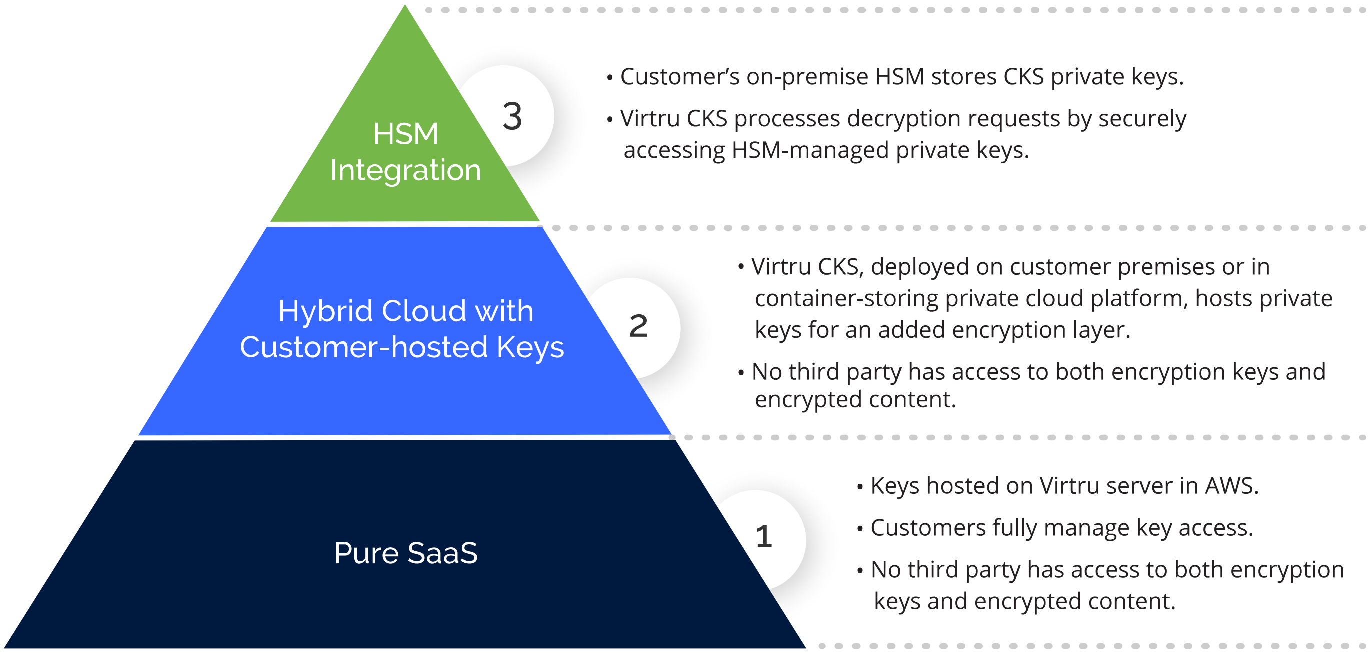
Different privacy, corporate security, and data residency regulations require different encryption key management precautions. As a result, the Virtru TDP offers enterprises three tiered options for key storage and transmission:

- Pure SaaS
- Hybrid Cloud with Customer-Hosted Keys
- Hardware Security Module (HSMs) Integration

Pure SaaS

The Virtru TDP's Pure SaaS key management option utilizes a split knowledge architecture where encrypted content is stored separately from the key that can unlock it. A unique Advanced Encryption Standard (AES) 256-bit symmetric data key is created on the client to protect each email and file, then the key is delivered via a secure TLS-protected channel to Virtru Access Control Manager (described in the next section on TDP's functional architecture). The Amazon Key Management Service (KMS) protects the symmetric data keys with an additional layer of asymmetric encryption that is protected by a set of AWS managed HSMs. Content travels encrypted through normal channels, and is never stored in the clear in any cloud system or by any service provider. Keys are hosted separately on the Virtru TDP, but access to them is always managed by the content creator and enterprise administrators.

This split knowledge architecture means that a single compromise would not result in the exposure of any encrypted content. An attacker would have to compromise both the Virtru TDP server and the recipient's client device or email service provider in order to decrypt protected content.



- Customer's on-premise HSM stores CKS private keys.
- Virtru CKS processes decryption requests by securely accessing HSM-managed private keys.

- Virtru CKS, deployed on customer premises or in container-storing private cloud platform, hosts private keys for an added encryption layer.
- No third party has access to both encryption keys and encrypted content.

- Keys hosted on Virtru server in AWS.
- Customers fully manage key access.
- No third party has access to both encryption keys and encrypted content.

Three key management configurations offered on the Virtru TDP

While the Pure SaaS method satisfies most encryption requirements, some enterprises require complete control and exclusive access to the encryption keys protecting their data. Although cloud platform providers and legacy security vendors have attempted to meet this need via various customer-held key management approaches, these solutions require that organizations trust the providers to take possession of the keys directly encrypting their content. Because they can access those keys, legacy providers also could access the underlying plaintext content inherently accessible in these solutions.

Hybrid Cloud with Customer-Hosted Keys

Virtru's Hybrid Cloud configuration leverages customer-hosted keys to provide a key distribution service in which no third party can ever access unprotected content or the keys directly encrypting it. The Virtru Customer Key Server (CKS) makes this possible. The CKS is a device that the customer hosts entirely on their premises or in the container-storing private cloud platform of their choice. It adds asymmetric encryption to Virtru's pure SaaS offering to give the customer complete and exclusive access to the keys encrypting their data.

When an enterprise shares content under this model, the originating Virtru client generates a message key that is encrypted with a CKS public key. The CKS hosts the private key needed to decrypt this public key and unwrap the message key, but only the enterprise can access it, since the CKS is hosted on its premises. Virtru's servers only store encrypted keys, so they never have access to decrypted message keys.

Receiving Virtru clients—either Virtru's Secure Reader or a Virtru-enabled device, client, or server—also have public/private key pairs. The CKS rewraps message keys with the receiving client's public key before it is transmitted to Virtru's servers and eventually to the receiving client itself. The receiving client, which sits on the recipient's premises, contains the private key needed to unlock the rewrapped message key and finally decrypt the content.

HSM Integration

Organizations with more sophisticated security processes and requirements can leverage their existing HSM infrastructure with our HSM integration. This deployment option builds upon the customer-hosted key option described above. The customer organization's private keys are stored in an on-premises HSM, and the Virtru CKS is only used to facilitate communication between HSM and Virtru ACM. Leveraging the PKCS #11 and KMIP protocols, the CKS processes encryption and decryption requests by securely accessing HSM-managed private keys. Virtru ACM continues to support authorization workflows on the front-end.

5. The TDP: Functional Architecture

The Virtru TDP architecture is broadly composed of four components described below and outlined in the figure below.

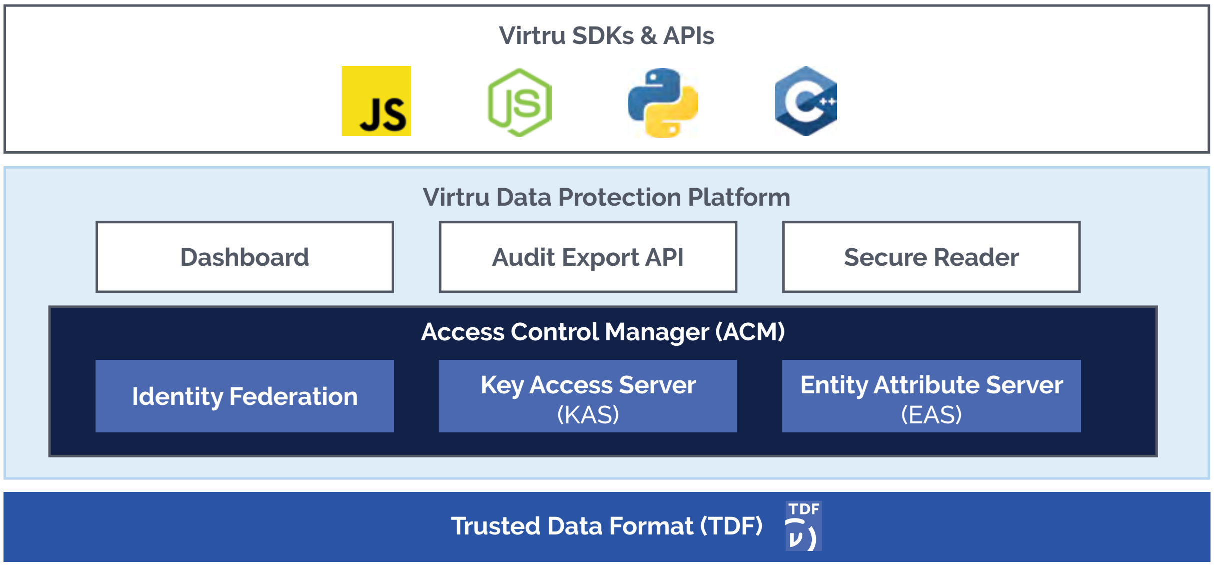
Access Control Manager (ACM): Core component of Virtru's SaaS key management infrastructure that lets organizations set, enforce, and manage policies to protect and control access to their data. The Virtru ACM hosts encryption keys, manages associated policies and entity attributes, and brokers authentication and authorization workflows using federated identities to mediate access to encryption keys and ensure only authorized parties can access protected content.

Dashboard: Centralized administration panel that offers visibility of all protected data, access, and sharing activity, along with users and groups management, email content rule configuration for Data Loss Prevention, and other organization settings.

Audit Export API: Supports export and integration of Virtru event logs, including all protection, access, control, and administrative activity, with security information and events management (SIEM) tools and security operations center (SOC) processes for behavior monitoring, incident detection and remediation, forensic analysis, and compliance management.

Secure Reader: Secure web-based browser application that enables seamless access to protected messages and files for external recipients and collaborators.

Virtru SDKs and APIs: toolkits that give developers access to the Virtru Platform so that they can independently embed data-centric protections and control features into their applications and workflows. Currently available for Client-side JavaScript, Node.js, C++, and Python.


Virtru SDKs & APIs
JS
Virtru Data Protection Platform
Dashboard
Audit Export API
Secure Reader
Access Control Manager (ACM)
Identity Federation
Key Access Server (KAS)
Entity Attribute Server (EAS)
Trusted Data Format (TDF)
TDF

The Virtru TDP architecture

Virtru Encryption Key Management Functions and Operations

Key Storage	Encryption keys are always stored separately from encrypted content for split knowledge; symmetric keys are hosted in Virtru's SaaS key management infrastructure; additional asymmetric keys can be hosted exclusively on customer premises via Virtru CKS.
Policy Management	TDF's metadata assertions via control policies are bound to encrypted content, enabling expiration, disable forwarding, and watermarking upon encryption; revoke and view read receipts for shared content.
Authentication	Performed by Virtru ACM when recipients attempt to access protected content, using recipient's existing credentials. Support for OAuth, SAML, OpenID, or email workflow with verification link or code.
Authorization	Managed via Virtru ACM; after authentication, ACM checks the policy tied to the encrypted data to confirm whether the authenticated identity is authorized to access the data.
Key Transmission	Keys are always transmitted separately from protected content; shared via TLS between Virtru clients and servers with perfect forward secrecy (PFS).

5.1 How the Virtru TDP Works

The Virtru TDP uses a split-knowledge approach to data protection. Content and encryption keys are stored separately, so that only authorized parties can access unencrypted content. This architecture ensures that Virtru can never access unencrypted content or decrypt user content outside of customer-controlled Virtru clients. Only recipients authorized by the content creator can access and decrypt protected content.

When a user enables Virtru protection, all encryption activities occur on Virtru-enabled clients using client-generated AES-256 bit symmetric encryption keys. Separate object encryption keys are generated to encrypt each individual email or file. When encrypted content is sent or uploaded, the creating Virtru client uploads these keys and their policies to the Virtru ACM via a secure TLS connection.

The Virtru ACM is a SaaS service that mediates access to protected content. It distributes encryption keys to authorized parties, enforces access control policies, and communicates with federated identity services to authenticate users. The Dashboard also surfaces management interfaces to end users and administrators.

Object stores, such as Amazon Web Services (AWS) S3, or email servers, such as Google G Suite, Microsoft Exchange, and Office 365, store encrypted content. The Virtru Zero-Trust architecture ensures separation of keys and content at all times. In instances when Virtru has the keys, it cannot access the content. In instances when Virtru services have the content, Virtru does not have access to the keys.

Virtru allows authorized parties to receive and decrypt protected content without installing Virtru's software. To access protected content, recipients must authenticate with the Virtru TDP. To do this, they use their existing email credentials, rather than having to establish new usernames or passwords. The Virtru TDP supports Federated Authentication via OAuth, SAML, and OpenID and grants access to protected content to authorized parties once they have authenticated.

The following sections explore how open standards and specific encryption implementations make these key management and authentication activities possible within the Virtru TDP components.

5.1.1 Virtru TDP Standards & Protocols

Using existing open standards and protocols, rather than proprietary vendor approaches, enables both a higher level of security and interoperability for the Virtru TDP. Security experts coalesce around the very best standards, ensuring continued innovation and rapid reaction to new threats. In addition, the use of standards significantly streamlines integration with other applications.

In addition to the TDF standard, the Virtru TDP architecture leverages other open standards and protocols that are widely accepted in the security community. For example, the Virtru Dashboard makes heavy use of the Key Management Interoperability Protocol (KMIP) from the Organization for the Advancement of Structured Information Standards (OASIS). KMIP can facilitate communications between a key management server and encryption/decryption clients. KMIP can also store and protect encryption keys and other sensitive information related to content encryption via the KMIP object model. The communications and storage/protection capabilities make KMIP a natural fit for the Virtru TDP.

The Virtru TDP uses KMIP in multiple ways. First, it leverages and extends the KMIP object model to support the storage and protection of Access Control Keys and Split Knowledge Keys (explained in more detail in the next section). Second, KMIP-compliant transport mechanisms, specifically the Hypertext Transfer Protocol (HTTP) over TLS using JavaScript Object Notation (JSON), enable communications between encryption servers and clients. Virtru's use of KMIP was not originally envisioned as a use case of KMIP, but Virtru has extended KMIP to improve its usability in support of the Virtru TDP.

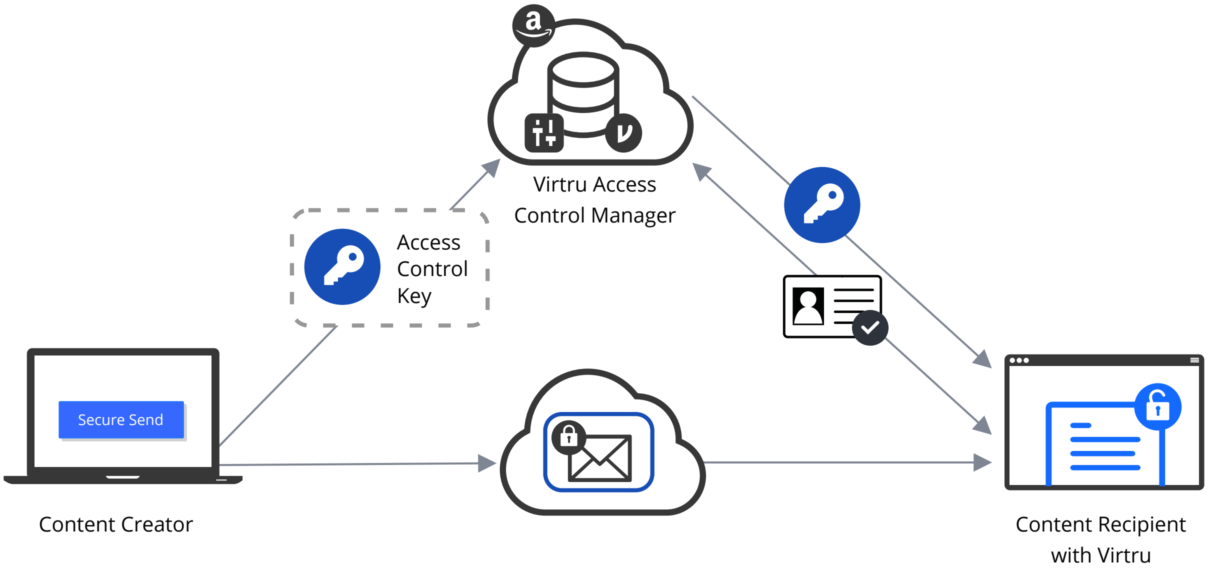
The Virtru TDP servers are designed to be federated and distributed, meaning that customers can choose where they want their keys to be stored and distributed. Virtru-enabled applications are designed to specify a pointer to the appropriate key management server at the time of encryption. By this method, a recipient's client-side software knows where to go to retrieve the key to decrypt their content.

5.1.2 Virtru TDP Encryption Implementations

The Virtru encryption model has two implementations. The first implementation is most commonly used when the content consumer uses a Virtru-supported service, such as Microsoft Outlook or Google G Suite, and has Virtru installed on the endpoint.

For the first implementation, a single secret key, the Access Control Key, is used to encrypt the content via 256-bit AES-Galois/Counter Mode (GCM). This key is securely transferred from the sender's client device to the Virtru ACM, using Elliptic Curve Diffie-Hellman Exchange (ECDHE). This connection, as well as all other key transmissions in this process, is established using perfect forward secrecy (PFS), which provides stronger security by ensuring that the connection's session establishment keys are ephemeral. At the same time that this key is being transferred, the encrypted content is sent directly to the recipient through normal channels.

Key Management and Exchange: Virtru SaaS, Recipient Has Virtru



Upon the initial email encryption and sending:

- The Virtru client creates a unique AES 256-GCM symmetric encryption key, the Access Control Key, to encrypt the message.
- The Access Control Key's policy is updated when recipients are added and access controls are applied, controlling who can access it, for how long, and whether recipients can share or forward.
- The encrypted message is sent to the cloud email server, and the Access Control Key is transmitted from the client to the ACM.

Upon recipient access attempt, the ACM:

- Authenticates recipient identity.
- Authorizes recipient identity against policy tied to Access Control Key.
- Grants access to Access Control Key (if authorized).
- Decrypts content for recipient access.

The second implementation builds on the first implementation outlined above and is used to maintain high levels of security and privacy when content consumers do not have a Virtru-enabled application and must access protected data via the Secure Reader. This requires Virtru to create a copy of the initial content payload, since without a Virtru client on the receiving end, the recipient's client will not be able to access the initial content payload. So immediately after the copy is created, it is encrypted with a separate key, referred to as the Payload Key. The Access Control Key from the first implementation is then used to encrypt the Payload Key (and sent to the Virtru as in the first implementation). From there, a third key, called the Split Knowledge Key, is used to double-encrypt the (already encrypted) Payload Key.

Crucially, the Split Knowledge Key ensures separation of keys from encrypted content to ensure split knowledge (reflected in its naming); it is stored alongside the initial encrypted content payload and sent via normal channels, typically through the customer organization's mailflow. Meanwhile, the encrypted message copy and double-encrypted Payload key are sent to Object Stores, for secure storage within AWS.

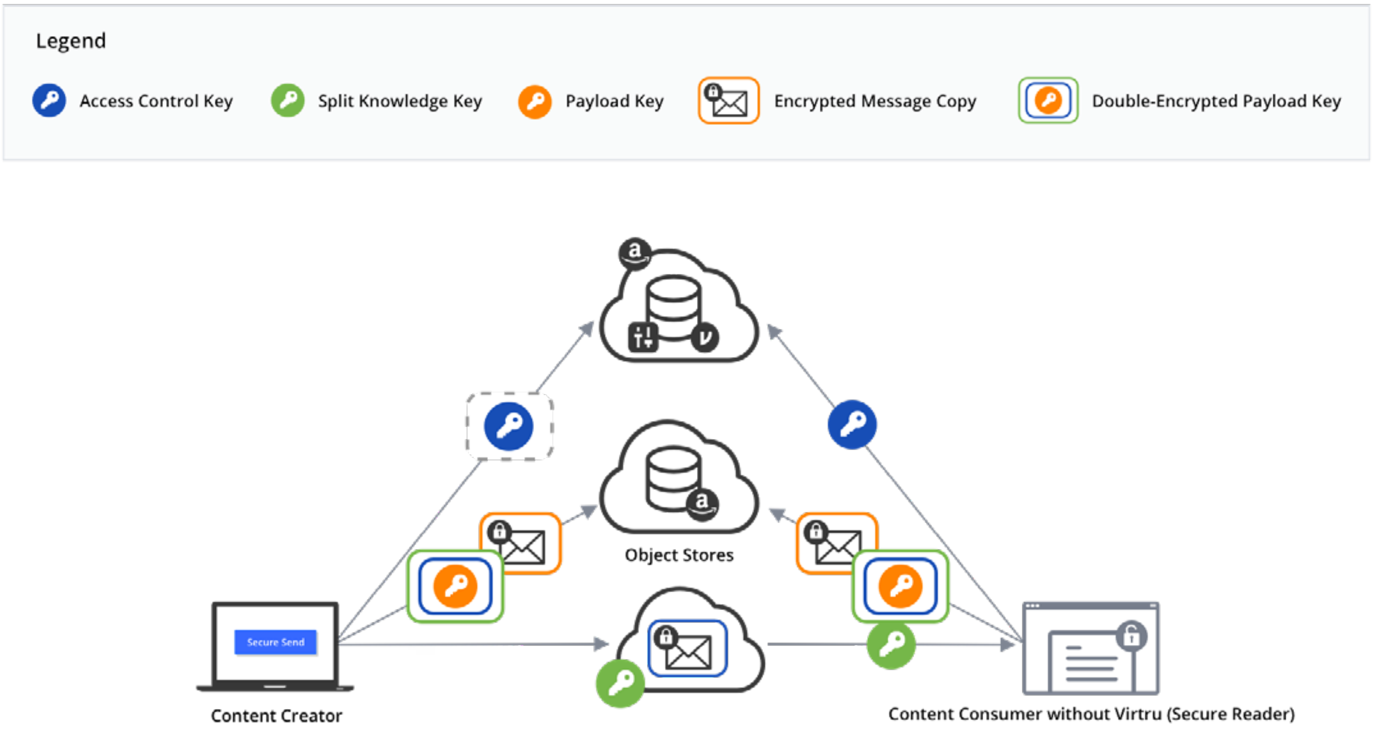
In both implementations, the authorized recipient gains access to the Access Control Key once a third-party identity provider service authenticates his or her identity and the ACM authorizes that identity is allowed to view the protected content.

In the first implementation, the recipient has the Virtru client installed on the endpoint, so once they are authenticated and authorized, the Virtru ACM sends the Access Control Key to the receiving client. From here the content decrypts within the client for seamless, secure, and transparent access by the recipient.

In the second implementation, the recipient is prompted to unlock the content via the Virtru Secure Reader, which initiates an authentication and authorization workflow for the Access Control Key as well as for the double encrypted Payload Key and the Split Knowledge Key. After authentication and authorization, the Split Knowledge Key is used to unwrap the first layer of encryption around the double encrypted Payload Key, and the Access Control Key unwraps the second layer of encryption. Finally, with the Payload Key decrypted, it can be used to decrypt the encrypted message copy, providing seamless secure access to the content by the recipient.

These advanced key management workflows ensure that, in instances when Virtru has the keys, it cannot access the content. In instances when Virtru services have the content, Virtru does not have access to the keys. And despite the complex nature of these key management operations, Virtru never requires manual key exchanges. Key exchanges are powered by the Virtru ACM and always happen transparently for end users and admins.

Key Management and Exchange: Virtru SaaS, Secure Reader



Upon the initial email encryption and sending:

- The Virtru client creates a copy of the email and encrypts with the Payload Key.
- The Payload Key is encrypted with the Access Control Key.
- The encrypted Payload Key is encrypted again with the Split Knowledge Key, which is stored with the initial email, never within Virtru's SaaS Key Management Infrastructure.
- Encrypted message copy and double-encrypted Payload Key are sent to external object stores, separate from the Split Knowledge Key.

Upon recipient access attempt:

- The Virtru ACM authenticates the identity and verifies whether it is authorized to access the content.
- If authorized, the ACM grants access to the Access Control Key, sending it to the content consumer's receiving client.
- Encrypted message copy and double-encrypted Payload Key are sent to the content consumer's receiving client from the Object Stores.
- The Split Knowledge Key is sent to the content consumer's receiving client with the original message.
- Within the receiving client, the Split Knowledge key decrypts the first layer of encryption on the Payload key, and the Access Control Key decrypts the second layer.
- Finally, the Payload Key is used to decrypt the message copy to enable access within the Secure Reader.

Case Study: Securing Email Communications with the Virtru TDP

The following outlines the steps used to leverage the Virtru TDP to provide access control, key management, and policy enforcement across different email services. The process consists of five main steps:

Step 1: Content Encryption

The sender places content into a Virtru-enabled email client and indicates that the content should be protected. The email client encrypts the content before it is sent. In order to perform this encryption, the email client generates unique encryption keys specifically for protecting the content (and this process is outlined in detail in the previous section). The email client also creates an access control policy for this content, which defines, through metadata assertions, any access control restrictions on recipient behavior (for example, when the content should expire, if ever).

Step 2: Content Distribution and Access Control Management

The sender's email client distributes the content through normal channels, such as sending an encrypted email message to the appropriate mail server for processing. At the same time, the sender's email client also handles access control management. This involves transferring encryption keys (and their associated access control policy) and any encrypted content copies to the Virtru ACM and object stores, respectively, for storage until the recipient attempts to access the email.

Step 3: User Authentication

When the recipient attempts to access the protected content through the recipient's Virtru-enabled email client, this triggers a three-party user authentication session between the email client, the Virtru ACM, and the third-party Identity Provider service holding the recipient's user credentials. All three major federated identity protocols—OAuth, OpenID, and the Security Assertion Markup Language (SAML)—are supported by Virtru for user authentication. Because the Virtru-enabled application coordinates all the communications between the ACM and the identity provider service, Virtru never has access to the user's authentication credentials.

Step 4: Key and Contract Distribution

If user authentication is successful and ACM confirms that the encryption key's policy authorizes the user to access the content, Virtru provides the protected Access Control Key to the recipient's Virtru-enabled email client.

Step 5: Content Decryption

If the terms of the security contract are met, such as the content not having already been expired by the sender, the recipient's email client uses the key to decrypt the protected content, making it available to the authorized recipient.

The Virtru TDP approach to email encryption provides significant advantages to legacy public key and portal-based approaches. Public key approaches such as PGP and S/MIME both offer client-side, end-to-end encryption, but are difficult to use and require complicated manual key exchanges. Portal-based systems are relatively easy for senders, but are far less usable for recipients.

Portal-based systems are also substantially less secure and private because they store a copy of the content on their server. A breach of that server could easily lead to unauthorized access to all the content, and thus cause major breaches of confidentiality for many users at once. The Virtru TDP approach combines persistent control and visibility with the security advantages of client-side, end-to-end encryption, all without sacrificing the convenience and ease of normal email.

6. Virtru's Trusted Privacy Technologies

Current Product Offerings

Virtru eliminates the tradeoff between ease of use and data protection by integrating into existing enterprise tools. Our flexible, easy to use, and trusted privacy technologies govern access to data throughout its full lifecycle—from creation through sharing, storage, analysis, and action. Virtru's portfolio of products include:

- Data privacy solutions that transparently integrate into commonly used applications, such as email and file sharing. Virtru adds object-level encryption, access control, audit, key management, and policy enforcement capabilities to Microsoft Outlook (for either on-premise Exchange or Office365) via an Outlook add-in, and Google Drive and Gmail within Google G Suite via Chrome browser extensions. For Salesforce, Workday, NetSuite, and other common business applications that automatically exchange data via messaging processes, Virtru's Data Protection Gateway ensures emails and attachments are protected with persistent visibility and control, without breaking your application workflows.
- A set of privacy engineering tools for developers that can be easily and seamlessly integrated into any application, connected device, and infrastructure. With the Virtru SDKs, companies can harness the Virtru TDP to integrate object-level protections into their apps quickly and easily. These capabilities provide a much higher level of data protection than most companies can build in-house, and they allow enterprise application providers to eliminate a single point of failure, just as Virtru's off-the-shelf solutions do.

The Virtru TDP at Work for In-House Applications

Through Virtru's SDKs, organizations are provided with a central console that can be used to set privacy policies and control access to data throughout all of the applications you use—even those developed in-house.

As an administrator, you'll be able to enforce domain-wide policies across all of your collaboration tools, and quickly control access on a per-user or group basis across all connected apps and devices. As the below use cases illustrate, we want to make it as easy as possible for enterprises to add data protections to existing tools and build them into new ones, all the while ensuring that these protections persist no matter where content is created or consumed.

Secure Analytics

In order to generate meaningful insights from their highest-impact analytic models, institutions must have access to massive amounts of data that can only be gathered by sharing information with other organizations.

Even though they understand the benefits of broader information exchanges, organizations are usually reluctant to share their most valuable data with analytics collaborators due to a lack of transparency into, control over, and ownership of their data once it's been transmitted

The Virtru TDP ensures that access to datasets remains cryptographically imposed by encrypting all data and enforcing policies on their associated key servers. The individual data points provided by separate organizations collaborating on the analytics project are never revealed to the other organizations, yet all parties are able toget seamless access to analytics, metrics, and other calculations derived from the individual data points.

Connected Devices

Manufacturers around the world are competing to develop new IoT devices and put them in consumers' hands to enable greater connectivity. But the rapid speed of product development does not always allow enough time for security considerations to be thoroughly considered and implemented.

IoT sensors continuously stream large volumes of sensitive data from devices to the cloud. This data must uphold protection standards across its entire lifecycle—from collection to transmission to analysis—even when the device itself may be insecure, to maintain consumer privacy and regulatory compliance.

Using Virtru SDKs, developers and security practitioners can incorporate persistent protection into IoT devices, encrypting data as it's collected and appending access control policies, defined by the admin or the end user. This keeps data collected and shared by connected devices private and compliant, while Virtru TDP's access, revocation, and expiration controls help protect IoT devices that can be lost or stolen.

Pandemic Response

Healthcare experts responding to the global coronavirus pandemic need access to data to track and slow its spread and allocate resources where they are most needed.

Assuring verifiable control builds trust in patients and other stakeholders that, in turn, allows healthcare providers, government officials, and others to quickly and accurately generate new and better insights, leading to more effective action plans that will allow us to reopen our economy sooner, without sacrificing privacy.

Similar to the Secure Analytics use case described above, the Virtru TDP ensures data is used only for its intended purpose and includes strong controls that give individuals the power to share, approve, and revoke access to their sensitive information at any time.

Application Security

While application security professionals remain focused on safeguarding data and staying compliant with changing regulations, developers are building new applications and data-sharing workflows at a record pace.

Open source tools, containers, and low code platforms have accelerated the release process, making it tough for security practitioners to keep up. When end-to-end data encryption and access control features are readily available and easy to implement, true DevSecOps execution becomes a reality.

With the Virtru TDP, your team can add object-level data protection to applications and workflows with ease.

7. Conclusion

Today's threat landscape demands data protection that provides persistent access control, meets enterprise security requirements, and is easy enough for widespread adoption. By providing granular access controls for any type of content—while making interfaces easy for senders, recipients, and administrators—the Virtru TDP is the first solution that eliminates the tradeoff between data protection and ease of use.

With its foundation comprised of mature, standards-based open protocols and data formats, Virtru offers highly scalable and flexible data protection for organizations of any size and composition. Virtru has adopted a federated model that allows organizations to leverage existing authentication services and manage their own encryption keys using Virtru-provided key servers.

Virtru minimizes the impact on client applications, cloud servers, and end users, while also taking advantage of powerful access control and security services on the cloud-based Virtru TDP. Using Virtru libraries and APIs, protection can be tightly integrated with existing application functionality, minimizing disruption to end users.

Taken together, the Virtru TDP enables enterprise organizations to achieve pervasive data protection while integrating into existing user workflows and business applications.

For more information or to see Virtru's TDP in action,
please contact us to schedule a demo. virtru.com/contact-us

About 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 20,000 organizations trust Virtru for data security and privacy protection. For more information, visit virtru.com or follow us on Twitter at @virtruprivacy.