KeyControl Vault for Cloud Key Management

Bring Your Own Key (BYOK) for control in multi-cloud environments

HIGHLIGHTS

For organizations who wish to maximize control of their cryptographic keys while leveraging the benefits of the cloud, Bring Your Own Key (BYOK) ensures not just the strong provenance of the keys but also provides lifecycle management, automation, and key backup capabilities independent of the cloud provider.

- Key lifecycle management enables fine-grained control and automation of:
  - Key rotation
  - Key expiry
  - Key deletion
  - Key backup
- Supports single, multi-cloud, and hybrid cloud deployments
- BYOK capability for AWS, Microsoft Azure and Google Cloud Platform cloud environments to maintain the creation and control of your cryptographic keys
- Provides seamless integration option with FIPS 140-2 Level 3 Entrust nShield® hardware security modules (HSMs) for a high-quality entropy source for key generation

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

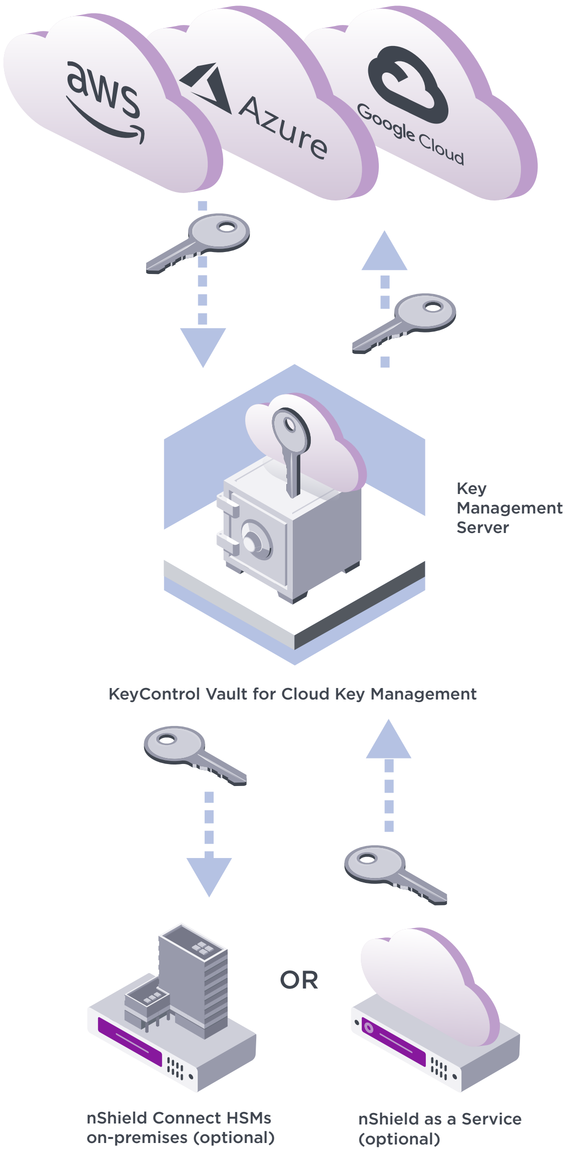
Organizations want to migrate workloads to the cloud but prefer to retain control over the keys used by their cloud service providers (CSPs).

- Cryptographic keys are used by the applications you use in the cloud
- Security-conscious organizations want to own and control these keys throughout their lifecycle
- CSP-generated keys are sticky and can make migration to other CSPs hard
- CSPs can be opaque – isn't it more reassuring when you know where and how your keys have been created and where they are backed up?
- Organizations want to automate their key management process from inception through to retirement

With Entrust KeyControl Vault for Cloud Key Management businesses can easily manage encryption keys at scale. Using Federal Information Processing Standards (FIPS) 140-2 compliant encryption, the vault simplifies the bring your own key process, allowing you to create your keys on premises under the control of your security team, automating and simplifying the lifecycle of encryption keys; including key storage, distribution, rotation, and key backup.

Learn more about KeyControl Vault for Cloud Key Management at entrust.com

Entrust KeyControl Vault for Cloud Key Management (BYOK)


aws
Azure
Google Cloud
Key Management Server
KeyControl Vault for Cloud Key Management
OR
nShield Connect HSMs on-premises (optional)
nShield as a Service (optional)

KEYCONTROL VAULT FOR CLOUD KEY MANAGEMENT (BYOK) FEATURES & BENEFITS

Enterprise scalability and performance

KeyControl Vault 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 servers can be added to a cluster.

Bring Your Own Key to AWS, Microsoft Azure, and Google Cloud Platform

The vault offers a single unified key management, single pane of glass experience for Microsoft Azure, Google Cloud Platform, and AWS customer master 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 AWS, Microsoft Azure, and Google Cloud Platform. This offers a range of benefits:

- Simplifies the process of securely creating encryption keys and uploading to AWS, Microsoft Azure, and Google Cloud Platform
- Leverages nShield HSMs for creating cryptographic key material from rich entropy source
- Full control over customer's master key in AWS, Microsoft Azure, and Google Cloud Platform
- Keys backed up (and recoverable) in the KeyControl vault, keeping customer in control
- Granular key lifecycle management – expiry actions (disable, delete key material) and key rotation

Learn more about KeyControl Vault for Cloud Key Management at entrust.com

Entrust KeyControl Vault for Cloud Key Management (BYOK)

How does BYOK work?

During a key import, the KeyControl vault interacts transparently with the CSP key management service following a 4-step process:

- The KeyControl vault requests the creation of an asymmetric key from the CSP. This key is referred to as a key encryption key (KEK).
- KeyControl then downloads a transport key (public key of KEK) that will be used to securely transfer key (BYOK) material to the CSP.
- The KeyControl vault generates and encrypts the key material using the transport key provided by the CSP.
- The KeyControl vault uploads the encrypted key (BYOK) material with the transport key provided by the CSP.

Platform support

Public cloud platforms: AWS Google Cloud Platform and Microsoft Azure

Operating system support

CentOS, Red Hat Enterprise Linux, Ubuntu, SUSE Linux Enterprise Server, Oracle Linux, AWS Linux, Windows Server Core 2012, 2016, and 2019, Windows Server 2012 R2, 2016, and 2019, Windows 8.1, and 10

Deployment media

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

Learn more about KeyControl Vault for Cloud Key Management at entrust.com

Entrust KeyControl Vault for Cloud Key Management (BYOK)

Technical specifications

- lVMware 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

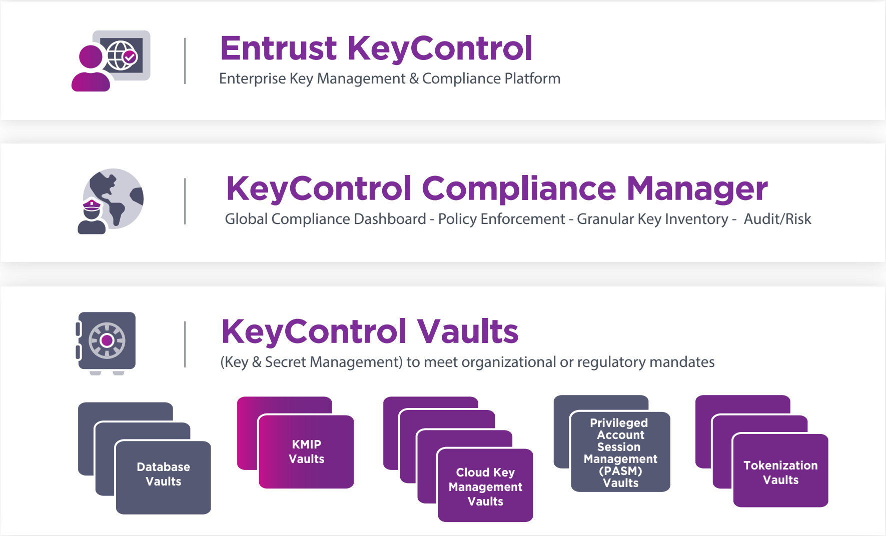
- lHigh availability (HA) support with active cluster (up to 8 KMS servers per cluster)

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

- lSupports the use of TLS 1.2 between all registered clients

Entrust KeyControl Platform

Entrust KeyControl Vault for Cloud Key Management is part of a suite of products designed to manage key lifecycles at scale for encrypted workloads in virtualized environments across on-premises, multi-cloud, and hybrid deployments.



Entrust KeyControl
Enterprise Key Management & Compliance Platform

KeyControl Compliance Manager
Global Compliance Dashboard - Policy Enforcement - Granular Key Inventory - Audit/Risk

KeyControl Vaults
(Key & Secret Management) to meet organizational or regulatory mandates

Database Vaults
KMIP Vaults
Cloud Key Management Vaults
Privileged Account Session Management (PASM) Vaults
Tokenization Vaults

Learn more at
entrust.com

ENTRUST

Entrust, nShield, and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.

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