DATASHEET

Entrust Cryptographic Security Platform – Compliance Manager

Get 360-degree visibility, automation, and seamless orchestration over the lifecycles of keys, certificates, and secrets.

Overview

The need for cryptography to establish identity, protect data from unauthorized alteration, and prevent denial of service has never been higher. Cryptographic techniques secure communications over networks, protecting information stored in databases and across many other critical applications.

These techniques involve the use of cryptographic assets that must be managed and protected throughout their lifecycle. Without proper key management, cryptographic assets can be lost, stolen, or compromised, leading to security breaches and the loss of confidential information. Additionally, effective cryptographic asset management is essential for ensuring compliance with regulatory and industry standards.

As organizations manage an increasing number and diversity of cryptographic assets such as keys, secrets, and certificates, a consistent global strategy for managing these assets across IT infrastructure should include full visibility as well as all related information such as the owner, the usage, the history, how the cryptographic asset was generated, and for what purpose.

Key Features

- Key, secret, and certificate inventory across on-premises and cloud key management systems
- Supports all types of keys and secrets (KMIP, TDE, SSH, cloud, and application keys; passwords; tokens; etc.)
- Supports AWS KMS, Azure Key Vault, Google Cloud Platform (GCP), KMS, Oracle Cloud Infrastructure (OCI), and Salesforce
- Cryptographic asset documentation workflows
- Key reporting and alerting
- Deployed as a virtual appliance on premises or in the cloud, via a cloud-as-a-service model, or as a managed service
- High-availability support with active-active clustering
- Supports separation of duties, least privilege, dual control, and multitenancy
- Audit logs and forensic export
- Automated compliance engine for PCI DSS, NIST 800-130, NIST 800-57, and other standards plus support for customized compliance operations

ENTRUST

SECURING A WORLD IN MOTION

Cryptographic Security Platform – Compliance Manager

Manual processes for creating and managing cryptographic assets often lead to poor key hygiene, including lack of key documentation, compliance, and key rotation, which further increases the risk of data breaches.

With Entrust Cryptographic Security Platform Compliance Manager, businesses can easily establish and maintain an inventory of cryptographic assets and achieve full visibility on all related information for these assets, across on-premises and cloud environments, including their history and usage.

In creating a single unified dashboard, the solution allows you to view and monitor your organization's cryptographic assets located in one or many vaults – whether configured locally or geographically distributed.

The Solution

The Entrust Cryptographic Security Platform, deployed on premises or as a service, addresses the growing need for comprehensive cryptographic asset management in an increasingly complex digital landscape. It unifies cryptographic management by combining the rich capabilities to operate PKI, certificate lifecycle management, key management, secrets management, and HSMs – all from a single cohesive system.

By integrating these critical components, the Cryptographic Security Platform offers unparalleled security, visibility, compliance support, and operational efficiency for organizations dealing with securing an increasing number of machine identities, helping them protect sensitive data while fulfilling complex cryptographic requirements.

Benefits

Unifies visibility on keys and automated documentation process

Cryptographic Security Platform Compliance Manager provides a singular dashboard view of your key inventory across on-premises, public cloud, and hybrid cloud. It provides granular details on which keys are being used and can include information about ownership, environment, purpose, and critical system.

With Cryptographic Security Platform Compliance Manager, organizations can answer questions like:

- Who is the key owner?
- How is the key generated?
- How critical is a key?

The answers to those questions trigger documentation workflow when a lack of information is detected or upon an event related to the lifecycle of a key.

The dashboard also considers the human factors related to key management. By streamlining and automating processes, Cryptographic Security Platform Compliance Manager helps to reduce the likelihood of human error.

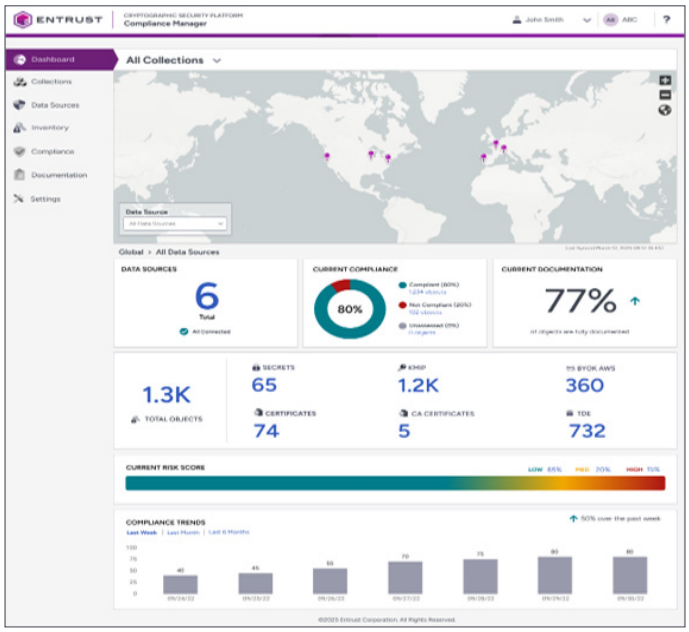


Figure 1: Illustrative view of the dashboard representing six decentralized vaults, cryptographic keys, and secrets.

Entrust Compliance Manager

Benefits

Facilitates compliance with regulatory requirements and standards

Beyond the cyber-threat risk, an increasingly complex regulatory environment brings its own risks to businesses. Ensuring compliance with legal requirements or standards is sometimes not possible when keys are not sufficiently documented or there is no centralized visibility into keys.

As your number of cryptographic assets increases, meeting compliance requirements will consume more and more resources, so the real question is how to ensure compliance while managing costs.

Compliance Manager provides an automatic approach to help support visibility, reporting, and complying with industry regulations such as Payment Card Industry Data Security Standard (PCI DSS), NIST SP 800-130, and NIST 800-53.

These capabilities provide a quick payback by reducing the need for staff and ensuring cryptographic assets are always documented and managed in accordance with a particular security policy or an industry-specific standard.

Cryptographic Security Platform Compliance Manager makes it easier to demonstrate compliance to auditors. Wherever you operate and whatever the regulation, Compliance Manager can help you achieve and maintain compliance, improving your security and managing your risks.

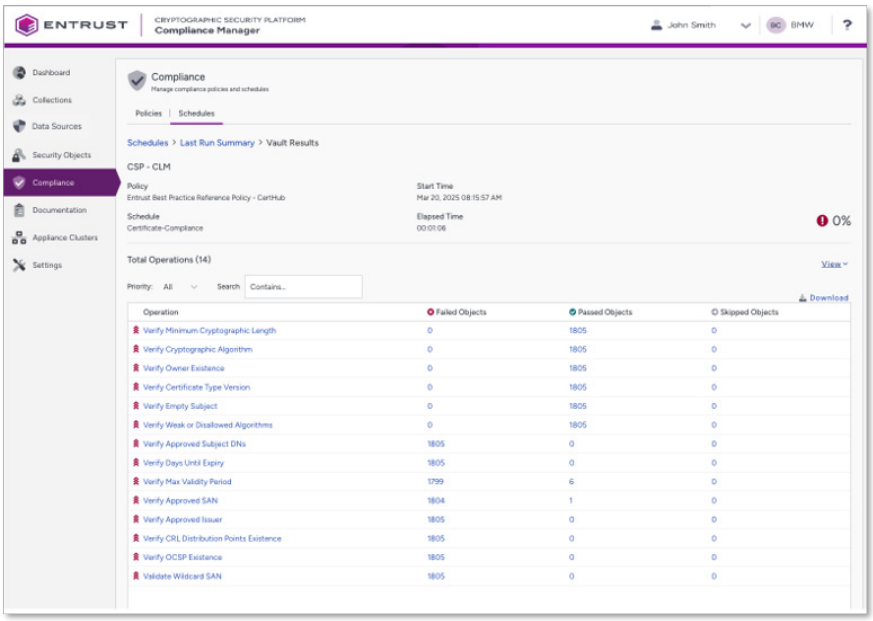


Figure 2: Compliance view of the dashboard detailing the inventory of keys and secrets in U.S. region and compliance results in relation to several regulatory templates.

Learn more about the Cryptographic Security Platform at entrust.com

Entrust Compliance Manager

Technical Specifications

Key, secrets, and certificates support:

KMIP keys, TDE keys, SSH keys, API keys, tokenization keys, passwords, container secrets, database secrets

Post-quantum readiness:

Certificate Manager supports robust, NIST-approved PQC algorithms to future-proof your organization against quantum threats, ensuring your cryptographic infrastructure meets the highest standards for security, compliance, and trust.

Cloud support:

AWS KMS, Azure Key Vault, GCP KMS

Authentication protocol:

Active Directory, LDAP, OIDC, SAMLv2

Management and monitoring:

- Centralized management with Web UI and REST API
- Syslog and Splunk integration
- Track PKI activities and get notifications on missed connects and outages
- Policy control and reporting on certificates

Platform support:

- Private cloud platforms: VMware Cloud Foundation (VCF), vSphere, VxRail, Nutanix
- Public cloud platforms: AWS, IBM Cloud, Microsoft Azure, VMware Cloud (VMC) on AWS, Google Cloud Platform (GCP)

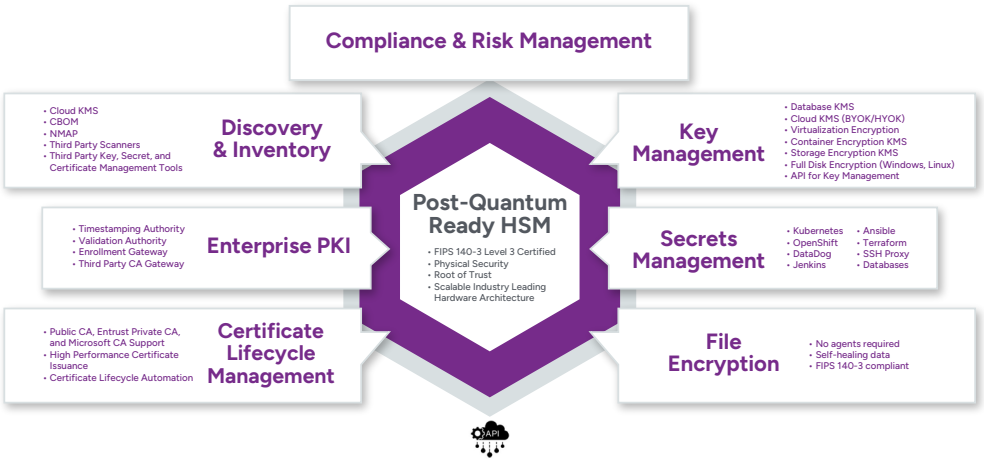
Deployment media:

ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services Marketplace), or VHD (Microsoft Azure Marketplace)

Entrust Cryptographic Security Platform

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.



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

ENTRUST
SECURING A WORLD IN MOTION