THALES

www.thalesesecurity.com

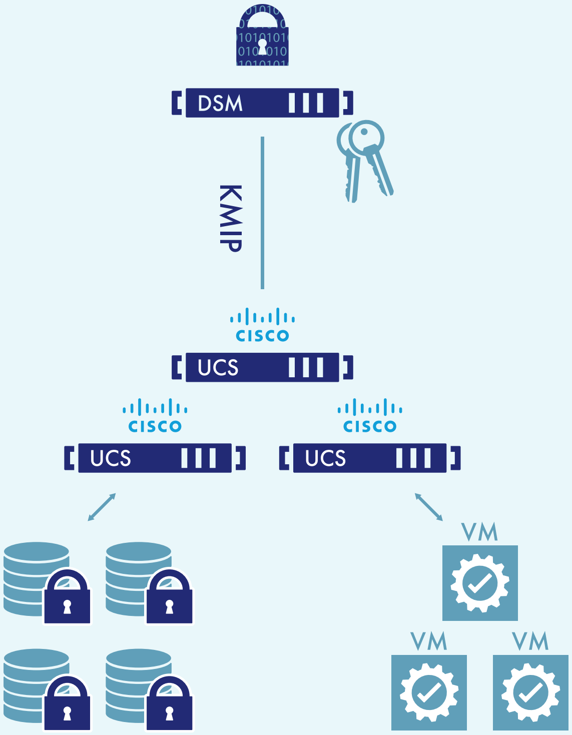
SUPERIOR NETWORK CONNECTIVITY AND MANAGEMENT WITH HIGH ASSURANCE ENCRYPTION FOR SECURITY COMPLIANCE

- Increases LAN and SAN efficiency, scalability, and security
- Supports low-latency, lossless 10 and 40 Gigabit Ethernet
- Affords a single, highly available management domain
- Leverages standards based APIs for encryption key management and key vaulting
- Provides a FIPS 140-2 Level 3 key management root of trust

CISCO

‹Thales e-Security›

CISCO AND THALES DELIVER SECURE DATA ACCESS AND ROBUST CRYPTOGRAPHIC KEY MANAGEMENT



Vormetric DSM protects and manages the cryptographic keys used by Cisco UCS within a FIPS 140-2 Level 3 appliance.

THE PROBLEM: LOSS OF ENTERPRISE DATA CAN SEVERELY AFFECT BUSINESSES' BOTTOM LINE

Data security now dominates boardroom discussions. As more organizations have increasing volumes of data at their disposal through distributed networks and storage services, data has become the life-blood of the enterprise. With data and processing power available on-demand, businesses can derive competitive knowledge quickly and cost-effectively. Encrypting data at rest is the new norm and a fundamental part of the IT infrastructure. Loss or compromise can result in severe fines, costly remediation efforts, and damage reputations.

THE CHALLENGE: IMPLEMENTING DATA SECURITY AND AT-REST ENCRYPTION WITHOUT INTRODUCING MANAGEMENT OVERHEADS AND IMPACTING OPERATIONAL FLEXIBILITY

Merging networking and storage with physical and virtual computing reduces cost and increases agility. However, ensuring that data security controls do not introduce management overheads over cryptographic key rotation and backups that impact operational flexibility, requires careful design. Encryption tops the list of technologies used by enterprises to secure data centers.* With this focus on data protection, effective solutions must balance networking, storage, and computing resources, and not rob processing power to perform cryptographic operations that consume bandwidth and introduce latencies.

*Information Security Media Group – 2016 Cisco Data Center Security Study

CISCO AND THALES DELIVER SECURE DATA ACCESS AND ROBUST CRYPTOGRAPHIC KEY MANAGEMENT

THE SOLUTION: CISCO UNIFIED COMPUTING SERVERS (UCS) AND VORMETRIC KEY MANAGEMENT PLATFORM FROM THALES E-SECURITY

Cisco UCS provides the management and communication backbone for high speed Ethernet, Fibre Channel, and Fibre Channel over Ethernet enterprise networks. Using a highly scalable architecture designed to meet variety of application demands with low-latency, Cisco UCS supports line rates up to 40 Gigabit. Offering transparent data encryption and management integration capabilities, the solution leverages OASIS PKCS #11 and KMIP APIs for encryption key management and key vaulting. Cisco UCS integrated infrastructure provides strong data protection by encrypting user and application data.

Delivering data at rest encryption through self-encrypting drives (SED), Cisco UCS relies on Vormetric Data Security Manager (DSM) from Thales to provide robust FIPS 140-2 Level 3 certified key management and role separation. The combined solution delivers non-disruptive encryption to ensure confidentiality of sensitive data, and to protect and manage underpinning cryptographic keys. The integration provides a cost-effective and comprehensive solution that meets the most stringent security requirements. Leveraging hardware-based data at rest encryption ensures no adverse impact to system performance.

Typical use cases involve financial services and healthcare applications that process confidential customer data and personally identifiable information. Not only are these organizations often the target of malicious attacks, but they are also increasingly subject to government and industry oversight and regulations. Use of Cisco UCS with Vormetric DSM delivers easy to implement secure data access and facilitates regulatory compliance.

WHY USE VORMETRIC DATA SECURITY PLATFORM?

The Vormetric DSM strengthens and simplifies security by streamlining the management of associated encryption keys. Vormetric DSM 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 the Vormetric DSM 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 plane for cryptographic keys and applications
- 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

The consolidation of enterprise encryption key management delivers consistent policy implementation between systems and reduces training and maintenance costs.

THALES

Thales e-Security is the leader in advanced data security solutions and services delivering trust wherever information is created, shared, or stored. Security solutions ensure that critical data is both protected and trusted in any deployment – on-premises, in the cloud, in data centers, or in big data environments – without sacrificing business agility. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales e-Security is part of Thales Group.

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.

For more detailed technical specifications, please visit **www.thalesesecurity.com** or **www.cisco.com**

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thalesesecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thalesesecurity.com