nCipher
AN ENTRUST DATACARD COMPANY

www.ncipher.com

Address the cryptographic key management needs of enterprise multi-cloud deployments with a robust HSM root of trust

- Ensure strong data security across distributed computing environments
- Manage key lifecycles centrally while supporting multi-cloud settings
- Scale to provision keys for tens of thousands of encrypted workloads
- Address the regulated market needs for reduced risks and compliance
- Support the industry API standard Key Management Interoperability Protocol (KMIP)
- Provide a FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust

HYTRUST

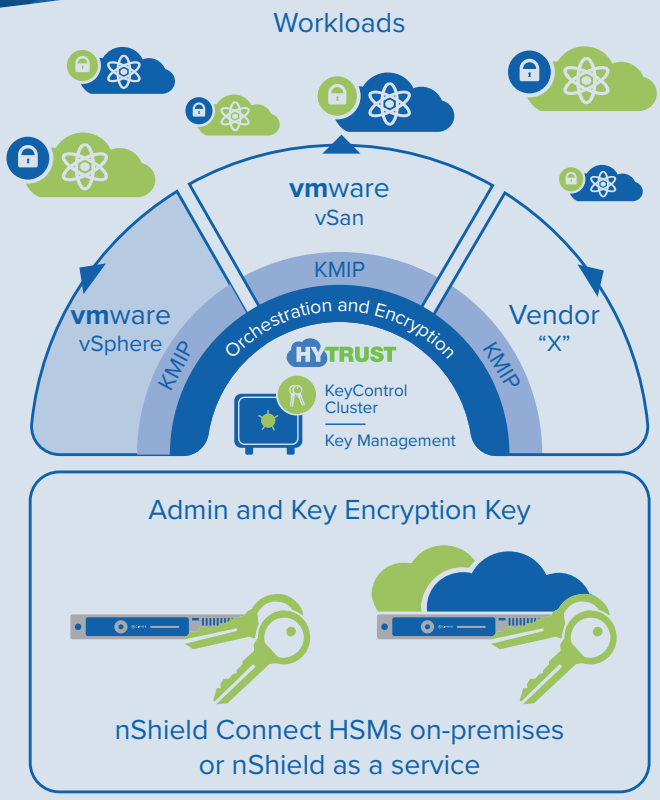
HyTrust and nCipher deliver universal key management for encrypted workloads

THE PROBLEM: MANAGING HIGH VOLUME KEY ENCRYPTION KEYS ACROSS MULTI-CLOUD WORKLOADS

As more enterprises today use multi-cloud computing environments to conduct business, managing encrypted workloads become increasingly difficult. Handling the encryption from each cloud management platform is complex and increases the risk of inconsistent policies. Migrating workloads and data between clouds requires them to be decrypted first, then migrated in clear-text, and subsequently re-encrypted, which creates a security gap.

THE CHALLENGE: SECURELY MANAGING KEY LIFECYCLES CENTRALLY WHILE SUPPORTING MULTI-CLOUD SETTINGS

Centralizing key management across multi-cloud deployments enables consistent security policy enforcement and reduced risks. However, aggregating keys in one central location requires additional security. Establishing a root of trust that protects the centralized key management platform is critical to ensure that the organization has access to encrypted workloads across a variety of on-premises and cloud environments.



nShield hardware security modules (HSMs) secure the admin key and key encryption keys used to protect the HyTrust KeyControl key management server.

HyTrust and nCipher deliver universal key management for encrypted workloads

THE SOLUTION: HYTRUST DATACONTROL AND KEYCONTROL WITH NCIPHER NSHIELD HSMs

HyTrust DataControl secures multi-cloud workloads throughout their lifecycle. The solution reduces the complexity of protecting workloads across multiple cloud platforms and helps organizations comply with government and industry data security regulations. DataControl includes the VMware-certified HyTrust KeyControl, a key management server (KMS) that manages encryption keys for virtual machines and encrypted data stores. KeyControl can scale to support thousands of encrypted workloads across multi-cloud deployments with policy-based key management. DataControl ensures policies are enforced, even when moving workloads across cloud platforms such as VMware, Microsoft Azure and Amazon AWS. Policy enforcement ensures that data within each VM is securely encrypted (AES-128/256-bit) throughout its lifecycle: from installation, upon boot, until each workload is securely decommissioned.

HyTrust KeyControl integrates with nCipher nShield Connect on-premises and nShield as a Service cloud-based HSMs to protect the admin and key encryption keys used by the KMS. The combined solution enhances security and facilitates regulatory compliance with a FIPS 140-2 Level 3 and Common Criteria EAL4+ root of trust.

WHY USE NCIPHER NSHIELD HSMs WITH HYTRUST KEYCONTROL?

Keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise through internal and external key theft. HSMs are a proven and auditable way to secure valuable cryptographic material.

nShield Connect HSMs and nShield as a Service integrate seamlessly with KeyControl to provide comprehensive logical and physical protection of admin and key encryption keys. The combination delivers an auditable method for enforcing security policies for foundational keys. By providing a mechanism to enforce security policies and a secure tamper resistant environment, customers can:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed
- Deliver superior performance to support demanding multi-cloud workload deployments

nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With nShield HSMs, customers can:

- Provide a tightly controlled tamper-resistant environment for safekeeping and managing cryptographic keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, CNG, nCore, and nShield Web Services Crypto API)

NCIPHER

nCipher, an Entrust Datacard company, is a leader in the general purpose HSM market, empowering world-leading organizations by delivering trust, integrity, and control to their business-critical information and applications. By using the same proven technology customers depend on today to protect against threats and meet compliance, nCipher underpins the trust of tomorrow.

HYTRUST

HyTrust's mission is to make private, public, and hybrid cloud infrastructure more trustworthy for enterprises, service providers, and government agencies. Available solutions automate security controls for software-defined computing, networking, and storage workloads to achieve the highest levels of visibility, granular policy control, and data protection. HyTrust customers benefit from being able to accelerate cloud and virtualization cost savings while improving their security posture by automating and enforcing security policies in real time, adapting quickly to compliance requirements, and preventing unplanned outages.

For more information visit www.ncipher.com and www.hytrust.com