DATA SHEET

Entrust KeyControl Vault for Cloud Keys

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, Google Cloud Platform, Salesforce, and Oracle Cloud Infrastructure environments to maintain the creation and control of your cryptographic keys
- KeyControl can be deployed on premises, as a service, or as a hybrid solution
- Provides seamless integration option with FIPS 140-3 Level 3 Entrust nShield® hardware security modules (HSMs) for a high-quality entropy source for key generation
- Scalable to manage tens of millions of keys

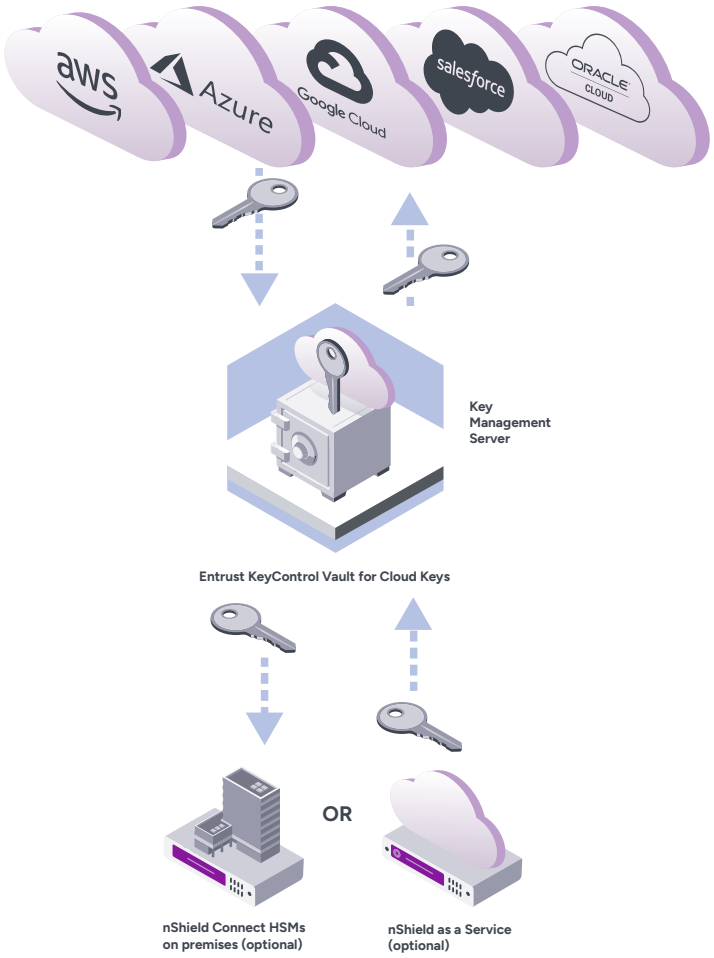
Managing the Security of Workloads in a Virtualized Environment Is a Complex Challenge for Administrators

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 Keys businesses can easily manage encryption keys at scale. The vault simplifies the Bring Your Own Key process.

ENTRUST
SECURING A WORLD IN MOTION



Entrust KeyControl Vault for Cloud Keys features & benefits

The vault offers a single unified key management, single pane of glass experience for Microsoft Azure, Google Cloud Platform, AWS, and Salesforce 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, Google Cloud Platform, Salesforce, and Oracle Cloud Infrastructure. This offers a range of 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, Google Cloud Platform, and Salesforce

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

- Simplifies the process of securely creating encryption keys and uploading to AWS, Microsoft Azure, Google Cloud Platform, Salesforce, and Oracle Cloud Infrastructure
- Leverages nShield HSMs for creating cryptographic key material from rich entropy source
- Full control over customer's master key in AWS, Microsoft Azure, Google Cloud Platform, Salesforce, and Oracle Cloud Infrastructure
- 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

How does BYOK work?

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

1. The KeyControl vault requests the creation of an asymmetric key from the CSP. This key is referred to as a key encryption key (KEK).
2. KeyControl then downloads a transport key (public key of KEK) that will be used to securely transfer key (BYOK) material to the CSP.
3. The KeyControl vault generates and encrypts the key material using the transport key provided by the CSP.
4. 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, Microsoft Azure, Salesforce, and Oracle Cloud Infrastructure

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 (Hyper-V, Nutanix, KVM), 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 140-3 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 Platform

Entrust KeyControl Vault for Cloud Keys (BYOK) 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.

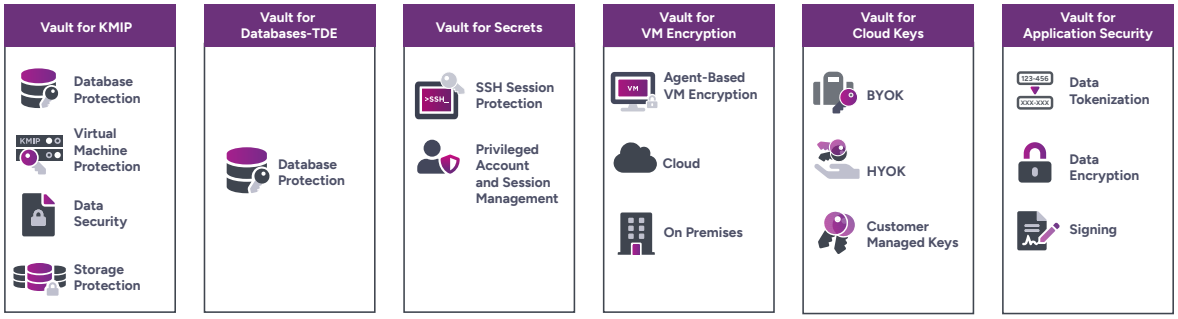
Compliance Manager

- Unified dashboard for inventory, risk, and compliance of cryptographic assets
- Policy enforcement (NIST SP 800-57, PCI DSS)

Lifecycle Management

- Lifecycle management for keys and secrets vaults
- Decentralized key and secret lifecycle management to meet business and regulatory needs

Vaults / Use Cases



entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION