cpl.thalesgroup.com

THALES

Thales CipherTrust Data Security Platform

Encryption & Key Management for VMware Cloud on AWS

VMware Cloud on AWS brings together VMware's enterprise-class Software-Defined Data Center (SDDC) software and elastic, bare-metal infrastructure from Amazon Web Services (AWS) to give organizations a consistent operating model and application mobility for private and public cloud. Thales CipherTrust Data Security Platform solutions enable VMware Cloud on AWS customers to deploy client-side encryption, centralized key management and tokenization to simplify security operations such as data visibility, compliance auditing and policy execution and enforcement.

The Challenge

Organizations want to move more of their sensitive data to cloud platforms because of the efficiency, flexibility and scalability that it promises. Yet, security and control continue to be a significant obstacle to this adoption. How can organizations feel comfortable that their data is safe when it is off-premises? Moreover, how can they demonstrate data control to their auditors when that data is no longer in their data center? Despite all of the advances made in virtualization technology, the fundamental challenges organizations face still remain, that is; security and compliance.

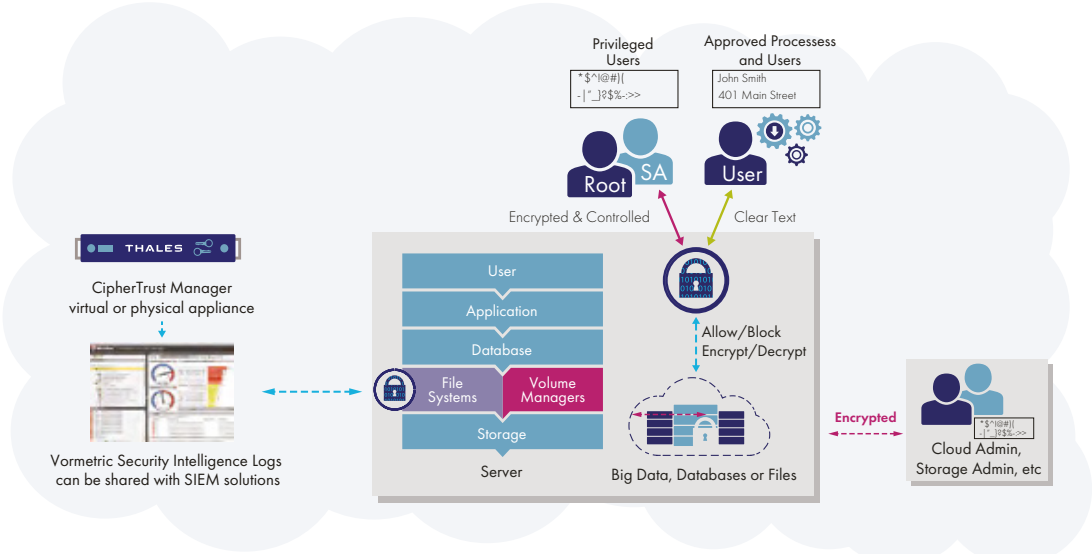
The Solution: Thales plus VMware Cloud on AWS: Facilitating Cloud Adoption Through Key and Data Control

Thales and VMware have teamed up so organizations can enjoy the benefits hosting data in the cloud has to offer. Organizations that run VMware Cloud on AWS can use the CipherTrust Data Security Platform solutions to keep data safe as it lives in the cloud.

Key Benefits

Heterogeneous Key Management: Manage keys for a variety of encryption and tokenization products including the CipherTrust Data Security Platform, self-encrypting drives, tape archives, Storage Area Networks, and a growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.

Full Lifecycle Key Support and Automated Operations: Simplify management across the entire key lifecycle including secure key generation, storage and backup, distribution, deactivation and deletion. Automated, policy driven operations simplify key expiry and rotation tasks.



Centralized Administration of Granular Access, Authorization Controls and Separation of Duties: Unify key management operations across encryption deployments in a central management console and restrict administrators according to the scope of their responsibilities. Use existing LDAP or AD directories to map administrative and key access for application and end users.

Auditing and Logging: Log and track all key state changes, administrator access and policy changes in detail. Securely store and sign audit trails for non-repudiation and make them available to leading 3rd party SIEM tools.

CipherTrust Manager Overview

CipherTrust Manager is a high-availability appliance that centralizes encryption key management for CipherTrust Data Security Platform products and third-party encryption solutions. The appliance manages key lifecycle tasks including generation, rotation, destruction, import and export.

The CipherTrust Manager additionally enhances key management by providing convenient back-up services and delivering strong separation of duties for increased security. The CipherTrust Manager can be separated into logical entities, or domains, dedicated to unique key management environments, providing additional security and ultimate separation of duties, where no single administrator has access to all domains.

The CipherTrust Manager is available as either a hardware or a virtual appliance. The k470 hardware appliance is certified to FIPS 140-2 Level 2 and the k570 hardware appliance, equipped with a hardware security module (HSM), is certified to FIPS 140-2 Level 3. The virtual appliance is certified to FIPS 140-2 Level 1.

Key Benefits

Centralization

Single, centralized platform for managing cryptographic content (keys and related data) and applications.

Simplify Compliance

Efficiently audit key management practices, save staff time, and simplify attainment of compliance mandates. Supports centralized auditing of key management practices such as FIPS 140-2, PCIDSS, HIPAA, and GDPR.

Lower Administration Costs

Lower the cost of key management and encryption with centralized administration and automated operations.

Boost Cloud Security

Customers can store and manage keys in central, hardened appliances, and gain the visibility and control they need to consistently and effectively enforce security controls.

Use Case Expansion

Transform your key management appliance into a server that includes support for the market's broadest portfolio of encryption and tokenization solutions. Secure data at any level in the cloud from its creation to rest.

CipherTrust Data Security Platform

Thales CipherTrust platform unifies data discovery, classification and data protection, as well as provides unprecedented granular access controls and centralized key management– all on a single platform. This simplifies data security operations, accelerates time to compliance, and secures cloud migrations, and reduces risk across your business. You can rely on Thales to help you discover, protect and control your organization's sensitive data, wherever it resides.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us