Entrust KeyControl

Redefining Key Management Systems (KMSs)

Overview

Traditional centralized, monolithic key management solutions no longer effectively meet the needs of organizations that face increasingly complex data security, regulatory, and compliance requirements. Combining visibility with the ability to document usage parameters is essential in offering fine-grained policy controls and ensuring compliance mandates can be met. Entrust KeyControl provides a feature-rich dashboard to monitor every facet of a key or secret while addressing the rigors of data sovereignty and residency regulations.

Entrust KeyControl combines key lifecycle management and a decentralized vault-based architecture with a comprehensive central policy and compliance management capabilities for a wide range of use cases.

Versatile Key and Secret Vaults: A decentralized security model helps mitigate aggregation risks across a cryptographic ecosystem. Data can be protected in line with differing local security policies and comply with regulatory mandates.

Compliance Dashboard: KeyControl Compliance Manager provides centralized visibility of an enterprise's cryptographic assets and a policy engine that allows fine-grained control of all cryptographic keys and secrets regardless of the vault locations.

Learn more about KeyControl at entrust.com

KEY FEATURES

- Scalable, cost-effective enterprise ready key management system that supports a wide range of use cases
- Unified dashboard for fine-grained visibility of keys and secrets
- Detailed metrics to identify level of compliance and alert on prohibited key usage
- Decentralized vault-based architecture
- Full key lifecycle management in FIPS 140-2 Level 1 certified virtual appliance
- Full HA configuration for resilient backup and recovery
- Optional upgrade to FIPS 140-2 Level 3 through seamless integration with Entrust nShield hardware security module (HSM)

Redefining key management systems

Highlights

KeyControl Vault
The flexible KeyControl architecture supports the following vault options for managing keys and secrets:

KeyControl Vault for KMIP
Provides a vault for KMIP workloads utilizing cryptographic keys including virtualization platforms, backup/recovery, database, and storage workloads.

KeyControl Vault for Databases
Provides key lifecycle management for encrypted SQL databases using transparent database encryption (TDE).

KeyControl Vault for Cloud Key Management
Provides organizations with control of their cryptographic keys while leveraging the benefits of the cloud. Supports customer-managed keys including Bring Your Own Key (BYOK) and cloud-managed keys (or native keys) and externally-stored keys including Hold Your Own Key (HYOK).

KeyControl Vault for Tokenization
Addresses a wide range of data protection use cases by providing data encryption, data tokenization, data signature with format-preserving encryption (FPE), data masking, and key management.

KeyControl Vault for Secrets Management
Enables organizations to securely store and strictly control access to passwords, tokens certificates, and cryptographic keys for protecting resources such as cloud services, databases, servers, or containers.

KeyControl Vault for VM Encryption
Provides agent-based virtual machine (VM) workload encryption, offering zero downtime encryption per VM. Unique keys can be assigned to encrypt each partition, including the boot (OS) disk and swap partitions.

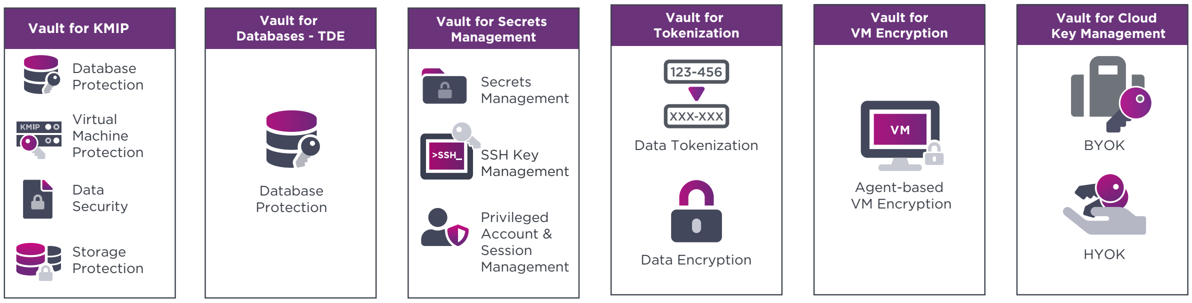
KeyControl

Enterprise Key Lifecycle Management & Compliance Platform

KeyControl Compliance Manager

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

KEYCONTROL VAULTS & USE CASES



Vault for KMIP: Database Protection; Virtual Machine Protection; Data Security; Storage Protection

Vault for Databases - TDE: Database Protection

Vault for Secrets Management: Secrets Management; SSH Key Management; Privileged Account & Session Management

Vault for Tokenization: Data Tokenization; Data Encryption

Vault for VM Encryption: Agent-based VM Encryption

Vault for Cloud Key Management: BYOK; HYOK

Learn more about KeyControl at entrust.com

Redefining key management systems

Key lifecycle management: Simplifies management of encrypted workloads by automating the lifecycle of encryption keys; including key storage, backup, distribution, rotation, and revocation.

Decentralized architecture: Supports national and regional data sovereignty mandates. Locate vaults based on business need. Reduced attack surface.

Unified dashboard: Single unified dashboard, KeyControl Compliance Manager, allows you to view and monitor your organization's cryptographic assets located in one or many vaults.

Wide range of vault use cases: The flexible vault architecture provides support for a wide range of features and services including KMIP, cloud key management (including BYOK and HYOK deployments), secrets management, privileged account session management, tokenization, and database protection.

MARKET
LEADER
SECRETS MANAGEMENT
LEADERSHIP COMPASS 2023
KUPPINGERCOLE ANALYSTS AG, APR 2023

MARKET
CHAMPION
SECRETS MANAGEMENT
LEADERSHIP COMPASS 2023
KUPPINGERCOLE ANALYSTS AG, APR 2023

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