

## DATASHEET

# Entrust Cryptographic Security Platform Vault for Secrets Management

## Securing Secrets Across Both On-Premises and Cloud-Based Applications

### OVERVIEW

Secrets are sensitive pieces of information, such as passwords, API keys, and other credentials, that are used to authenticate and authorize access for both humans and machines, to various services and resources.

Since the advent of the cloud, organizations increasingly rely on containerized technologies for their operations, which in turn has grown the number of secrets exponentially.

With this growth comes an ever-increasing need for security measures to protect secrets from malicious actors. In the wrong hands, compromised secrets can lead to major security events such as data breaches, and many of the recently publicized data breaches have originated from the compromise of machine and human secrets.

To mitigate that risk, secrets management – the art of managing the lifecycle of digital credentials such as passwords, API keys, certificate, tokens, etc. is essential to secure the environment and apply strict access control.

Having a global and consistent strategy for managing secrets across IT assets can significantly reduce cybersecurity risks, and specifically the access to critical information systems.

As organizations are facing an increasing diversity of secrets as well as secrets sprawl (where organizations no longer have visibility or control over the distribution of secrets), this strategy should include global and central management of all passwords, API keys, and other secrets associated with privileged account applications, tools, containers, or microservices deployed across the environment.

### KEY FEATURES

- Single pane of glass for the management of secrets across on-premises and cloud applications
- Validated integrations with leading CI/CD toolsets and container platforms
- Programmatic access to secrets using a RESTful API
- Policy-based access control
- Deployed as a virtual appliance
- High-availability (HA) support with active-active cluster
- Supports separation of duties, least privilege, dual control, and multitenancy
- Audit logs and forensic export
- (Optional) Hardware secret protection using FIPS 140-3 certified HSM root of trust
- (Optional) Automated compliance engine for PCI DSS, DISA STIGs, NIST SP 800-130, HIPAA, and other standards

Web application infrastructure makes up the highest percentage of disclosed secrets (39%). Of those, 66% of are JSON Web Tokens (JWT), commonly used in authentication, session management, and access control mechanisms.

## VERIZON 2025 DATA BREACH INVESTIGATIONS REPORT

Manual processing fosters poor secrets hygiene, including weak secrets, secret sharing, or lack of secret rotation, further increasing the risk of data breaches.

With Entrust Cryptographic Security Platform Vault for Secrets Management, businesses can easily manage secrets and access to credentials for resources across on-premises and cloud environments.

The solution is a scalable and feature-rich secrets vault that simplifies secrets lifecycle management and automates their lifecycle; including generation, storage, distribution, rotation, and revocation.

### BENEFITS

## Simplify secrets lifecycle management and protect your secrets with the highest level of assurance

Secrets management has become more complex with the adoption of cloud and container technologies, with serverless and cloud-provided micro-services. Secrets tend to be hard-coded and disseminated in scripts, configuration files, source code, file systems, etc. across the infrastructure.

In addition to secrets sprawl, administrators are faced with the complex and costly task of managing disparate secret forms such as SSH keys or short-lived tokens for multiple third-party solutions.

With the Entrust platform vault for Secrets Management, businesses can easily manage encryption secrets at scale. The solution securely catalogs and vaults each secret into a central encrypted, hardened location and simplifies management of secrets by providing a single pane of glass and automating the lifecycle of secrets.

The platform Key Management vault enables organizations to understand where secrets are used and

to enforce control over those secrets throughout the organization.

Finally, the Entrust Key Management vault provides runtime secret access, in the form of a programmatic access secret directly from the code (script, application, ...) with policy-based and identity-based access control. The secret is protected and provided at runtime, and not at build time.

## Facilitates compliance with regulatory requirements using Cryptographic Security Platform Compliance Manager

Beyond the cyber-threat risk, an increasingly complex regulatory environment brings its own risks to businesses.

Ensuring compliance with legal requirements and standards is sometimes not possible when keys or secrets are not segregated from the encrypted data.

While the Key Management vault offers a single pane of glass for the management of cryptographic keys and secrets, Entrust Cryptographic Security Platform Compliance Manager, deployed on premises or as a service, extends the vault capabilities by providing an automatic approach to help support compliance with industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the General Data Protection Regulation (GDPR).

The Entrust platform Compliance Manager makes an ideal complementary tool by making it easier to demonstrate compliance to auditors, not only for secrets vaults but also for all kinds of vaults across your organization.

Wherever you operate and whatever the regulation, it can help you achieve and maintain compliance, improving your security and managing your risk.

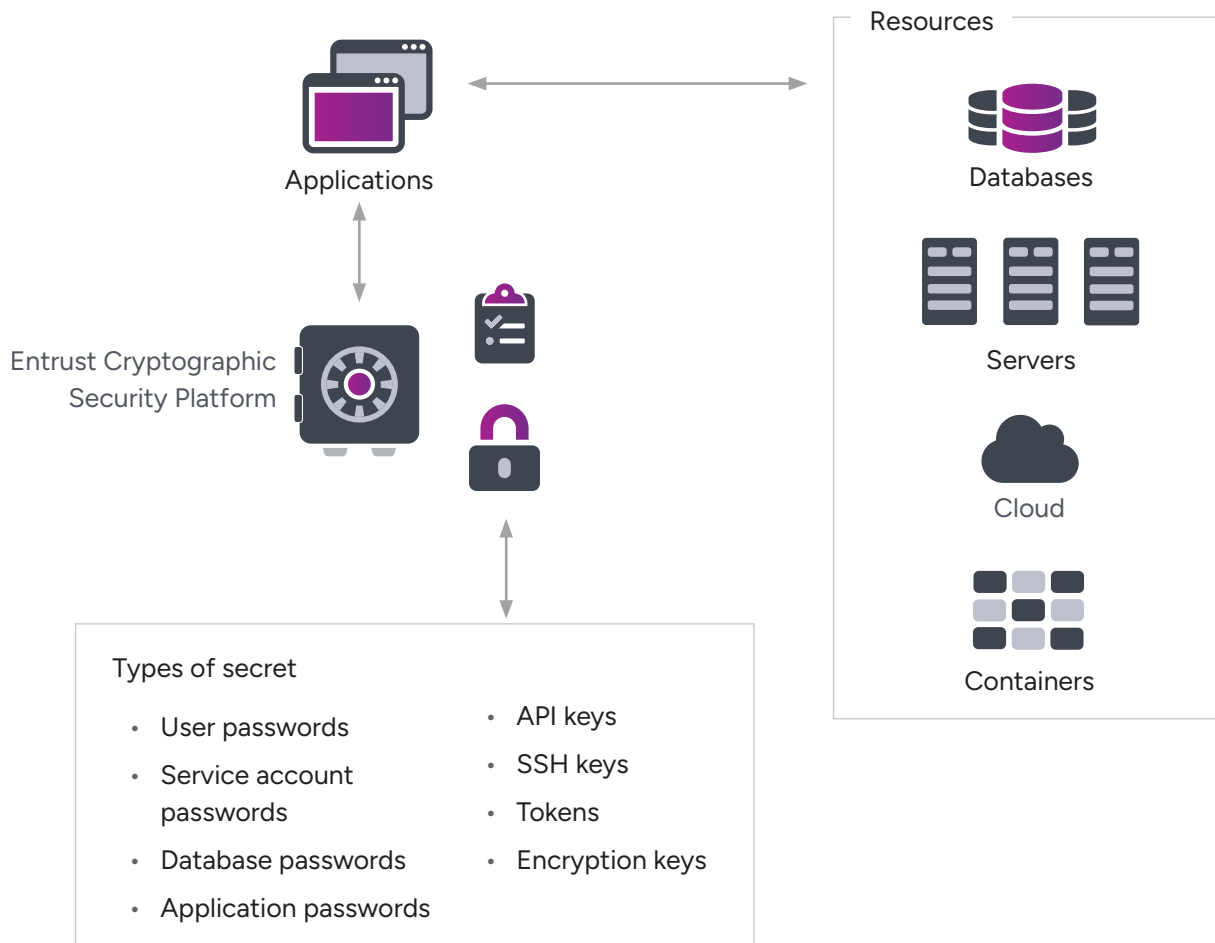
## How does it work?

The Key Management vault 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.

Secrets are centrally managed and securely stored across on-premises and cloud infrastructure using a highly available cluster of virtual appliances. The secrets can be accessed using either the vault web user interface, a command line tool, or a RESTful API.

The Key Management vault offers a centralized service providing secrets management and data encryption services across large estates of applications and engineering teams, while globally managing policies and delivering consistent security.

The Key Management vault access control mechanism supports different types of identity providers, such as Active Directories, LDAP Directories, and OIDC and SAML V2 identity providers.



Key Management Vault for Secrets typical architecture

## TECHNICAL SPECIFICATIONS

### Cloud Native and DevOps Integrations:

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

### Authentication:

- Active Directory, LDAP, OIDC, SAMLv2

### Management and Monitoring:

- Centralized management with Web UI and Rest API
- Syslog and Splunk integration

### Platform support:

- Private cloud platforms: vSphere, vCloud Air (OVH), VCE, VxRail, Quantum, NetApp, KVM
- Public cloud platforms: AWS, Google Cloud Platform (GCP), Microsoft Azure, IBM Cloud, VMware Cloud (VMC) on AWS
- Marketplace: AWS, Azur, and Google Cloud

### Certification:

- FIPS 140-3 Level 3 or eIDAS CC EAL4+ compliance via Entrust nShield HSM on premises or as a service

### Deployment media:

- ISO, OVA (Open Virtual Appliance)

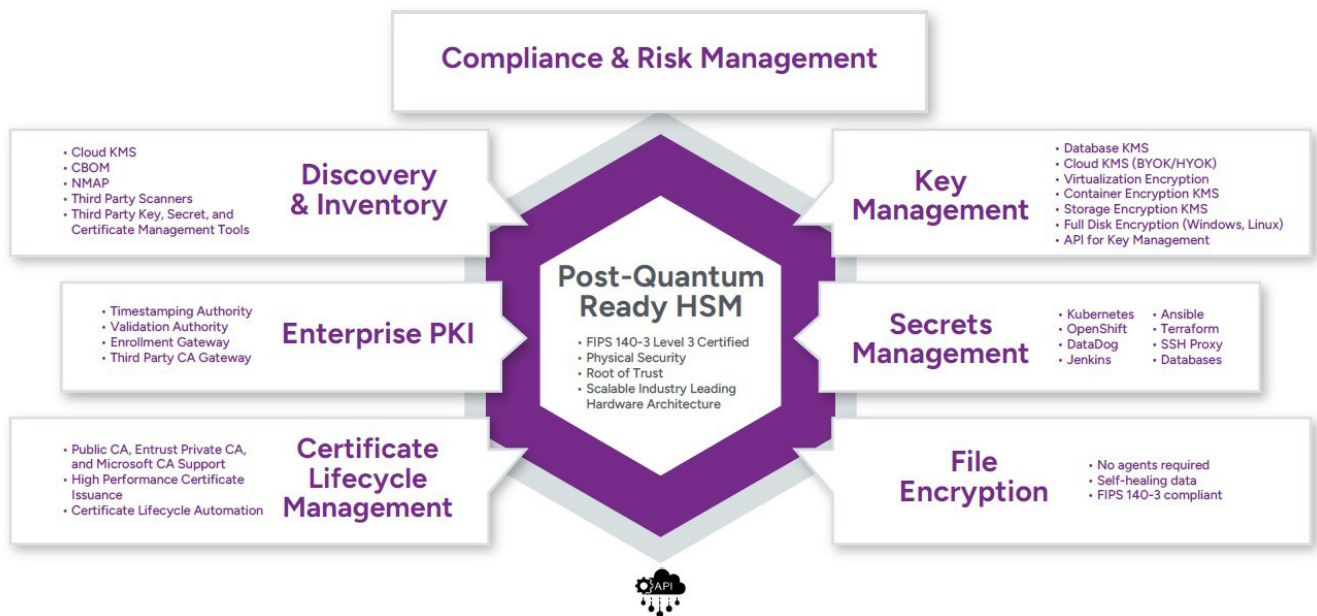
Learn more about the Cryptographic Security Platform at [entrust.com](https://www.entrust.com)



# Entrust Cryptographic Security Platform

The Entrust 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 support, and operational efficiency for organizations dealing with securing an increasing number of machine identities, protecting sensitive data, and navigating complex cryptographic requirements.



For more details on the Cryptographic Security Platform, Entrust platform Compliance Manager, and the range of vaults download the Entrust Platform Solution Brochure [here](#).