Entrust KeyControl

Universal key management for encrypted workloads

HIGHLIGHTS

- Deliver enterprise scale and availability, supporting Key Management Interoperability Protocol (KMIP[1])-compatible encryption agents

- Upgradeable to Entrust DataControl for complete, multi-cloud workload encryption

- Provide seamless integration with FIPS 140-2 Level 3 Entrust nShield® HSMs

- Validated by VMware® to support vSphere® and vSAN® virtualization platforms

Managing the security of workloads in a dynamic, virtualized environment is a time-consuming and complex challenge for administrators

Encrypting workloads significantly reduces your risk of data breaches; if data does fall into the wrong hands, it is unreadable. However, managing the keys for tens of thousands of encrypted workloads is nontrivial. To ensure strong data security, keys have to be rotated frequently, and transported and stored securely. Along with the high demand for strong data security, there is an ever-increasing business need to meet regulatory requirements for PCI-DSS, HIPAA, NIST 800-53, and GDPR compliance in virtual environments.

Many virtualization platforms such as VMware vSphere do not include native key management functionality, requiring a third-party external key management server (KMS). For multi-cloud environments, key management is even more complex as many key management systems cannot interoperate between different platforms.

Learn more about KeyControl at entrust.com

Entrust KeyControl

Entrust KeyControl

With Entrust KeyControl, businesses can easily manage encryption keys at scale. Using FIPS 140-2 compliant encryption, KeyControl simplifies management of encrypted workloads by automating and simplifying the lifecycle of encryption keys; including key storage, distribution, rotation, and key revocation.

Universal key management for KMIP clients

KeyControl is a VMware-certified, scalable, and feature-rich KMIP server that simplifies key management for encrypted workloads. It serves as a KMS for VMware vSphere and vSAN encrypted clients, and other products that support KMIP.

Enterprise scalability and performance

KeyControl manages the encryption keys for all your virtual machines and encrypted data stores and can scale to support thousands of encrypted workloads in large deployments. Up to eight key managers can be added to a cluster to increase availability and resiliency in high volume key request environments.

Enhanced multi-cloud workload encryption

KeyControl is easily upgraded to Entrust DataControl, which enables multi-cloud workload encryption and policy-based key management. It ensures policies are enforced, even when moving across cloud platforms (private and public) such as Microsoft Azure and Amazon Web Services (AWS). DataControl 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.

Platform support

- Private cloud platforms: vSphere, vCloud Air (OVH), VCE, VxRail, Pivot3, NetApp, Nutanix

- Public cloud platforms: AWS, IBM Cloud, Microsoft Azure, VMware Cloud (VMC) on AWS, Google Cloud Platform (GCP)

- Hypervisor support: ESXi, Hyper-V, Xen, AWS, Azure
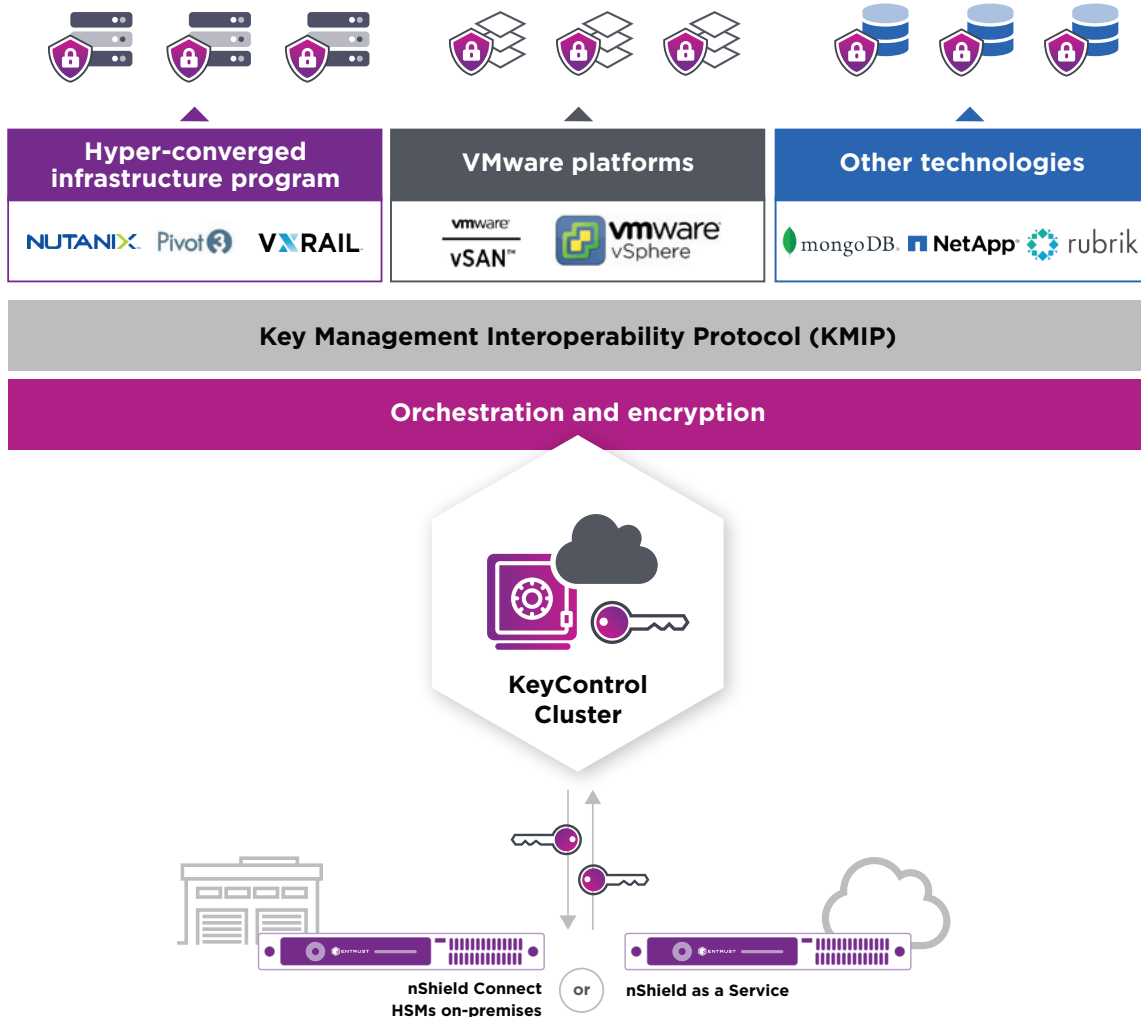
Operating system support

CentOS, Red Hat Enterprise Linux, Ubuntu, SUSE Linux Enterprise Server, Oracle Linux, AWS Linux, Windows Server Core 2012 and 2016, Windows Server 2012 and 2016, Windows 7, 8, 8.1, and 10

Deployment media

ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services marketplace), or VHD (Microsoft Azure marketplace)

[1]The Key Management Interoperability Protocol (KMIP) standard was introduced in 2010, by an alliance of vendors led by Hewlett-Packard, IBM, and EMC/RSA Security, in order to simplify the interoperability of encryption keys.

Learn more about KeyControl at entrust.com

Entrust KeyControl

Hyper-converged infrastructure program
NUTANIX. | Pivot3 | VXRAIL

VMware platforms
vmware vSAN | vmware vSphere

Other technologies
mongoDB. | NetApp | rubrik

Key Management Interoperability Protocol (KMIP)

Orchestration and encryption

KeyControl Cluster

nShield Connect HSMs on-premises — or — **nShield as a Service**

Technical specifications

- VMware certified KMS for:

  - vSphere 6.5, 6.7, and 7.0
  - vSAN 6.6, 6.7, and 7.0
  - vSphere Trust Authority 7.0

- Supports KMIP 1.1 – 1.4

- High availability (HA) support with active-active cluster (up to 8 KMS servers per cluster)

- FIPS 140-2 Level 3 compliance via Entrust nShield HSM on premises or as a service

- Enables the use of Virtual Trusted Platform Module (vTPM) cryptoprocessors in your VMs

- Supports the use of TLS 1.2 between all registered clients

Entrust KeyControl is part of a suite of data encryption and multi-cloud key management products that include Entrust DataControl and CloudControl. This enables cross-platform virtualization with advanced security and audit controls, strong encryption, key management, and workload geo-fencing solutions.

Learn more at
entrust.com

ENTRUST