Entrust delivers universal key management for encrypted workloads

Address the cryptographic key management and compliance needs of enterprise multi-cloud deployments with a robust Entrust nShield® HSM root of trust

HIGHLIGHTS

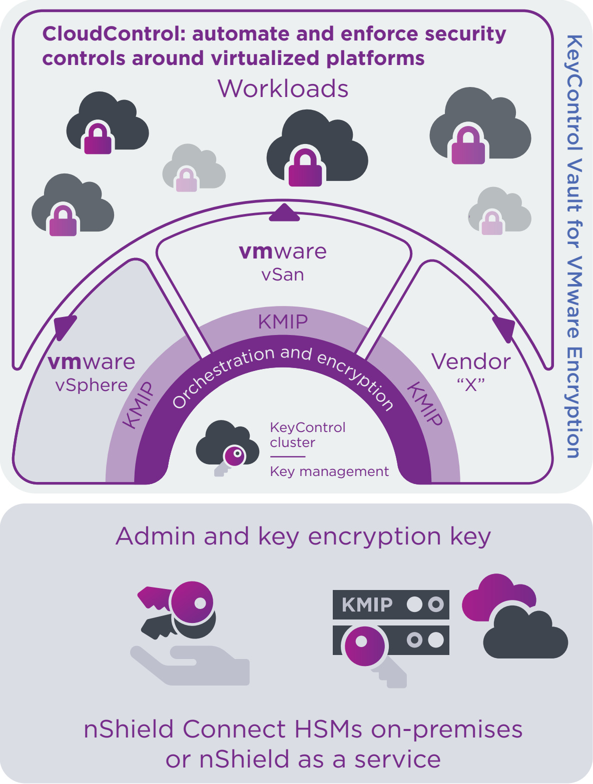
- Ensure strong data security across distributed computing environments
- Manage key lifecycles centrally while supporting multi-cloud settings
- Scale to provision keys for tens of thousands of encrypted workloads
- Address the regulated market needs for reduced risks and compliance
- Support the industry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

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.

Learn more at entrust.com/HSM

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.


CloudControl: automate and enforce security controls around virtualized platforms
Workloads
KeyControl Vault for VMware Encryption
vmware vSan
vmware vSphere
Vendor "X"
KMIP
KMIP
KMIP
Orchestration and encryption
KeyControl cluster
Key management
Admin and key encryption key
KMIP
nShield Connect HSMs on-premises or nShield as a service

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

Entrust delivers universal key management for encrypted workloads

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.

The solution: Entrust KeyControl Vault for VMware Encryption and KeyControl with nShield HSMs

Entrust KeyControl Vault for VMware Encryption 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. KeyControl Vault for VMware Encryption is included with Entrust 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. KeyControl Vault for VMware Encryption 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.

Entrust KeyControl integrates with nShield® Connect HSMs 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 nShield HSMs with Entrust 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

Learn more at entrust.com/HSM

Entrust delivers universal key management for encrypted workloads

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)

Entrust CloudControl

Comprehensive security for distributed private cloud environments, including enhanced role-based controls, secondary approvals, centralized authentication, and compliance automation.

- Granular role-based access controls for virtual admins
- Secondary approval – defining and enforcing actions requiring "second eyes" prior to authorization
- Built-in compliance templates for hardening virtual machine and containerized environments
- Extended and customizable compliance templates, with automated assessment and remediation
- Unified policy, visibility, and administrative guardrails, establishing a baseline that can constantly monitor deployments
- Secure separation of workloads
- "Security as code" automation for DevSecOps
- Seamless integration with and support for VMware Cloud Foundation (VCF) environments
- Unique functionality defines who can see, what can be seen and what can be acted upon following a least privilege / Zero Trust model.

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations.

Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about
Entrust nShieldHSMs

HSMinfo@entrust.com
entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters

1187 Park Place, Minneapolis, MN 55379
HSMinfo@entrust.com