SOLUTION BROCHURE

Entrust Cryptographic Security Platform

Key and Secrets Management

ENTRUST

SECURING A WORLD IN MOTION

Contents

Introduction 3

Cryptographic Security Platform Deployment Options

Cryptographic Security Platform Overview 5

Compliance Manager 6

Cryptographic Security Platform Compliance Pack
nShield HSM Integration

Cryptographic Security Platform Vaults 8

Vault for KMIP
Vault for Secrets
Vault for Databases
Vault for Cloud Keys
Vault for Application Security
Vault for VM Encryption

Conclusion 17

INTRODUCTION

Redefining Cryptographic Key and Secrets Management

As enterprises use cryptographic keys and secrets at scale to protect applications, workloads, and data, traditional key management solutions often struggle with tracking and controlling the use of keys or secrets 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 can we get regular risk reporting on our cryptographic assets for non-compliance?
- 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.

The Entrust Cryptographic Security Platform, deployed on premises or as a service, redefines cryptographic key management by combining traditional key lifecycle management and a decentralized vault-based architecture with centralized visibility and governance. 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 flexible approach not only meets stringent security and data sovereignty requirements but also is better suited to the complex infrastructures of organizations. For instance, vaults are better adapted to network segmentation needs or the requirement to delegate vault management to distinct entities or different business activities.

Deployment Options

To meet the requirements of the market, the Cryptographic Security Platform can be deployed on premises, as a service, or as a hybrid solution.

The on-premises Cryptographic Security Platform combines traditional key lifecycle management with comprehensive central policy and compliance management. To implement the on-premises Cryptographic Security Platform, the customer will need to purchase, provision, configure, and maintain an on-premises environment.

Cryptographic Security Platform Key and Secrets Management as a Service, available in the U.S. and European regions, provides a cloud-based solution. It combines traditional key lifecycle management with comprehensive central policy and compliance management, streamlining your operations by eliminating the need to purchase, provision, configure, and maintain an on-premises environment.

Both deployment options provide seamless integration with various applications and cloud services, allowing organizations to efficiently meet compliance requirements, regulatory mandates, and industry best practices for data security.

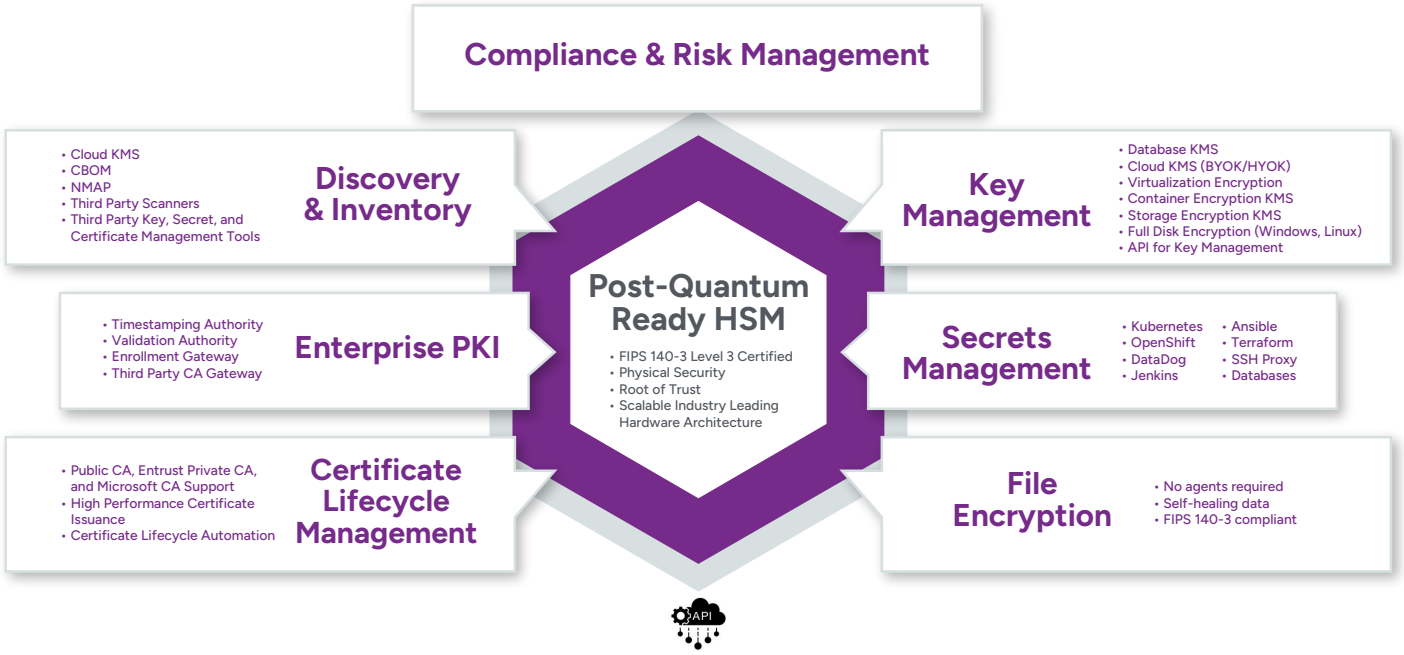
Additionally, both deployment options are compatible with FIPS 140-3 certified nShield Hardware Security Modules (HSMs) and third-party HSMs, ensuring robust root of trust protection.

KEY MANAGEMENT AND COMPLIANCE PLATFORM

Cryptographic Security Platform Overview

Entrust's Cryptographic Security Platform is an innovative solution that unifies cryptographic management by combining the rich capabilities to operate PKI, Certificate Lifecycle Management, Key and Secrets Management, and HSMs all from a single, cohesive system.

This platform addresses the growing need for comprehensive cryptographic asset management in an increasingly complex digital landscape. By integrating these critical components, the Cryptographic Security Platform offers unparalleled security, compliance, and operational efficiency for organizations dealing with securing an increasing number of machine identities, protecting sensitive data and navigating complex cryptographic requirements.



Compliance Manager

Entrust Compliance Manager provides a single, unified dashboard that allows you to view and monitor your organization's cryptographic assets located in Key and Secrets Management Vaults. The Compliance Manager inventories keys, secrets, and certificates distributed across your infrastructure, whether stored in vaults or managed by third-party solutions.

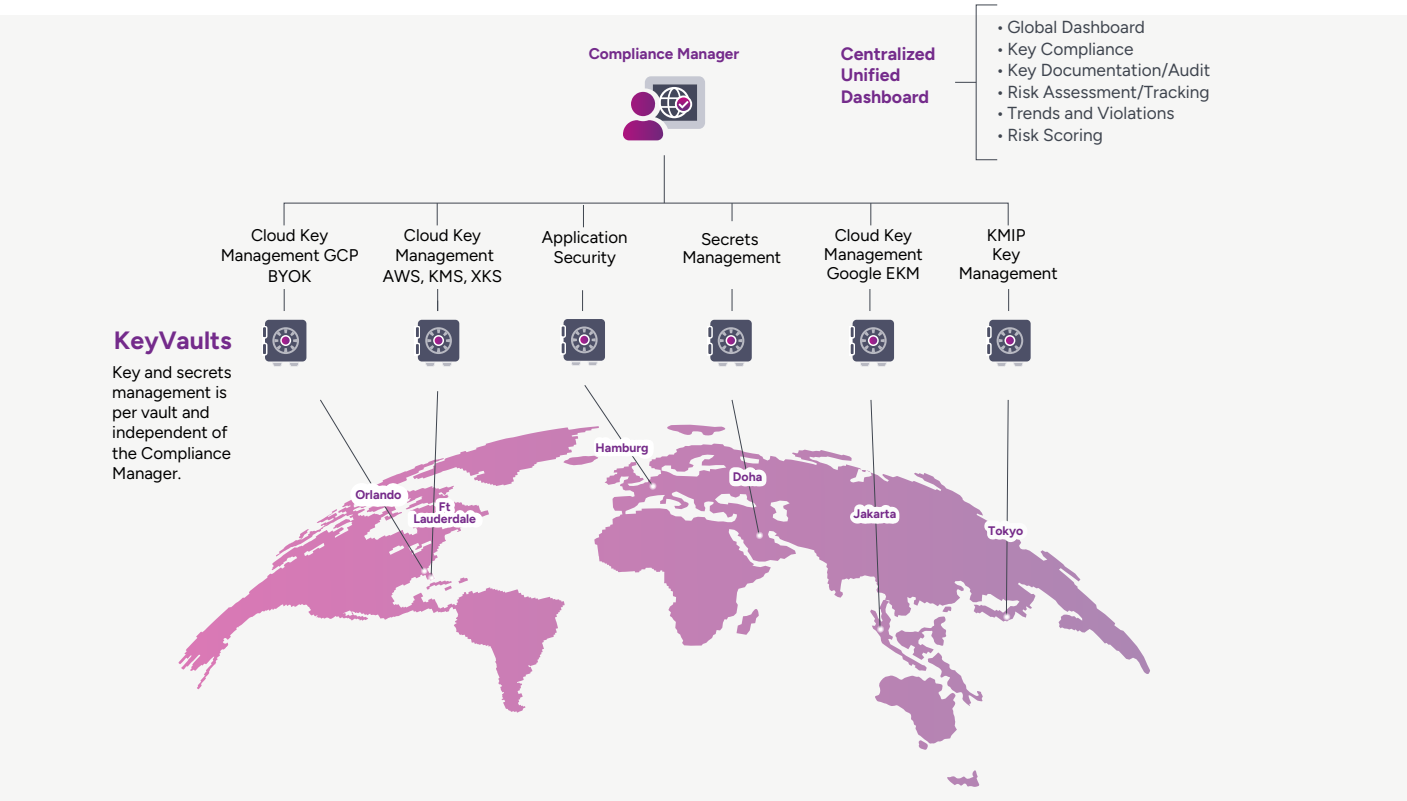
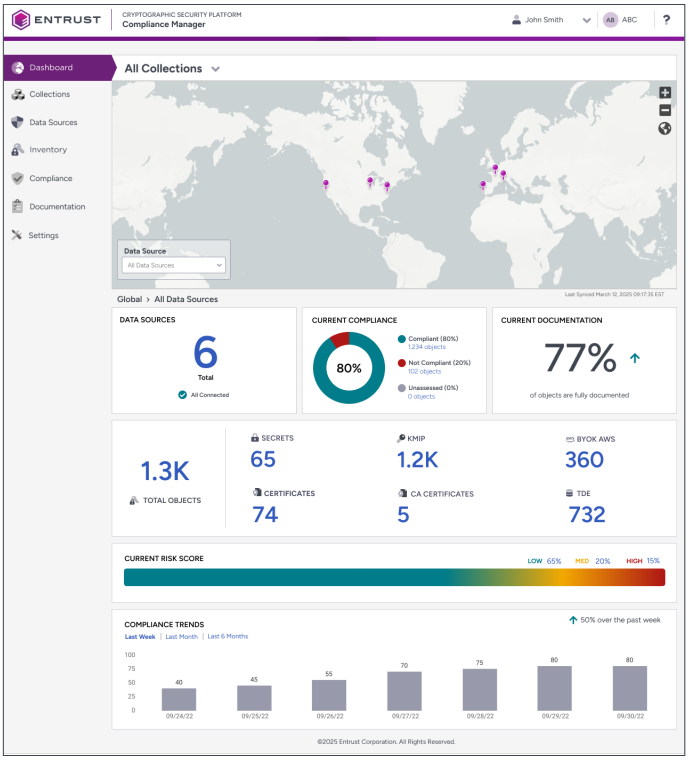
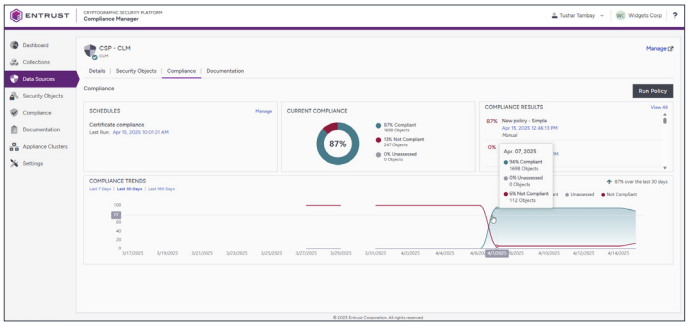


Illustration of a typical global organization with a range of key and secret vaults geolocated based on their business and compliance needs.

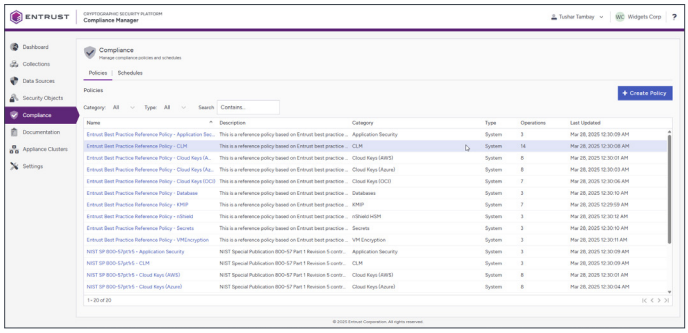
The Compliance Manager policy engine allows fine-grained control of your cryptographic assets and provides all the answers to the five Ws and the H discussed on page 3, offering full visibility, traceability, compliance tracking, risk scoring, and an immutable audit trail of cryptographic assets. If 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 inventory of keys, secrets, and certificates metadata, day-to-day cryptographic asset lifecycle management is decentralized to the vaults and is not in the purview of Compliance Manager. Keys and secrets (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.



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

Compliance and Policy Management

Compliance Manager enables organizations to assess the compliance of keys, secrets, and certificates with regulations, standards, or corporate policies. It provides a set of built-in compliance policies to evaluate various key types, such as KMIP keys, TDE keys, and API keys. Organizations can also define their own custom policies to meet their specific security needs.

nShield HSM Integration

For organizations requiring higher levels of assurance, the Cryptographic Security Platform can be seamlessly integrated with a FIPS 140-3 Level 3 Entrust nShield® Hardware Security Module (HSM). The optional HSM is used to protect the master keys for the Cryptographic Security Platform. 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 Cryptographic Security Platform vaults irrespective of which vault type is deployed.

Cryptographic Security Platform Vaults

The Entrust Cryptographic Security Platform offers a flexible way to architect and deploy keys 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 or secret management solutions that only offer a single, monolithic, centralized repository for storing keys, the vaults in the 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 regional or national boundaries while providing convenient, easily manageable vaults and simplifying maintenance and disaster-recovery operations.

The Cryptographic Security Platform 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 activities. 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.

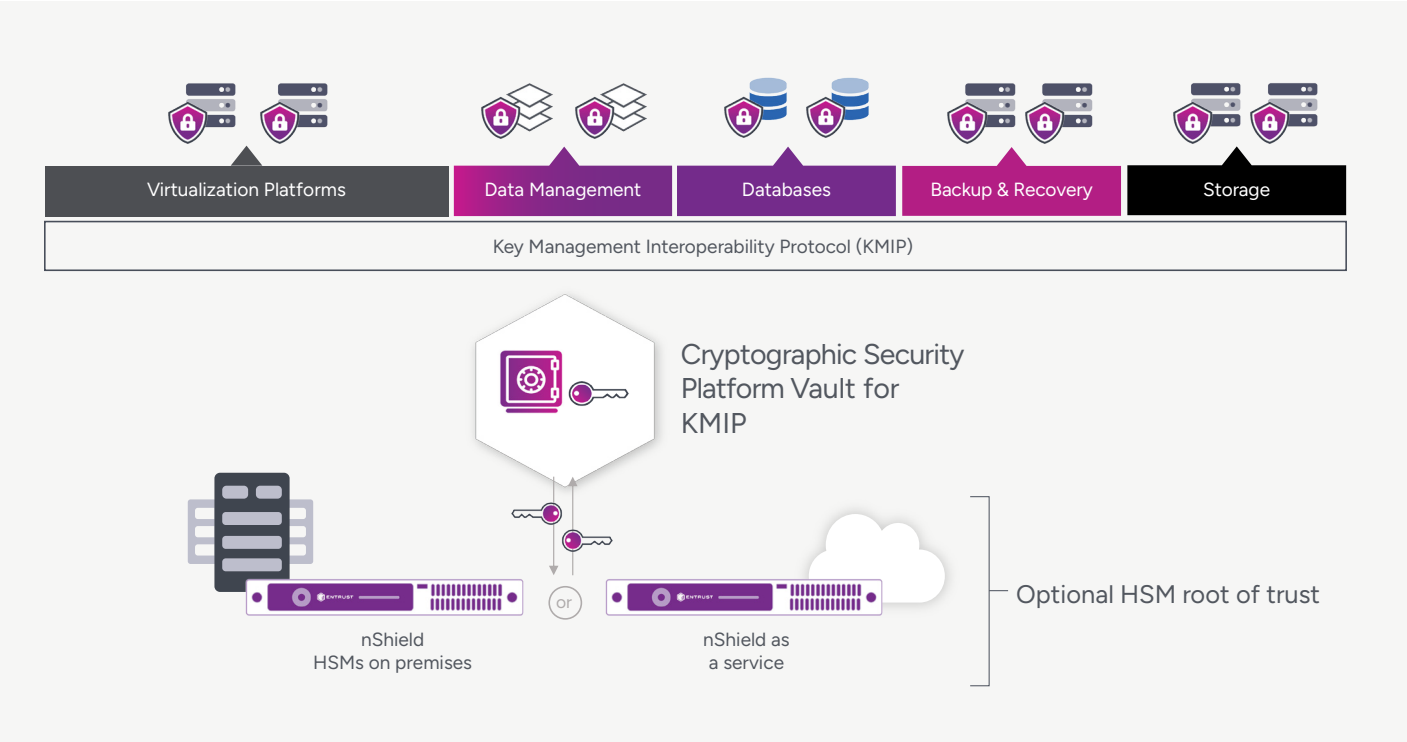
Another advantage of the Cryptographic Security Platform vault-based architecture is the ability to manage keys and secrets in segmented environments, preventing data transfer between network segments. This makes the vault architecture attractive to organizations that perform critical infrastructure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

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

The platform supports a wide range of use cases and integrations with leading vendors in databases, cloud keys, VM encryption, storage, backup and recovery, and more as illustrated below.

Cryptographic Security Platform 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. The Cryptographic Security Platform 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.



Cryptographic Security Platform for KMIP

Backup and Recovery Use Case

Entrust Cryptographic Security Platform Key and Secrets Management integrates with a wide range of commonly used backup and recovery applications, providing key management via the KMIP open standard.

For organizations requiring higher levels of assurance, the platform seamlessly integrates with a FIPS 140-3 Level 3 Entrust nShield® Hardware Security Module (HSM). This optional HSM protects the master key for the platform's KMIP vault. It also helps to ensure high-quality entropy from the random-number generator when used in keys created and managed by the platform's vaults – regardless of which vault type is deployed.

The HSM also protects the Key Encryption Key (KEK), which adds an extra layer of security by encrypting all individual KMIP objects within each KMIP vault. When an HSM is deployed, each KMIP vault is assigned a KEK generated in the HSM, which wraps all KMIP objects in the vault.

Cryptographic Security Platform Vault for Secrets

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.

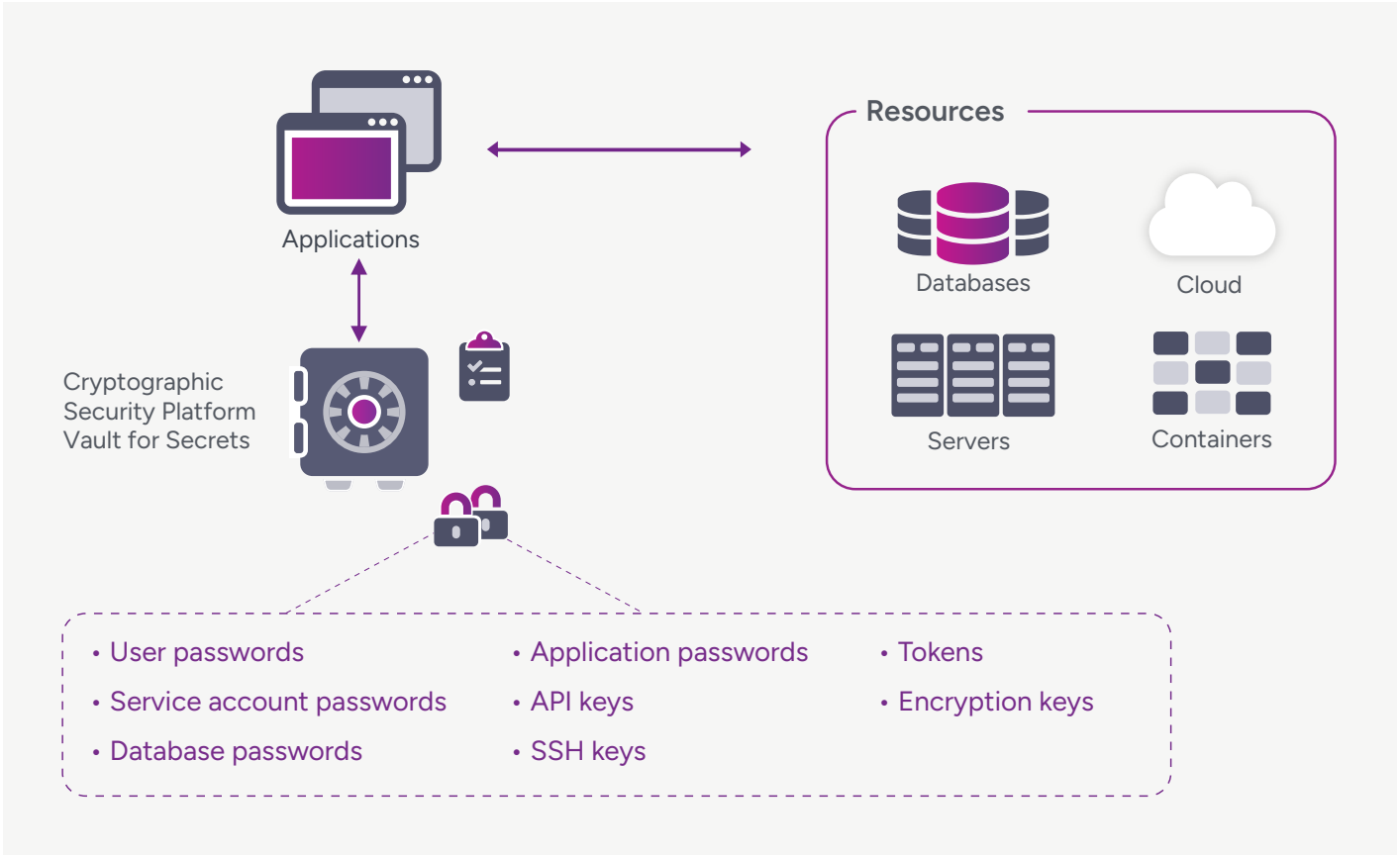
The absence of any centralized secret management tool makes it challenging to answer the "5 W" questions: What secret, Why, Where, When, and by Whom was it accessed? Cryptographic Security Platform Vault for Secrets protects, manages, and secures access to secrets, proactively enforcing security policies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

The following secrets and other sensitive data are stored in a vault:

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

The Cryptographic Security Platform Vault for Secrets 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 Cryptographic Security Platform Vault for Secrets.



Cryptographic Security Platform Vault for Secrets offers a range of cloud-native and DevOps integrations, including:

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

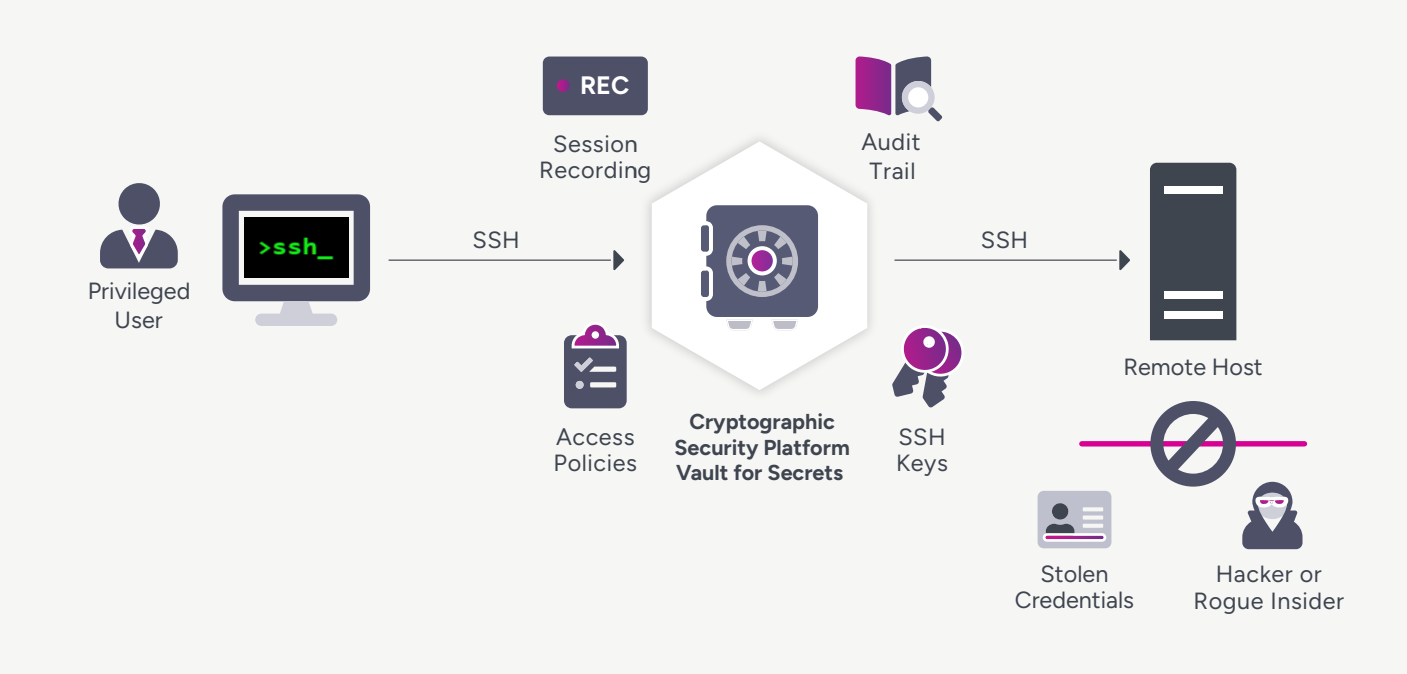
Privileged Account and Session Management (PASM)

Privileged accounts 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.

Cryptographic Security Platform Vault for Secrets enables your organization to rigorously control SSH access and usage of administrative and privileged accounts. Unique to the Cryptographic Security Platform, its proxy design means your organization's valuable SSH keys are never accessible to privileged users.

The Cryptographic Security Platform, deployed on premises or as a service, 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.

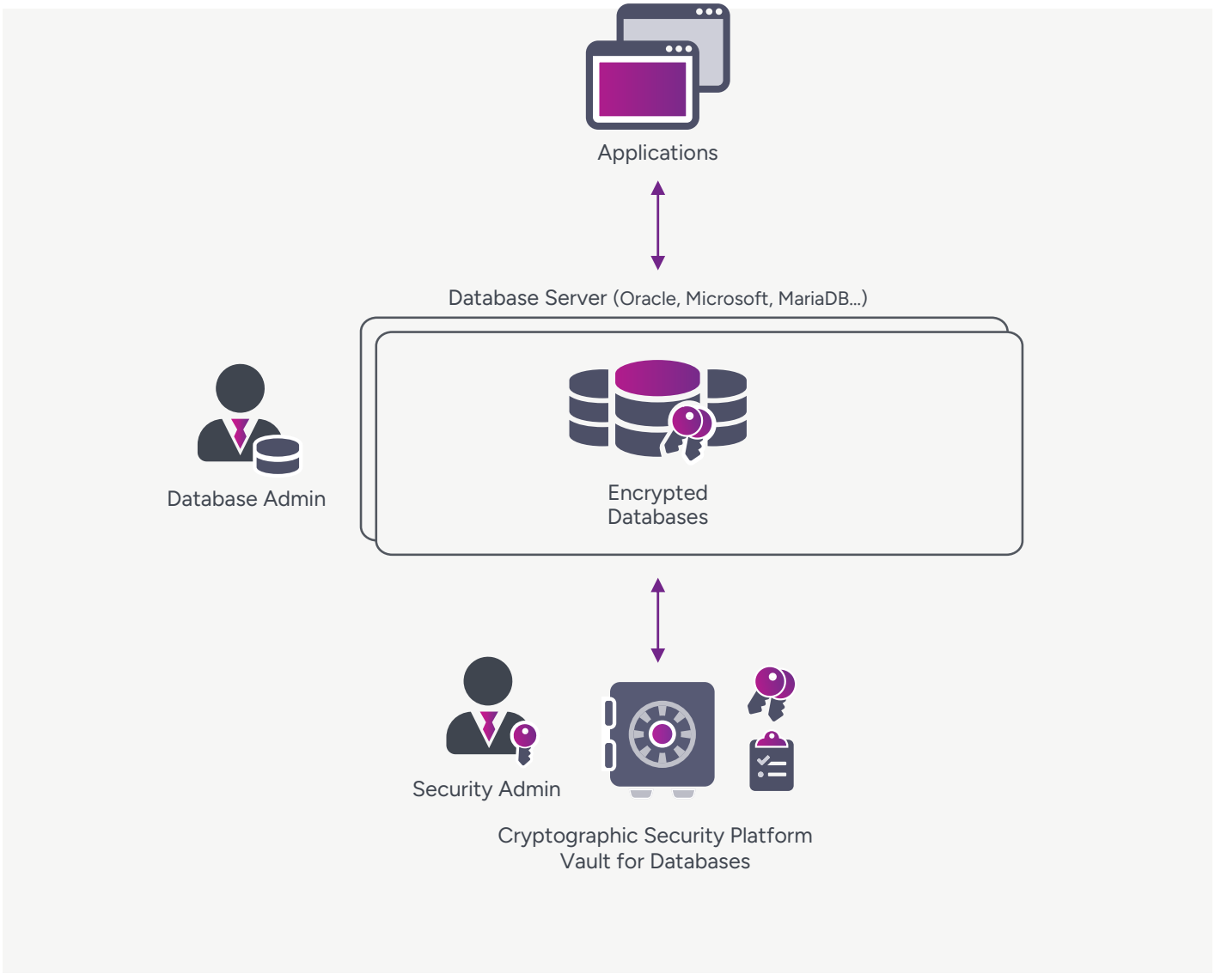
The Cryptographic Security Platform simplifies the management of SSH access by leveraging corporate identity and access management (IAM) systems and automating the lifecycle of SSH keys, including key storage, backup, rotation, and key revocation.



Cryptographic Security Platform for Databases

Cryptographic Security Platform Vault for Databases provides key lifecycle management for encrypted 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. The Cryptographic Security Platform 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, MariaDB, and Oracle databases.



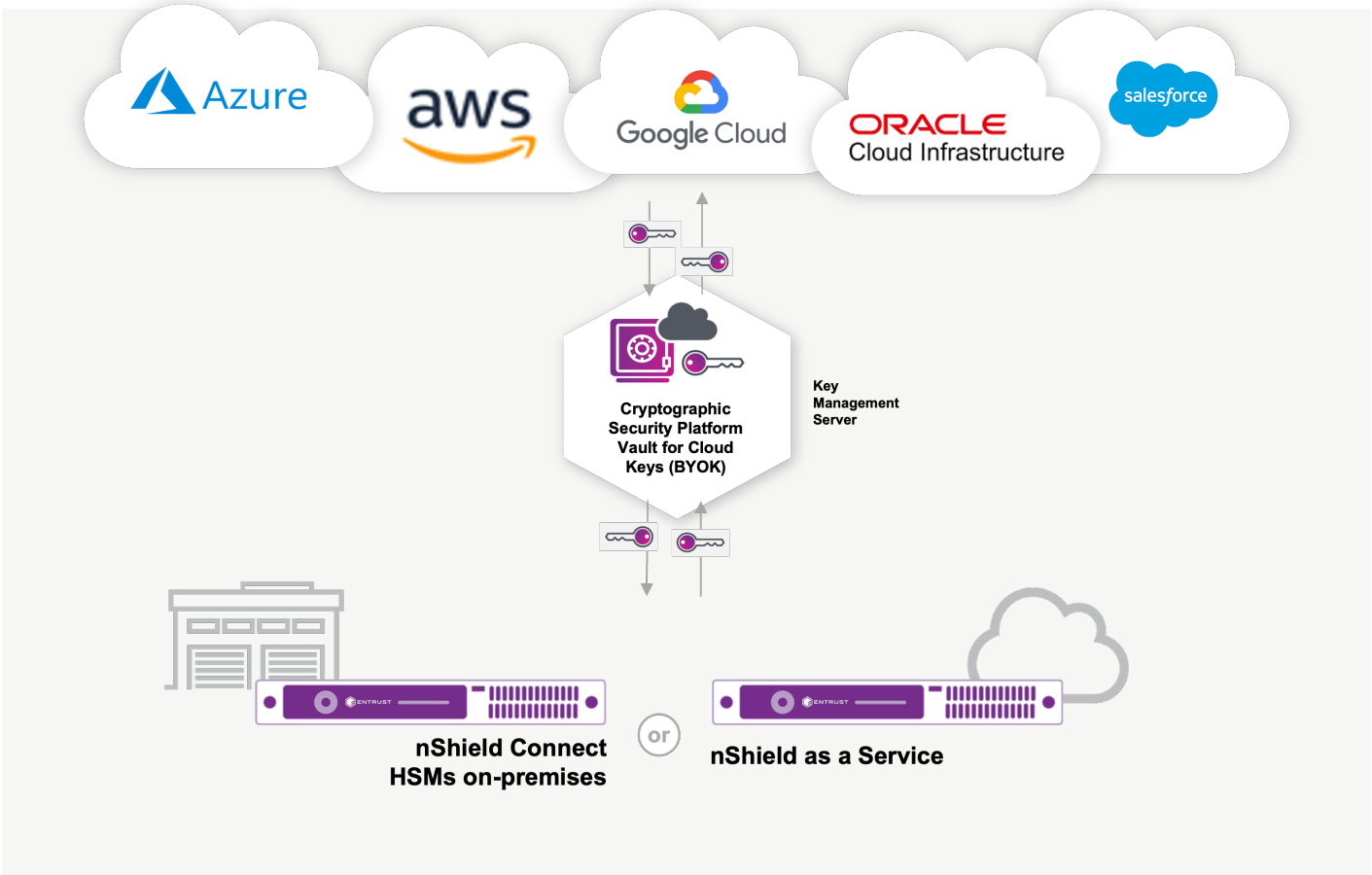
Cryptographic Security Platform Vault for Cloud Keys

Cryptographic Security Platform Vault for Cloud Keys helps your organization maximize control of cryptographic keys and encrypted data while leveraging cloud services. There are two deployment models:

Bring Your Own Key (BYOK)

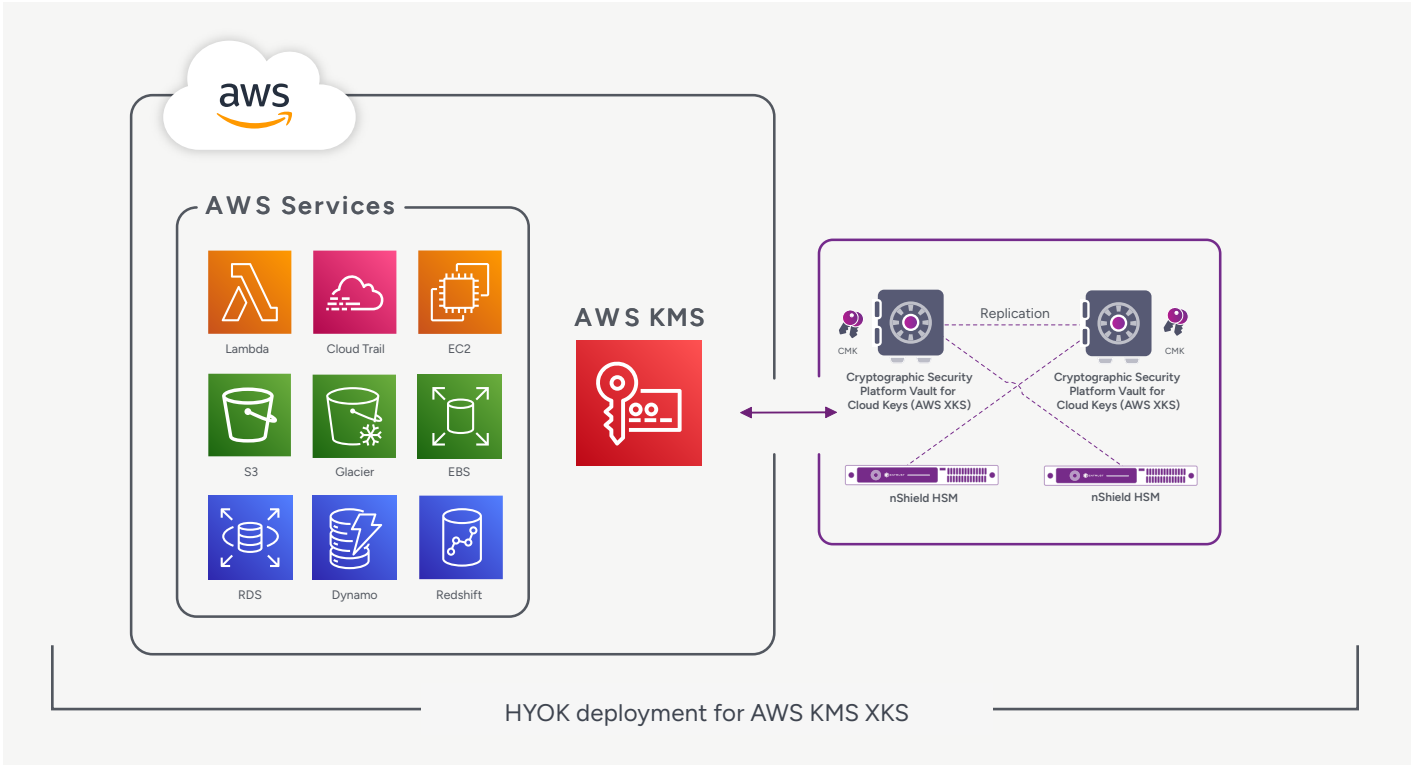
A Bring Your Own Key (BYOK) deployment model ensures not just the strong provenance of the keys but also provides lifecycle management, automation, and key backup capabilities independent of the cloud provider.

- 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 (GCP), Amazon Web Services (AWS), Oracle Cloud Infrastructure (OCS), and Salesforce cloud environments maintains the creation and control of your cryptographic keys.
- Seamless integration option with FIPS 140-3 Level 3 Entrust nShield® Hardware Security Modules (HSMs) as a hardware root of trust provides high-quality entropy source for key generation.

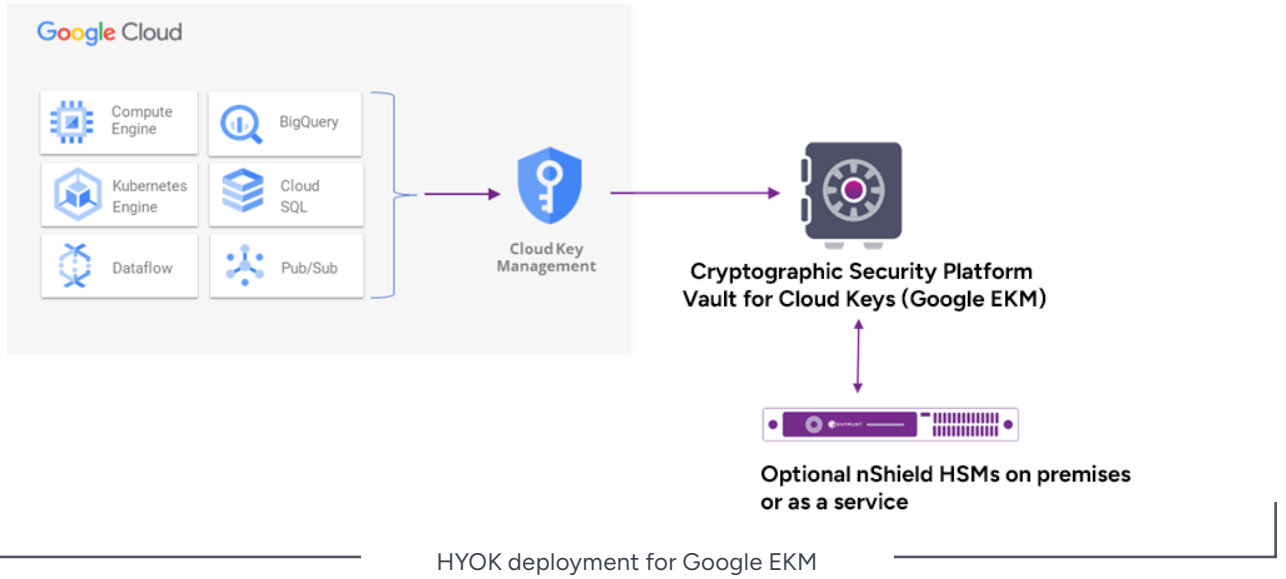


Hold Your Own Key (HYOK)

Organizations using cloud service provider 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 cloud service provider to use the keys on your behalf. HYOK shifts the shared responsibility model away from the cloud service provider to your organization, which is responsible for maintaining the HYOK proxy, key vault, and HSM. The Cryptographic Security Platform supports Microsoft DKE, AWS KMS XKS, and Google EKM, and the respective HYOK implementations of Azure, AWS, GCP, and Salesforce.



HYOK deployment for AWS KMS XKS



HYOK deployment for Google EKM

Cryptographic Security Platform Vault for Application Security

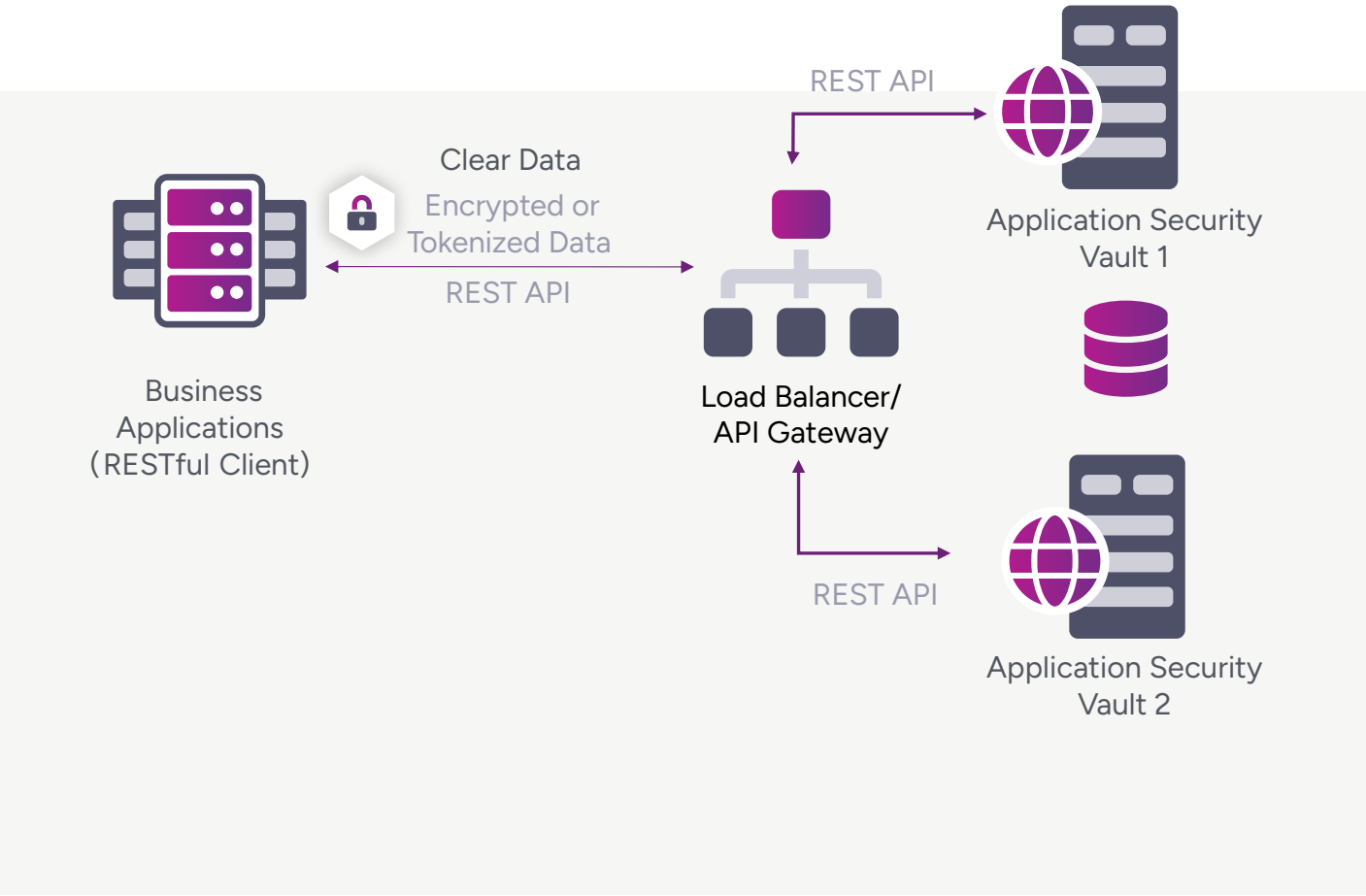
As data security becomes increasingly important, your organization can protect your sensitive data by using a variety of techniques such as encryption, tokenization, obfuscation, and data masking.

The Vault for Application Security provides a REST-like API for applications that require cryptographic key and data protection services, including key management system, encryption, signature and tokenization.

The Cryptographic Security Platform Vault for Application Security 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.

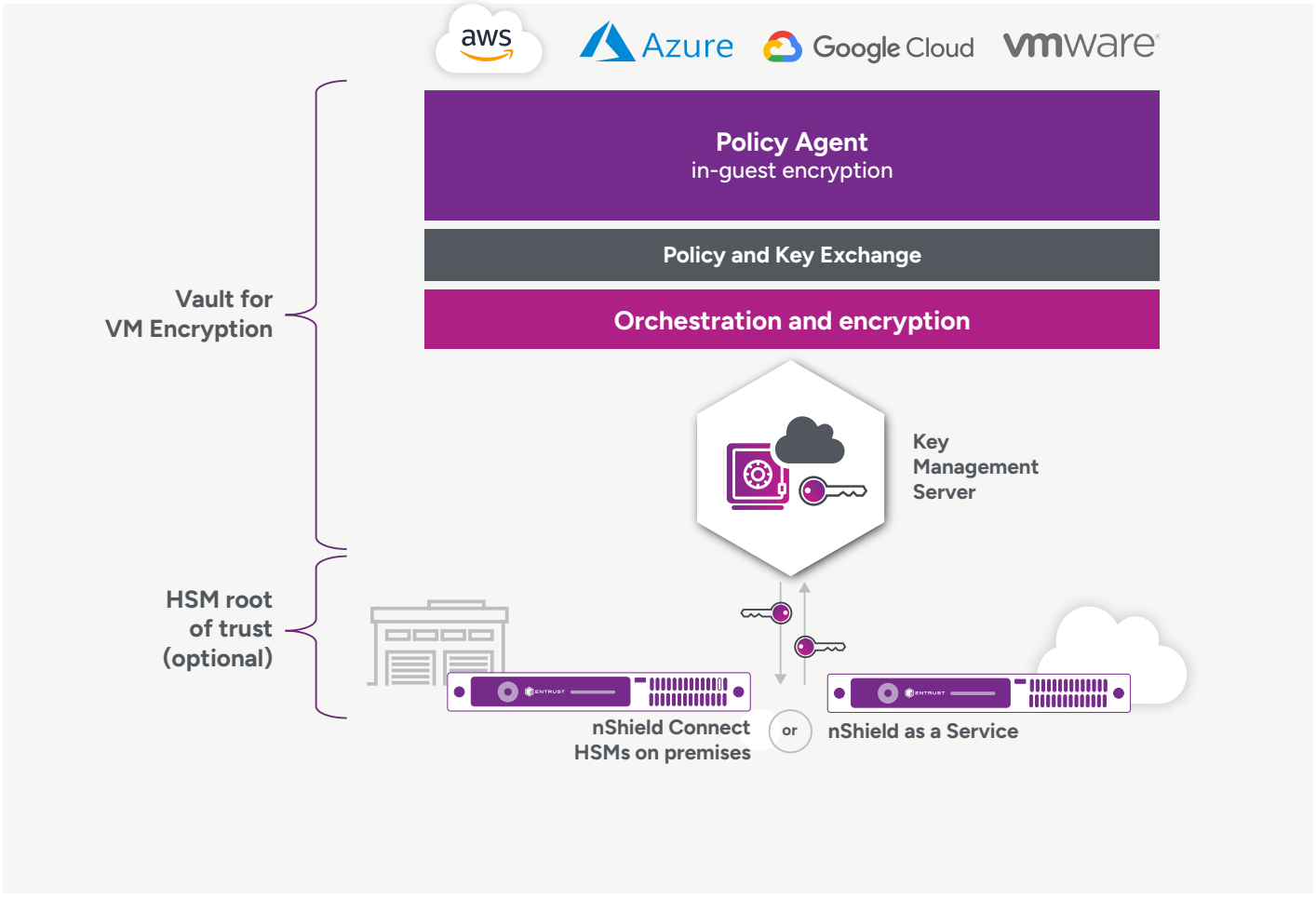


Cryptographic Security Platform Vault for Virtual Machine (VM) Encryption

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

The Cryptographic Security Platform 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 violations, 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. It should be possible to manage keys and secrets and certificates 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 – needs to be documented, managed, audited, and controlled. A comprehensive policy and compliance management system should enable security teams to ensure compliance with best practices, established security frameworks, and applicable regulations 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.

The Entrust Cryptographic Security Platform delivers decentralized security with centralized visibility across your entire cryptographic asset ecosystem. Its flexible vault architecture supports a wide range of features and services, ensuring that data and workloads are protected in compliance with stringent regulatory standards. Additionally, keys and secrets can be geolocated and managed to adhere to data sovereignty mandates.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

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

ENTRUST
SECURING A WORLD IN MOTION