DATASHEET

# Entrust Data Security Solutions

Entrust's data security solutions provide the cryptographic foundation for trusted digital interactions across the identity lifecycle. Spanning public key infrastructure (PKI), hardware security modules (HSMs), and key, certificate, and secrets lifecycle management, our solutions deliver the visibility, control, and automation organizations need to manage cryptography at scale and secure the enterprise. The Entrust Cryptographic Security Platform (CSP) brings these capabilities together to help organizations strengthen security and compliance while building the agility to respond to evolving threats and technologies.

**Business Benefits:**

- Reduced operational overhead
- Stronger security posture
- Enterprise-wide cryptographic visibility
- Simplified compliance
- Built-in crypto agility
- Readiness for post-quantum migration
- Trusted security for AI agents, workloads and infrastructure

## Entrust Cryptographic Security Platform

The Entrust Cryptographic Security Platform (CSP) provides centralized visibility, management, and automation across the cryptographic environment. By bringing together PKI, certificate lifecycle management, HSMs, and key and secrets management, Entrust CSP helps organizations discover and manage cryptographic assets, automate lifecycle operations, enforce policy, and prepare for post-quantum migration.

**With Entrust CSP, you can:**

- Gain enterprise-wide visibility into cryptographic assets from a centralized dashboard
- Automate key, certificate, and secrets lifecycle operations, including issuance, rotation, renewal, and expiration tracking
- Enforce policies and simplify compliance with risk scoring and audit-ready reporting
- Reduce the risk of certificate-related outages through automated management and monitoring
- Support public and private trust ecosystems across cloud, on-premises, and hybrid environments
- Integrate with existing infrastructure and Entrust nShield HSMs for hardware-backed assurance
- Built-in compliance management with risk scoring and audit readiness
- Automated management and monitoring to reduce risk and eliminate outages
- Build crypto-agility and prepare for migration to NIST-standardized post-quantum algorithms
- Establish cryptographic trust for AI agents, workloads, and infrastructure

## nShield HSMs: Hardware-Rooted Assurance

Entrust nShield® hardware security modules (HSMs) provide the tamper-resistant root of trust your cryptography depends on – delivering trusted execution for key generation, digital signing, encryption, and more. nShield HSMs are FIPS 140-3 Level 3 and Common Criteria certified, with flexible deployment across cloud, on-premises, and hybrid environments. They're engineered for crypto-agility, enabling organizations to adopt new algorithms and adapt as algorithms, standards and cryptographic requirements evolve.

### nShield HSMs can help you:

- Secure encryption keys and sensitive cryptographic operations
- Integrate seamlessly with leading cloud service providers and 150+ technology partners
- Support countless use cases, including encryption, PKI, and code signing
- Prepare for post-quantum threats with NIST-standard algorithm support
- Integrate with Entrust CSP for centralized visibility and management
- Scale with Security World architecture and support virtually unlimited key storage

## PKI: Establishing Trust Across Your Ecosystem

Public key infrastructure provides the foundation for authenticating identities, protecting communications and securing transactions across increasingly complex digital ecosystems.

Entrust delivers a comprehensive and scalable PKI portfolio trusted by enterprises, governments, and financial institutions in more than 150 countries. Whether you're building out a Zero Trust architecture, securing the Internet of Things, or managing millions of certificates, Entrust PKI provides the flexible foundation to authenticate users, protect data, and verify transactions at scale.

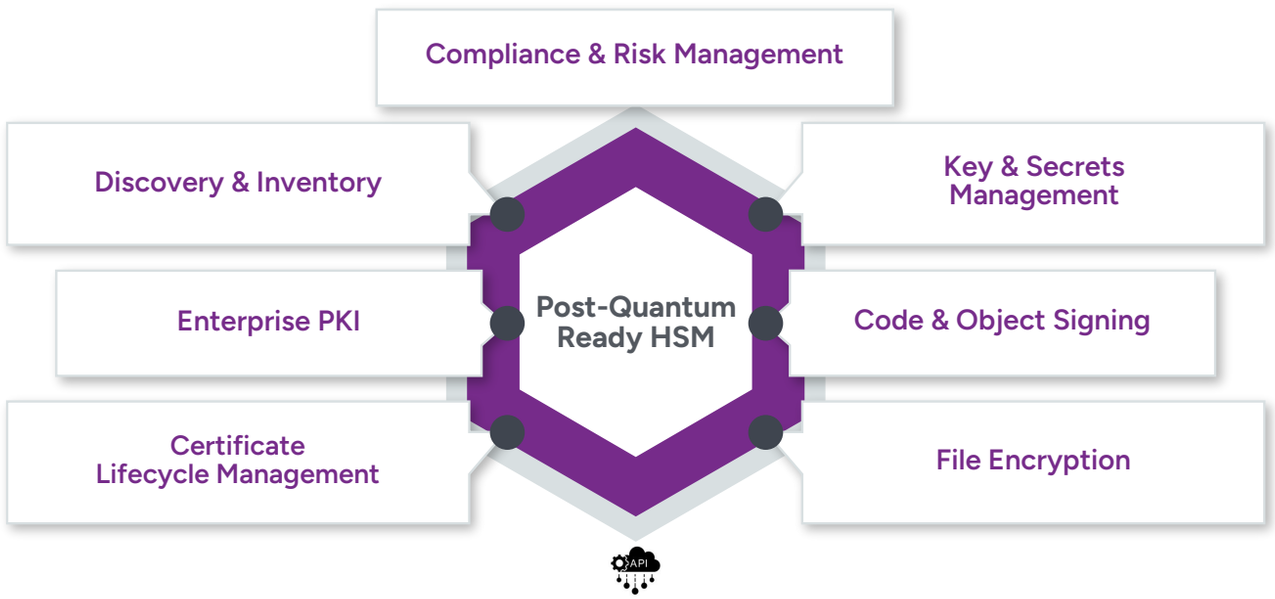
### With Entrust PKI, You Can:

- Choose from on-premises, managed, or hybrid deployment options
- Integrate PKI with cloud services, enterprise applications, and connected ecosystems
- Automate certificate issuance, renewal, and revocation
- Support Zero Trust, IoT, device identity, and other high-scale use cases
- Prepare PKI environments for migration to post-quantum cryptography

## Explore the Entrust Data Security Portfolio

See how Entrust can help you gain control of your cryptographic environment, automate operations, simplify compliance, and prepare for what comes next. **Visit Entrust.com**

## Cryptographic Security Platform Components and Capabilities




©2026 Entrust Corporation. All rights reserved. Entrust, Datacard, and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. DS27Q2-entrust-data-security-ds

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

ENTRUST
SECURING A WORLD IN MOTION