KeyControl

Enterprise Key Management and Compliance Platform

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

INTRODUCTION

Redefining cryptographic key management

As enterprises use cryptography at scale to protect applications, workloads, and data, traditional key management solutions often struggle with tracking and controlling the use of keys throughout their lifecycle while also lacking features to enable an enterprise to deliver on their compliance mandates and data sovereignty requirements. Consider the 5 W’s and an H....Who, What, Why, Where, When, and How, in the context of your cryptographic keys and secrets, when your audit or compliance team ask:

- How do you know if you are compliant with corporate security and data protection policies?
- Where are your keys and secrets being stored?
- Are you following industry best practice when managing keys and secrets?
- Who created this key?
- Who has permissions to access those keys?
- How do you know these keys cannot be exported to another country, violating data sovereignty mandates?
- What data or workload are the keys being used to protect?
- Do we have any critical high-value keys that require hardware protection?
- Do we have granular documentation with an accurate audit trail of your keys and secrets?
- What type of key and security strength is specified?
- Why is this key being used in a production environment when it was created solely for test purposes?
- When do the keys need to be rotated/retired?

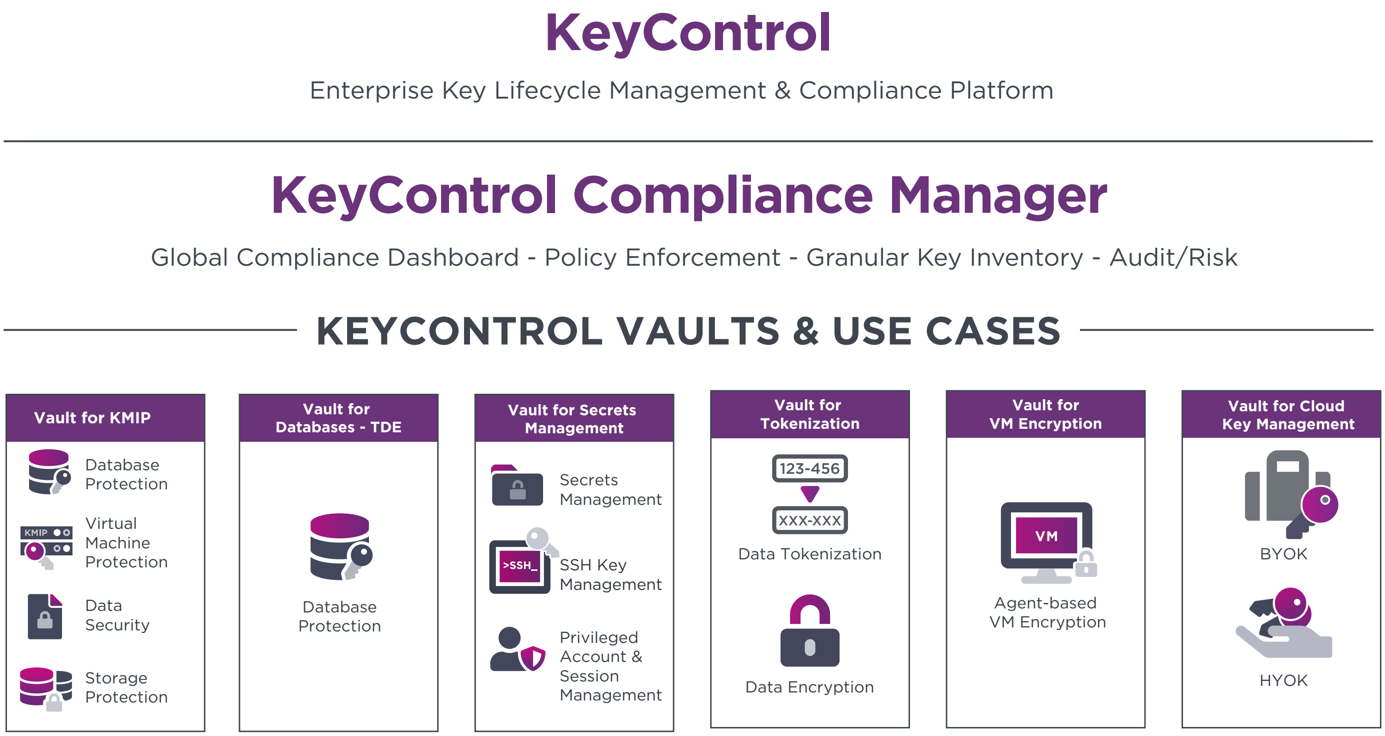
It’s a lot to consider for any organization team, especially when distributed across different applications, business units, deployment locations, and geographical regions. Traditional key management systems lack important context on the use of keys, and often only manage their activation and expiration dates. System Administrators and professionals from the Security, Compliance, and Risk teams need to have the visibility to enable them to have a firm, canonical understanding of their keys and secrets repositories/vaults, their contents, and granular details for regulatory compliance.

Entrust KeyControl redefines cryptographic key management by combining traditional key lifecycle management and a decentralized vault-based architecture with a comprehensive central policy and compliance management dashboard. The platform offers decentralized security with centralized visibility across the enterprise’s cryptographic ecosystem. This powerful feature combination ensures data is protected in line with stringent regulatory compliance mandates.

KEY MANAGEMENT & COMPLIANCE PLATFORM:

KeyControl

The Entrust KeyControl key management and compliance platform helps organizations tightly manage, monitor, and control keys and secrets to comply with industry, national, and international standards and regulations.



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

KeyControl includes the following products:

KeyControl Vault for PASM

Enables organizations to requiring Privileged Account and Session Management control Secure Shell (SSH) access and usage of administrative and privileged accounts, proactively enforcing security policies and recording privileged user activity across virtual, cloud, and physical environments.

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 (BYOK)

Provides organizations with control of their cryptographic keys while leveraging the benefits of the cloud.

KeyControl Vault for Cloud Key Management (HYOK)

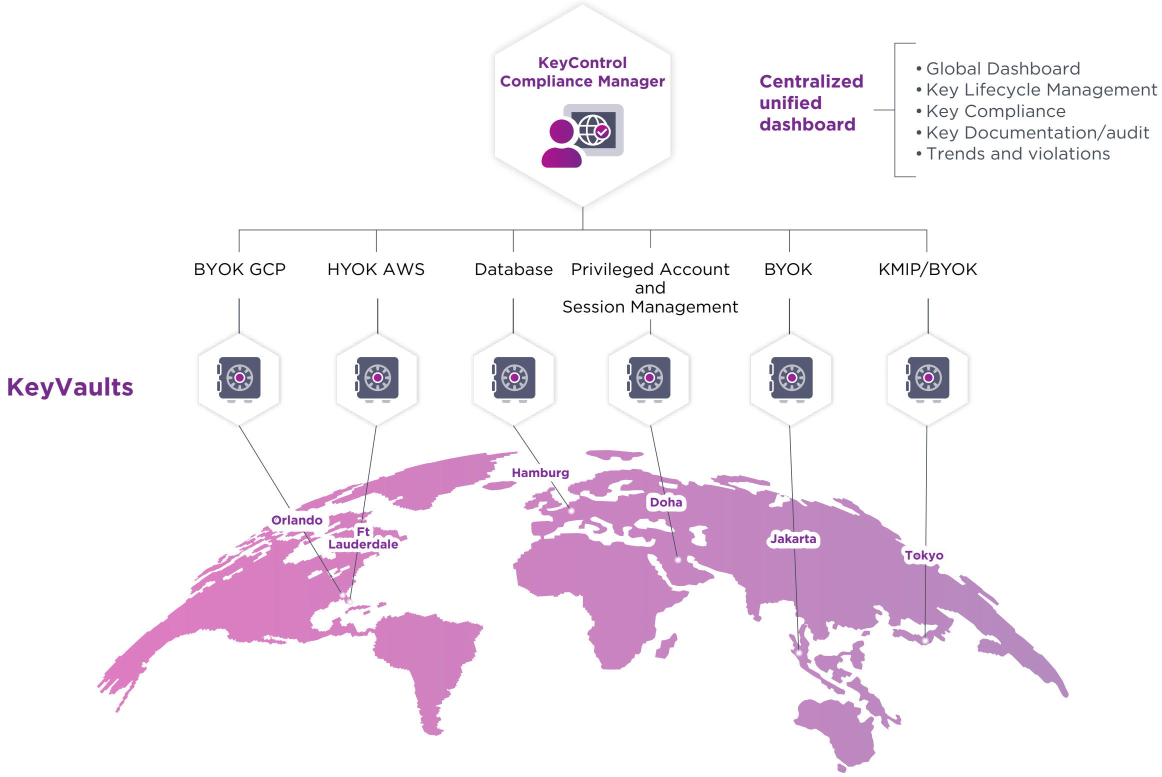
Enables the end-customer to generate and maintain control of cryptographic keys throughout their lifecycle, while allowing the CSP to use the keys on your behalf.

KeyControl Vault for Tokenization

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

KeyControl Compliance Manager

At the apex of the KeyControl platform is KeyControl Compliance Manager, which provides granular management and control of cryptographic keys and secrets across your enterprise. It's a single unified dashboard that allows you to view and monitor your organization's cryptographic assets located in one or many vaults. The vaults can be configured locally or geographically distributed. The KeyControl Compliance Manager policy engine allows fine-grained control of your cryptographic keys and secrets and provides all the answers to the 5 W's and the H discussed earlier, offering full visibility, traceability, compliance tracking, and an immutable audit trail of all keys and secrets.If business requirements demand a more discrete, regional compliance and monitoring deployment, multiple KeyControl Compliance Managers can easily be configured, for example, to isolate U.S., EMEA, and APAC regions or by organizational locations as required.


KeyControl Compliance Manager
Centralized unified dashboard
• Global Dashboard
• Key Lifecycle Management
• Key Compliance
• Key Documentation/audit
• Trends and violations
BYOK GCP
HYOK AWS
Database
Privileged Account and Session Management
BYOK
KMIP/BYOK
KeyVaults
Hamburg
Doha
Orlando
Ft Lauderdale
Jakarta
Tokyo

KeyControl Compliance Pack

The compliance pack offers a set of customizable documentation forms that can help fill any gaps in an organization's existing key documentation and enable effective risk and compliance management. It provides a range of built-in compliance templates that can be used to assess the compliance of different types of keys, for example, KMIP keys, TDE keys, and API keys.

KeyControl Vaults

The Entrust KeyControl platform offers a flexible way to architect and deploy key and secret vaults using either a single centralized approach or a decentralized model more suited to local regulations or security posture. Each vault manages keys and secrets for a wide range of use cases requiring a robust security key management posture.

To ensure strong data security, keys must be rotated frequently, and transported and stored securely. KeyControl Compliance Manager enforces your internal security policy by requiring role-based authorization and separating security and database administration, making it easier to demonstrate compliance to auditors. Unlike many traditional key management solutions that only offer a single, monolithic, centralized repository for storing keys, the vaults in the KeyControl platform deployment can be configured in a decentralized model. This approach allows organizations to meet the needs of geographical data sovereignty mandates for cryptographic assets, ensuring customer data and the keys protecting that data remain within geographic boundaries. Furthermore, the vault architecture reduces the attack surface, avoiding a single "all-in-one repository" deployment while providing flexible arrangements for disaster recovery (DR) and contingency planning.

Another advantage of the KeyControl vault architecture is the ability to manage keys for air-gapped systems, which prohibit any data transfer outside of the environment. This makes the vault architecture attractive to organizations that perform critical infrastructure operations or process sensitive data, such as via payment systems.

Privileged Account and Session Management (PASM) Vault

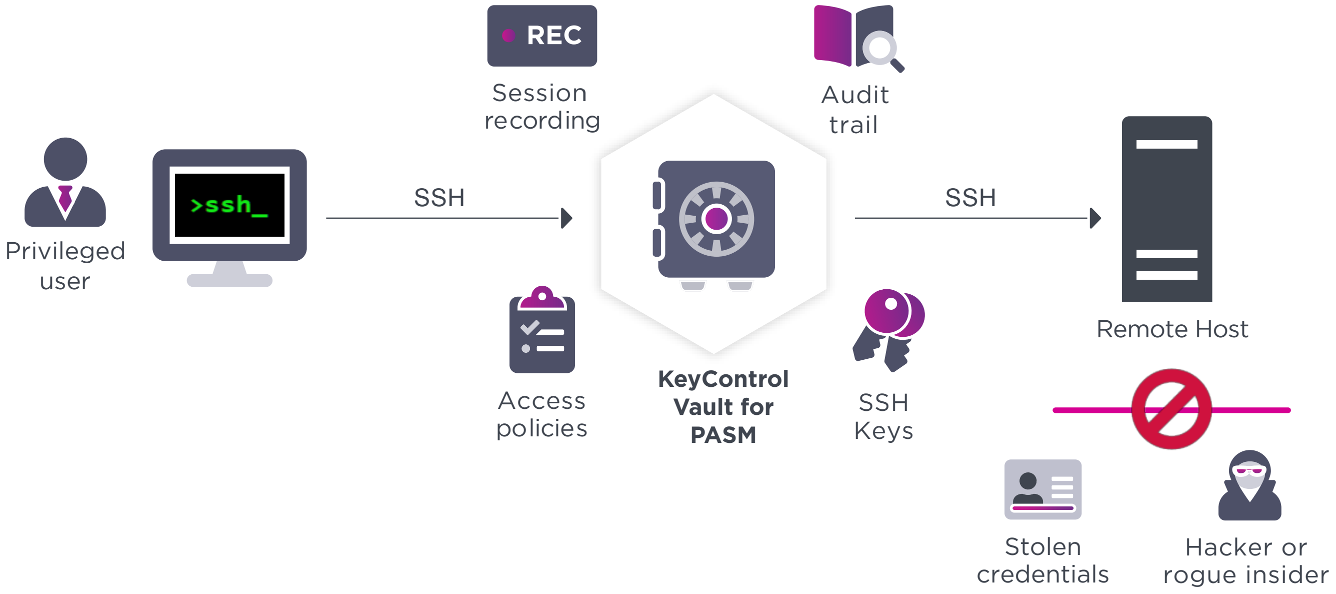
Privileged accounts often controlled using Secure Shell (SSH) keys pose a significant risk to your organization. Hackers and malicious insiders can use privileged credentials to gain access to critical systems and steal sensitive data or cause service disruption. To further complicate matters, privileged accounts and access rights are not just granted to employees, but also to vendors, contractors, business partners, and others.

KeyControl Vault for PASM enables organizations to rigorously control SSH access and usage of administrative and privileged accounts. Unique to KeyControl, its proxy design means your organization's valuable SSH keys are never accessible to privileged users.

KeyControl proactively enforces security policies with whitelisting of approved users and actions while recording privileged user activity across virtual, cloud, and physical environments and creating a granular, immutable audit trial of those accessing the system.

KeyControl Vault for PASM is underpinned by Federal Information Processing Standards (FIPS) 140-2 certified key protection with optional FIPS 140-2 Level 3 hardware security module protection.

KeyControl simplifies the management of SSH access by leveraging corporate identity and access management (IAM) systems and automating the lifecycle of SSH keys, including key storage, backup, rotation, and key revocation.



Generic Secrets

As organizations use an increasing number of credentials and secrets to access business applications, the volume of secrets has dramatically increased. Organizations need to have processes and controls in place to manage secrets sprawl, whether for third-party solutions, APIs, or in-house, custom solutions.

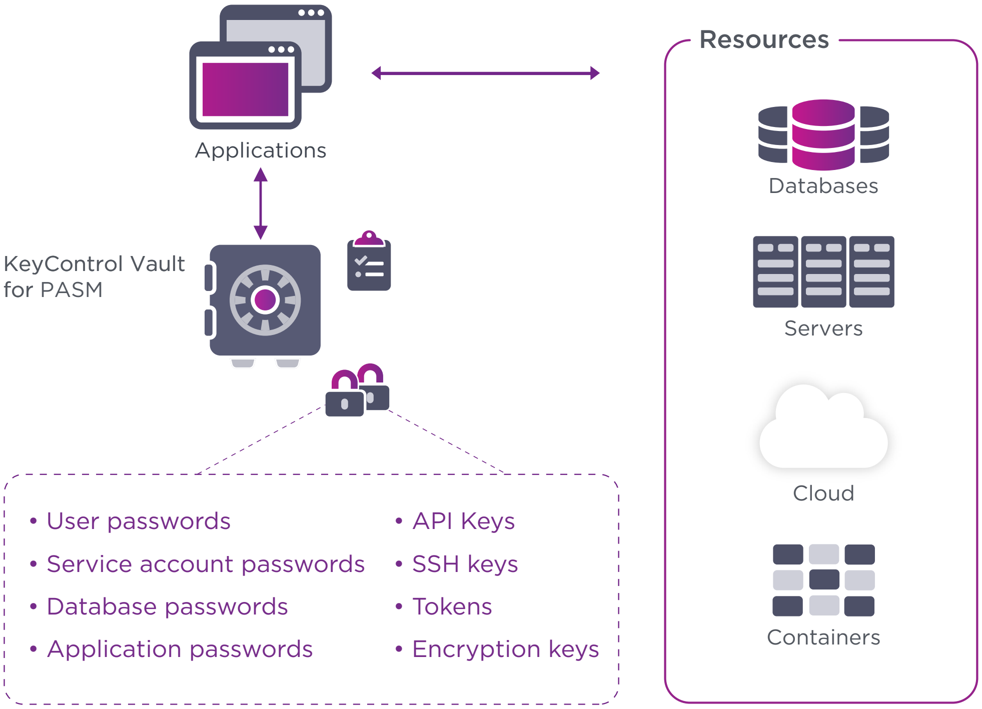
The absence of any centralized secret management tool makes it challenging to answer the “5 W” questions: What secret, Why, Where, When, and by Whom was it accessed? KeyControl Vault for PASM protects, manages, and secures access to secrets, proactively enforcing security policies and auditing privileged user or application activity across virtual, cloud, and physical environments.

The following secrets and other sensitive data are stored in a FIPS 140-2 certified vault:

- Passwords
- Key value pairs
- Plain text-based secrets
- File-based secrets

The KeyControl Vault for PASM provides a centralized secret management and auditing platform that helps you to control access to secrets and monitor their use.

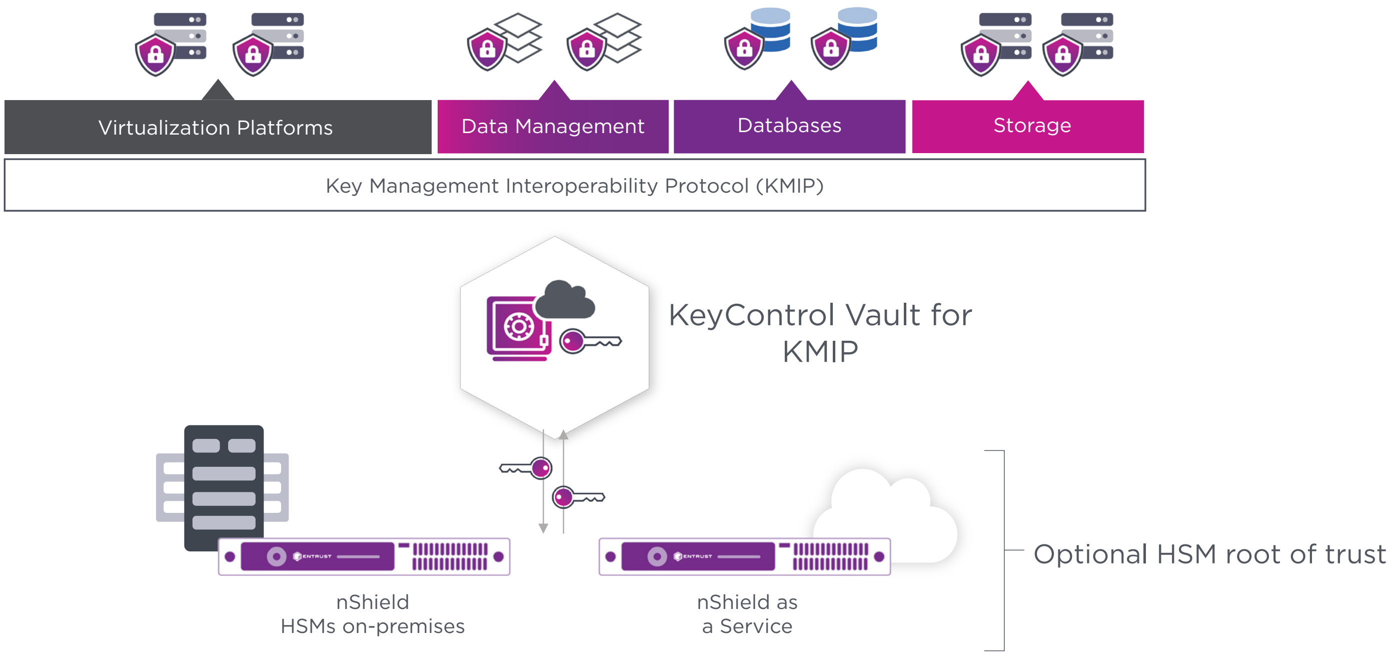
Secrets are managed and accessed using either the Web UI, CLI, or the RESTful API provided by the KeyControl Vault for PASM.



The flexible vault architecture provides support for a wide range of services as described below:

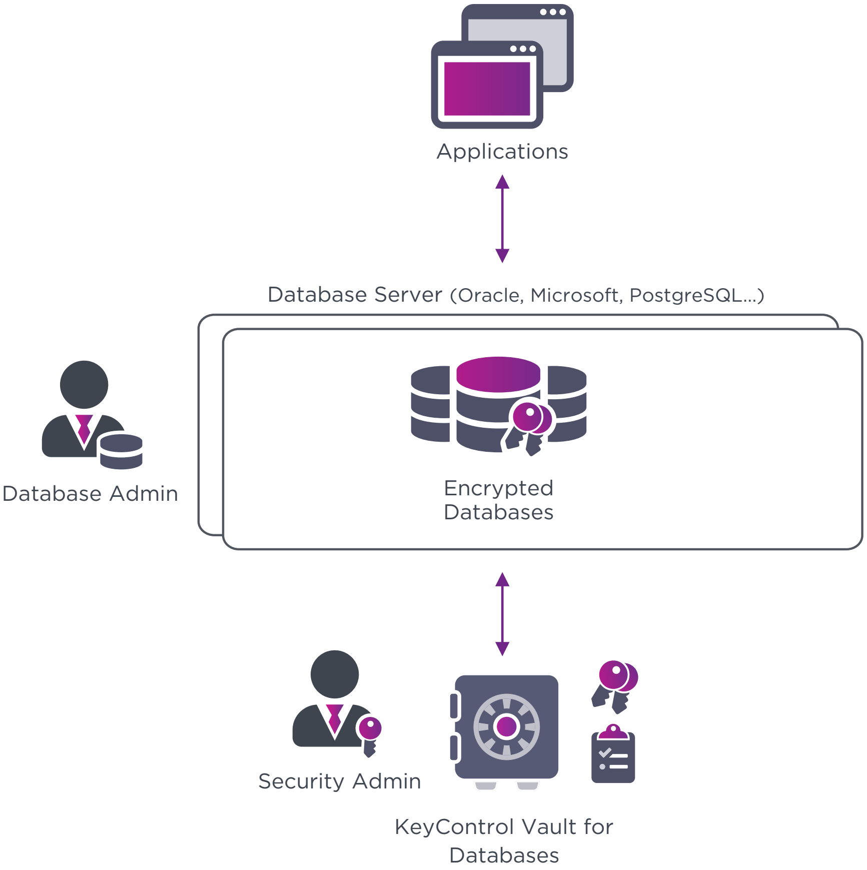
Vault for KMIP

KeyControl Vault for KMIP provides key lifecycle management for third-party solutions supporting the KMIP protocol. Providing universal key management for KMIP clients, KeyControl is a scalable and feature-rich KMIP server that simplifies key lifecycle management for encrypted workloads. It serves as a KMS for VMware vSphere and vSAN encrypted clients, and a wide range of other KMIP-compatible products such as NetApp, Nutanix, IBM Db2, Rubrik, Cohesity, and MongoDB.



Database Vault

KeyControl Vault for Databases provides key lifecycle management for encrypted SQL databases. As organizations store growing volumes of sensitive data in databases, protecting and managing the encryption keys that secure the data becomes increasingly challenging. Encryption keys underpin the security of databases, and if stored alongside the database tables, it puts them at increased risk of compromise. To mitigate risks and eliminate insider threats, master TDE keys should be carefully managed with role-based access controls and stored separately, when possible, in dedicated hardware. Entrust offers a comprehensive and unified database security platform that ensures critical data is always secured from external and internal threats and available for uninterrupted business. KeyControl protects underpinning TDE master keys and provides the flexibility you need to speed up processes – all while helping you mitigate risks and facilitate compliance. The Vault for Databases supports Microsoft SQL Server and Oracle databases. See separate data sheets for more details and specific versions supported.


Applications
Database Server (Oracle, Microsoft, PostgreSQL...)
Database Admin
Encrypted Databases
Security Admin
KeyControl Vault for Databases

Cloud Key Management Vaults

KeyControl Vault for Cloud Key Management is for organizations who wish to maximise control of their cryptographic keys and encrypted data while leveraging the services of the cloud.

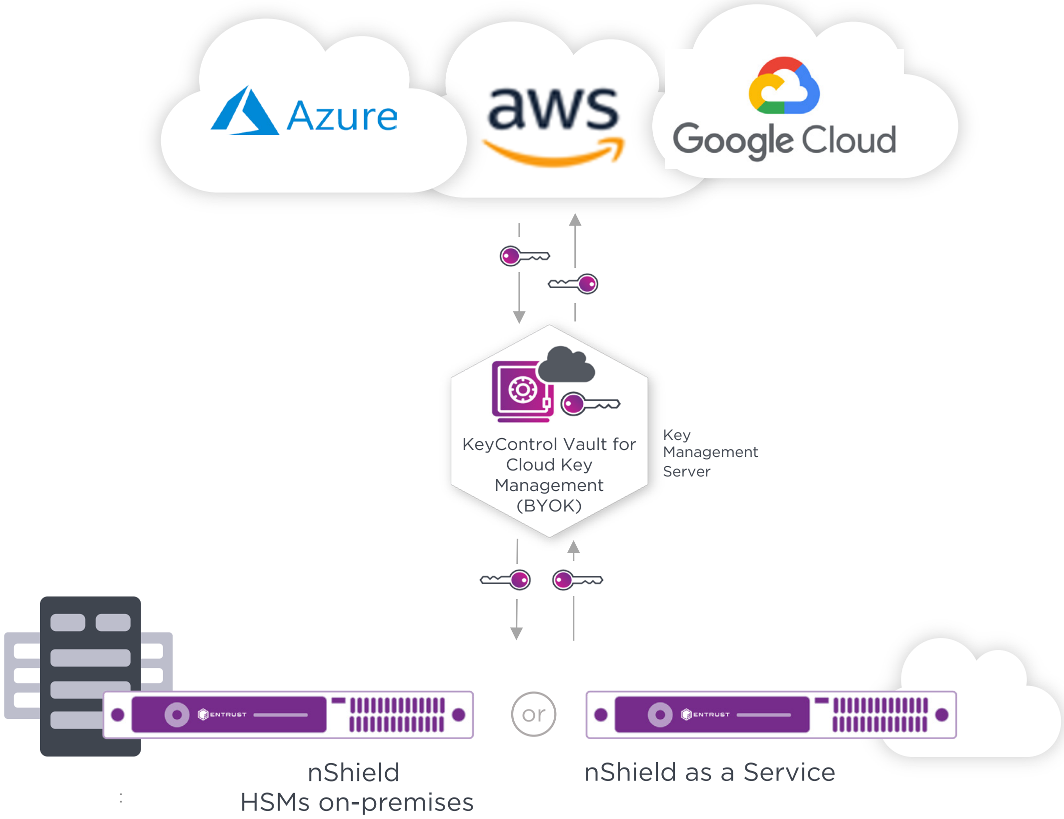
Bring Your Own Key (BYOK)

A Bring Your Own Key (BYOK) deployment model 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, and key backup

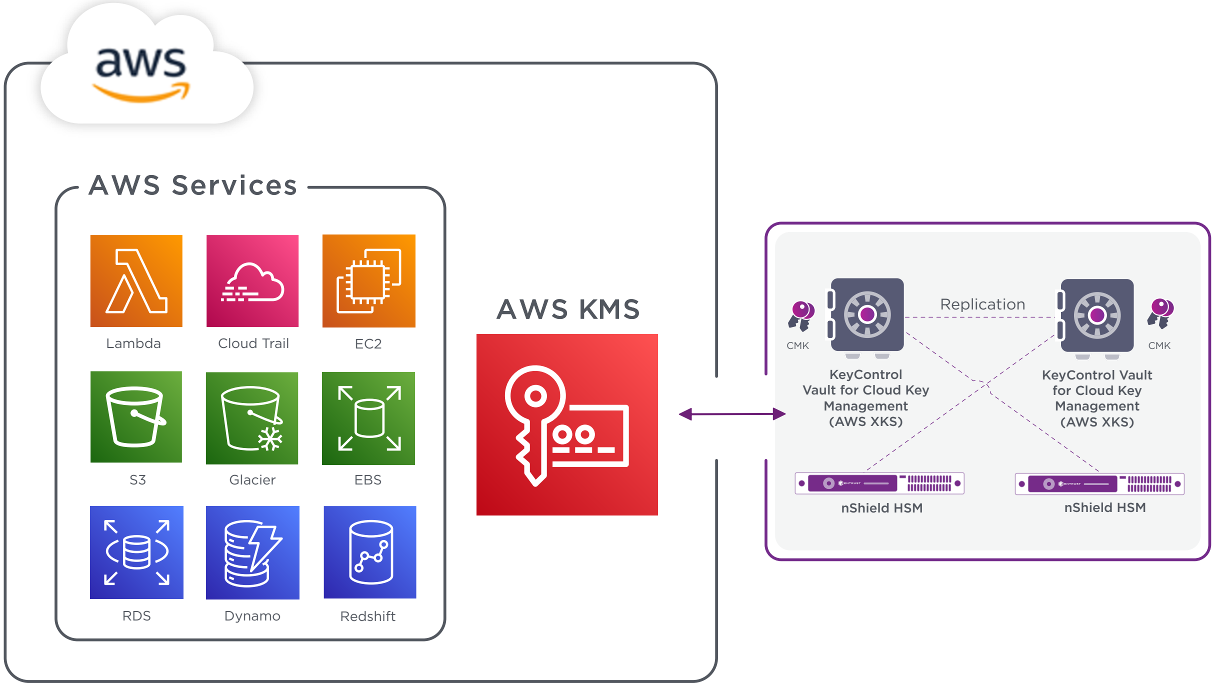
- Bring Your Own Key capability for Microsoft Azure, Google Cloud Platform and AWS (Amazon Web Services) cloud environments to maintain the creation and control of your cryptographic keys

- Provides seamless integration option with FIPS 140-2 Level 3 Entrust nShield® hardware security modules (HSMs) as a hardware root of trust providing high-quality entropy source for key generation.



Hold Your Own Key (HYOK)

Organizations using cloud service provider (CSP) applications but facing regulatory or compliance mandates that require maximum control of their cryptographic keys can choose a HYOK deployment model. An HYOK deployment model enables the end-customer to generate and maintain cryptographic keys throughout their lifecycle, while allowing the CSP to use the keys on your behalf. HYOK shifts the shared responsibility model away from the CSP to the organization, which is responsible for maintaining the HYOK proxy, key vault, and HSM. KeyControl supports AWS KMS XKS and Google EKM HYOK solutions.

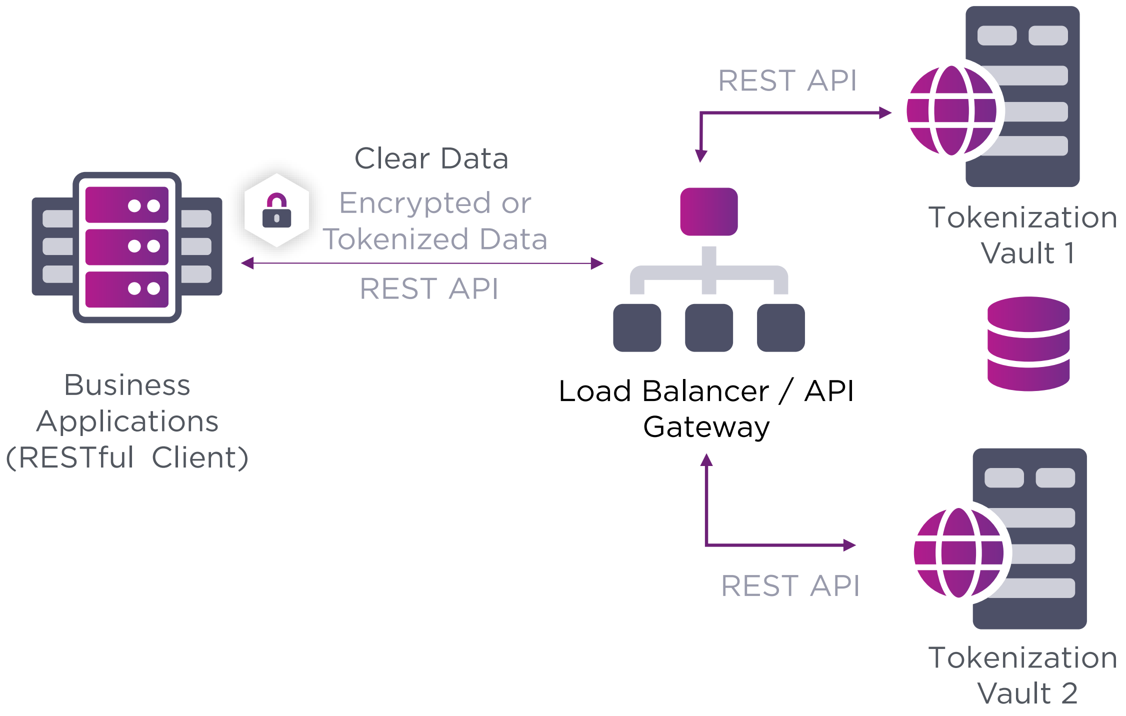


Tokenization Vault

As data security becomes increasingly important, enterprises can protect their sensitive data by using a variety of techniques such as encryption, tokenization, obfuscation, and data masking.

The KeyControl Vault for Tokenization enables organizations to strengthen their data security posture and meet compliance standards like Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST) 800-53, and General Data Protection Regulation (GDPR).

This feature addresses a wide range of data protection use cases by providing data encryption, data tokenization with format-preserving encryption (FPE), data masking, and key management.



CONCLUSION

Enabling decentralized security with centralized visibility

The traditional centralized and monolithic solutions that exist on the market today no longer meet the needs of organizations required to meet demanding data security, regulatory, and compliance needs. Furthermore, with the proliferation of cryptographic keys and secrets organizations need an innovative platform that not only offers a decentralized vault architecture that mitigates against the single point of failure construct, enabling compliance against rigorous data residency or sovereignty regulations while also providing a feature-rich centralized compliance dashboard to monitor and track every facet of a key or secret throughout its lifecycle.

Procedural violations such as using a test key in a production environment will be detected, reported, and remediated. Keys and secrets will no longer be mislaid or difficult to identify and will be securely managed in a FIPS 140-2 Level 1 environment or optionally underpinned by a FIPS 140-2 Level 3 hardware security module root of trust. Every key and secret will be managed throughout its lifecycle. The Who, What, Why, Where, When, and How of keys and secrets will be documented, managed, audited, and controlled. Comprehensive policy and compliance management will enable enterprise information security teams to centrally manage encryption keys for protecting sensitive data across on-premises, multi-cloud, and hybrid environments.

Is your organization seeking a versatile, next-generation key management system? Entrust KeyControl offers decentralized security with centralized visibility across the enterprise's cryptographic asset ecosystem. The flexible vault architecture provides support for a wide range of features and services including KMIP, cloud key management (including BYOK and HYOK deployments), privileged account session management, and tokenization (including secrets management). The powerful feature set ensures data and workloads are protected in line with stringent regulatory compliance and keys and secrets can be geolocated and managed to respect data sovereignty mandates. Choose Entrust KeyControl 10 – redefining cryptographic key management systems.

Separate data sheets are available on request for:

KeyControl Compliance Manager
KeyControl Vault for PASM
KeyControl Vault for KMIP
KeyControl Vault for Databases (Oracle SQL)
KeyControl Vault for Databases (Microsoft SQL Server)
KeyControl Vault for Cloud Key Management (BYOK)
KeyControl Vault for HYOK - AWS XKS
KeyControl Vault for Cloud Key Management (AWS XKS)

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions associated with them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most trusted organizations trust us.

Learn more at
entrust.com

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