Stop data breaches by safeguarding the encryption keys protecting access to sensitive data

Databases are a significant repository of sensitive information in most organizations. Corporate databases contain customers' credit card data, confidential competitive information, and intellectual property. Lost or stolen data puts organizations at significant risk of reputation and brand damage as well as serious fines. By protecting critical data from both internal and external threats, organizations mitigate the risk of data breaches and comply with regulatory and legislative mandates, including the Payment Card Industry Data Security Standard (PCI DSS).

Amongst methods available for protecting sensitive data, database encryption has emerged as a leading approach because without the encryption keys data is inaccessible. Beginning with SQL Server 2008, Microsoft introduced the ability to encrypt an entire database using transparent data encryption (TDE), an addition to the existing feature of cell level encryption. With TDE, databases can be secured without changing existing applications, database structures, or processes.

Safeguard your database with the highest level of assurance

Encrypting the data in your database protects the data, but the encryption keys that unlock the data must also be protected. The use of hardware security modules (HSMs) safeguards encryption keys by storing the keys separately from the data. Thales HSMs shelter encryption keys away from applications and the operating system with proven, trusted encryption. Access to encryption keys is enforced by policy, protecting your database from compromise.

Seamless integration with Microsoft SQL Server

Thales HSMs integrate quickly and easily with Microsoft SQL Server utilizing Microsoft’s Extensible Key Management (EKM). EKM enables Thales HSMs to provide key management for multiple databases. You can also use Thales HSMs to protect keys used by other applications, such as those employing secure sockets layer (SSL). Thales HSMs safeguard the keys, affording protection from unauthorized access and ensuring the long-term usability of encrypted data.

Supporting your disaster recovery and data retention needs, Thales HSMs ease the burden of managing encryption with flexible deployment and management options. Available as a dedicated appliance for a single server or as a shared network appliance for virtualized environments, Thales HSMs are designed to meet the changing demands of your business.
Protect your brand and data
Validated to stringent security standards, such as FIPS 140-2 Level 3 and Common Criteria EAL 4+, Thales HSMs are ready to protect your data in even the most challenging and demanding security situations. Thales HSMs are:

> Approved for high-security environments
  Appropriate for public sector and security-conscious organizations.

> Reviewed by experts
  Accepted by regulatory and compliance organizations.

Control access to database encryption
Thales HSMs enable you to manage encryption keys for Microsoft SQL Server and other databases. To enforce your policies, security functions are separate from administrative functions. Thales HSMs deliver:

> Hardware key protection
  Stores database encryption keys in a secure, tamper-resistant environment to prevent copying or tampering.

> Enforcement of users and roles
  Extends access rights established in Microsoft SQL Server for accessing encrypted data.

> Tight control of keys
  Smart card authentication of administrators firmly controls access to database encryption keys.

> Separation of roles
  Responsibility for important tasks and procedures can be split across multiple administrators.

Easy setup and integration
Thales HSMs integrate seamlessly with Microsoft SQL Server and provide:

> Extensible Key Management configuration
  Easily configures TDE and cell-level encryption modes and the protection of applicable encryption keys.

> Smooth deployment
  Fully tested and supported by Thales and Microsoft for quick deployment.

> Out of the box integration
  Tested and fully documented configurations.

Solution Specifications
Microsoft SQL Server 2008 and 2008 R2 support Thales HSMs to secure the encryption keys.
Thales HSMs are available in the following variants:

> nShield Edge: a portable USB-attached HSM ideal for offline root CAs and developer code signing.

> nShield Solo: an embedded PCI or PCIe HSM ideal for SSL web servers and security appliances.

> nShield Connect: a high performance, network-attached HSM for high availability data center environments.

Thales HSMs are designed and certified to provide encryption services for systems running Microsoft SQL Server 2008 and 2008 R2, providing FIPS 140-2 Level 3 and Common Criteria EAL 4+

For more detailed technical specifications, please visit www.thales-esecurity.com

Scale to meet your changing needs
Thales HSMs integrate out of the box with leading enterprise applications, including web and application servers and public key infrastructures. Network attached HSMs can be shared by several servers providing:

> Support for virtualized environments
  Hardware-based key storage for virtualized servers, including Hyper-V and VMware.

> Simplified administration
  Manages the encryption keys for many databases as well as keys used by other applications.

> Performance
  Hardware acceleration enables organizations to avoid bottlenecks.

> Clustering and failover
  Thales HSMs can be clustered and support Microsoft SQL Server clusters to ensure business continuity of critical systems.

> Disaster recovery
  Simple and secure processes for archiving and recovering keys.

> Cost-effective resource
  Shared use of the module across several servers reduces hardware, licensing, and operational costs.

Thales - Security Solutions & Services

Protect your brand and data
Validated to stringent security standards, such as FIPS 140-2 Level 3 and Common Criteria EAL 4+, Thales HSMs are ready to protect your data in even the most challenging and demanding security situations. Thales HSMs are:

> Approved for high-security environments
  Appropriate for public sector and security-conscious organizations.

> Reviewed by experts
  Accepted by regulatory and compliance organizations.

Control access to database encryption
Thales HSMs enable you to manage encryption keys for Microsoft SQL Server and other databases. To enforce your policies, security functions are separate from administrative functions. Thales HSMs deliver:

> Hardware key protection
  Stores database encryption keys in a secure, tamper-resistant environment to prevent copying or tampering.

> Enforcement of users and roles
  Extends access rights established in Microsoft SQL Server for accessing encrypted data.

> Tight control of keys
  Smart card authentication of administrators firmly controls access to database encryption keys.

> Separation of roles
  Responsibility for important tasks and procedures can be split across multiple administrators.

Easy setup and integration
Thales HSMs integrate seamlessly with Microsoft SQL Server and provide:

> Extensible Key Management configuration
  Easily configures TDE and cell-level encryption modes and the protection of applicable encryption keys.

> Smooth deployment
  Fully tested and supported by Thales and Microsoft for quick deployment.

> Out of the box integration
  Tested and fully documented configurations.

Solution Specifications
Microsoft SQL Server 2008 and 2008 R2 support Thales HSMs to secure the encryption keys.
Thales HSMs are available in the following variants:

> nShield Edge: a portable USB-attached HSM ideal for offline root CAs and developer code signing.

> nShield Solo: an embedded PCI or PCIe HSM ideal for SSL web servers and security appliances.

> nShield Connect: a high performance, network-attached HSM for high availability data center environments.

Thales HSMs are designed and certified to provide encryption services for systems running Microsoft SQL Server 2008 and 2008 R2, providing FIPS 140-2 Level 3 and Common Criteria EAL 4+

For more detailed technical specifications, please visit www.thales-esecurity.com

Scale to meet your changing needs
Thales HSMs integrate out of the box with leading enterprise applications, including web and application servers and public key infrastructures. Network attached HSMs can be shared by several servers providing:

> Support for virtualized environments
  Hardware-based key storage for virtualized servers, including Hyper-V and VMware.

> Simplified administration
  Manages the encryption keys for many databases as well as keys used by other applications.

> Performance
  Hardware acceleration enables organizations to avoid bottlenecks.

> Clustering and failover
  Thales HSMs can be clustered and support Microsoft SQL Server clusters to ensure business continuity of critical systems.

> Disaster recovery
  Simple and secure processes for archiving and recovering keys.

> Cost-effective resource
  Shared use of the module across several servers reduces hardware, licensing, and operational costs.