Entrust KeyControl BYOK

Multi-cloud key management for encrypted workloads

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
- Simple, unified GUI management experience for:
  - Keys originated in KeyControl and native Microsoft Azure Key Vault and AWS KMS keys
- Bring Your Own Key capability for Microsoft Azure and AWS 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

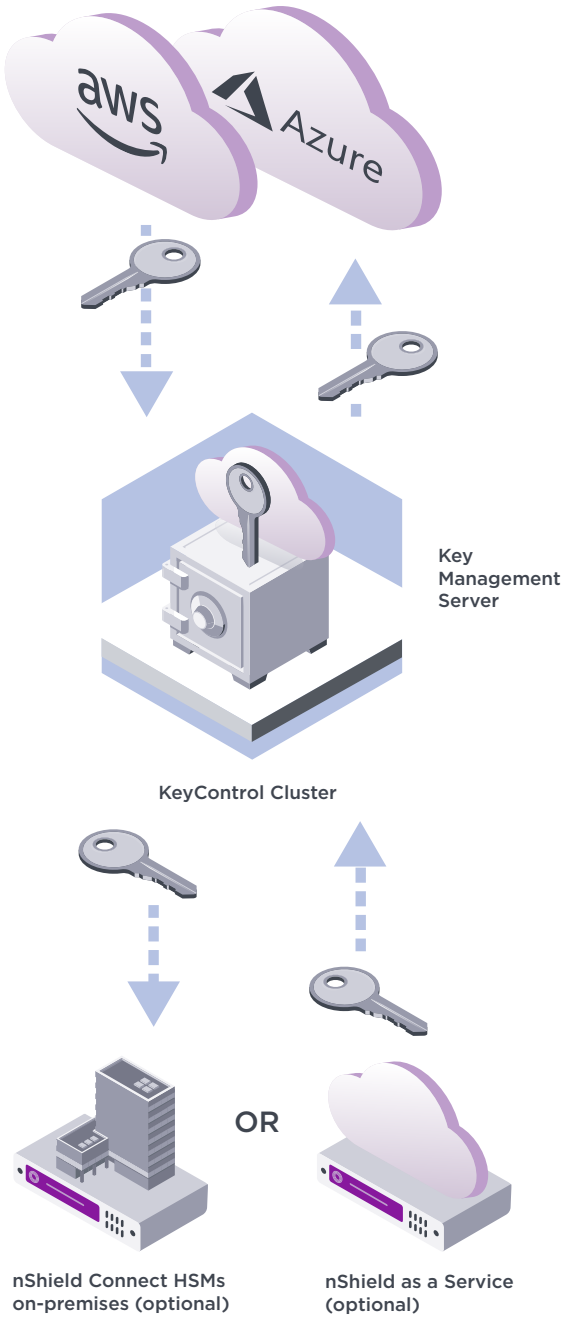
Organizations want to migrate workloads to the cloud but prefer to retain control over the keys used by their cloud service providers (CSPs).

- 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 BYOK (formerly HyTrust), businesses can easily manage encryption keys at scale. Using Federal Information Processing Standards (FIPS) 140-2 compliant encryption, KeyControl BYOK 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

Learn more about KeyControl BYOK at entrust.com

Entrust KeyControl BYOK



KEY FEATURES & BENEFITS

Enterprise scalability and performance

KeyControl BYOK 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 Azure and AWS

KeyControl BYOK 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 the process of securely creating encryption keys and uploading 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 BYOK, keeping customer in control
- Granular key lifecycle management - expiry actions (disable, delete key material) and key rotation

Learn more about KeyControl BYOK at entrust.com

Entrust KeyControl BYOK

Platform support

Public cloud platforms: AWS 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)

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

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

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

Supports the use of TLS 1.2 between all registered clients

Entrust KeyControl BYOK is a separate licensed product from the standard KeyControl product (for KMIP compatible workloads). It can be licensed stand-alone or deployed together with the standard KeyControl product. KeyControl BYOK is part of a suite of data encryption and multi-cloud key management products. See table below for details.

ENTRUST PRODUCT	DESCRIPTION	ADDITIONAL INFORMATION
KeyControl BYOK	For generating and bringing your own cryptographic keys to AWS, Microsoft Azure, or Google Cloud Platform	Licensed standalone or can be deployed with KeyControl and/or DataControl
KeyControl	Enterprise encryption key management for KMIP enabled workloads	Licensed standalone or can be deployed with KeyControl BYOK and/or DataControl
DataControl	For fine-grained, agents based control and encryption key management of virtual machine encryption in multi-cloud environments	Licensed standalone or can be deployed with KeyControl and/or KeyControl BYOK
CloudControl	For automated workload security policy enforcement and compliance in virtualized and containerized environments protecting sensitive data against misconfigurations in the cloud.	

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