Entrust Secure Data Solution

Support your Zero Trust journey by securing the cryptographic keys and secrets that protect your most sensitive organizational data.

Overview

Zero Trust requires that all sensitive data be rendered unreadable through encryption while in storage, use, and transit and that it is only accessible to explicitly authenticated users or entities. With exponential growth of cryptographic assets across more rigorous regulatory environments, organizations today struggle to manage the keys and secrets used to protect and to gain access to their critical data. This is particularly challenging as organizations process data across on-premises and distributed multi-cloud environments while seeking to maintain compliance with security policies.

Key and Secrets Lifecycle Management

Keys and secrets underpin the security of cryptographic processes. Managing the complete lifecycle of keys and secrets is critical for comprehensive security. Lifecycle management begins with the initial generation of keys and secrets and continues with their controlled delivery and distribution. The process includes the automated rotation, possible revocation, and eventual retirement and destruction to ensure best practices.

Compliance and Risk Management

Creating, using, and subsequently destroying key and secrets is not enough. Comprehensive management also needs to consider what keys and secrets are used for and who and/or what has access to them, and under what circumstances. Documenting how keys and secrets are used not only mitigates risks but also facilitates compliance.

The Solution

Keys and secrets management

The Entrust Secure Data Solution ensures the secure and efficient management of organizations' sensitive data and cryptographic assets, critical to supporting a comprehensive Zero Trust journey. Protecting keys and secrets used to encrypt and control access to critical data assets, the Entrust Secure Data Solution enables organizations to fulfill the data security pillar of the Zero Trust framework.

Compliance and risk management

With an innovative combination of centralized data asset visualization and compliance management, paired with decentralized key and secret storage, the Entrust Secure Data Solution is unique in the market.

Secure Data Solution

Hardware root of trust
With FIPS Level 3 hardware security modules (HSMs), available on premises or as a service, the Entrust Secure Data Solution enables organizations to implement and enforce best practices. HSMs provide a robust key generation capability as well as providing security for the keys both in use and at rest from within a scalable, highly available and resilient on-premises, cloud, or hybrid deployment. Master keys used to protect encryption keys, secrets, and access credentials are given the highest level of protection with the flexibility and scalability needed to address a wide variety of regulatory compliance-driven use cases.

The Entrust Difference

The Entrust centralized-decentralized security (CeDeSec) approach enables organizations to maintain full control of their data, ensuring the confidentiality and integrity of and controlled access to critical assets while facilitating compliance with security regulations.

Zero Trust emphasizes the protection of data, which relies on encryption as a fundamental means to secure sensitive assets. Effective data encryption requires the use of cryptographic keys that need to be managed securely over their lifecycle while complying with an enterprise's security policies and regulatory controls.

The Entrust Secure Data Solution includes a unique key management system (KMS) that allows organizations to adopt best security practices for key management. With robust key generation, protected key storage, controlled key distribution, and key auditing and reporting, the solution plays a critical role in organizations' Zero Trust strategy.

Redefining keys and secrets lifecycle management, the Entrust Secure Data Solution extends traditional key management beyond key lifecycle and distribution through multiple interfaces including Key Management Interoperability Protocol (KMIP), PKCS#11, CSP APIs, and RESTful APIs. The solution also provides access control to the cryptographic keys and secrets, and automation capabilities including key rotation and expiration to fulfill organizations' Zero Trust data security requirements.

The CeDeSec vault-based architecture consolidates visibility of cryptographic assets regardless of the number of vaults. Workflows enable keys used to be documented based on templates and continuous compliance assessment is achieved using built-in or custom policies.

Supported Use Cases

The Entrust Secure Data Solution supports a wide range of Zero Trust use cases including data protection (databases, storage, backups) and tokenization, as well as cloud security though bring-your-own-key (BYOK) and hold-your-own-key (HYOK) mechanisms. Secrets management, virtual machine encryption, and privilege account session management (PASM) are also supported. Extending functionality beyond traditional data security, the solution also supports public key infrastructures (PKIs), digital signatures, code signing, timestamping, TLS/SSL, and secure code execution.

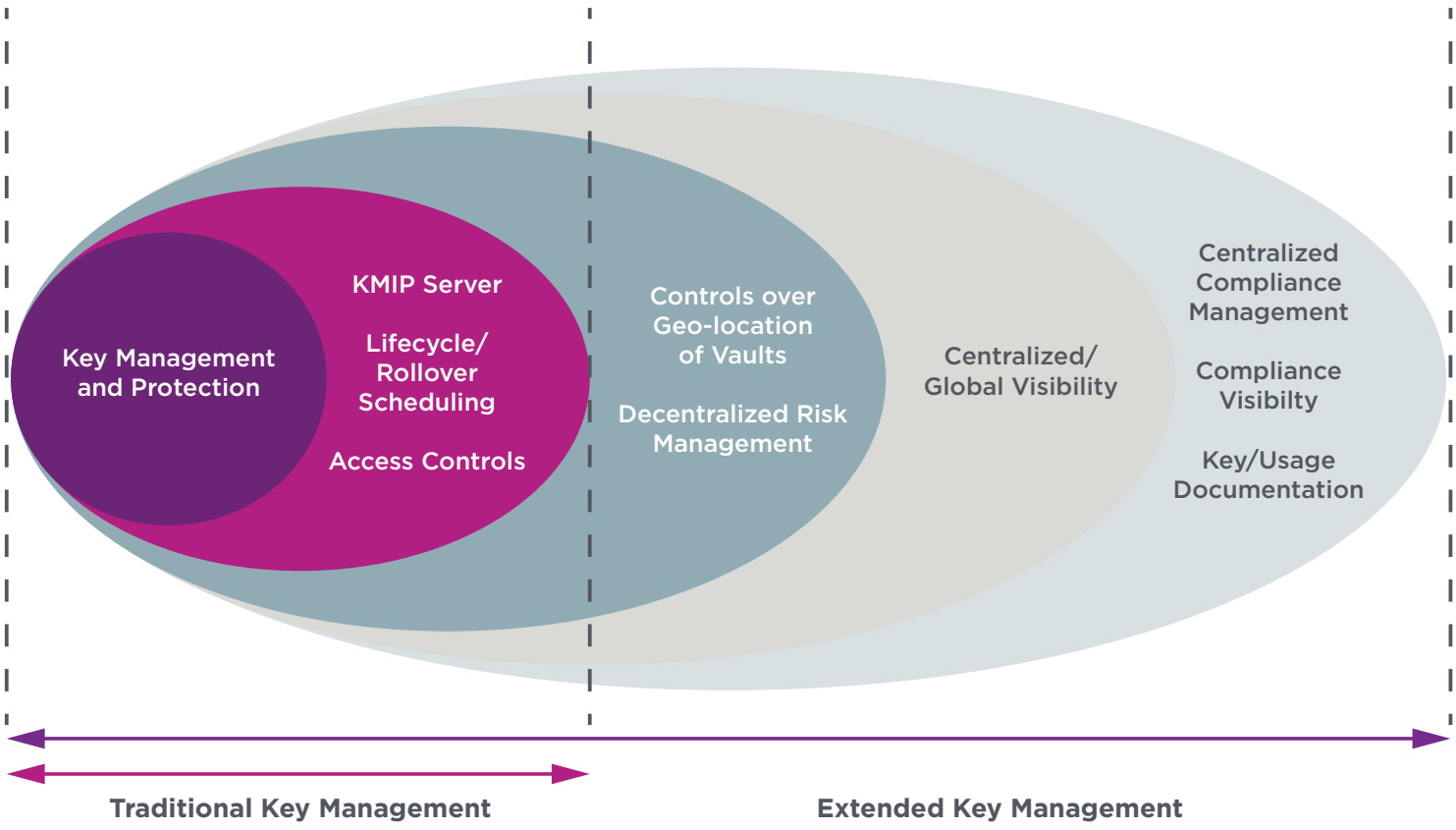
Secure Data Solution

Features

- Centralized compliance management
- Decentralized protected key storage
- Data encryption – at rest and in transit
- FIPS Level 3 HSM root of trust
- Robust cryptographic key generation
- Dual-controls and separation of duties
- Support for post-quantum algorithms

Benefits

- Mitigate exposure to data breaches
- Ensure compliance to data security regulations
- Maintain visibility of critical data assets
- Ensure data and keys only reside where they are required by regulation
- Maximize application of best practices
- Facilitates enforcement of never trust, always verify approach
- Future-proof security investment



Learn more about our Zero Trust solutions at entrust.com

Secure Data Solution

Features

Traditional Key Lifecycle Management: Generate, deliver, and distribute cryptographic keys to a range of supported applications through multiple standard interfaces including KMIP. Provide access control to keys and enable automated capabilities including key rotation and key expiration.

Secure Root of Trust: Foundational element of the data protection pillar of the Zero Trust framework enables FIPS-certified high assurance secure cryptographic key generation and lifecycle management with dual-controls and separation of duties.

Decentralized Vault-Based Architecture: Distributed key storage ensures that keys and data are kept within the geographical areas where they are supposed to be maintained to facilitate compliance with geo-fencing and data sovereignly regulations.

Comprehensive Central Policy: Unified visibility across cryptographic assets regardless of the number of vaults deployed across the distributed environment.

Compliance Management Dashboard: Enables the documentation of keys and secrets based on templates for continuous compliance assessment using built-in or custom policies.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223