Meet Data Sovereignty and Maintain True Privacy for Data Stored in the Cloud

Data Sovereignty in the Cloud

As the popularity of cloud computing and SaaS solutions continues to rise, data sovereignty has become a greater focus for organizations. Data sovereignty is a country-specific requirement that data is subject to the laws of the country in which it is collected or processed and must remain within its borders. Therefore, organizations must pay close attention to how they are managing their data in different locations.

Because of the distributed nature of the cloud, organizations have concerns about the ability to meet data sovereignty and GDPR requirements and the reliability of true data privacy and protection against unauthorized access. But, the push for digital workflows is driving the need to find solutions to these obstacles. End-to-end encryption is the preferred method for securely sharing and storing data in the cloud and the method to manage encryption keys is critical to maintain control of data to meet corporate privacy and data sovereignty requirements.

Virtru Helps You Move to the Cloud With Confidence

End-to-End Encryption

Protect data the moment it's created and ensure only an authorized recipient can decrypt it. You're never forced to trust Virtru or any cloud service provider with access to your data.

Customer-Hosted Encryption Key Management

Store encryption keys in their required geographic region to resolve data sovereignty concerns and have the freedom to use the multinational cloud vendor of your choice.

On-Demand Access Control

Add or adjust access controls like the ability to revoke access, disable forwarding, and add an expiration date to manage where your data is going and who it's shared with.

Flexible, Layered Encryption Key Management Options

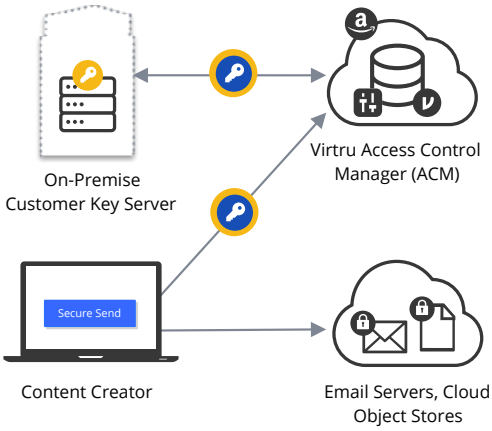
Choose where encryption keys are stored and accessed in order to prevent the decryption of sensitive data outside of specified regions.

Fully-Hosted Keys for Secure Scalability

Virtru generates a unique encryption key for each email or file, which is then protected by Amazon KMS. Encrypted data is hosted within the cloud provider's email servers but stored separately from the key that can decrypt it to fulfill a split knowledge architecture. The Virtru Access Control Manager (ACM) enforces the policies you set to control access to encrypted data.

Customer-Hosted Keys for Added Control

Add asymmetric encryption that you host on-premises for an added layer of protection. Create an additional key pair to protect your underlying encryption keys that never leaves your environment for true "hold your own key" security. Virtru only manages policies and brokers key exchanges.



Virtru Customer Key Server (CKS)

HSM Integration for the Highest Level of Security

The Virtru Customer Key Server (CKS) brokers encryption and decryption requests on the Virtru platform and can be integrated with your HSM to manage private keys. This method leverages PKCS (Public Key Cryptographic Standard) #11 and KMIP protocols, allowing integration with a variety of HSM manufacturers.

Your Data is Your Own and Virtru Helps Keep it That Way

Virtru supports your essential need to share and store data in the cloud. We are a cloud-enabler because we offer end-to-end encryption that protects data from third party or unauthorized access, while keeping it easy to send an email or share a file. Virtru secures any data you deem important and empowers you to have full control with access controls like message revocation and the ability to host your own encryption keys to meet data sovereignty.

Enabling Privacy and Security with High Data Protection Standards

Virtru is certified by The French National Cybersecurity Agency (ANSSI) with the CSPN First Level Security Certification for cyber security to resist cyber attacks and support the growing global mandate for high data security standards.

Learn how Virtru can help your organization meet data sovereignty requirements for compliance with GDPR and other data privacy regulations. **virtru.com/contact-us**