Confidential computing with *Always Encrypted with secure enclaves*

Pieter Vanhove
Program Manager - Microsoft

Motivation

Enable customers to confidently store their most sensitive data in the cloud

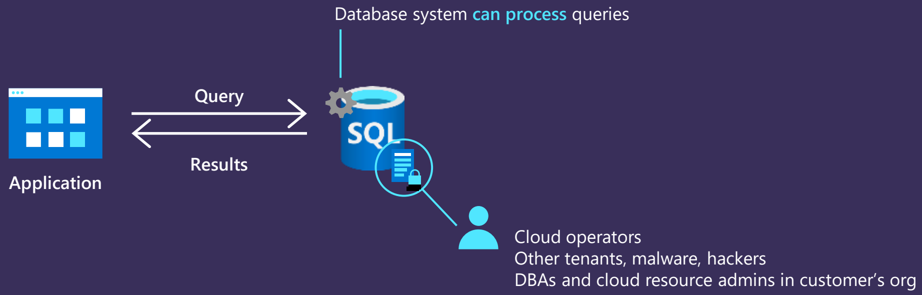
Customers can stay in control of their data

Protect sensitive data in use from high-privileged yet unauthorized users

Traditional access control (SQL permissions, RBAC) and encryption technologies (TDE/TLS) are insufficient
Third-party client-side encryption solutions make it impossible to query and process the protected data in the cloud

Support confidential computations

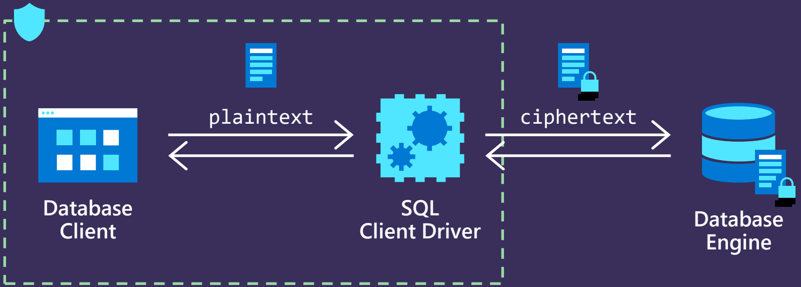
Query processing without exposing data to admins


Database system **can process** queries
Query
Results
Application
SQL
Cloud operators
Other tenants, malware, hackers
DBAs and cloud resource admins in customer's org

SQL Server 2016 and later, Azure SQL Database/Managed Instance
Cosmos DB

Always Encrypted

Protects data in-use from malicious DBAs, OS admins, and malware



Client-side encryption

Client-side encryption of sensitive data using keys that are never given to the database system

Encryption transparency

Client driver transparently encrypts query parameters and decrypts encrypted results

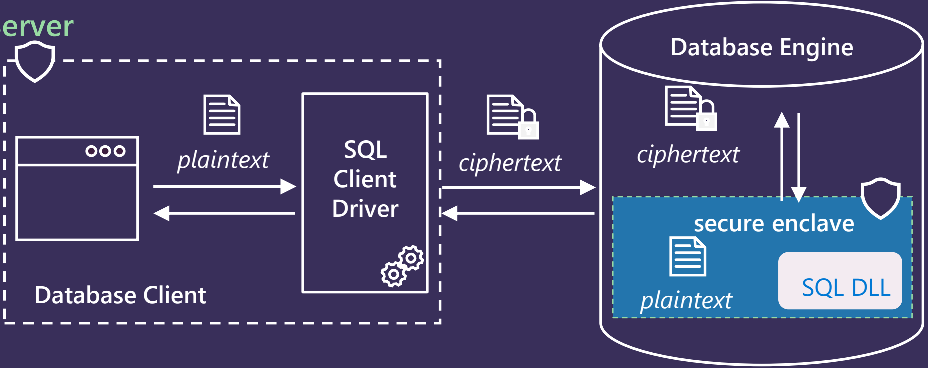
Confidential equality comparisons

Point lookup searches, equality joins, grouping via deterministic encryption

Always Encrypted with secure enclaves

In Azure SQL Database and SQL Server

Protects sensitive data in use
while providing rich confidential computing capabilities



Secure computations inside the enclave

Database Engine delegates operations on encrypted data to the enclave, where the data can be safely decrypted and processed

Rich queries

Pattern matching (LIKE), range queries (<, >, etc.), sorting, indexing, and more

In-place encryption

The enclave can perform initial data encryption and key rotation, without moving the data out of the database

What are enclaves?

Enclave

An isolated region of memory

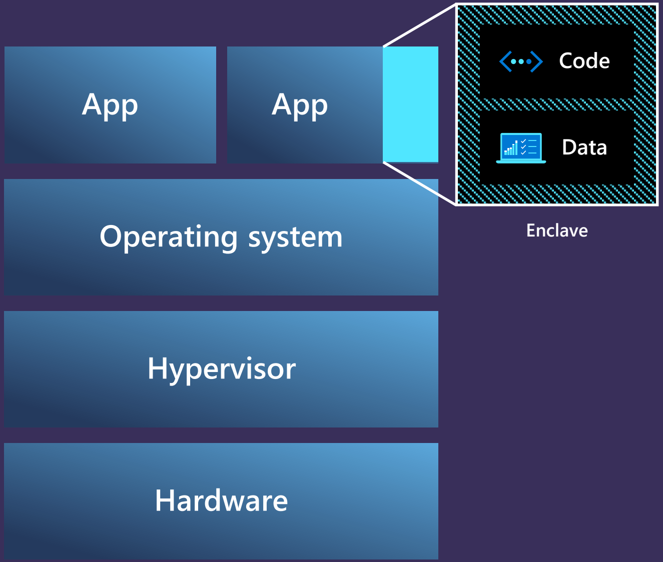
Provides a trusted execution environment

Data stored inside the enclave cannot be accessed outside of the enclave

Secure isolation powered by:

Hypervisor, e.g., Virtualization-Based Security (VBS) in Windows Server 2019 and later, Windows 10, v. 1809 and later

Hardware, e.g., Intel Software Guard Extension (Intel SGX)



Secure Enclaves in Azure SQL Database

	Intel Software Guard eXtensions (SGX)	Virtualization-based security (VBS)
	Available in DC-series hardware configuration	No hardware dependency
Purchasing model	vCore model	DTU and vCore
Compute mode	Provisioned	Provisioned and serverless
Compute size	Up to 40 (physical) vCores	Any (up to 128 vCores in vCore model)
Regional availability	Regional availability: East/West US, North/West EU, East Canada, UK South, Southeast Asia	All Azure regions (at general availability)
Security	Protection from rogue customer's DBAs	Protection from rogue customer's DBAs
	Protection from attacks originating from both guest and host OS (rogue cloud operators, malware)	Protection from attacks originating from guest OS (rogue cloud operators, malware), but **not** host OS

DEMO

Always Encrypted with VBS enclaves
in Azure SQL Database

Resources Always Encrypted

Blog Post	aka.ms/sqldb-enclaves-blog
Documentation	aka.ms/AlwaysEncryptedEnclavesAzureSQLDB
Tutorial	aka.ms/AlwaysEncryptedEnclavesAzureSQLDBTutorial
Data Exposed	aka.ms/AlwaysEncryptedEnclavesDataExposed
Always Encrypted Podcast	The Azure Security Podcast
Sample Code	aka.ms/AlwaysEncryptedEnclavesSampleCode

We’d love to hear your feedback

Please contact us at

alwaysencryptedpg@microsoft.com

Contact us!

info@oc3.dev