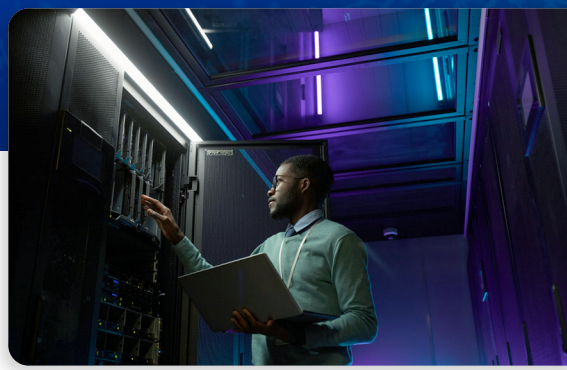
Virtru Private Keystore

Enhance your Data-Centric Security with Key Management



Store the encryption keys for all of your Virtru solutions in a location of your choosing while Virtru still does the heavy lifting of managing policies and key exchanges. Ensure regulatory compliance and data sovereignty wherever your data is created, stored, or shared.

Collaboration And Compliance Conundrum

SaaS, cloud, and hosted collaboration solutions have enabled companies to increase their productivity and data sharing capabilities. But many organizations using these solutions are facing increased regulatory and data sovereignty requirements. The Virtru Private Keystore solves for these requirements by using encryption to enforce access control.

Cryptographic keys are the basis of all encryption. These keys are used to scramble data such as text, images, etc., so that it is not possible to see what the data is or says unless the data is then unscrambled - or said another way - decrypted. In order to unscramble or decrypt the data, the private encryption key is needed.

Since the private key controls access to encrypted data, the data can be seen as *regulated* by that key. The location of the key functionally *becomes* the location with access to the data, regardless of where the data is stored. This distinction is becoming increasingly important as organizations leverage the benefits of online and shared solutions.

To fulfill regulatory and data sovereignty requirements, organizations can encrypt data that is shared within online and collaborative solutions, and store the private keys used to access that data within their own private data center or private cloud. In order to manage the access to the encryption keys, the organization needs to run private keystore management software. The Virtru Private Keystore is designed to do exactly that and further your Zero Trust data-centric security goals. It is an integrated solution that supports all of Virtru's offerings and Google's cloud and collaboration solutions.

The Virtru Private Keystore ensures you maintain exclusive access and secure your data where you need it secured:

- Create additional key pairs to protect underlying encryption keys where the private key never leaves your environment for true "hold your own key" security.
- Host on your premises, in a private cloud, or on any public cloud service.
- Have visibility over all encryption key exchanges and policies.
- Integrate with your SIEM to strengthen threat response and compliance.
- Prevent any third-party (including Virtru and other cloud, email, and security vendors) from accessing your data.

Encryption Keys and Regulatory Compliance

Compliance Support

Help meet data sovereignty, residency, and data protection requirements including CJIS, GDPR, HIPAA, PCI, CCPA, ITAR, and more.

Surveillance Prevention

Strengthen privacy by ensuring any request to access data (including a government subpoena) has to come to your organization.

Supported Virtru Solutions

- Virtru Data Control for Gmail, Outlook, and Google Drive
- Virtru Data Protection Gateway
- Virtru Secure Share

Google Cloud Private Key Solutions

Both Google Workspace and Google Cloud Platform offer very high levels of data security. But in order to work, Google's systems need to access and process your data. For many organizations, this can raise concerns over data privacy, regulatory compliance, and data sovereignty. So, how can your organization benefit from Google's cloud and collaboration solutions while still maintaining control over access to your data?

Google offers technologies that allow you to host the private encryption keys to your data within your own data center or private cloud. Respectively, these technologies are called Client Side Encryption (CSE) for Google Workspace, and External Key Manager (EKM) for Google Cloud Platform. In order to manage access to the private encryption keys, your organization will need to run private keystore management software. The Virtru Private Keystore supports both of these Google Workspace and Google Cloud Platform (GCP) technologies. Store your private encryption keys in any secure location that satisfies your requirements.

- Virtru Private Keystore for Google Workspace Client Side Encryption (CSE)
- Virtru Private Keystore for Google Cloud Platform External Key Manager (EKM)

Flexible Encryption Key Hosting Options

Choose from several hosting options to align with your key management processes and security requirements.

Customer-Hosted Keys
You host asymmetric encryption keys on-premises that protect every Virtru client key or Google cloud request, for a crucial layer of protection.

HSM Integration
Virtru Private Keystore brokers encryption and decryption requests by securely accessing your HSM-managed private keys leveraging the PKCS #11 and KMIP protocols.

HSM Proxy Connector
If you have an HSM proxy or caching service, the Virtru Private Keystore Proxy Connector can integrate with it, brokering encryption and decryption requests. Proxies can reduce load requests on your Hardware Security Module as well as protect from users or systems making inadvertent or unintentionally brokering illicit requests directly to your HSM.

More than 7,000 organizations trust Virtru for data security and privacy protection.

verizon Maryland Better omada BROWN

How We Do It

Virtru Private Keystore is part of Virtru's Trusted Data Platform, a holistic suite of data protection products and solutions.

Virtru strives to protect your data everywhere it flows through your organization: through email, enterprise applications, file sharing solutions, and collaboration tools.

virtru **To learn more about Virtru Private Keystore and how Virtru can assist you, visit: www.virtru.com**

MKT-5414 2/23