Securely Create & Consume Sensor Data with Virtru

Protect & Synchronize Technical Intelligence Collections with Virtru for Richer Situational Awareness

Executive Summary

The ability to quickly, securely, and appropriately share data with external partners is critical to mission success. This is increasingly true with the rise of distributed workforces, and it is even more so for teams deployed into hostile, emergency, or disaster environments, where new information can emerge and change rapidly. Whether sharing data with a colleague on the other side of the planet or with coalition partners in the same field, data owners must have tools at their disposal that ensure timely access to data that is limited to those teammates and partners who *should* have access. Further, when collecting and analyzing aggregated data, often of different types and from different sources, recipients must have tools at their disposal to verify the integrity of the data as well as the identity of the sender.

The Virtru Trusted Data Platform (TDP) tackles the challenges associated with secure data collection, rapid intelligence production, and controlled dissemination by protecting data from creation with cryptographic enforcement of access control policy as defined by the data owner (originator). The enclosed solution brief will detail how the components of the Virtru TDP work in concert to not only ensure data protection across the intelligence cycle but, through the trust built on the foundation of protection, also unlock insights that can only be gained through enhanced collaboration across teams and coalitions.

Problem Statement

Many organizations have turned to "stovepipes" as the default mode of protecting their data, walling off environments wherein only authorized users are allowed. In other words, the paradigm has been to protect the perimeter "moat & castle" style, while trusting *anyone* within that perimeter. Working with data from multiple stovepipes simultaneously becomes problematic, and not just for analysts or data scientists conducting longitudinal analysis or other assessments wherein time is not of the essence. Individuals needing access to real-time data in operational environments would have to flip through multiple screens, somehow finding a way to "knit together" their real-world view of the situation, potentially risking their lives and others' by missing essential details.

The Virtru Solution

Leveraging the Trusted Data Format (TDF), the open standard embraced by ODNI[1] and the broader U.S. intelligence community, Virtru technology facilitates access control at the data layer – rather than through isolated applications or networks – wrapping data in protection from the moment of creation so that it remains secure no matter where it resides or travels. The organization that owns the data determines who is allowed to see it, in any environment in which it's used, by cryptographically enforcing access control policy. In this way, operational controllers can bring together all data sources into a single, real-time common operating picture

1 https://www.dni.gov/index.php/who-we-are/organizations/ic-cio/ic-cio-related-menus/ic-cio-related-links/ic-technical-specifications/trusted-data-format

(COP), showing them a collated view of the environment without the need to view it in piecemeal fashion. They also are able to tailor each operational partner's view of the COP based on need to know and other delimiters. Additionally, further analysis can be conducted on the data contributed from different sources while preserving data owners' ability to revoke access and influence access rights to the outputs of analysis, as determined by any data use agreement in place between the respective organizations of the data owner and the analyst.

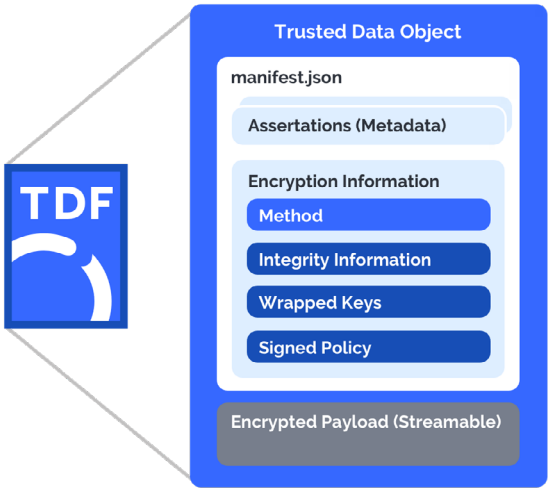
The Virtru Trusted Data Platform

The Virtru TDP protects institutional and individual data by cryptographically assuring that original data owners always control how others can access their data. The platform orchestrates several components to mediate data access, analysis, and audit through the entire shared collaboration lifecycle, including a split knowledge architecture that separates management of encryption keys from the data they protect. Based on extensible and scalable cryptographic proof instead of inherited or implied trust, the platform's model assumes zero trust – that any party could pose a threat – and allows data owners to assign protections more granularly than the majority of trust models today. This empowers data owners and downstream users to share insights, while also maintaining awareness and control over the ongoing access and usage of any outputs.

By ensuring that data remains protected wherever it is transmitted, used, or stored, the TDP reduces security dependencies on traditional ephemeral "data in transit" or "data at rest" protections, and instead ensures protections persist with the data, wherever it may travel or be consumed, rather than only protecting a perimeter. Data owners gain full lifecycle control over the information while still being able to safely share it for approved analysis or use, leading to faster, more frequent insights and therefore driving meaningful operational outcomes.

The Trusted Data Format

The Virtru TDP leverages the Trusted Data Format (TDF), an open data format that keeps data protected and under the data owner's control no matter where it is created or shared. With the TDF, an organization can apply discrete policies and rules leveraging Attribute-Based Access Control (ABAC) that travel with the content. By enabling data owners to tie security tags to specific data objects and update these policies over time, the TDF prepares data for ingestion into the TDP. Furthermore, the TDF is agnostic to encryption algorithms, which means that organizations are free to choose their own cryptographic method or easily swap methods in the future as threats evolve (e.g., quantum attacks).



Local client-side applications – even on very lightweight devices with minimal compute resources – built via the TDF software development kit (SDK) categorize and protect each data object by wrapping it with the TDF, which contains encrypted data that is cryptographically bound to any already applied tags and associated access or handling policies. The local clients then send the encrypted, tagged data to the TDP for processing.

NanoTDF

The true power of TDF is that it is simple and lightweight enough to be implemented on platforms with very small footprints. Virtru's lightweight implementation of TDF is called "NanoTDF" and can be enabled onboard very small sensors. As data is recorded by the sensor, it is encrypted into a TDF *before ever leaving the device*. In this manner, data is truly protected throughout the environment. For example, each video segment (even as short as *one second* of video), or each individual value of a sensor reading, is its own encrypted identity with all of the relevant components: key management, access control, and auditing, all within the zero-trust environment of TDP. This process only adds *bytes* to the data object and has minimal, almost unmeasurable, impact on the device's performance.

How Does Virtru Enable Zero Trust?

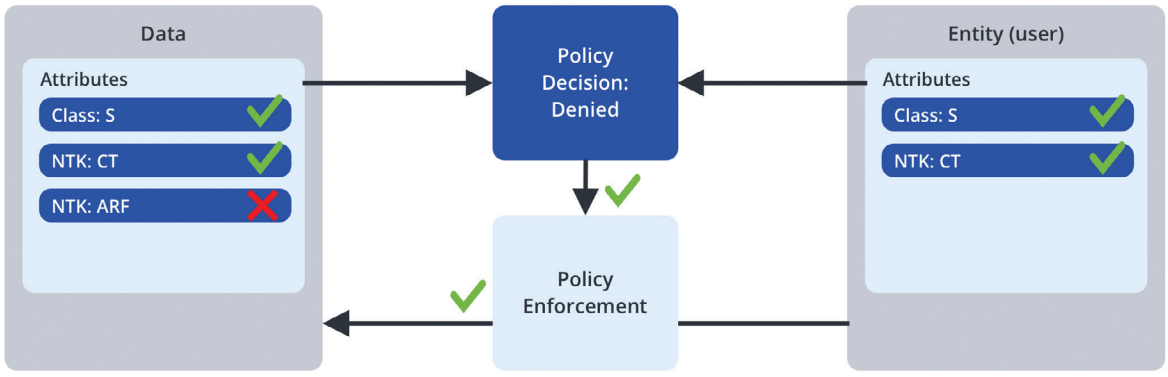
Key Authorization & Access Control

In order to process any encrypted data, the data owner must first grant authorization to the object encryption keys, which are stored in servers separate from the data itself. Data owners can independently control and audit the use of their data by managing the data tags and associated policies used by the key servers, even after the data is mixed with other data, be it in a cloud object storage service or another type of container.

Data owners may choose to use on premise, cloud, or third party hosted key servers. In order for analytics to request keys, the TDP gives each process a strong digital identity that can be used to connect to the data owner's key server. After data is encrypted and co-located, data owners can approve access to their data. This offers data owners the flexibility they need to grant greater or fewer privileges based on their intimate understanding of situational context, which can change rapidly from moment to moment, including who is considered a trusted collaborator and under what circumstances.

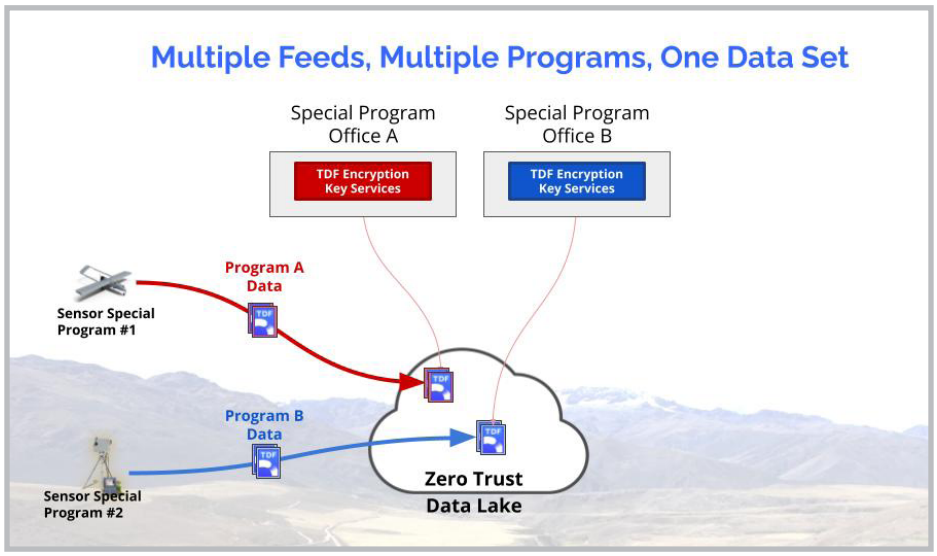
Policy Tagging & Configuration with ABAC

In the Attribute-Based Access Control (ABAC) model, access decisions are made based on policy logic and attributes applied to data and entities (people and NPEs). Before they can gain access to a dataset, data tag owners must assign all applicable data entitlements to their users and analytics. The TDP ensures that access to datasets remains cryptographically enforced by encrypting all data and enforcing access policies on their associated key servers. Binding policies to those tags is a powerful way to ensure persistent, secure, multi-party control of data at scale.

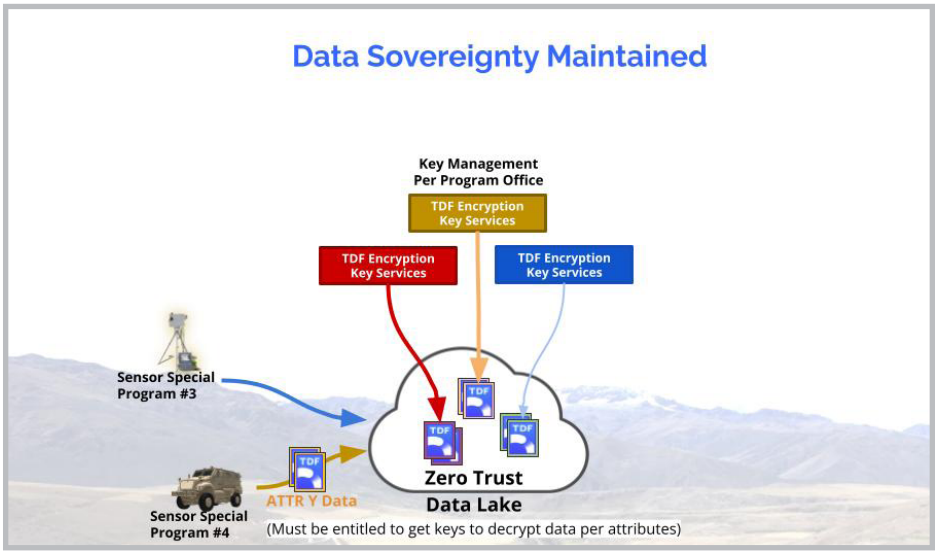


Use Case: COP for Protected Sensor Streaming

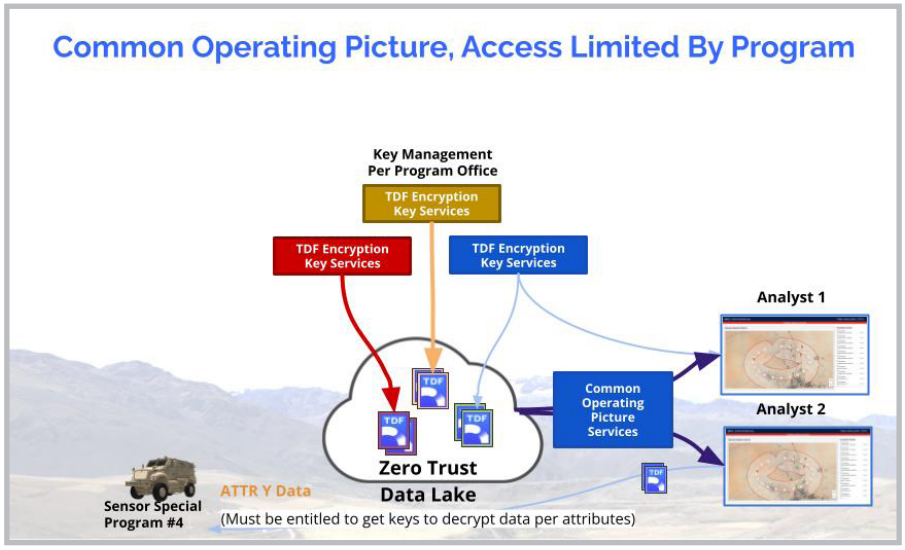
Because each element within an environment is producing TDF-protected data, this data can be stored in a single data environment while still maintaining cooperating organizations' sovereignty over that data. Individual sensors, such as a camera monitoring a location or an operator's body-worn camera, streams its protected data into a single, shared data repository. Individual organizations maintain their own key server for the data which they control.



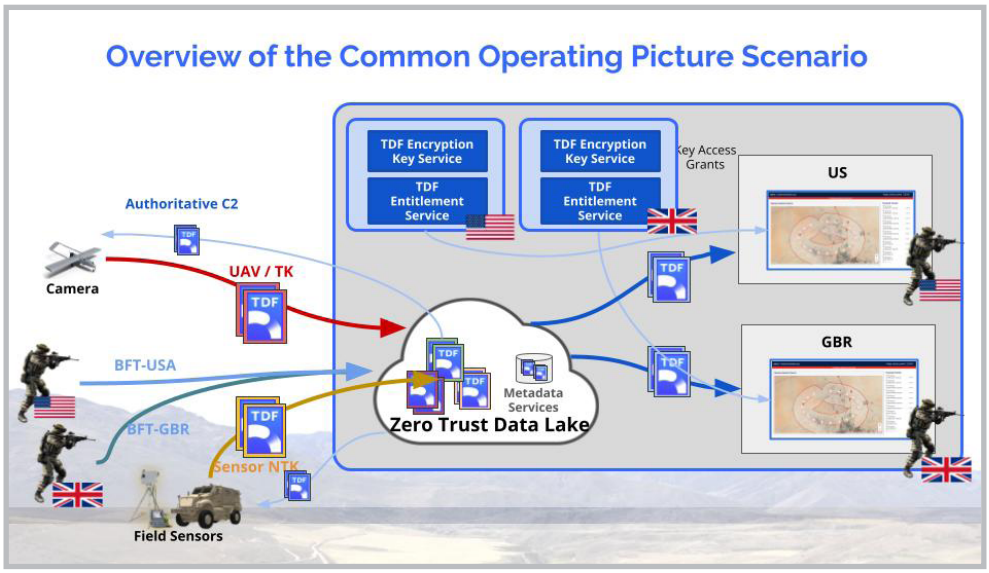
As additional sensors are added to the operating environment, such as camera-equipped drones or other monitoring devices, they continue to stream their encrypted data into the same shared repository. Even the addition of new coalition partners (having their own key servers) are simple to add into the same shared data environment.



Any approved application can access data from the shared repository. In order for a piece of software to be granted access to the data and the TDP, it must be able to prove its identity and confirm it has been securely configured. Analysts or operators using those applications then can only see data *for which they are individually authorized by the owning organization* within those tools. But they can see multiple organizations' data *within the same interface*.



Downstream tools, such as an operational application showing assets on a map or an analytics tool producing visualizations, have access to all of the TDF-protected data. Due to the rigid protections around each granular piece of data, only those objects *to which the end user has been granted access* can be shown within those tools. In this way, the same user interface will look quite different based on who is logged into it. Users from within an organization owning the bulk of the data will obviously be able to see vastly more within that same application as would, for example, a coalition partner only granted access to a small portion of the data.



The resulting system allows disparate organizations to have complete control over who can see what when, including the ability to dynamically turn access to individual pieces of data on and off in real time on a person-by-person basis. All of these actions are robustly audited and cryptographically protected in a zero-trust environment.

Summary

With Virtru's TDF platform running onboard sensors as they collect data, ownership and control can be exerted wherever this data is used. This allows a single pane of glass to view data from multiple sources, with each relevant consumer only able to access data that they rightfully should.

To learn more about Virtru's solutions for Federal mission partners and customers, please contact us at federal@virtru.com.

Trusted by Federal Agencies, State and Local Governements.

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 6,000 customers trust Virtru for data security and privacy protection.

virtru.com