A Trusted Platform for Zero Trust Implementations

Apply Data-Centric Security with Virtru's Trusted Data Format

Organizations handling sensitive data need a data-centric platform based on cryptographic proof instead of trust — a platform that allows any authorized parties to easily collaborate with each other while maintaining control and visibility of all data.

For true Zero Trust security, protect the data itself

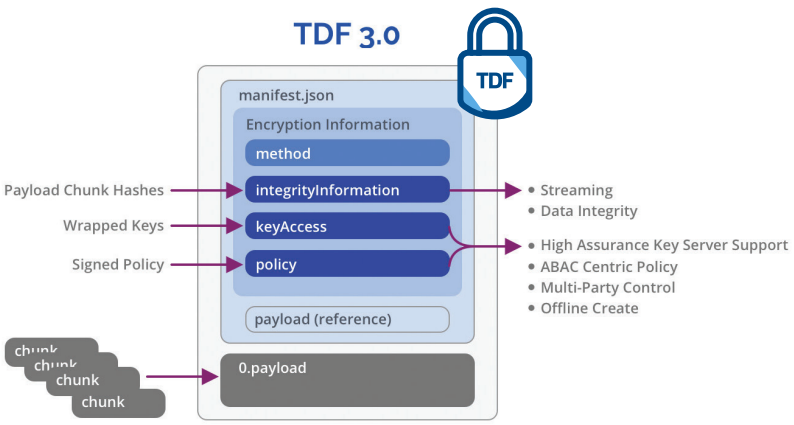
Zero Trust is an entirely new way of thinking. Simply protecting the network isn't enough anymore. On average, **intruders spend over 150 days on a protected network before being discovered**. With Zero Trust, don't just protect the network, *protect everything*. The security perimeter surrounds each piece of data individually, and each endpoint – each server, or system component – separately.

With a Zero Trust approach, access privileges can be customized based on specified parameters — including devices, users, locations, bots or characteristics of the data itself. **Individual data elements become the new perimeters.**

A data-centric approach embraces the broader tenets of Zero Trust, but simplifies it to avoid reliance and trust on any third-party provider or service, while introducing data control wherever it travels.

The Trusted Data Format for Zero Trust

Virtru's Trusted Data Format (TDF) provides a protective wrapper that cryptographically binds protections to the data at the attribute level. TDF leverages Attribute Based Access Control (ABAC) to enable customized and granular data access privileges that fulfill the least privileged access approach of a Zero Trust strategy. TDF allows file locking, content expiration, and access revocation for both structured and unstructured data of any size, regardless of the data's location. Organizations and data owners can tag, encrypt, revoke, expire, and audit access to data, **even after content has been accessed or after it has left the organization's systems**.



Virtru's Trusted Data Platform is built on the TDF, equipping agencies to leverage:

Identity Management: Virtru's Trusted Data Platform integrates with in-place organizational identity management systems, such as PKI, OAuth, Active Directory, and LDAP.

Data Tagging: Apply discrete data tags that are bound to the content and associated with ABAC policies and rules.

Key Authorization and Access Control: Object encryption keys are stored separately from the data in on-premise, cloud, or third-party-hosted key servers. Independently control and audit the use of your data by managing the data tags and associated policies used by the key servers.

Audit Data Integrity: Encryption of audit data ensures that audit records cannot be tampered with. As audit data is created, it is encrypted into TDFs just as production data is encrypted into that same format.

The Cornerstone of Zero Trust

Virtru has been an important enabler for a data-centric vision and transformations to Zero Trust models. Virtru products have a proven history of protecting and sharing sensitive data for numerous areas within the US Federal Government, their coalition partners, combatant commands, as well as thousands of commercial customers. With a wide range of customers that must meet industry requirements for securing their data, our expertise can support your missions.

Trusted by over 7,000 customers to include numerous Agency, Coalition Partners, and Combatant Commands

virtru

To learn more about how Virtru can equip your agency to implement data-centric, Zero Trust security, contact **federal@virtru.com**.