Solution Brief

THALES

CYBERSECURITY

virtru

Hardware-Backed Encryption and Data Protection for the Enterprise: Virtru Data Security Platform + Thales Luna HSMs

cpl.thalesgroup.com

THALES

CYBERSECURITY

virtru

The Challenge

Enterprises operate across borders, clouds, and regulatory jurisdictions while managing unprecedented volumes of sensitive data. From financial records and healthcare information to intellectual property and customer data, organizations must protect information assets while navigating GDPR, HIPAA, PCI-DSS, and industry-specific mandates.

Software-based encryption provides a foundation, but encrypted data is only as secure as the cryptographic keys protecting it. When master encryption keys reside in software memory or on general-purpose servers, they remain vulnerable to sophisticated attacks, insider threats, and compliance audit findings. For organizations in regulated industries, hardware-backed key protection is no longer optional. The challenge: achieving that protection while maintaining operational agility across hybrid and multi-cloud environments.

The Solution

Virtru Data Security Platform embeds protection directly into data, ensuring access controls, encryption, and governance policies travel with sensitive information wherever it's stored or shared. Unlike perimeter-based approaches, Virtru's data-centric security maintains protection across email, file sharing, cloud storage, analytics pipelines, and partner collaboration, even when data leaves the organization's network.

With Thales Luna HSMs, Virtru delivers this enterprise-grade data protection with hardware-backed key security. The integration ensures cryptographic keys are generated and protected within tamper-resistant hardware, eliminating software key exposure while enabling secure collaboration across cloud environments, on-premises systems, and partner ecosystems.

Deployment Modes

The integration supports two modes, enabling organizations to balance operational requirements with security assurance:

Envelope Mode: A root symmetric key stored in the Luna HSM wraps the Key Access Service private keys before they are stored in the platform database. AES-based symmetric key wrapping provides hardware-backed protection while maintaining operational flexibility.

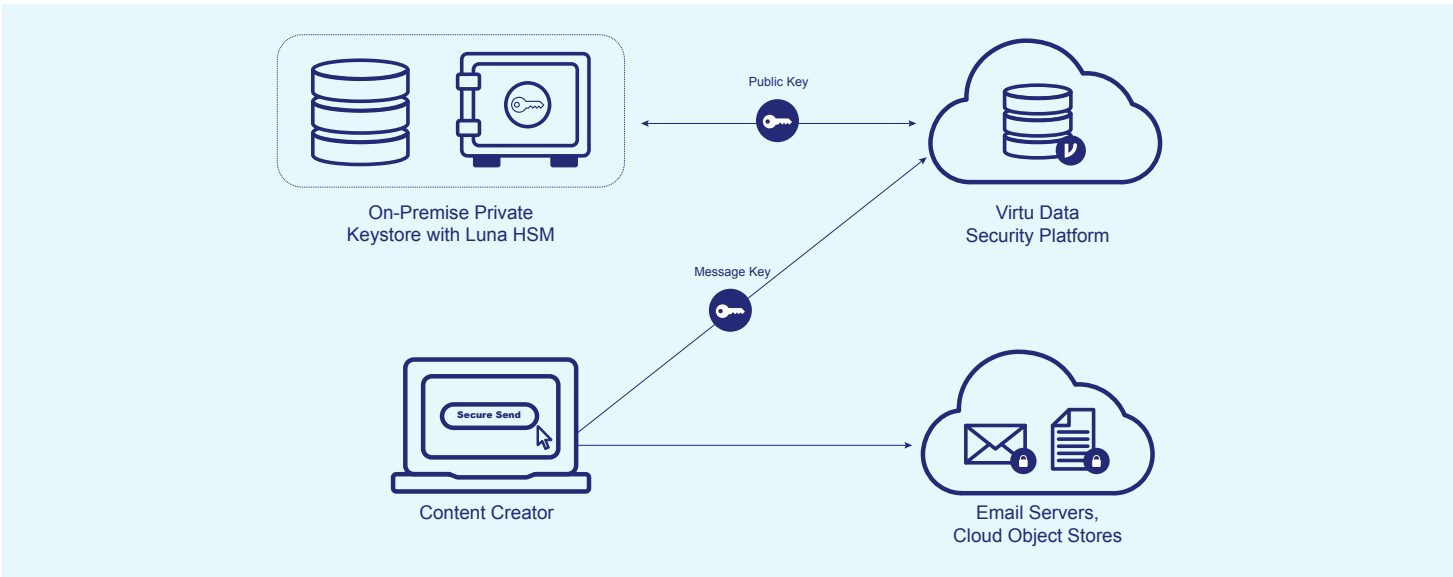
Delegated Mode: Key Access Service private keys never leave the Luna HSM. All cryptographic operations—including RSA key generation (2048/3072/4096 bit), data encryption key wrapping, and unwrapping—occur directly within the HSM. No key material is exposed outside the secure boundary.

Persistent Attribute-based Data Security

Attribute-based access control policies travel with encrypted data, enabling organizations to enforce governance across cloud providers, geographic boundaries, and partner networks. The platform supports comprehensive audit logging and stores cryptographic key material in FIPS 140-3 Level 3 validated Luna HSMs to ensure that customers remain in control of their data wherever it resides.

Enterprise Scalability & High Availability

Multiple Luna HSMs can be deployed in load-balanced, high-availability configurations to ensure continuous cryptographic service availability for mission-critical operations. Organizations can deploy across AWS, Microsoft Azure, Google Cloud, or on-premises environments—maintaining consistent hardware-backed key protection regardless of where data and workloads reside.



Key Benefits

Hardware-Based Secure Key Storage

Master encryption keys are generated, stored, and utilized exclusively within tamper-resistant Luna HSMs, eliminating software-based key exposure risks.

Global Regulatory Compliance

Meet GDPR, HIPAA, PCI-DSS, SOC 2, and industry-specific regulatory requirements with hardware-backed key protection and comprehensive audit capabilities.

Hardware-Accelerated Cryptographic Operations

All cryptographic operations leverage dedicated HSM capabilities, supporting RSA cryptography within the secure hardware boundary for maximum performance and security.

Flexible Key Protection Modes

Support for both envelope mode (HSM-wrapped keys in database) and delegated mode (keys never leave HSM) enables organizations to balance operational requirements with maximum security assurance.

Multi-Cloud and Hybrid Support

Consistent hardware-based key protection across AWS, Microsoft Azure, Google Cloud Platform, and on-premises environments without CSP vendor lock-in.

Enterprise Scalability

Support for high-volume cryptographic operations with multiple HSMs in load-balanced configurations to meet demanding enterprise workloads.

Robust High Availability

Multiple Luna HSMs can be deployed in high-availability configurations to ensure continuous cryptographic service availability for mission-critical operations.

Industry-Proven Technology

Thales Luna HSMs have been the HSM market leader for over 30 years, protecting data, identities, applications and transactions for the world's largest financial institutions, healthcare organizations, telecommunications providers, and government agencies.

Flexible Deployment Models

Thales Luna HSMs can be deployed on-premises, in the cloud, as a service (available on Thales Data Protection on Demand), or across multiple environments to create a purpose-built hybrid HSM solution to match organizational infrastructure and security requirements.

Advanced Key Management & Access Controls

Comprehensive key management including generation, rotation, backup, and recovery with role-based access controls and separation of duties.

Zero Trust Data Protection

Attribute-based access control policies embedded in encrypted data, ensuring protection follows information throughout its lifecycle regardless of location.

About Virtru

Virtru is pioneering the shift from network-centric to data-centric security — embedding protection directly into data so mission owners maintain control wherever sensitive information is shared. The Virtru Data Security Platform is built on OpenTDF, an open standard evolved from technology developed at the NSA by co-founder Will Ackerly, and supports ACP 240, the Five Eyes-ratified Zero Trust standard for secure coalition operations. Trusted by over 6,000 public and private sector organizations — including the U.S. Department of Defense, JPMorgan Chase, and Salesforce — Virtru enables secure collaboration across classification boundaries at mission speed, with integrations across leading defense, cloud, and cross-domain solution providers. Virtru is headquartered in Washington, D.C. For more information, visit virtru.com.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.