Securing Your Data

Our identity-centric solutions help secure the cryptographic keys and secrets that protect your most sensitive data

Market Overview

Organizations face an ever-pressing need to reappraise their security posture with respect to data protection. When it comes to protecting customer and company data, they need controls and processes in place to ensure resilience against cyberattacks while adhering to corporate, industry, and government regulations.

Governance, risk, and compliance are key issues of today. Service outages, customer dissatisfaction, reputation damage, detrimental impact on share price, and fines are all top of mind for C-level executives.

Keys, Secrets, and Certificate Lifecycle Management

Managing cryptographic assets such as keys and secrets is the foundation of any organization's data protection strategy. But these assets can quickly grow exponentially and become unwieldy and difficult to maintain. Our tools can help you manage these assets through their entire lifecycle, simplifying risk reporting, visibility, and auditing – while also saving IT and compliance teams' time.

Compliance and Risk Management

Time and resourcing can be a headache for any C-level executive with the responsibility for risk and compliance. It's not just about getting the best out of their team; it's also about streamlining tasks and seeking opportunities to apply tools that offer real value in applying control, visibility, and risk reporting while saving valuable time. And of course, time equates to budget spend.

The Solution

Keys and secrets management

Our solution ensures the secure and efficient management of sensitive data and cryptographic assets, critical to supporting your organization's security posture.

Compliance and risk management

Entrust uniquely combines traditional key lifecycle management and decentralized vault-based architecture with a cryptographic asset inventory and a compliance and risk management dashboard.

Learn more about our user-centric Zero Trust solutions at entrust.com

Securing Your Data

Hardware root of trust

With FIPS Level 3 hardware security modules (HSMs), available on-premises or as a managed service, our solution empowers organizations to implement and enforce key and secret management best practices.

HSMs offer robust key-generation capabilities while securing keys both in use and at rest within a scalable, highly available, and resilient deployment – be it on-premises, in the cloud, or hybrid. Master keys that safeguard encryption keys, secrets, and access credentials receive the highest level of protection, delivering the flexibility and scalability necessary to address a wide range of regulatory compliance-driven use cases.

The Entrust Difference

CeDeSec approach

Entrust's 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.

Extended key management

Best practices emphasize 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.

Our solution includes a unique key management system (KMS) that allows you 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 supporting a strong security posture.

Redefining keys and secrets lifecycle management, our 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. It also provides access control to the cryptographic keys and secrets, and automation capabilities – including key rotation and expiration – to fulfill the most stringent security requirements.

Decentralized vault-based architecture

Our decentralized vault-base architecture consolidates visibility of cryptographic assets regardless of the number of vaults. Keys can be documented based on templates while built-in or custom policies enable continuous compliance assessment.

Supported Use Cases

Our solution supports a wide range of use cases, including:

- Data protection (databases, storage, cloud backups)
- Tokenization
- Cloud security – though bring-your-own-key (BYOK) and hold-your-own-key (HYOK) mechanisms
- Secrets management
- Virtual machine encryption
- Application security

Extending functionality beyond traditional data security, the solution also supports:

- Public key infrastructures (PKIs)
- Digital signatures
- Code signing
- Timestamping
- TLS/SSL
- Secure code execution

Learn more about our user-centric Zero Trust solutions at entrust.com

Securing Your Data

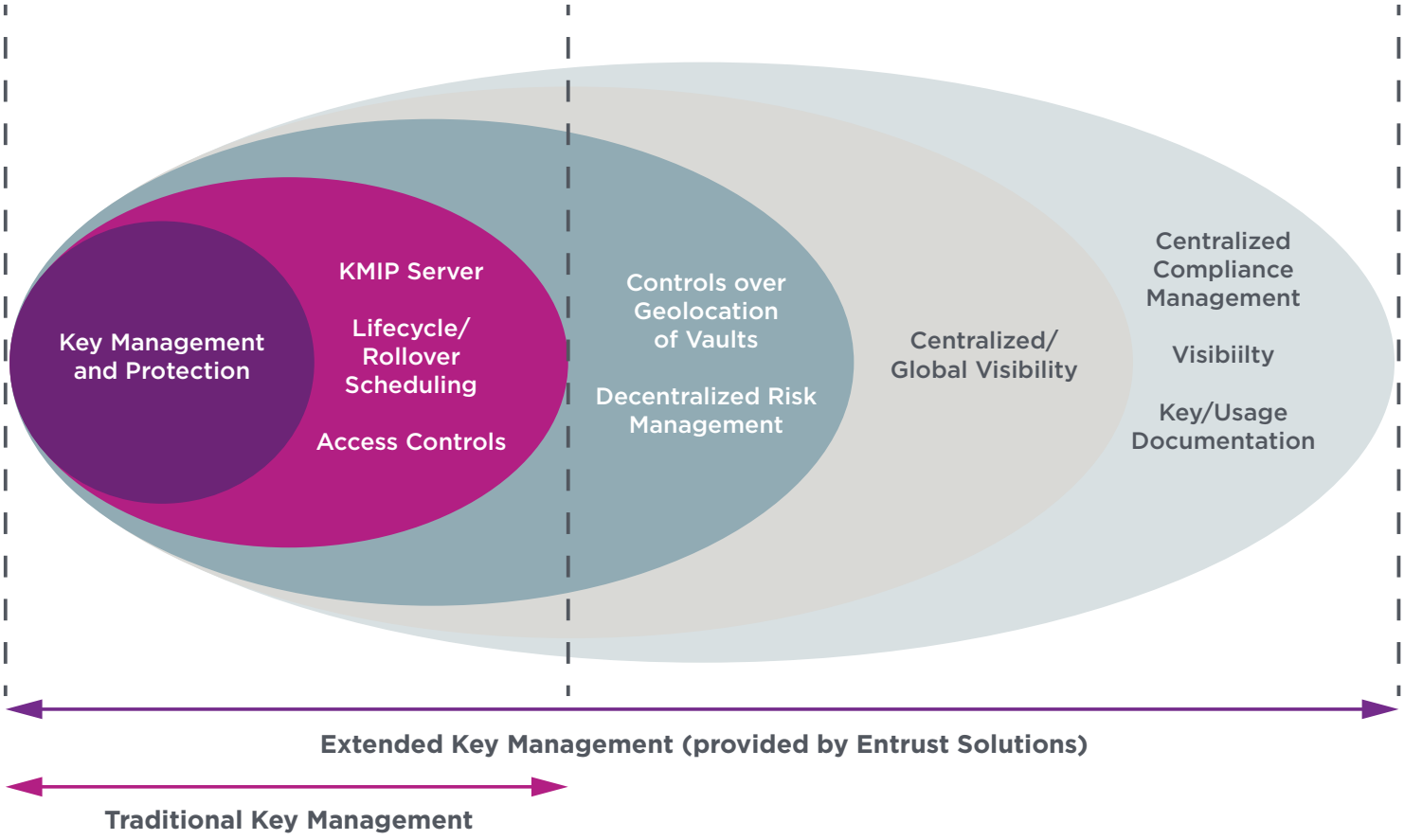
Features

- 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
- Facilitiate compliance with data security regulations and stringent auditing and risk-reporting requirements
- Maintain visibility of critical data assets
- Ensure data and keys only reside where they are required by regulation
- Maximize application of best practices

How It Works



Learn more about our user-centric Zero Trust solutions at entrust.com

Securing Your Data

Key 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 data protection 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 geofencing and data sovereignty regulations.

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

Compliance Management Dashboard: Streamlined auditing and risk reporting tasks saves time and effort. Enables the detailed inventory 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