Entrust KeyControl

Multi-cloud key management for encrypted workloads

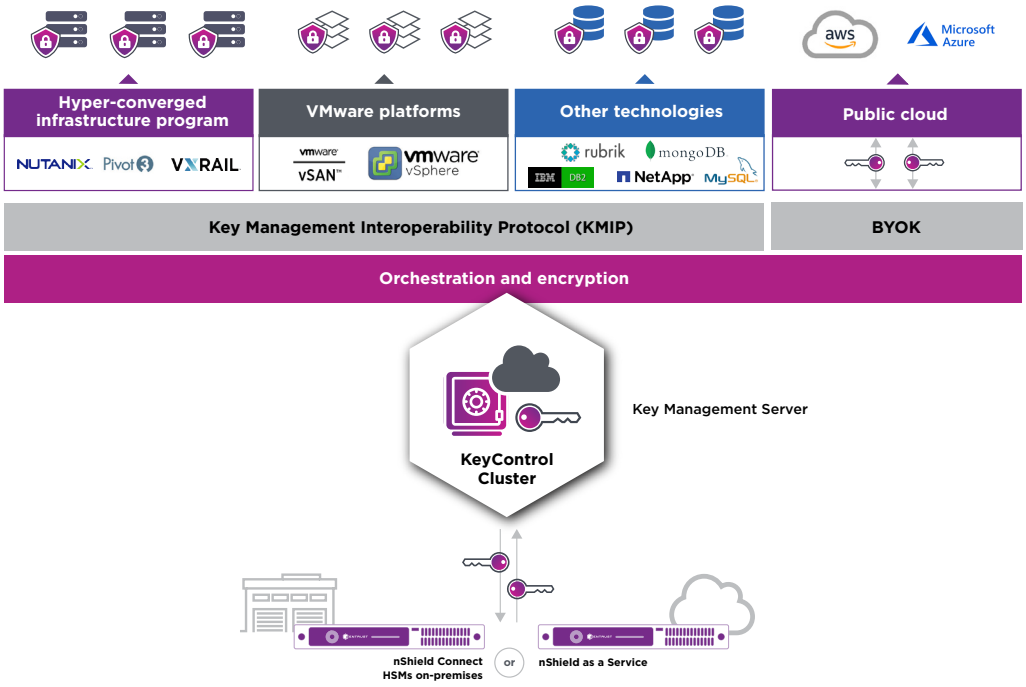
Managing the security of workloads in a virtualized environment is a complex challenge for administrators

Encrypting workloads significantly reduces your risk of data breaches. 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 Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST) 800-53, and GDPR compliance in virtual environments.

With Entrust KeyControl (formerly HyTrust), businesses can easily manage encryption keys at scale. Using Federal Information Processing Standards (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.

HIGHLIGHTS

- Deliver enterprise scale and availability, supporting Key Management Interoperability Protocol (KMIP)-compatible encryption agents
- Upgradable to Entrust DataControl for complete, multi-cloud workload encryption
- Provide seamless integration with FIPS 140-2 Level 3 Entrust nShield® Hardware Security Modules (HSMs)
- Validated by VMware® to support vSphere® and vSAN® virtualization platforms
- Bring Your Own Key capability for Microsoft Azure and AWS cloud environments



Learn more about KeyControl at entrust.com

Entrust KeyControl

KEY FEATURES & BENEFITS

Universal key management for KMIP clients

KeyControl is a VMware-certified, scalable, and feature-rich KMIP server that simplifies key lifecycle management for encrypted workloads. It serves as a KMS for VMware vSphere and vSAN encrypted clients, and other KMIP compatible products such as NetApp, Nutanix, Pivot3, DB2, MySQL and MongoDB.

KMIP multi-tenancy support

Allows administrators to isolate different tenant environments for security and compliance.

Enterprise scalability and performance

KeyControl manages the encryption keys for all of 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.

Bring Your Own Key to Azure and AWS

KeyControl offers a single unified key management, single pane of glass experience for Microsoft Azure and AWS customer master keys and native AWS and Azure keys. This provides maximum control, automation, and management for organizations who want to generate their own cryptographic keys, allowing them to bring keys created in their environment to Microsoft Azure and AWS as well as managing the lifecycle of native Microsoft Azure and AWS generated keys. This offers a range of benefits:

- Simplifies process of creating Bring Your Own Keys (BYOKs) and exporting to Microsoft Azure and AWS
- Leverages nShield HSMs for creating cryptographic key material from rich entropy source
- Full control over customer's master key in Microsoft Azure and AWS
- Keys backed up (and recoverable) in KeyControl, keeping customer in control
- Granular key lifecycle management - expiry actions (disable, delete key material) and key rotation

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 – 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)

Technical specifications

- VMware certified KMS for vSphere 6.5, 6.7, and 7.0; vSAN 6.6, 6.7, and 7.0; and 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.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223