KeyControl

Enterprise Key Management and Compliance Platform

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

Introduction 3

KeyControl Overview 5

Compliance Manager 6

- KeyControl Compliance Pack 7

- HSM Integration 7

KeyControl Vaults Overview 8

Vault for KMIP 9

Vault for Secrets Management 10

- Privileged Account and Session Management (PASM) 11

Vault for Databases 12

Vault for Cloud Key Management 13

- Bring Your Own Key 13

- Hold Your Own Key 14

Vault for Tokenization 15

Vault for VM Encryption 16

Conclusion 17

Other Resources 18

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. These solutions also often lack advanced features that enable enterprises to deliver on their compliance mandates and security policy requirements.

Consider the five Ws 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 asks:

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 team in any organization, especially when distributed across different applications, business units, deployment locations, and geographical regions. Traditional key management systems typically offer only basic management of key lifecycles and often lack the ability to add information regarding their usage or intended purpose. System Administrators and professionals from your Security, Compliance, and Risk teams need to have visibility in order to have a firm, canonical understanding of your 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 your enterprise’s cryptographic ecosystem.

The concept of decentralized security refers to a system where an organization’s cryptographic assets are not confined to a single, central repository. Instead, these assets are distributed and located wherever the organization deems appropriate.

This approach not only meets network segmentation and data sovereignty requirements but also ensures that keys are stored within easily manageable and maintainable distributed vaults.

KEY MANAGEMENT AND COMPLIANCE PLATFORM

KeyControl

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

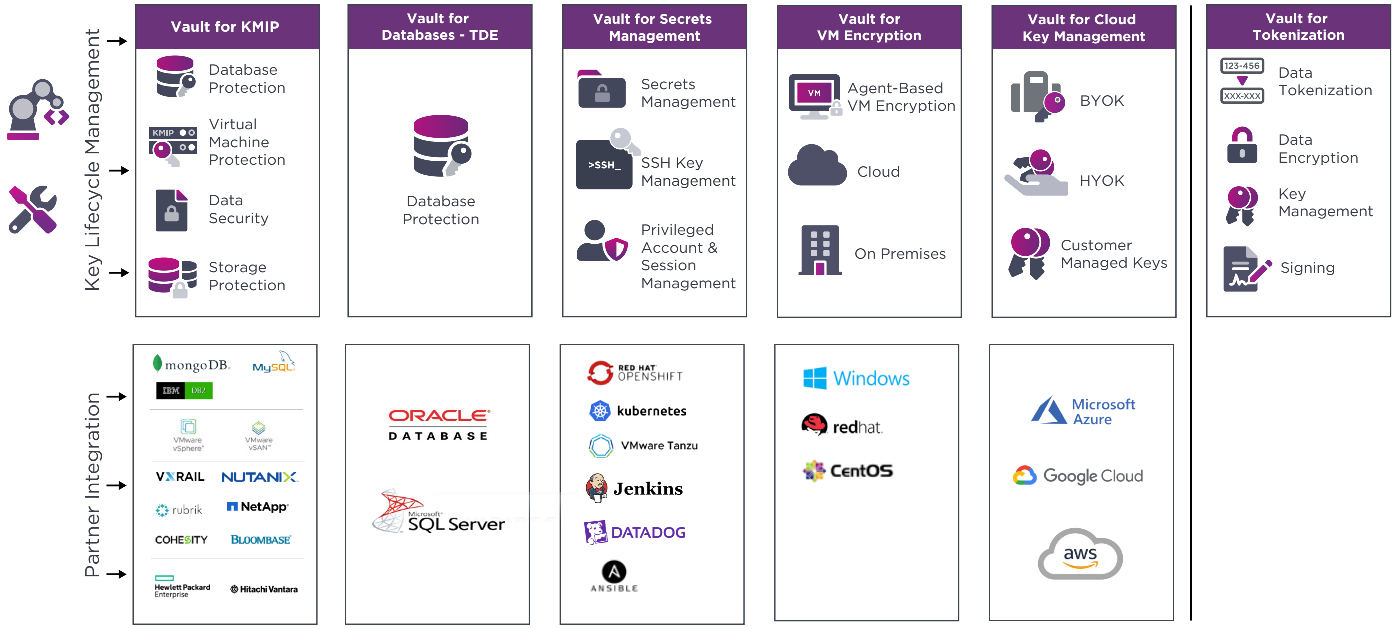
KeyControl

Enterprise Key Lifecycle Management and Compliance Platform

Compliance Manager

Global Compliance Dashboard - Policy Enforcement (NIST 800-57, PCI DSS) -
Key Documentation and Inventory - Audit/Risk

KEYCONTROL VAULTS, USE CASES, AND INTEGRATIONS

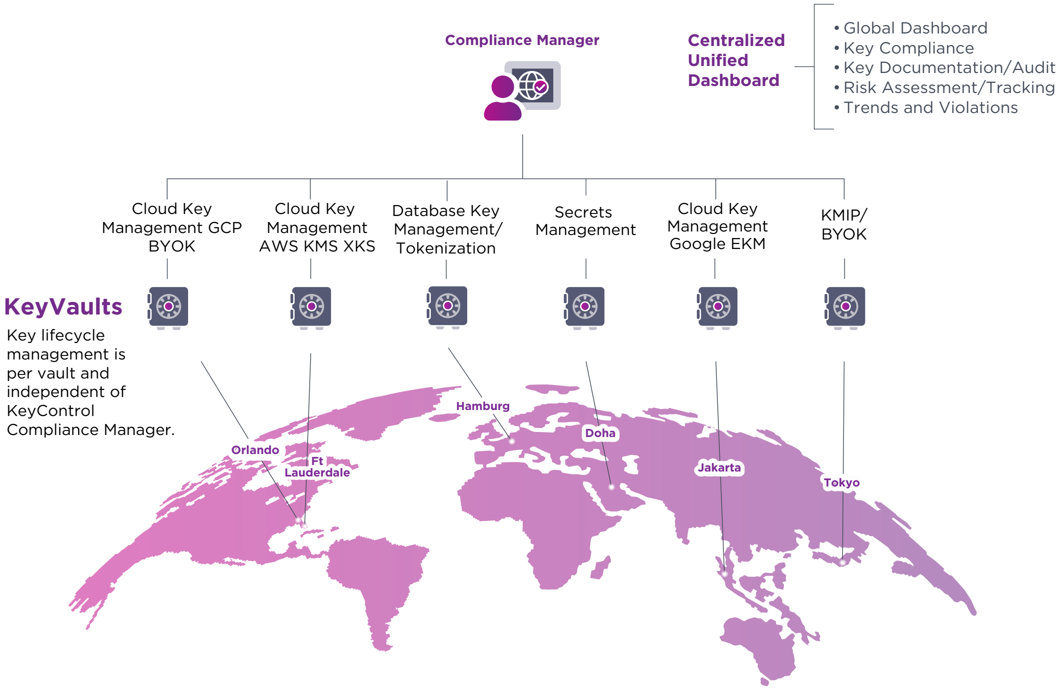


	Vault for KMIP	Vault for Databases - TDE	Vault for Secrets Management	Vault for VM Encryption	Vault for Cloud Key Management	Vault for Tokenization
Key Lifecycle Management	Database Protection Virtual Machine Protection Data Security Storage Protection	Database Protection	Secrets Management SSH Key Management Privileged Account & Session Management	Agent-Based VM Encryption Cloud On Premises	BYOK HYOK Customer Managed Keys	Data Tokenization Data Encryption Key Management Signing
Partner Integration	mongoDB MySQL IBM DB2 VMware vSphere VMware vSAN VXRAIL NUTANIX rubrik NetApp COHESITY BLOOMBASE Hewlett Packard Enterprise Hitachi Vantara	ORACLE DATABASE Microsoft SQL Server	RED HAT OPENSHIFT kubernetes VMware Tanzu Jenkins DATADOG ANSIBLE	Windows redhat CentOS	Microsoft Azure Google Cloud aws	

Learn more about KeyControl at entrust.com

Compliance Manager

At the apex of the KeyControl platform is Compliance Manager, which provides 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.

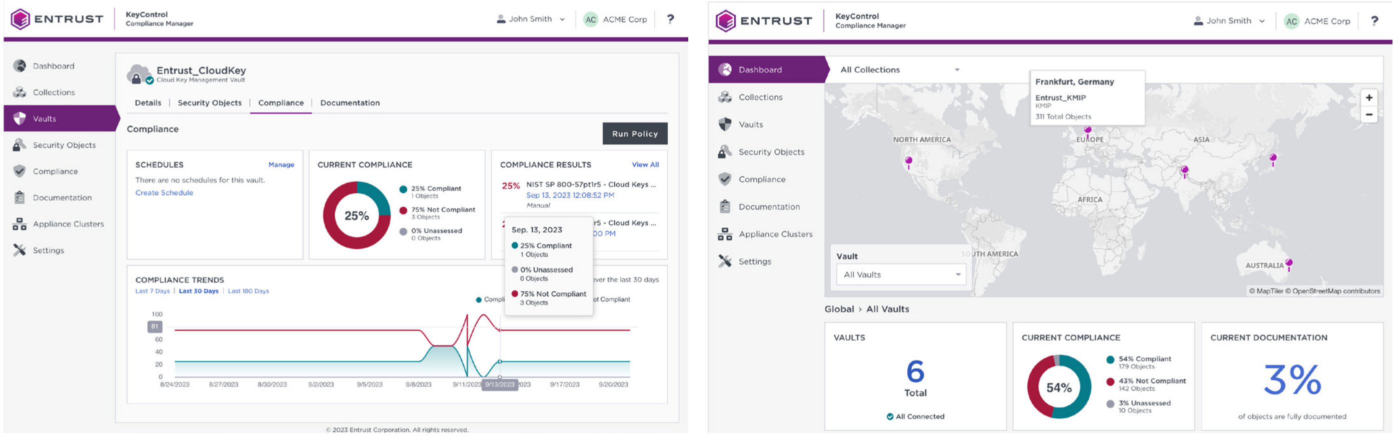

Compliance Manager
Centralized Unified Dashboard
• Global Dashboard
• Key Compliance
• Key Documentation/Audit
• Risk Assessment/Tracking
• Trends and Violations
Cloud Key Management GCP BYOK
Cloud Key Management AWS KMS XKS
Database Key Management/ Tokenization
Secrets Management
Cloud Key Management Google EKM
KMIP/ BYOK
KeyVaults
Orlando
Ft Lauderdale
Hamburg
Doha
Jakarta
Tokyo

Key lifecycle management is per vault and independent of KeyControl Compliance Manager.

Illustration of a typical global organization with a range of key and secret vaults geolocated based on their business and compliance needs.

The Compliance Manager policy engine allows fine-grained control of your cryptographic keys and secrets and provides all the answers to the five Ws and the H discussed on page 3, 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 Compliance Managers can easily be configured, for example, to isolate U.S., EMEA, and APAC regions or by organizational locations.

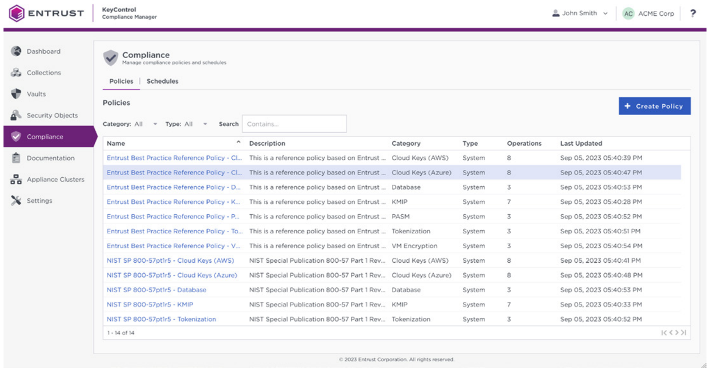
While the Compliance Manager provides a comprehensive dashboard of key and secrets metadata, day-to-day key lifecycle management is decentralized to the key vaults and is not in the purview of Compliance Manager. Keys (even as encrypted tokens) never leave their vaults except to authorized endpoints.



The Compliance Manager dashboard shows a granular level of compliance and global distribution of key vaults as well as metadata documentation.

KeyControl Compliance Pack

The Compliance Pack offers a set of customizable documentation forms that can help fill any gaps in your 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 (KMIP keys, TDE keys, and API keys, for example). Compliance Manager is a prerequisite for all KeyControl deployments. KeyControl Compliance Pack purchases are optional, offering a template to specific standards.



Policies

Name	Description	Category	Type	Operations	Last Updated
Entrust Best Practice Reference Policy - Cl...	This is a reference policy based on Entrust ...	Cloud Keys (AWS)	System	8	Sep 05, 2023 05:40:39 PM
Entrust Best Practice Reference Policy - Cl...	This is a reference policy based on Entrust ...	Cloud Keys (Azure)	System	8	Sep 05, 2023 05:40:47 PM
Entrust Best Practice Reference Policy - D...	This is a reference policy based on Entrust ...	Database	System	3	Sep 05, 2023 05:40:53 PM
Entrust Best Practice Reference Policy - K...	This is a reference policy based on Entrust ...	KMIP	System	7	Sep 05, 2023 05:40:28 PM
Entrust Best Practice Reference Policy - P...	This is a reference policy based on Entrust ...	PASM	System	3	Sep 05, 2023 05:40:52 PM
Entrust Best Practice Reference Policy - To...	This is a reference policy based on Entrust ...	Tokenization	System	3	Sep 05, 2023 05:40:51 PM
Entrust Best Practice Reference Policy - V...	This is a reference policy based on Entrust ...	VM Encryption	System	3	Sep 05, 2023 05:40:54 PM
NIST SP 800-57pt1r5 - Cloud Keys (AWS)	NIST Special Publication 800-57 Part 1 Rev...	Cloud Keys (AWS)	System	8	Sep 05, 2023 05:40:41 PM
NIST SP 800-57pt1r5 - Cloud Keys (Azure)	NIST Special Publication 800-57 Part 1 Rev...	Cloud Keys (Azure)	System	8	Sep 05, 2023 05:40:48 PM
NIST SP 800-57pt1r5 - Database	NIST Special Publication 800-57 Part 1 Rev...	Database	System	3	Sep 05, 2023 05:40:53 PM
NIST SP 800-57pt1r5 - KMIP	NIST Special Publication 800-57 Part 1 Rev...	KMIP	System	7	Sep 05, 2023 05:40:33 PM
NIST SP 800-57pt1r5 - Tokenization	NIST Special Publication 800-57 Part 1 Rev...	Tokenization	System	3	Sep 05, 2023 05:40:52 PM

1 - 14 of 14

© 2023 Entrust Corporation. All rights reserved.

View of the Compliance Manager dashboard detailing Compliance Pack templates applied to specific vaults.

nShield HSM Integration

KeyControl is certified to FIPS 140-2 Level 1. For organizations requiring higher levels of assurance, KeyControl can be seamlessly integrated with a FIPS 140-2 Level 3 Entrust nShield® Hardware Security Module HSM. The optional HSM is used to protect the master key for the KeyControl virtual appliance. It's also used in the process when generating cryptographic keys, ensuring high-quality entropy from the HSM's random number generator is used in keys created and managed by KeyControl vaults irrespective of which vault type is deployed.

KeyControl Vaults

The Entrust KeyControl platform offers a flexible way to architect and deploy key and secrets 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 high level of security.

Unlike many traditional key management solutions that only offer a single, monolithic, centralized repository for storing keys, the vaults in the KeyControl platform 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 while providing convenient, easily manageable vaults and simplifying maintenance and disaster-recovery operations.

The KeyControl distributed architecture simplifies maintenance tasks, reducing the complexity of operations such as upgrades and backup/restore and readily supporting scenario planning activities such as disaster recovery. Key vaults can be isolated without facing the scheduling challenge, risk, and unpredictability of taking your entire organization's KMS off-line and then back online, thereby lowering the risk of service disruptions.

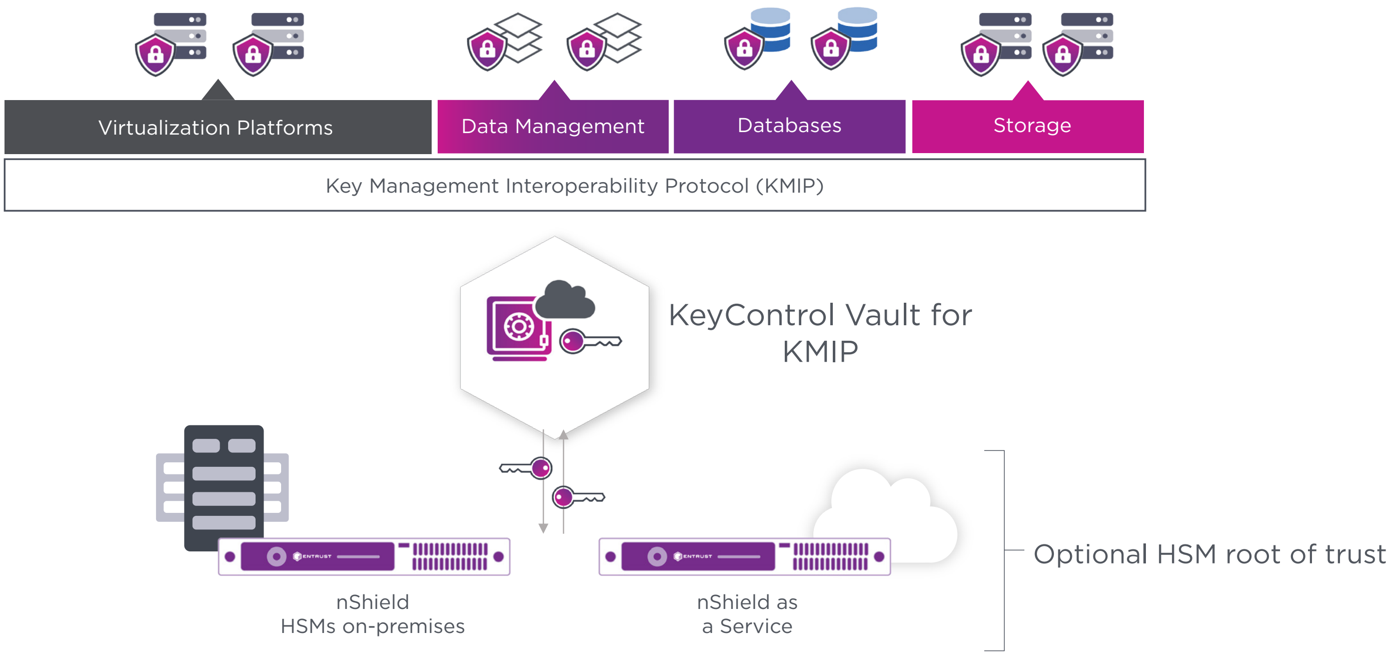
Another advantage of the KeyControl vault-based architecture is the ability to manage keys in segmented environments, preventing data transfer between network segments. This makes the vault architecture attractive to organizations that perform critical infrastructure operations or process sensitive data, such as via payment systems.

KeyControl Vaults provides cost-effective key packs per vault, meaning you only pay for what you need. There is no heavy capital investment required to get you up and running. Increase your quantity of key packs as your deployment needs grow and extend into other use cases in the KeyControl ecosystem.

The flexible vault architecture provides support for a wide range of services as described in the following pages.

KeyControl Vault for KMIP

Key Management Interoperability Protocol (KMIP) is a widely adopted protocol for handling cryptographic keys and secrets for virtualization solutions, databases, endpoints, applications, storage appliances, cloud solutions, and much more. KeyControl provides universal key management for KMIP clients with its 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 virtual machines, and a wide range of other KMIP-compatible products such as NetApp, Nutanix, IBM Db2, Rubrik, Cohesity, Bloombase, HPE, Hitachi Vantara, and MongoDB.



KeyControl Vault for Secrets Management

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

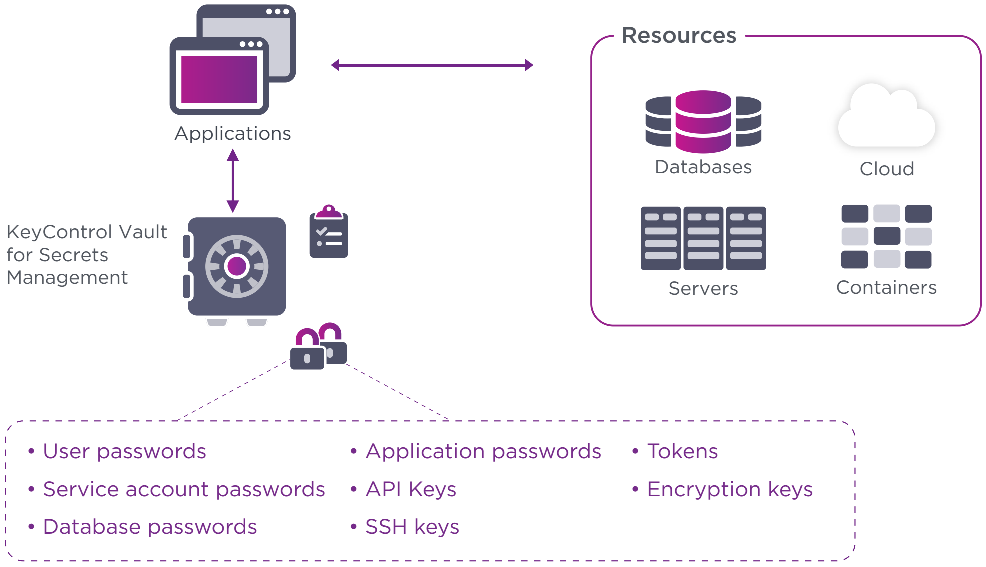
The absence of any centralized secret management tool makes it challenging to answer the "5 W" questions: What secret, Why, Where, When, and by Whom was it accessed? KeyControl Vault for Secrets Management protects, manages, and secures access to secrets, proactively enforcing security policies and auditing 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:

- User passwords
- Service account passwords
- Database passwords
- Application passwords
- API keys
- SSH keys
- Tokens
- Encryption keys

The KeyControl Vault for Secrets Management 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 Secrets Management.



KeyControl Vault for Secrets Management offers a range of cloud-native and DevOps integrations, including:

- **Tools/Toolchains:** Ansible, Jenkins, Datadog
- **PaaS/Container Orchestration:** Kubernetes, Red Hat OpenShift, VMware Tanzu

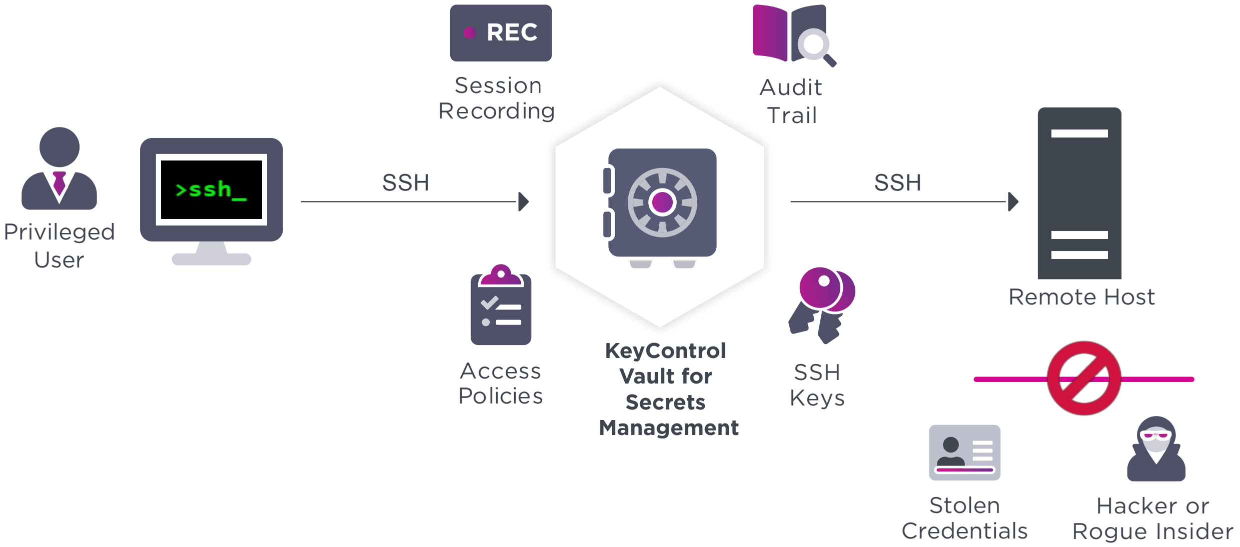
Privileged Account and Session Management (PASM)

Privileged accounts often accessed 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 Secrets Management enables your organization 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 by whitelisting approved users and actions while recording privileged user activity across virtual, cloud, and physical environments – creating a granular, immutable audit trial of those accessing the system.

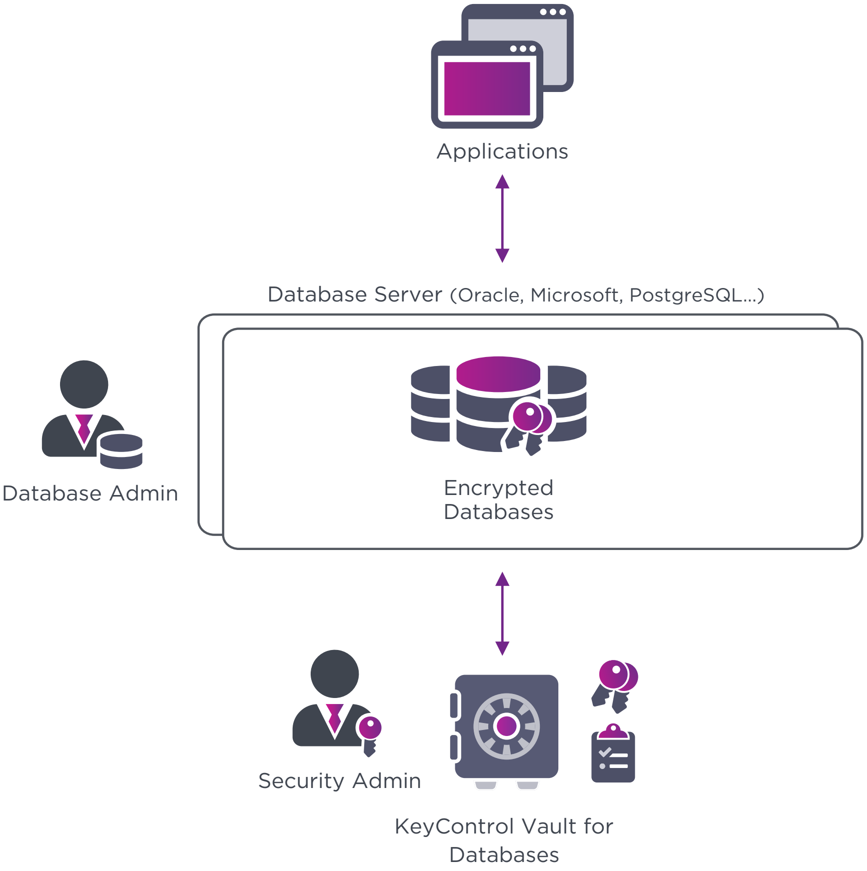
KeyControl simplifies the management of SSH access by leveraging corporate identity and access management (IAM) systems and automating the lifecycle of SSH keys, including key storage, backup, rotation, and key revocation.



KeyControl Vault for Databases

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 from the database using hardware protection.

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.


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

KeyControl Vault for Cloud Key Management

KeyControl Vault for Cloud Key Management can help your organization maximize control of your cryptographic keys and encrypted data while leveraging the services of the cloud. There are two deployment models:

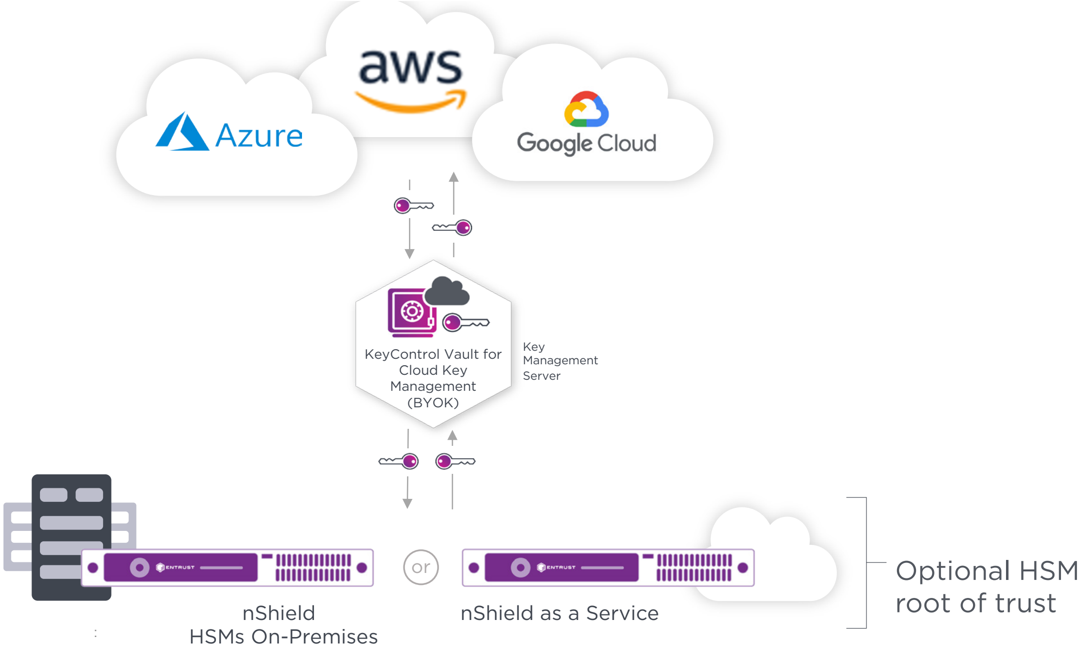
Bring Your Own Key (BYOK)

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
  - key backup

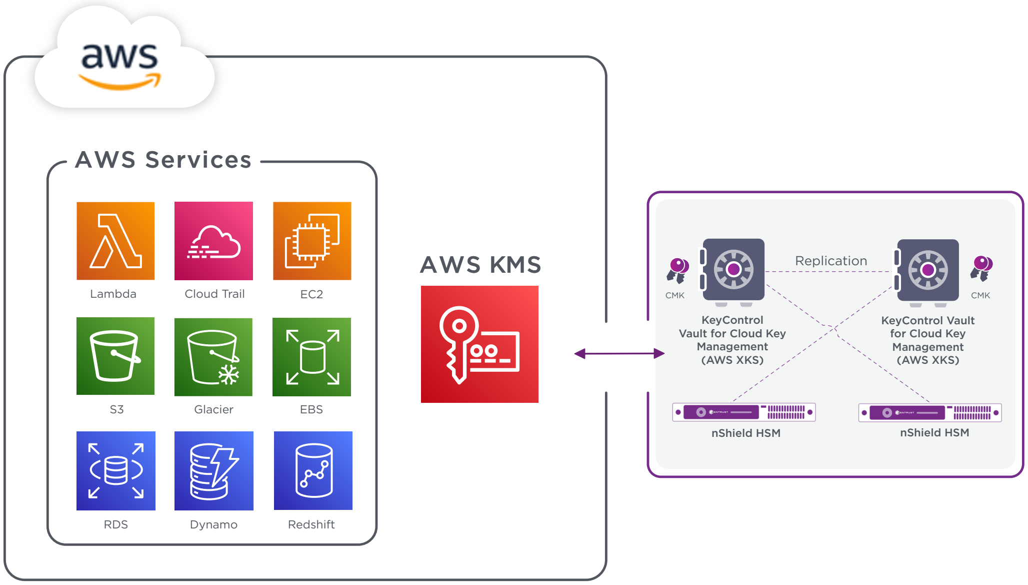
- BYOK capability for Microsoft Azure, Google Cloud Platform, and AWS (Amazon Web Services) cloud environments maintains the creation and control of your cryptographic keys

- Seamless integration option with FIPS 140-2 Level 3 Entrust nShield® Hardware Security Modules (HSMs) as a hardware root of trust provides high-quality entropy source for key generation

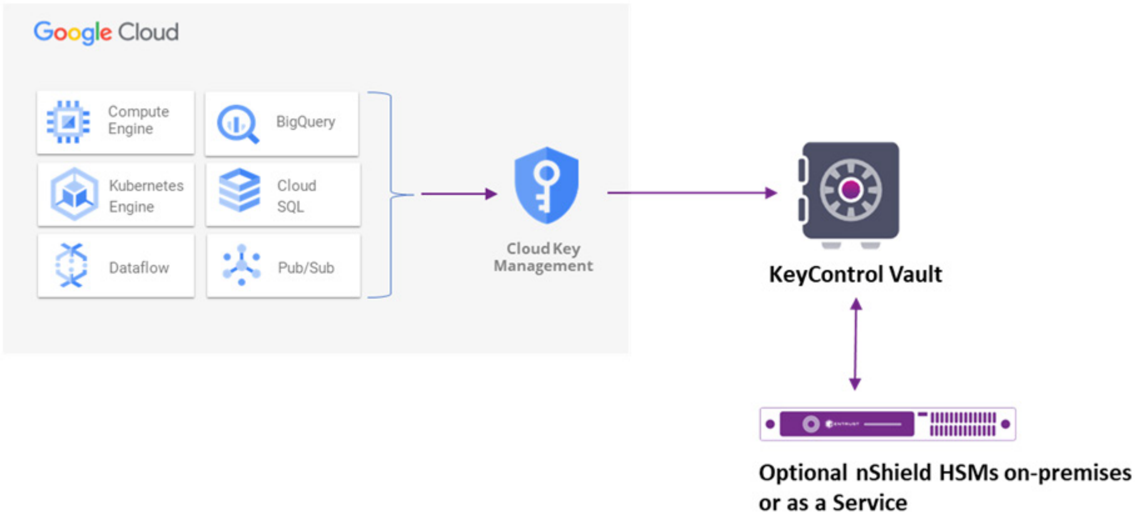


Hold Your Own Key (HYOK)

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. This model enables you 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 your organization, which is responsible for maintaining the HYOK proxy, key vault, and HSM. KeyControl supports Microsoft DKE, AWS KMS XKS, and Google EKM, which are the respective HYOK implementations of Azure, AWS, and Google.



HYOK deployment for AWS KMS XKS



HYOK deployment for Google EKM

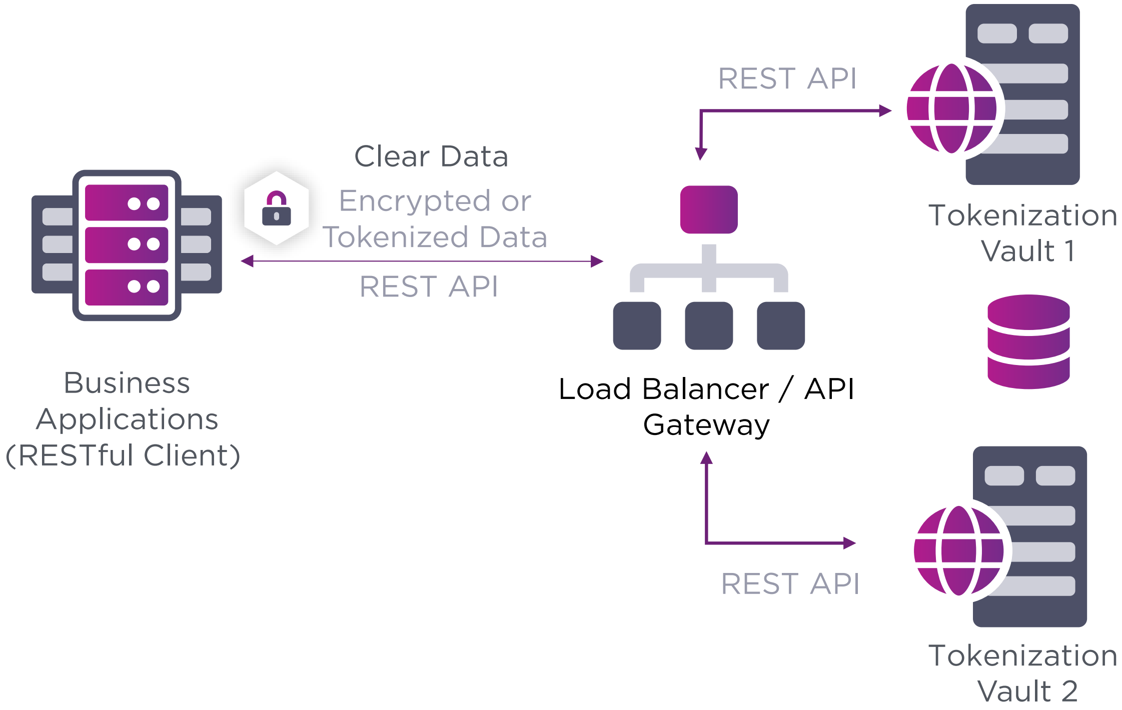
KeyControl Vault for Tokenization

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

The KeyControl Vault for Tokenization enables you to strengthen your data security posture and meet compliance standards such as:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- National Institute of Standards and Technology (NIST) 800-53
- General Data Protection Regulation (GDPR)

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

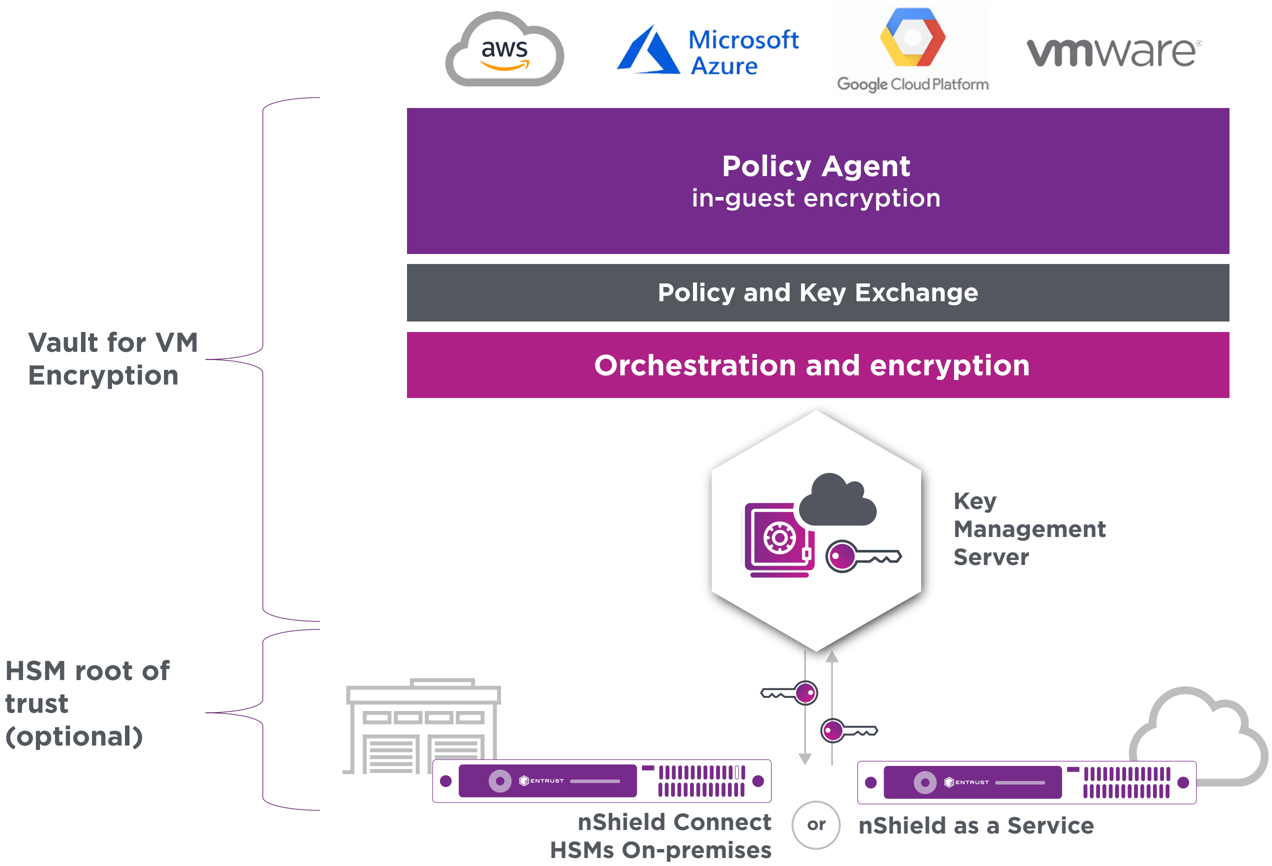

REST API
Clear Data
Encrypted or Tokenized Data
REST API
Tokenization Vault 1
Business Applications (RESTful Client)
Load Balancer / API Gateway
REST API
Tokenization Vault 2

KeyControl Vault for Virtual Machine (VM) Encryption

Entrust KeyControl Vault for VM Encryption provides agent-based, in-guest encryption and key management for virtual machines located in data centers and private, public, or hybrid cloud environments. It secures multicloud workloads throughout their lifecycle and reduces the complexity of protecting workloads across multiple cloud platforms.

KeyControl provides:

- Granular encryption for better security. The protection boundary does not stop at the hypervisor or at the data store; VMs are individually encrypted. Inside the VM, unique keys can be assigned to encrypt each partition, including the boot (OS) disk and swap partitions.
- Robust policy-based access controls to enforce separation of duties across different user personas. You can prevent root users or system administrators from accessing sensitive data by enforcing access controls on encrypted volumes.
- Deduplication support with a unique approach that offers AES 256-bit encryption while maintaining 91% of storage deduplication benefit.



CONCLUSION

Enabling decentralized security with centralized visibility

With the proliferation of cryptographic keys and secrets, traditional centralized and monolithic solutions no longer meet the needs of organizations required to meet demanding data security, regulatory, and compliance requirements. Policy violation, like using a test key in a production environment, must be swiftly detected, reported, and remediated. Keys and secrets should not be mislaid or challenging to identify. They should be securely managed in a FIPS 140 Level 1 environment or, optionally, underpinned by a FIPS 140 Level 3 HSM as the root of trust. It should be possible to manage keys and secrets throughout their entire lifecycle via a decentralized vault architecture to meet the requirements of regional regulations.

Every aspect of keys and secrets – including the Who, What, Why, Where, When, and How – need to be documented, managed, audited, and controlled. A comprehensive policy and compliance management system should enable enterprise information security teams to centrally manage encryption keys for protecting sensitive data across on-premises, multi-cloud, and hybrid environments. Organizations need an innovative platform that offers a flexible approach for mitigating against the single point of failure constructs, 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.

Entrust KeyControl offers decentralized security with centralized visibility across your entire cryptographic asset ecosystem. The flexible vault architecture provides support for a wide range of features and services, and 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.

Want more information?

Click on the titles below to download data sheets.

KeyControl Overview

KeyControl Compliance Manager

KeyControl Compliance Pack

KeyControl Vault for Secrets Management

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 Cloud Key Management (AWS XKS)

KeyControl Vault for VM Encryption

KeyControl Vault for Tokenization

To complement KeyControl, Entrust offers a range of solutions in digital certificates/ PKI, identity, policy enforcement, role-based access control, and compliance to help you solve complex business issues while reducing risk.

Please contact us to learn more.

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

ENTRUST

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