

Secure Enterprise Storage with Centralized Encryption Key Management

Strengthen data protection, support compliance, and maintain independent control of encryption keys with Thales and Synology

Key Benefits

- Centralize encryption key lifecycle management across storage environments
- Maintain independent control of encryption keys by separating them from stored data
- Reduce risks from insider threats, unauthorized access, and key compromise
- Simplify compliance with centralized policies, auditability, and reporting
- Support Zero Trust architectures with independent access controls and security boundaries
- Improve governance and visibility across encryption key operations

Securing Data While Meeting Evolving Compliance Requirements

Organizations face mounting pressure to protect sensitive data while complying with increasingly complex regulatory and security requirements. Frameworks such as GDPR, HIPAA, and PCI DSS require organizations to demonstrate strong controls over the encryption, access, and management of sensitive data across hybrid IT environments.

While encryption is a foundational security control, managing encryption keys across enterprise environments remains a significant challenge. Without centralized oversight, key lifecycle operations such as generation, rotation, distribution, and revocation often become fragmented across multiple systems and administrators. This can lead to inconsistent security practices, increased operational complexity, and a higher risk of unauthorized access or audit failures.

The challenge is compounded when encryption keys are stored alongside the systems they protect. Insider threats, compromised administrators, misconfigurations, or physical attacks can weaken encryption protections and expose sensitive information. As infrastructure becomes more distributed, organizations need a centralized, independent approach to managing cryptographic assets.

Centralized Key Management with Thales and Synology

Thales [CipherTrust Data Security Platform \(CDSP\)](#), integrated with [Synology storage platforms](#), provides a centralized approach to protecting sensitive data through enterprise encryption key management and cryptographic control. At the core of the solution,

[CipherTrust Manager](#) delivers centralized key lifecycle management through standards-based KMIP integration, enabling organizations to generate, distribute, rotate, revoke, and audit encryption keys from a single platform while maintaining strict separation between data and cryptographic assets.

By managing encryption keys independently from the storage infrastructure, organizations maintain greater control over their cryptographic assets while applying consistent security policies across multiple storage platforms. This centralized approach simplifies key management, reduces administrative complexity, and eliminates the risk associated with isolated, device-based key management.

Separating encryption keys from the storage infrastructure establishes a clear separation of duties and supports regulatory requirements for independent control of cryptographic assets. Even if a storage environment is compromised, encryption keys remain protected under centralized control.

The joint solution also aligns with Zero Trust security principles by establishing independent security boundaries between data, infrastructure, and cryptographic controls. Centralized policy enforcement and role-based access controls help reduce the attack surface while ensuring that only authorized users and systems can access protected resources.

By consolidating encryption key management into a single platform, organizations can improve governance, simplify compliance reporting, and reduce the operational burden of managing multiple siloed key management systems.

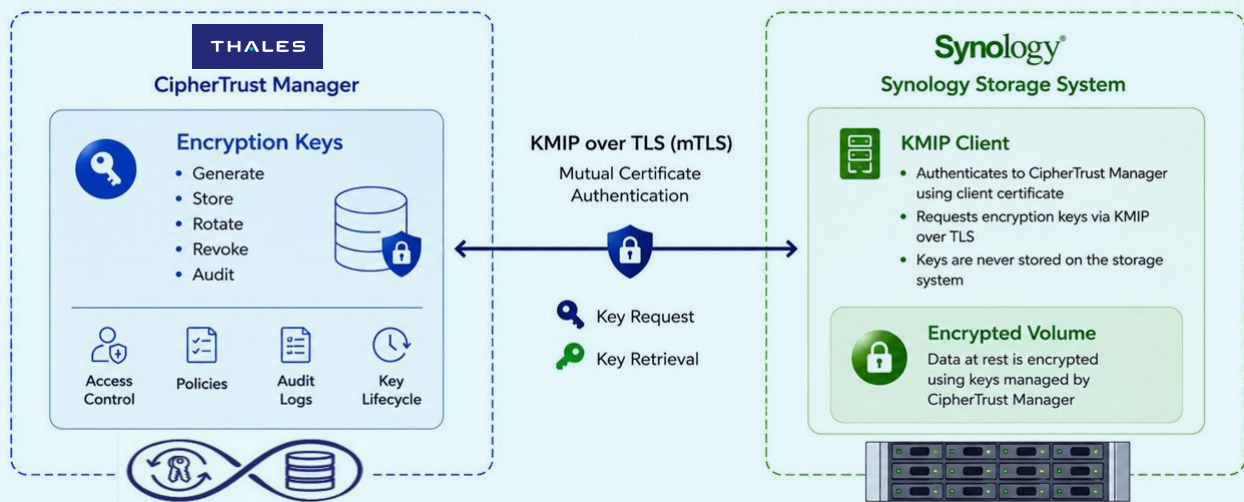
Why Thales and Synology Together

Together, Thales and Synology provide an end-to-end approach to protecting enterprise data by combining secure enterprise storage with centralized encryption key management, helping organizations strengthen cyber resilience, simplify compliance, and maintain independent control of cryptographic assets.

Thales and Synology deliver complementary capabilities that provide security storage with centralized encryption key management.

Thales CipherTrust Manager

- Centralizes encryption key lifecycle management across hybrid and on-premises environments
- Supports KMIP-based integration with enterprise storage platforms
- Enables centralized policy enforcement, auditing, and reporting
- Supports separation of duties and Zero Trust security architectures
- Supports audit readiness and compliance initiatives through centralized policy enforcement and reporting



Synology Storage Platforms

- Provide scalable enterprise storage for file, block virtualization, and mission-critical workloads
- Protect data with built-in volume encryption and self-encrypting drive (SED) support
- Integrate with external KMIP servers for centralized encryption key management
- Strengthen enterprise security and support regulatory compliance

Additional Thales Data Security Capabilities

Organizations can further strengthen their data security strategy with additional capabilities from CDSP and the broader Thales data security portfolio:

- [Luna Hardware Security Modules \(HSMs\)](#): Establish a hardware root of trust for protecting encryption keys and cryptographic operations with FIPS-certified hardware security modules.
- [Data Security Fabric \(DSF\)](#): Centralize visibility, policy enforcement, and security operations across hybrid cloud, on-premises, SaaS, and AI environments to improve governance and reduce risk.
- [Data Security Posture Management \(DSPM\)](#): Discover, classify, and assess sensitive data across cloud and hybrid environments to identify security risks, reduce data exposure, and support compliance initiatives.

Centralized Data Security for Enterprise Storage

As organizations expand enterprise storage environments and face evolving regulatory and cybersecurity requirements, maintaining independent control of encryption keys has become essential for protecting sensitive data and reducing risk. By combining Synology storage platforms with the Thales CipherTrust Data Security Platform

(CDSP), powered by CipherTrust Manager for centralized encryption key management, organizations can strengthen security, simplify compliance, improve governance, and maintain centralized control of cryptographic assets across hybrid environments.

About Synology

Synology creates network-attached storage, IP surveillance solutions, and network equipment that transform the way users manage data, conduct surveillance, and manage networks in the cloud era. By taking full advantage of the latest technologies, Synology helps users centralize data storage and backup, share files on-the-go, implement professional surveillance solutions, and manage networks in reliable and affordable ways. Synology is committed to delivering products with forward-thinking features and best-in-class customer services.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. 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.