Entrust supports leading database providers to enhance security across cloud deployments

Solution securely manages lifecycle of critical keys that encrypt your most sensitive data

HIGHLIGHTS

- Protects data at rest for both on-premises and cloud-based deployments
- Addresses stringent data security policies and compliance mandates
- Delivers stronger security by separating keys from databases
- Centrally manages cryptographic key lifecycles, policies, and access
- Secures encryption keys in a tamper-resistant FIPS 140-2 Level 3 and Common Criteria EAL4+ certified hardware security module

The Challenge

Enterprises use sophisticated databases to house sensitive data like consumer personal information, intellectual property, and financial records. Without suitable protection, organizations can face reputational damage, compliance failure, and substantial financial impact in the event of a breach. Organizations protect valuable data-at-rest using encryption features native to leading database offerings.

Depending on the database product, encryption can be implemented at the database, tablespace, column, or cell level, and many organizations also encrypt the associated log and report files that may contain sensitive information. This means that the keys used to encrypt these files and databases must be protected, so they never land in the wrong hands. Theft or misplacement of keys can lead to exposure of the database records, resulting in financial damage from compliance violations and at worst case in a breach that can have significant implications on the business.

To ensure robust protection of the encryption, keys should always be isolated from the assets they protect, and maintained in a manner that aligns with data protection regulations and industry best practices. At the same time, keys must always be readily available to ensure optimum performance of the database and the applications that rely on its content.

Learn more about our HSMs at entrust.com/HSM

Enhanced database protection with Entrust high assurance key management

The Solution

Entrust KeyControl (formerly HyTrust) key management software (KMS) and Entrust nShield® hardware security modules (HSMs) integrate with leading database vendors to deliver enhanced database protection with centralized, automated cryptographic key management, and a root of trust for critical encryption keys.

Integration of the KeyControl KMS and nShield HSMs with leading databases including IBM DB2, Microsoft SQL Server, Mongo DB, and Oracle MySQL, ensures that underpinning cryptographic keys used to protect data are generated and managed throughout their lifecycle, and afforded the strongest security. Entrust KeyControl manages encryption keys across customer deployments, on-premises or in multi-cloud and hybrid environments. Using the Key Management Interoperability Protocol (KMIP), KeyControl establishes and enforces key use policies protecting encrypted data in storage. With the added option to integrate Entrust nShield HSMs, the solution can generate strong, high quality keys and safeguard them within a robust FIPS 140-2 Level 3 and Common Criteria EAL4+ security envelope.

Protection of keys is enforced by policy, which reduces the likelihood of an insider attack and mitigates the risk of data breaches. The combination delivers auditable security and facilitates compliance with regulatory and legislative mandates, including the Payment Card Industry Data Security Standard (PCI DSS) , the revised Directive for Payment Services (PSD2), the Healthcare Insurance Portability and Accountability Act (HIPAA), and other regulations.

The Entrust Difference

Entrust eases the burden of generating, managing, and safeguarding database encryption keys with flexible deployment options including clustering and failover. These capabilities ensure business continuity of critical systems in line with disaster recovery and data retention needs.

Entrust KeyControl manages keys across encrypted databases, and can scale to support thousands of encrypted workloads in large deployments. Up to four key managers can be added to a cluster to increase availability and resiliency in high volume key request environments. Integration of KeyControl with leading database solutions:

- Capitalizes on the KMIP open standard to establish the interface
- Enforces key use policies to separate security functions from administrative tasks

Addition of nShield HSMs to the integrated solution:

- Provides a tamper-resistant environment for generating high entropy keys
- Delivers certified root of trust to facilitate auditing and regulatory compliance

Learn more about our HSMs at entrust.com/HSM

Enhanced database protection with Entrust high assurance key management

nFinity partners

Learn more

To find out more about Entrust KeyControl visit entrust.com/digital-security/cloud-security-encryption-key-management. To find out more about Shield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications, and data visit **entrust.com**

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