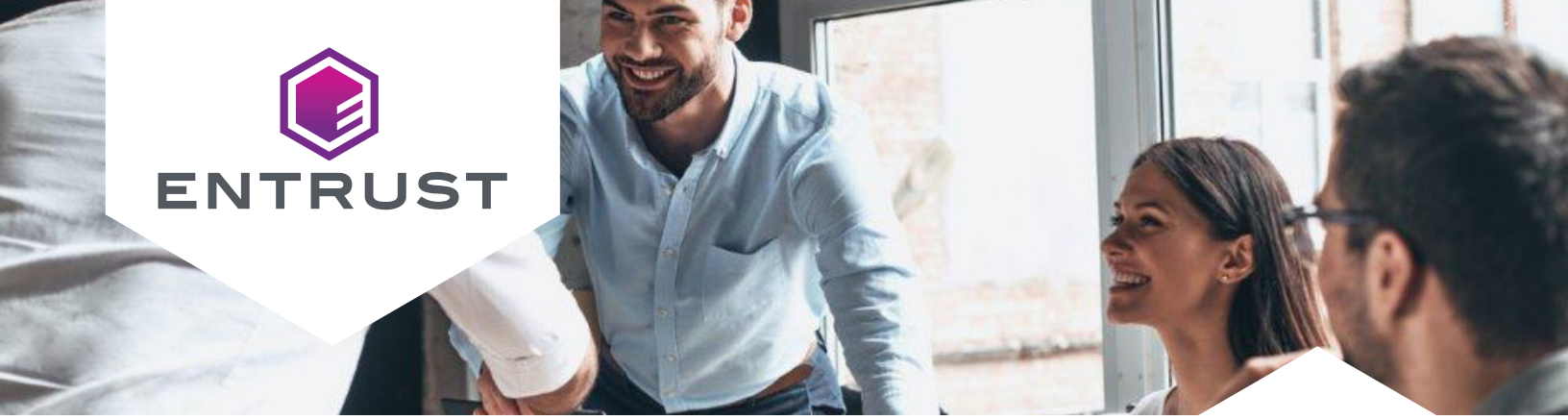


Entrust encryption solution for Microsoft Azure SQL databases

Microsoft

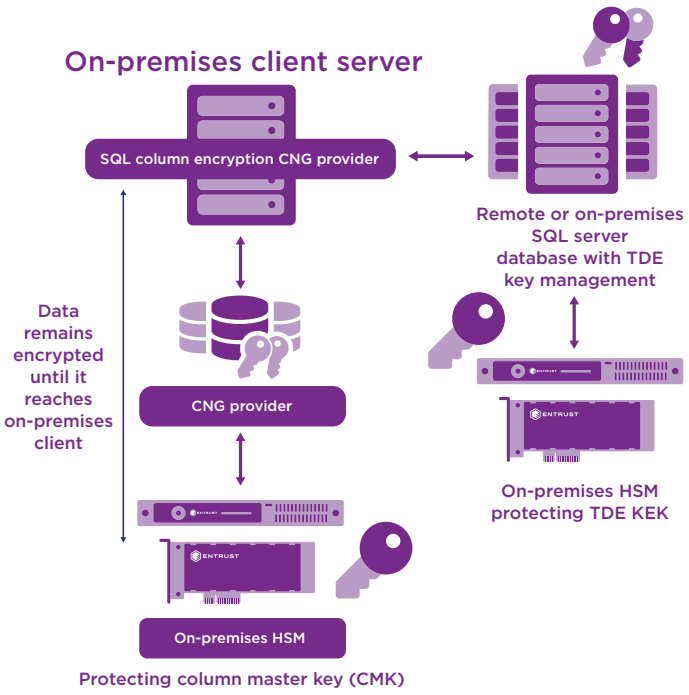
Protect sensitive data at rest and in use across on-premises and Azure-based client applications

HIGHLIGHTS

- Encrypt data at rest in the database and in flight between databases
- Protect encryption keys within customers' trusted environment
- Prevent hosted service provider from viewing your sensitive data
- Ensure database administrators cannot access the sensitive data
- Reduce scope of audit and facilitate compliance (GDPR, HIPAA)

The problem: sensitive data stored in databases is increasingly the target of attacks

With more sensitive data maintained across on-premises and cloud-based environments, databases have become targets of advanced attacks. While encryption offers a mechanism to protect the confidentiality and integrity of data in storage, it does not protect data traveling to and from databases. Encryption can also affect the ability of applications to receive and use data, and does not prevent administrators with elevated privileges from accessing encrypted data.



Entrust nShield hardware security modules (HSMs) protect and manage the column master key (CMK) that wraps the column encryption keys (CEKs) that encrypt the data.

LEARN MORE AT ENTRUST.COM/HSM

Entrust encryption solution for Microsoft Azure SQL databases

The challenge: securing senstive data while enabling database transactional and analytical processes to work unhindered

Needing to first decrypt sensitive data from encrypted storage can expose sensitive data to internal and external threats. Enabling clients to encrypt sensitive data inside their applications, while never revealing the encryption keys to the database engine, provides the separation needed between those who own the data and can view it, and those who only manage it and should not have access. Protecting databases in a manner that enables applications to perform their transactions and/or analytical processes requires specialized technology.

The solution: Microsoft Azure SQL databases with Entrust nShield HSMs

Always Encrypted is a feature in Windows Server 2016 designed to protect sensitive data at rest and in use between on-premises client application servers and Azure SQL Server databases. Always Encrypted can be used in conjunction with transparent data encryption (TDE), but while TDE runs on the SQL Server, Always Encrypted runs on the client – protecting data before it hits the server. Data protected by Always Encrypted remains unreadable until it reaches the on-premises client application – effectively mitigating man-in-the-middle attacks, and providing assurances against unauthorized activity from rogue database administrators or administrators with access to SQL Server/ Azure databases.

When used with Entrust nShield Solo and Connect HSMs the critical master key that protects the encryption keys is secured within a high assurance hardware environment. Entrust nShield HSMs support Microsoft Azure SQL Server 2016 Always Encrypted and enable customers to confidently store sensitive data outside of their direct control.

Why use Entrust nShield solo and connect HSMs with Microsoft SQL server 2016 always encrypted?

HSMs enhance the security of valuable cryptographic material. Entrust nShield HSMs integrate with Microsoft SQL Server 2016 Always Encrypted to extend the logical and physical protection of critical master keys. The combined solution delivers an auditable method for enforcing security policies. Entrust nShield HSMs enable Microsoft SQL Server 2016 Always Encrypted customers to:

- Secure keys within a carefully designed cryptographic boundary that uses robust access control mechanisms, so keys are only used for their authorized purpose
- Ensure key availability by employing sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed by the database engine
- Deliver superior performance to support demanding applications

Entrust encryption solution for Microsoft Azure SQL databases

Entrust nShield HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. nShield:

- Provides a tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Enforces key use policies, separating security functions from administrative tasks
- Integrates with Always Encrypted using industry recognized APIs (CAPI and CNG).

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Microsoft

SQL Server has transformed the way organizations utilize their mission-critical data. SQL Server not only maintains protected storage and control access to database resources, but also enables real-time insight across transactional and analytical assets, establishing trustworthy business environments.

Microsoft SQL Server:

- Protects data at rest and in use
- Controls user access
- Enables real-time advanced analytics
- Scales across the enterprise and cloud
- For more detailed technical specifications, please visit

www.microsoft.com

Gold Microsoft Partner Microsoft

SQL Server 2016 Certified

Learn more

To find out more about Entrust nShield® HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com