SOLUTION BROCHURE

Entrust Cryptographic Security Platform

End-to-end cryptographic security management for machine identities and data security

ENTRUST

SECURING A WORLD IN MOTION

Overview

For over 30 years cryptographic security has been at the core of traditional and critical business use cases, ensuring that as we connect, transact, and communicate identities are verified and sensitive data is encrypted. Today, we still rely heavily on cryptographic hardware, software, and credentials (such as keys, certificates, and secrets), but not without challenges. We're securing more things than ever from increasingly sophisticated attacks while trying to keep up with compliance and regulatory changes and requirements. Some challenges include:

- Organizational complexity of multiple, fragmented tools being used to manage cryptography, as well as independent teams managing different tools, assets, and data
- Lack of visibility into keys, certificates, and secrets – from where they reside to what they're securing
- The need for centralized control and automation over cryptographic assets throughout their lifecycle to mitigate policy issues or outages due to expiry
- Compliance and risk management issues that arise from not having enterprise-wide policy and governance defined
- Post-quantum threatens the traditional public key cryptography in use today, making the multi-year transition to post-quantum cryptography (PQC) a necessity

The Solution

The Entrust Cryptographic Security Platform is an innovative solution that unifies cryptographic management by combining the rich capabilities used to operate public key infrastructure (PKI), certificate lifecycle management, key and secrets management, and hardware security modules (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.

Benefits

- Single pane of glass visibility of keys, certificates, and secrets across environments
- Secure key storage and cryptographic operations
- Automated issuance and management of public and private certificates
- Vulnerability and compliance monitoring
- Remediation of security issues and policy enforcement

The Entrust Difference

The Cryptographic Security Platform leverages Entrust's broad portfolio of market-leading cryptographic solutions and unifies them in a single, cohesive system

Compliance Management
The Compliance Manager provides a powerful compliance dashboard with granular policy management and control over the cryptographic assets across your enterprise as well as fine-grained control of your cryptographic assets, offering full visibility, traceability, compliance tracking, risk scoring, and an immutable audit trail of all keys and secrets. The unified dashboard allows you to view and monitor your organization's cryptographic assets in vaults configured locally or geographically distributed.

PKI and Certificate Lifecycle Management
The Entrust Cryptographic Security Platform includes a comprehensive, high-performance, container-based PKI, certificate lifecycle management, and automation solution. It comprises all the components required to run a secure, PQ-ready PKI, deploy in a range of applications, and expand on demand.

Deployed as a pre-packaged virtual appliance that includes Compliance Manager, it enables customers to streamline PKI and CLM while providing the flexibility to scale across enterprise and cloud environments.

Key and Secrets Management
A robust key and secret lifecycle management system with a decentralized vault-based architecture provides centralized visibility and compliance management. It ensures that management practices align with stringent regulatory and corporate requirements, enabling keys and secrets to be geo-located and managed in accordance with data sovereignty mandates

File Encryption
Entrust CSP File Encryption provides agentless, transparent encryption for unstructured data across on-premises, hybrid, and multi-cloud storage. It sits between applications and storage to encrypt files – and strip or obfuscate metadata – without changing workflows, protecting data even if storage is breached or misconfigured. With centralized key and policy management and built-in ransomware resilience, it reduces risk while enabling secure, compliant use of modern storage environments.

Hardware Security Modules (HSMs)
The inclusion of HSMs with the Cryptographic Security Platform delivers cryptographic services to applications across the network, in the cloud, and in hybrid environments. They are hardened, tamper-resistant, FIPS 140-3 Level 3 certified security appliances that perform encryption, digital signing, and key generation and protection. With their comprehensive capabilities, flexible hybrid deployments, quantum crypto-agility, and 100% compatibility with existing nShield® HSM deployments and APIs, these HSMs can support an extensive range of applications, including certificate authorities, code signing, and more.

Components of the Cryptographic Security Platform include:

- Compliance Manager
- Certificate Authority
- Certificate Lifecycle Management
- Key and Secrets Management
- Enhanced PKI Services
- Enrollment Services
- CA Gateway (RESTful API)
- Timestamping
- Validation Authority (OCSP)
- File Encryption
- Third-Party Cryptographic Assets
- Vault Cluster

Key Features

Enterprise-Wide Cryptographic Security:

Rich capabilities to operate PKIs and HSMs and manage keys, certificates, and secrets in a complex enterprise environment.

Single Pane of Glass Visibility:

Dashboard providing centralized visibility over your full cryptographic estate, such as keys, certificates, and secrets.

Compliance and Risk Management:

Enterprise-wide compliance policy definition, enforcement, management, and reporting across your cryptography estate.

Scalable Architecture:

High-volume, high-performance cryptographic asset management and built-in HSM protection with unparalleled scale.

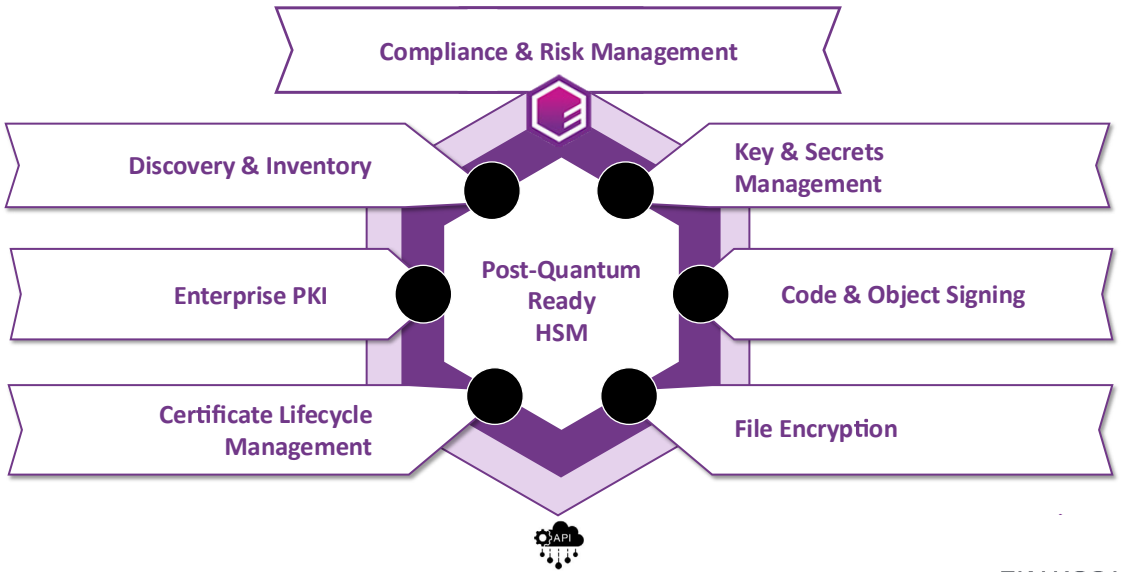
Interoperable:

Extensive partner ecosystem and protocol support to enable seamless integration with your organization's existing and future infrastructure.

Post-Quantum Secure:

The combination of PKI and HSM provides high-performance post-quantum cryptography certificate issuance capabilities to help future-proof your organization against the quantum threat.

Cryptographic Security Platform Components and Capabilities



View of the Compliance Manager dashboard

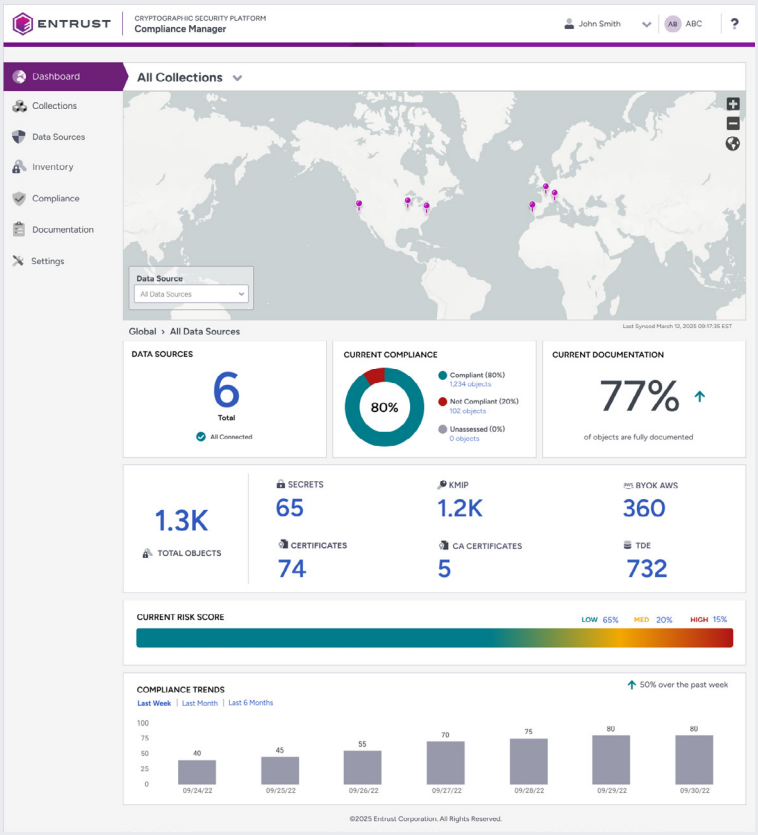
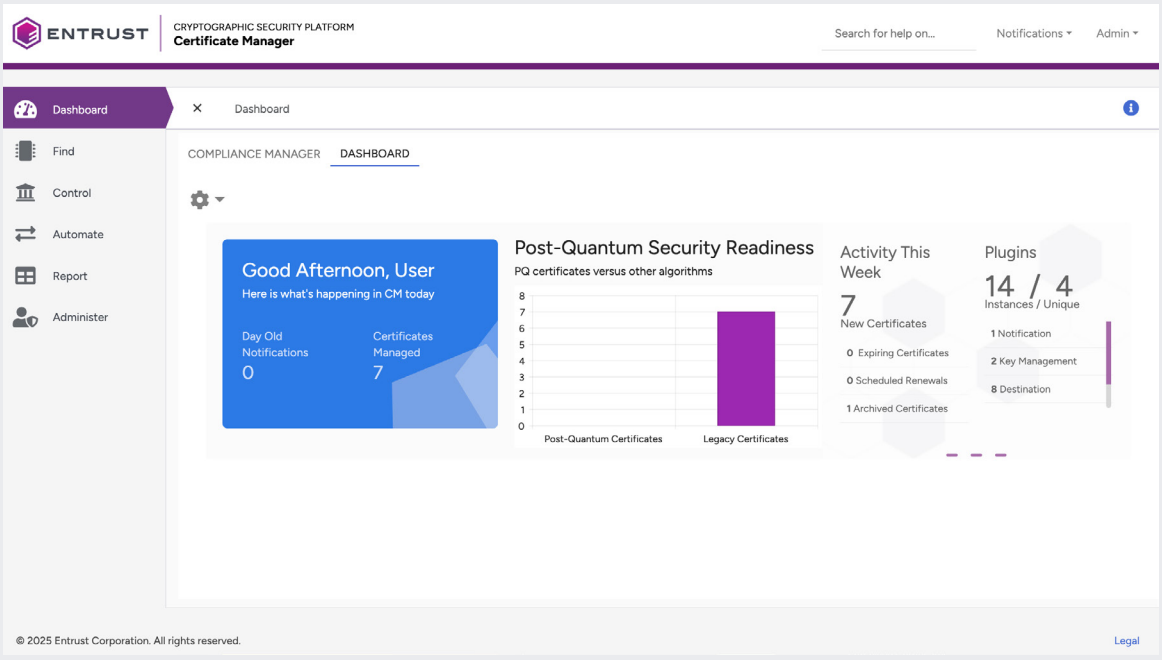
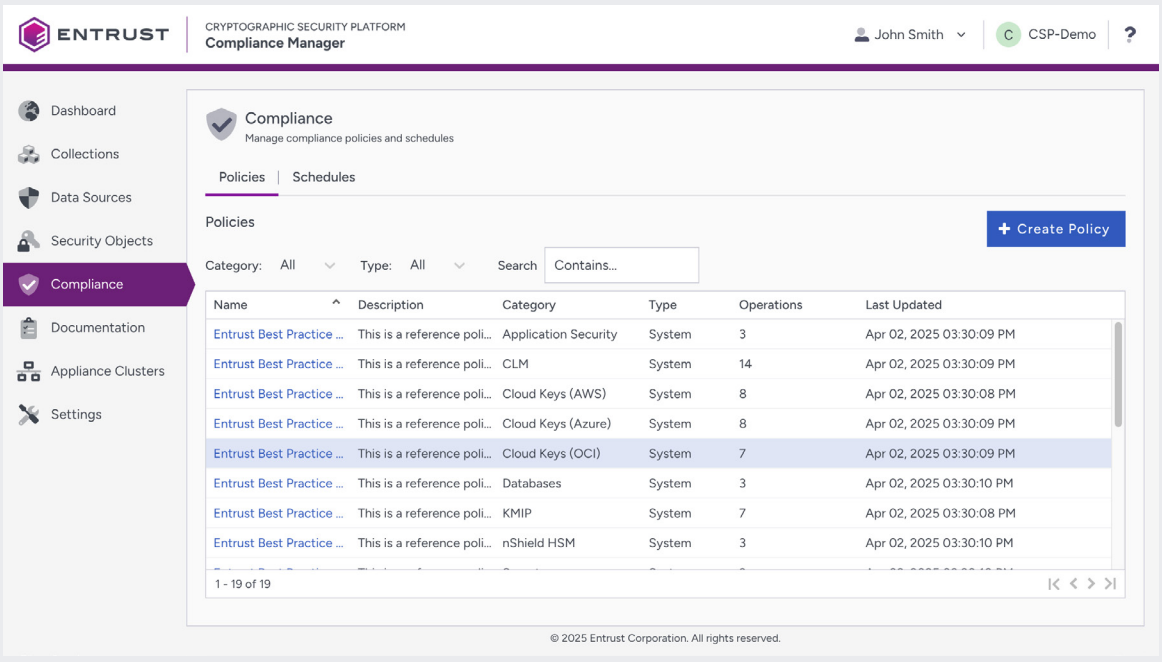


Illustration of the consolidated level of compliance and documentation with trends.



Dashboard view providing inventory of legacy and post-quantum certificates.



View of Compliance templates. Each template can be applied to a specific data source.

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