Accelerate Secure Data Sharing with Integrated Protection for Sensitive & Classified Data

Powered by the Trusted Data Format, Virtru Secure File Collaboration Automates Encryption and Access Control, Streamlining Federal Data Sharing Workflows

Executive Summary

For federal agencies, it's critical to ensure sensitive data doesn't fall into the wrong hands, and that it is only accessed by those with a need to know. Because many organizations have numerous levels of access rights, as well as numerous channels and products by which data is disseminated, data tagging and access management have become extremely complex.

Federal organizations need to efficiently and securely share sensitive information. Unfortunately, managing that data is often inefficient and full of friction: Some organizations have dozens of distinct servers and/or networks, each with their own unique access parameters, containing different sets of data. Additionally, sharing information with partners on shared drives is highly manual, with end users passing data to admins to ensure information is properly protected before being uploaded to a shared repository. With users navigating between these disparate interfaces, only able to view data on one server at a time, this introduces inefficiency, user error, and risk to agency missions.

Agencies need a more efficient way to balance security with visibility. Virtru Secure File Collaboration equips end users to securely share data with colleagues and coalition partners by automating encryption and applying access controls from existing tools.

The result is an environment where sensitive and classified data can be shared quickly and efficiently, with fewer bottlenecks and reduced risk — tying encryption and access controls to the data itself, everywhere it travels.

Virtru Secure File Collaboration is built on the open, IC-standard Trusted Data Format (TDF) to secure data flowing through core collaborative workflows, including Microsoft 365, Sharepoint, Google, and custom applications. This enables users to see the big picture while data remains secure and under the data owner's control at all times, even after it leaves the originating organization. Should circumstances or access needs change, data access can be adjusted or revoked at any time, instantly.

Solving a Persistent Legacy Problem

Large segments of the U.S. government are tasked with the creation, distribution, and continuous protection of sensitive or controlled classified data and files. This task occupies significant time, effort, and resources — and the workflows frequently rely on legacy or patchwork solutions, even though many government employees and contractors must work with these files and data every day. If such data and files need to cross organizational boundaries due to mission needs, the task of ensuring data remains properly protected and within compliance becomes exponentially more difficult.

There are a number of reasons this problem is difficult to solve:

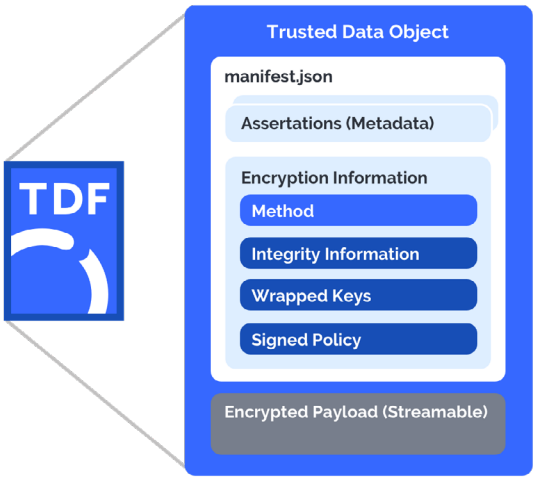
- **Data is not properly tagged when it's created.** As data and documents are created, they are often not properly tagged in such a way that systems can determine who should and shouldn't access them, and when and where. These tags are often granular and complex in nature, so some users need significant assistance to ensure that they properly mark their documents and data.

- **Tags don't always travel with the data.** Even when data is properly tagged, metadata often doesn't properly tie into systems' enforcement mechanisms. There are several possible underlying causes for this disconnect. For example, the rules underpinning these systems can be incompatible or in flux. This challenge is particularly prevalent when data moves from one agency to another.
- **Many enforcement mechanisms rely on legacy techniques instead of newer, stronger, and more user-friendly protections.** For example, some agencies resort to creating large numbers of isolated networks when sharing data with international partners, with a separate network for each permutation of permissions. This places most or all security at the network perimeter, rather than individually protecting each data element, as is called for in Executive Order 14028. A large array of disparate networks also makes it difficult for users to collate common data, ensure proper access control of data across all networks, or maintain adequate visibility by data owners from outside organizations.

A Zero-Trust Approach to Federal Data Management

Zero Trust helps to address the aforementioned challenges. The concept of Zero Trust largely centers on gaining greater visibility and eliminating the need for network trust. It introduces a deny-by-default mentality, limiting access to prevent lateral movement within systems.

Instead of creating disparate environments with varying levels of security, federal agencies can instead leverage a Zero Trust strategy that applies access controls to the data itself — this way, data can be stored and managed in a single place, under a unified framework, with access granted or denied based on the individual user's credentials, location, and other designated parameters. Virtru's Trusted Data Format is designed to facilitate this data-centric, Zero-Trust protection.



With a Zero Trust approach, access privileges can be customized based on specified parameters, including devices, users, locations, or characteristics of the data itself. A Zero Trust data strategy therefore requires object-level data protection with customizable and granular access privileges, ideally based on identity attributes. For a data-centric approach, protections must persist as the data travels across devices, environments, and applications, as well as physical locations or organizational boundaries, and apply to any data type.

If each piece of data is protected individually, and control of its access is maintained by the owning organization, *where* the data resides becomes much less important. This means that data assets can be co-located for ease of use with less consideration given to security. Systems can then access all data relevant to an application's functionality, and since access control is considered for each individual data element, each user only accesses data for which they are authorized.

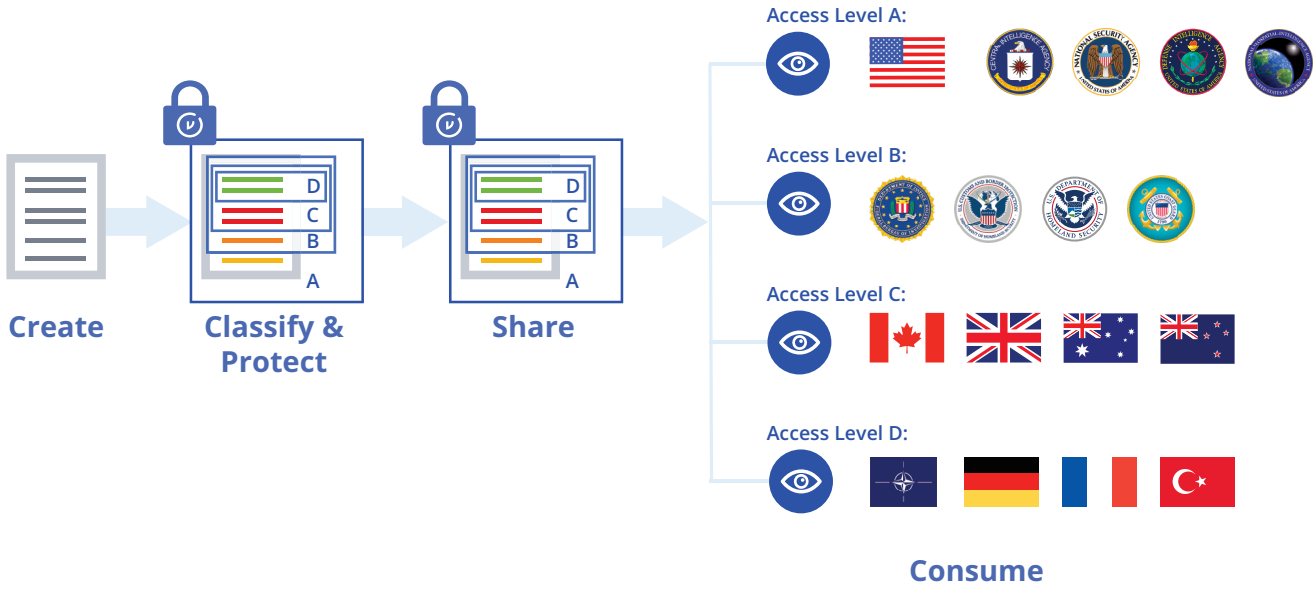
Virtru solutions such as Secure File Collaboration, based on the TDF standard, provide protection of data via robust encryption and attribute-based access control (ABAC) via embedded tags containing relevant metadata

Content Creation

As documents are authored or other data is created in one environment, Virtru Secure File Collaboration ensures appropriate protection is applied before data moves to a shared environment.

With Virtru Secure File Collaboration, agencies can:

- **Accelerate existing workflows by automating data protection.** Virtru's access controls integrate with many existing dissemination points, such as Microsoft SharePoint or Windows shared drives.
- **Reduce the risk of human error.** When a user decides to upload a file to a shared drive, Virtru encrypts data prior to upload. This ensures that files uploaded to shared drives are fully protected and that their metadata carries all existing access control parameters and tags.
- **Align tags with established classification regimes**. With attribute-based access control, agencies can appropriately tag data under CAPCO Classification & Control Markings, STANAG 4774 (NATO's confidentiality metadata syntax), or other classification or categorization structures defined within standard tools.
- **Pull in classification metadata from other tools**. Virtru Secure File Collaboration supports classification metadata written by existing solutions such as Titus or Boldon James, and is even able to perform remediation of misclassified data within those tools. Additional tools are integrated with Virtru Secure File Collaboration on an ongoing basis, ranging from commercial solutions to agency-developed applications.
- **Quickly adapt and respond to changes.** Virtru provides persistent control of encrypted, shared data. Should circumstances or agency relationships change in any way — whether at the user level, organization level, or country level — agencies can leverage Virtru to revoke access or instantly make adjustments to how data is shared with those entities.



It's All In The Tags

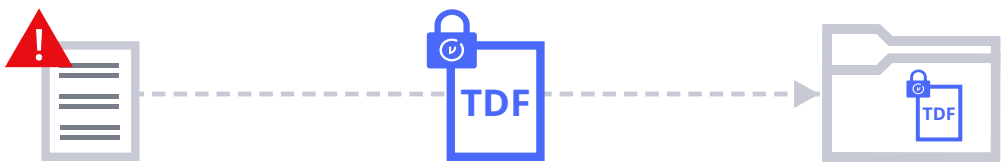
Like other Virtru solutions, Virtru Secure File Collaboration protects data via embedded tags containing relevant metadata. For granular pieces of data, such as a single image, one set of tags likely applies to the entire piece of data (the image). For more complex items, such as a long report written in a Microsoft Word document, one set of tags might not apply to all of the content.

This is why classified or controlled documents contain portion marks – classification markings which apply only to a specific part of a document, like a paragraph, an illustration, or a table. In these cases, each marked portion has its own distinct set of tags, and access control is performed individually upon that portion. In the example of a Word document containing multiple sections with different levels of sensitivity, the main Word document is a TDF-protected file, and each portion-marked section within that file is its own TDF object embedded within.

When a user opens the Word document, they request an encryption key to the whole document, as well as a key for each portion. For the portions to which they don't have access, they only see redacted content. As users rely on tools like Titus or Boldon James to portion mark their documents, Virtru Secure File Collaboration turns those portion marks into ABAC tags for that portion of the document and enforces it by making the portion a TDF. This creates a seamless experience for both the document creator — who only has to apply portion marks in order to set access control — and the recipient, who is granted access only to the portion of the file that they are authorized to view (and is not denied access to the file itself).

Tagged Data In Motion

Data obviously doesn't stay where it was created, though. As users finish creating their content, or as system-generated data moves out to be viewed within applications, it will be moved or copied from one location to another. Virtru Secure File Collaboration integrates with system components to ensure that only data meeting the organization's protection standards moves from one place to another. For example, it may be acceptable to store unencrypted data and documents on a tightly controlled and team-specific shared drive. Copying those to a SharePoint repository seen by a much broader audience, however, requires that the documents be encrypted. Today, the responsibility of encryption and uploading to SharePoint often falls to an administrator, which can cause delays in sharing urgent information.



Step 1:
User attempts to upload an unencrypted file to a shared location.

Step 2:
Virtru automatically encrypts the file before it's uploaded. The TDF-protected file carries existing classification metadata.

Step 3:
All data on this shared location is encrypted and appropriately tagged.

Because Virtru Secure File Collaboration is integrated with sharing tools such as Microsoft SharePoint, it "watches" as documents are copied to the repository. Should a user attempt to copy an unencrypted document into it, Virtru Secure File Collaboration will automatically encrypt that file, converting the document into a TDF, and using its existing classification metadata to create the appropriate ABAC tags. In this way, only protected data is placed on shared locations.

By using TDF as the standard for data protection, applying ABAC tags to categorize that data, and ensuring appropriate protection of data in transit, data owners can share data with the confidence that cryptographically enforced tags will accompany the data wherever it goes. Even if data leaves the federal organization's network, it requires the same authentication to ensure that information cannot be opened by anyone without the necessary access rights. If a requesting user, system, or non-user entity does not possess the required attributes for access, regardless of where they are, they are denied access to the data

Open Standards for Secure Workflows

VIrtru strongly believes in, and supports, open software standards. All Virtru products, including Virtru Secure File Collaboration, are built upon these standards. As such, there are certain components federal customers must have in place to leverage Virtru Secure File Collaboration in an enterprise environment.

Chief among these would be a means of ensuring that users and non-user entities are who they attest to be. In the case of Virtru Secure File Collaboration, this is built upon OpenID Connect (OIDC, which is built upon the OAuth standard) and relies on an Identity Provider (IdP), which is a common set of standards allowing software components to securely verify the identity of an end user and obtain some profile information about that user (such as what they should be able to access) in a secure manner. Secure File Collaboration implements OIDC, which allows a number of different means by which a user can assert their identity, such as digital certificates/ PKI, SAML, etc. Use of OIDC also allows for federation to multiple entitlement providers as well as standard entitlement extensions. Virtru Secure File Collaboration can use any OIDC capable IdP.

Data Storage

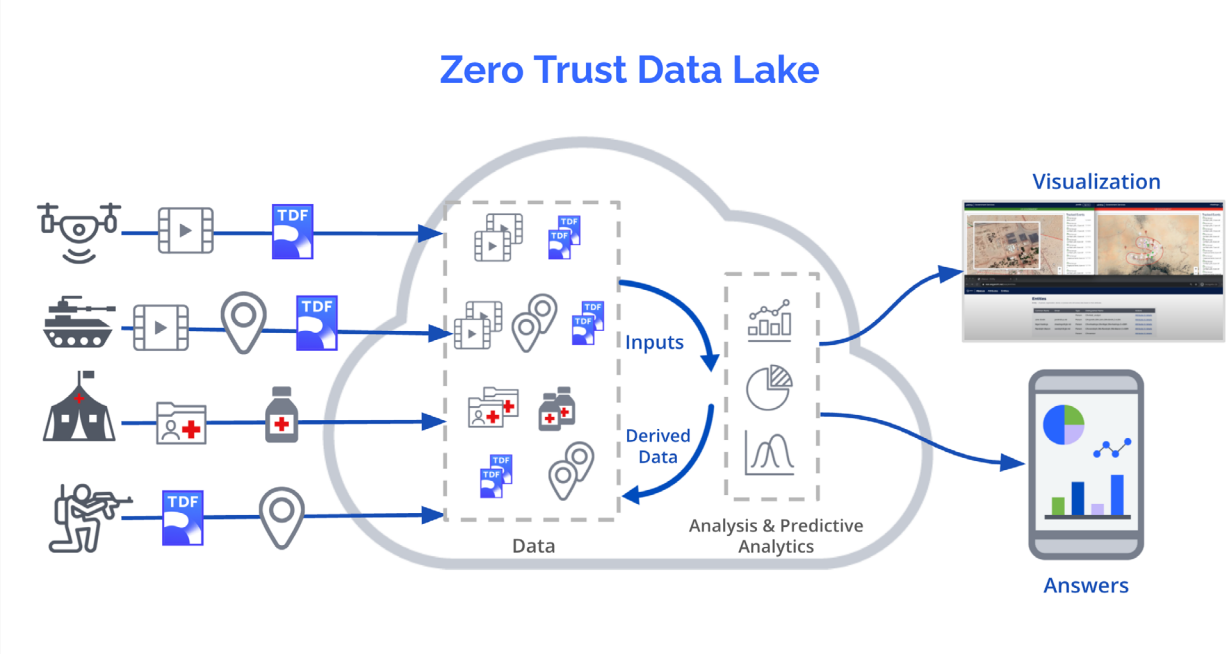
Location, Location, Location

As mentioned above, one legacy approach for access control is to create a separate network for each permutation of access control or dissemination attributes applied to data collections. Users are then granted access to the networks relevant to their permissions and functions. This is problematic for a number of reasons:

- The number of networks involved can be dozens or more, quickly becoming an expansion *ad absurdum*.
- The administrative overhead of maintaining such an environment is not only exceedingly complex, it is also labor intensive, error prone, resource-heavy, and expensive.
- Most importantly, users are unable to view all of their data in one place, so users must mentally "collate" multiple data sets from multiple networks. This is difficult and introduces unnecessary risk, errors, and omissions.

- This approach makes multiple copies of data pervasive across the enterprise. In order to have an accurate audit record for data, numerous audit records would have to be re-consolidated, which is a significant data management problem.

With Virtru Secure File Collaboration, each data owner – whether they are a separate organizational branch, agency, or even a foreign mission partner – maintains their own encryption key server that they control. Regardless of where the data itself is located, this key server is always involved in making an access control decision. All actions on those data holdings are also audited individually, for each data owner, so each owner has complete visibility into who is doing what with their data, when, and where. This means that the data owner has continuous, assured control over their data, wherever the data object itself happens to be.



In essence, it matters much less where the data or the documents reside. The need to separate data into multiple protected networks no longer brings any advantage. Data and documents from multiple organizations and domains can now be securely co-located into a common data lake. Shared services, such as operational applications, secure analytics environments, and other IT services, can securely operate on these secure, shared data repositories, providing meaningful operational capabilities and relevant analytics programs.

Consumption Flows

Just as the storage location of the data becomes less important with data-centric protection enabled by the TDF, the consumption of this data also becomes more flexible. Applications also can continue to access data within these commonly understood and accessible platforms and display secured data appropriately. PDFs secured within Virtru Secure File Collaboration as TDFs can still be rendered via applications that view PDFs, but at the time of access, an encryption key is requested and an access control decision is made. Thus, data remains secure and accessible in commonly understood platforms and familiar applications, yet completely under the control of the data owner and well audited.

Next Steps

Prior to Virtru's Secure File Collaboration, approaches to securing sensitive or classified data were often fragmented, inconsistent, or unenforced. Virtru Secure File Collaboration changes that, transforming the way federal teams operate, freeing up valuable resources, and integrating the persistent protections of TDF with other infrastructure components in a meaningful way to provide a real, effective Zero Trust implementation.

As a critical part of the technical and cultural change required for a data-centric approach, Virtru is an important enabler for transformations to Zero Trust models. Virtru products have a proven history of protecting and sharing sensitive data across business and mission workflows for the U.S. intelligence community, the Department of Defense, other elements of the U.S. federal government, and thousands of commercial customers. Virtru's Trusted Data Platform contains the necessary elements for implementing a modern Zero Trust strategy, and Virtru's implementation teams and professional services partners have the experience and expertise to guide federal agencies as they navigate this new and emerging security landscape.

Contact federal@virtru.com to learn more about how the TDF can help your agency streamline collaboration and accelerate secure data sharing. Our team has deep federal government expertise, which we leverage to help you improve data protection, reduce friction — and support your mission.

Trusted by Federal Agencies, State and Local Governements.

USAID FROM THE AMERICAN PEOPLE

Lawrence Livermore National Laboratory

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of encryption solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 7,000 customers trust Virtru for data security and privacy protection.