



ENTRUST

Entrust and leading database providers enhance data security and compliance



Enhanced database protection with nShield hardware security modules (HSMs)

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 keys, 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 face reputational damage, compliance failure and substantial financial impact in the event of a breach. Organizations typically protect this valuable data-at-rest using the transparent data

encryption (TDE) or cell-level encryption (CLE) capabilities that are 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 are critical to protect, and must never land in the wrong hands. Theft or misplacement of the keys could lead to exposure of the database records, resulting in financial damage from compliance violations.

To ensure robust protection of the encryption keys, they should 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, the keys must always be readily available to ensure optimum performance of the database and the applications that rely on its content.

LEARN MORE AT [ENTRUST.COM/HSM](https://www.entrust.com/hsm)

Enhanced database protection with nShield HSMs

The solution: database encryption integrated with nShield HSMs

Entrust nShield hardware security modules (HSMs) integrate with leading database vendors to provide the root of trust for database encryption keys.

Using Entrust nShield HSMs, the master keys used to protect database encryption keys are afforded an additional layer of security. nShield HSMs deliver FIPS 140-2 Level 3 and Common Criteria EAL4+ certified security for your critical keys without requiring any changes to existing applications, database structures, or processes.

Protection of keys is enforced by policy, which reduces the likelihood of an insider attack and mitigates the risk of a data breach. The combination delivers auditable security, and facilitates compliance with regulatory and legislative mandates, including the Payment Card Industry Data Security Standard (PCI DSS).

The nShield difference

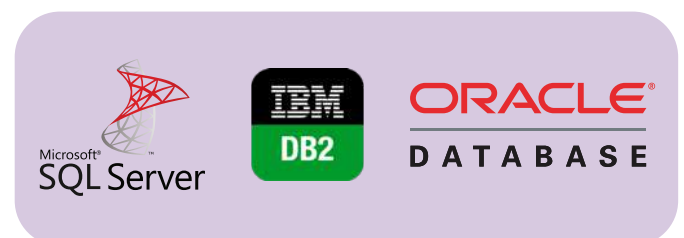
nShield HSMs ease the burden of safeguarding and managing database encryption keys with flexible deployment options including clustering and failover. These capabilities ensure business continuity of critical systems in line with your disaster recovery and data retention needs.

Available as a dedicated card for single server applications, or as a shared network appliance for virtualized environments, nShield HSMs separate security policy management from administrative functions, helping you meet the changing demands of your business.

nShield® HSMs deliver:

- Hardware key protection – Store database encryption keys in a secure, tamper-resistant environment isolated from the database administration to prevent copying or tampering
- Enforcement of users and roles – Extend access rights established in the databases for accessing encrypted data
- Tight control of keys – Smart card authentication of administrators firmly controls access to database encryption keys
- Separation of roles - Split responsibility for important tasks and procedures across multiple administrators
- Compliance support - Aligns with mandates requiring strong protection of customer information

nFinity partners



Learn more

To find out more about Entrust nShield HSMs visit [entrust.com/HSM](https://www.entrust.com/HSM). To learn more about Entrust's digital security solutions for identities, access, communications and data visit [entrust.com](https://www.entrust.com)

Learn more at [entrust.com/HSM](https://www.entrust.com/HSM)

