nCipher
AN ENTRUST DATACARD COMPANY

www.ncipher.com

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

- 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)

Microsoft

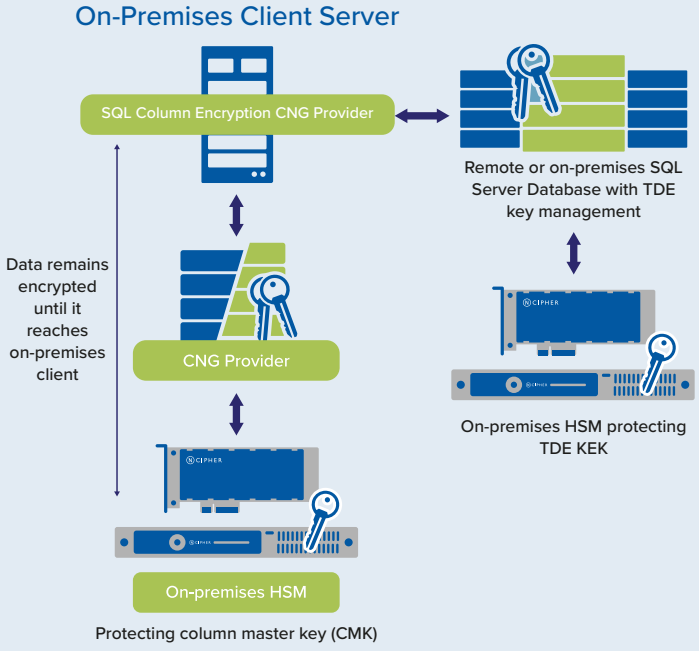
nCipher encryption solution for Microsoft Azure SQL databases

THE PROBLEM: SENSITIVE DATA STORED IN DATABASES IS INCRESINGLY 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.

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.



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

nCipher encryption solution for Microsoft Azure SQL databases

THE SOLUTION: MICROSOFT AZURE SQL DATABASES WITH NCIPHER NSHIELD HARDWARE SECURITY MODULES (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 nCipher nShield Solo and Connect HSMs the critical master key that protects the encryption keys is secured within a high assurance hardware environment. nCipher 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 NCIPHER NSHIELD SOLO AND CONNECT HSMs WITH MICROSOFT SQL SERVER 2016 ALWAYS ENCRYPTED?

HSMs enhance the security of valuable cryptographic material. nCipher 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. nCipher 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

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

- 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).

NCIPHER - AN ENTRUST DATACARD COMPANY

Today's fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks. nCipher Security empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications.

Our cryptographic solutions secure emerging technologies—cloud, IoT, blockchain, digital payments—and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control—today, tomorrow, at all times.

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.ncipher.com or www.microsoft.com

Gold Microsoft Partner Microsoft

SQL Server 2016 Certified

Search: nCipherSecurity

www.ncipher.com

nCipher AN ENTRUST DATACARD COMPANY