Cisco And Thales Facilitate Organizational Digital Transformation

The Problem: Federal agencies need systems that can quickly adapt to changing operational needs without compromising national security

As agencies strive to adapt to fast-changing operational and security requirements driven by the market's digital transformation, they find themselves migrating business applications to more flexible systems. Combining computing, storage, and networking resources into a hyperconverged infrastructure (HCI) that can deliver agility and economies of scale has become the solution of choice. However, the combination and sharing of computing and networking resources can often create vulnerabilities that lead to data security concerns.

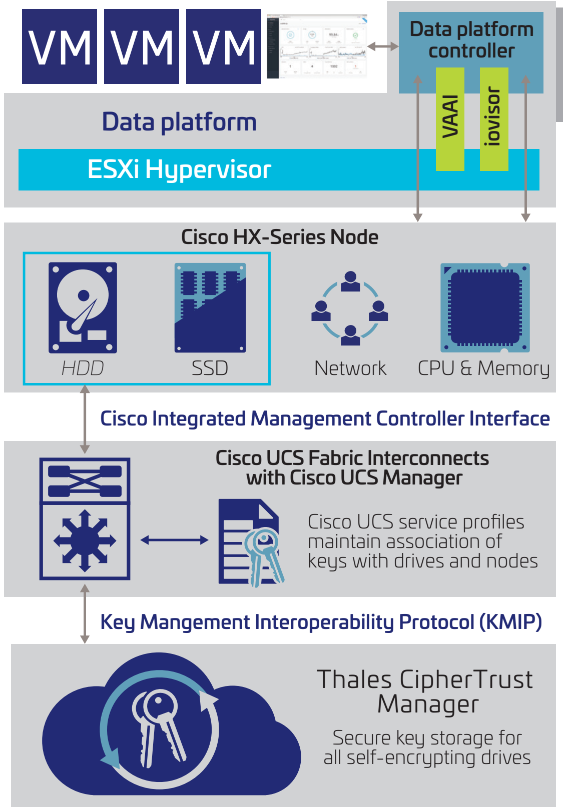
The Challenge: Enabling hyperconvergence and protecting sensitive data without impacting operational performance

Hyperconverged infrastructures can easily adapt to changing operational requirements and quickly scale to meet growing demand. As enterprise applications are migrated to these configurations, keeping sensitive data secured is critically important. Managing data protection at the hardware and software layer is mandated. Achieving data protection requirements/mandates, guidelines, and security management has never been so easy. Encryption keys are automatically managed, rotated, and reported on with only limited resources and effort. Security and high performance infrastructure are provided without negatively impacting performance nor complexity.

The Solution: Cisco Hyperflex and Thales CipherTrust Manager

The Cisco HyperFlex system delivers hyperconvergence, combining computing, storage, and networking resources into a simplified platform. Engineered on the Cisco Unified Computing System™ (Cisco UCS®), the platform provides the agility, scalability, and pay-as-you-grow economics of the cloud, with the benefits of an on-premises infrastructure. HyperFlex combines software-defined computing and software-defined networking to deliver a pre-integrated cluster that scales resources independently to closely match your application needs.

Applying a consistent policy ensures encryption and key management are deployed uniformly across every node in a cluster, Cisco HyperFlex relies on Thales CipherTrust Manager to provide robust FIPS 140-2 Level 3 and common criteria certified key management. The combined solution establishes a certificate-based chain of trust between the HyperFlex platform and the key management server in order to transfer keys to unlock self-encrypting drives (SED).



VM
VM
VM
Data platform controller
VAAI
iovisor
Data platform
ESXi Hypervisor
Cisco HX-Series Node
HDD
SSD
Network
CPU & Memory
Cisco Integrated Management Controller Interface
Cisco UCS Fabric Interconnects with Cisco UCS Manager
Cisco UCS service profiles maintain association of keys with drives and nodes
Key Mangement Interoperability Protocol (KMIP)
Thales CipherTrust Manager
Secure key storage for all self-encrypting drives

Thales enterprise key management integrated with Cisco Hyperflex

Why use CipherTrust Manager with Cisco Hyperflex?

CipherTrust Manager strengthens and simplifies security by streamlining the management of associated encryption keys. CipherTrust Manager uses certificates to authenticate Cisco UCS SEDs for system level security. The SEDs generate new encryption keys, which are then uploaded to the DSM. In the event of a power cycle or host reboot, the Cisco UCS software retrieves the keys from CipherTrust Manager and uses them to unlock the drives.

Security keys can be instantly reprogrammed to meet site-specific security policies. Security mechanisms enable compliance with data-at-rest encryption requirements set forth in HIPAA, PCI DSS and SOX standards among others. The security platform:

- Provides a single, centralized management plan for cryptographic keys and applications across the full key lifecycle
- Offers high availability and standards-based enterprise encryption key management using KMIP
- Centralizes third-party encryption keys and securely stores certificates
- Enables vaulting and an inventory of certificates
- Implements a two-factor authentication mechanism to further safeguard keys and certificates against theft

Federal Guidelines and Mandates

- NIST 800-53 security controls
- FIPS 140-2 L3 and Common Criteria certified
- HIPAA, PCI, FISMA
- Continuous Diagnostics and Mitigation (CDM) and FedRamp
- Multitenancy for delegation of duty and enclave independence

Cisco

Cisco is the worldwide technology leader that has been making the Internet work since 1984. Cisco's people, products and partners help society securely connect and seize tomorrow's digital opportunity today.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.