Entrust KeyControl as a Service

Redefining Key Management Systems (KMSs)

Overview

Traditional key management solutions no longer effectively meet the needs of organizations that face increasingly complex data security, regulatory, and compliance requirements. Entrust KeyControl combines key lifecycle management and a decentralized vault-based architecture with comprehensive central policy and compliance management capabilities for a wide range of use cases. Combining visibility with the ability to document usage parameters is essential in offering policy controls and ensuring compliance mandates can be met. The decentralized vault-based architecture avoids the aggregation risks caused by solutions using single key and secrets stores and makes complying with the rigors of data sovereignty and residency regulations straightforward.

Entrust KeyControl can be deployed as a service, streamlining your operations by eliminating the need to purchase, provision, configure, and maintain an on-premises environment.

KEY FEATURES

- Scalable, cost-effective, enterprise-ready key management and data protection services that support a wide range of use cases
- Unified dashboard for fine-grained visibility of keys, secrets, and certificates
- Detailed metrics to identify level of compliance and alert on prohibited key usage
- Decentralized vault-based architecture
- High availability (HA), automated backups, and failover for resiliency
- Full key lifecycle management in FIPS 140-2 Level 1 certified virtual appliance
- Optional upgrade to FIPS 140-2 Level 3 through seamless integration with Entrust nShield hardware security module (HSM)

Learn more about Entrust KeyControl at entrust.com

Entrust KeyControl as a Service

Versatile Vaults for Your Crypto Assets:
Entrust KeyControl's support for geographical distributed vaults enables highly effective management of keys, secrets, and certificates while mitigating aggregation risks within a cryptographic ecosystem. This approach enables data protection that aligns with varied local security policies and ensures compliance with regulatory mandates.

Compliance Dashboard:
Entrust KeyControl provides centralized visibility of all cryptographic keys, secrets, and certificates across all the deployed vaults. This provides the capability to assess, in real time, compliance with defined policies for each cryptographic asset and the level of risk in areas of non-compliance.

Highlights

Entrust KeyControl Vaults

Each vault can be configured to support one or more of the following key and secrets management use cases.

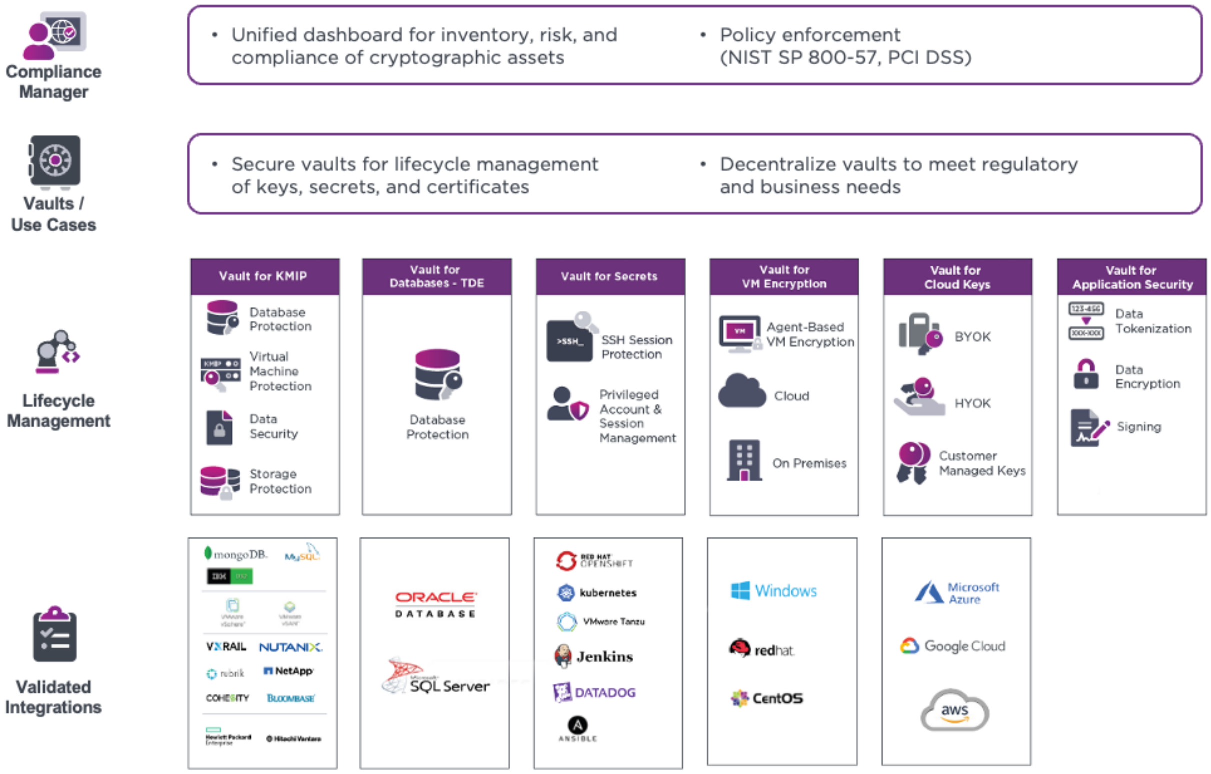
Entrust KeyControl Vault for KMIP

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

Entrust KeyControl Vault for Databases

Provides key lifecycle management for databases using transparent database encryption (TDE).

Entrust KeyControl as a Service



Compliance Manager

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

Vaults / Use Cases

- Secure vaults for lifecycle management of keys, secrets, and certificates
- Decentralize vaults to meet regulatory and business needs

Lifecycle Management

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

Vault for Databases - TDE: Database Protection

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

Vault for VM Encryption: Agent-Based VM Encryption; Cloud; On Premises

Vault for Cloud Keys: BYOK; HYOK; Customer Managed Keys

Vault for Application Security: Data Tokenization; Data Encryption; Signing

Validated Integrations

Learn more about Entrust KeyControl at entrust.com

Entrust KeyControl as a Service

Entrust KeyControl for Cloud Keys
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).

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

Entrust KeyControl Vault for Secrets
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.

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

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 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.

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