Securing your Data is easier than ever with Azure SQL Database
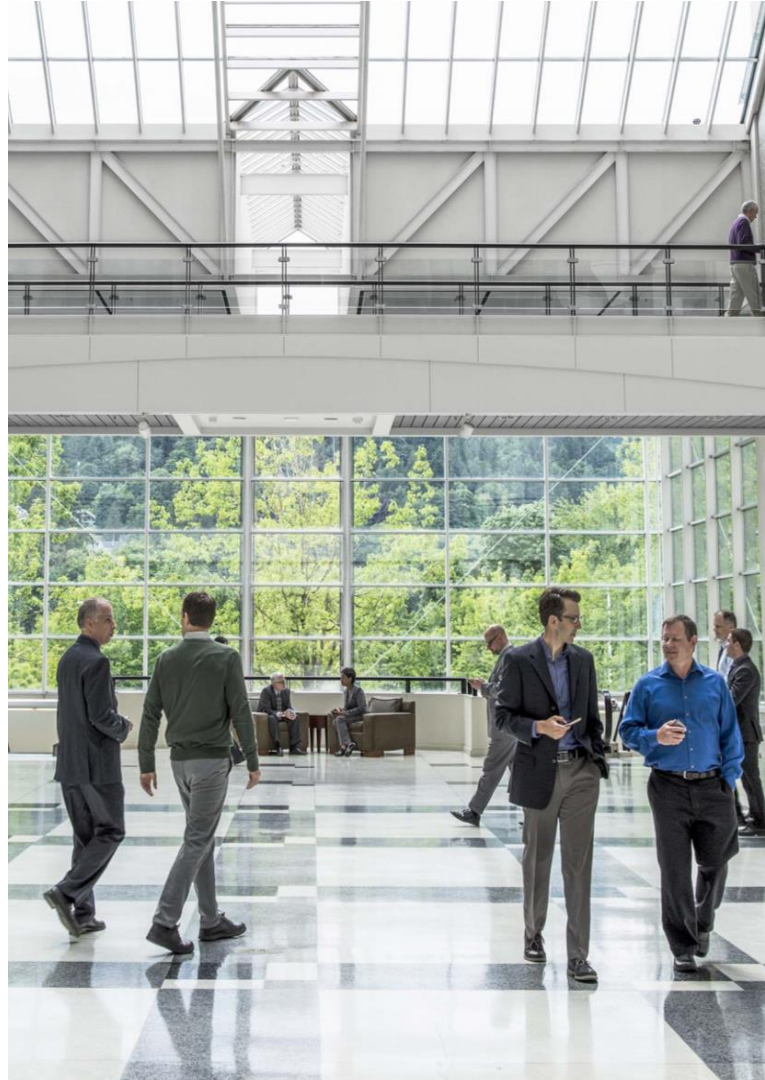
A walk around the security toolset

Ronit Reger, Senior Program Manager, Microsoft

TURBULENT TIMES

2 Billion records compromised in the last year

140+ DAYS between infiltration and detection

$150 MILLION average cost of a breach by 2020

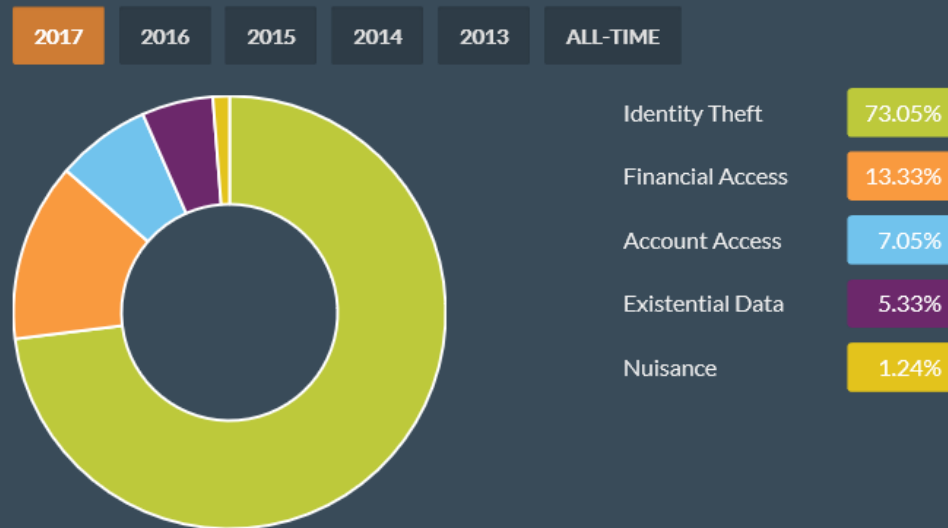# Data Privacy in today's world

5,286,896 data records breached **each day**

ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless

91% of adults agree that consumers have **lost control** of how personal information is collected and used by companies.

67% of CISOs believe their companies are likely to be targeted by a cyberattack or face a data breach in **2018**

NUMBER OF BREACH INCIDENTS BY TYPE

| 2017 | 2016 | 2015 | 2014 | 2013 | ALL-TIME |

Identity Theft	73.05%
Financial Access	13.33%
Account Access	7.05%
Existential Data	5.33%
Nuisance	1.24%

Sources: http://breachlevelindex.com/, http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/, http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/, http://src.bna.com/vAu

Data Privacy in today's world

"Three quarters of us don't trust businesses to do the right thing with our emails, phone numbers, preferences and bank details. I find that shocking."

Elizabeth Denham, UK Information Commissioner, Jan. 2017

Data protection landscape

Standards of data protection: Data privacy standards and policies + information security - new standards to protect data

Regulations: Legislations and regulations across the globe

GDPR – May 25, 2018 – **"Game changer"**

Industry activity: Data protection and compliance-supporting products and solutions; consultation services and specialists

Microsoft's commitment to GDPR

Microsoft believes GDPR is an important step forward for clarifying and enabling individual privacy rights

Together with our partners, Microsoft is prepared to help customers meet policy, people, process, and technology goals on the journey to GDPR
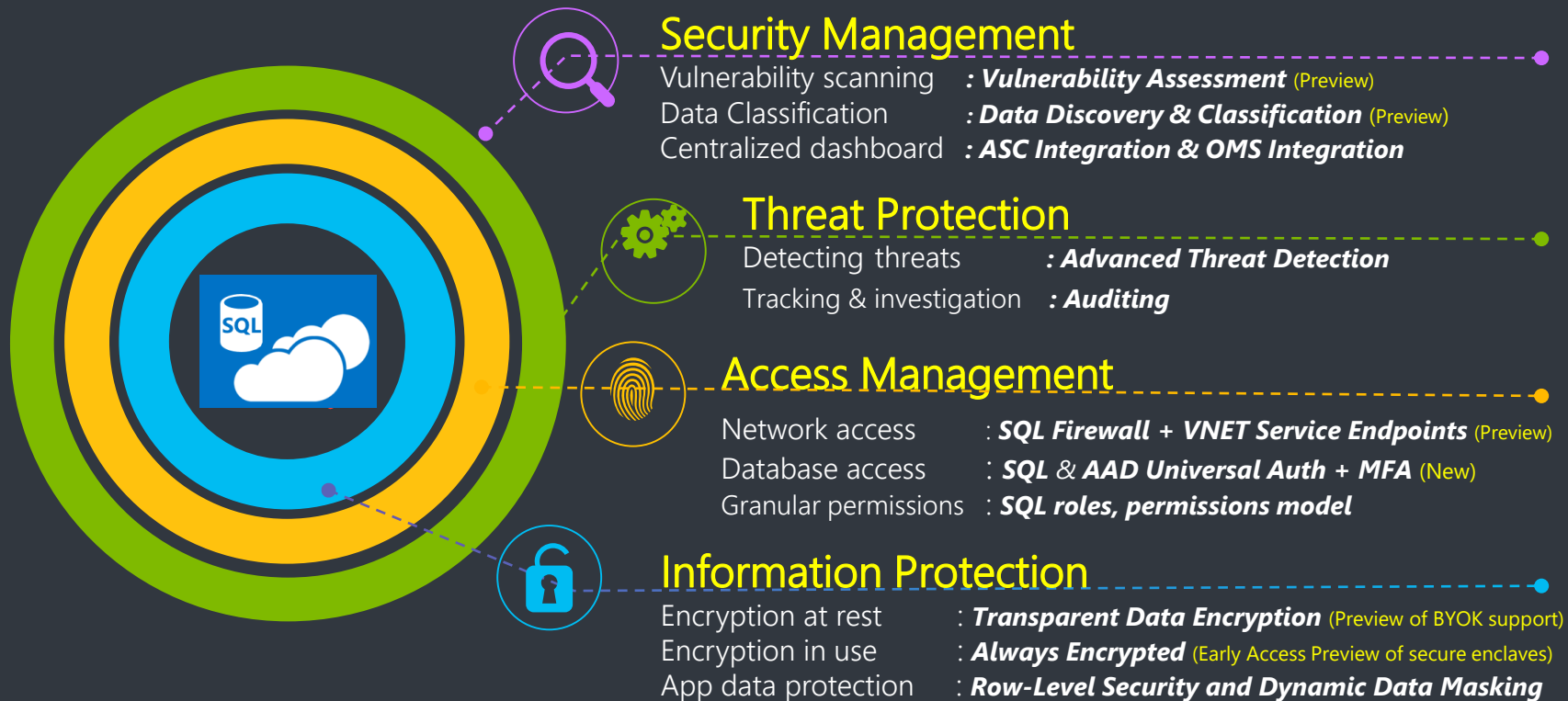
Microsoft commitment → Innovations

Investments across the company to help customers with GDPR and data privacy;

In SQL: Introducing new advanced security features and tools that can help support data privacy efforts;

Protection and Intelligence: Fundamental data security + automation and intelligent insights

Microsoft

SQL Security in layers

Security Management
Vulnerability scanning   **: Vulnerability Assessment** (Preview)
Data Classification   **: Data Discovery & Classification** (Preview)
Centralized dashboard   **: ASC Integration & OMS Integration**

Threat Protection
Detecting threats   **: Advanced Threat Detection**
Tracking & investigation **: Auditing**

Access Management
Network access   : **SQL Firewall + VNET Service Endpoints** (Preview)
Database access   : **SQL** & **AAD Universal Auth + MFA** (New)
Granular permissions   : **SQL roles, permissions model**

Information Protection
Encryption at rest   : **Transparent Data Encryption** (Preview of BYOK support)
Encryption in use   : **Always Encrypted** (Early Access Preview of secure enclaves)
App data protection   : **Row-Level Security and Dynamic Data Masking**

Compliance:
FedRAMP,   HIPAA,   PCI,   EU Model Clauses, GDPR, UK G-Cloud, ISO,
(government),   (healthcare), (payment), (personal),   (public sector)

Security Management

Effective database security requires

Visibility

CUSTOMERS NEED...

Security best practices

Keep up with recommended settings

Visibility

Tracking changes which can introduce vulnerabilities

Compliance

Regulatory audits, internal or external reviews

SQL VULNERABILITY ASSESSMENT

A one-stop-shop to **track** *and* **improve** *your SQL security state*

Get Visibility
Discover sensitive data and potential security vulnerabilities

Remediate
Actionable remediation and security hardening steps

Customize
Baseline policy tuned to your environment, so you focus on deviations

Report
Pass internal or external audits, facilitates compliance
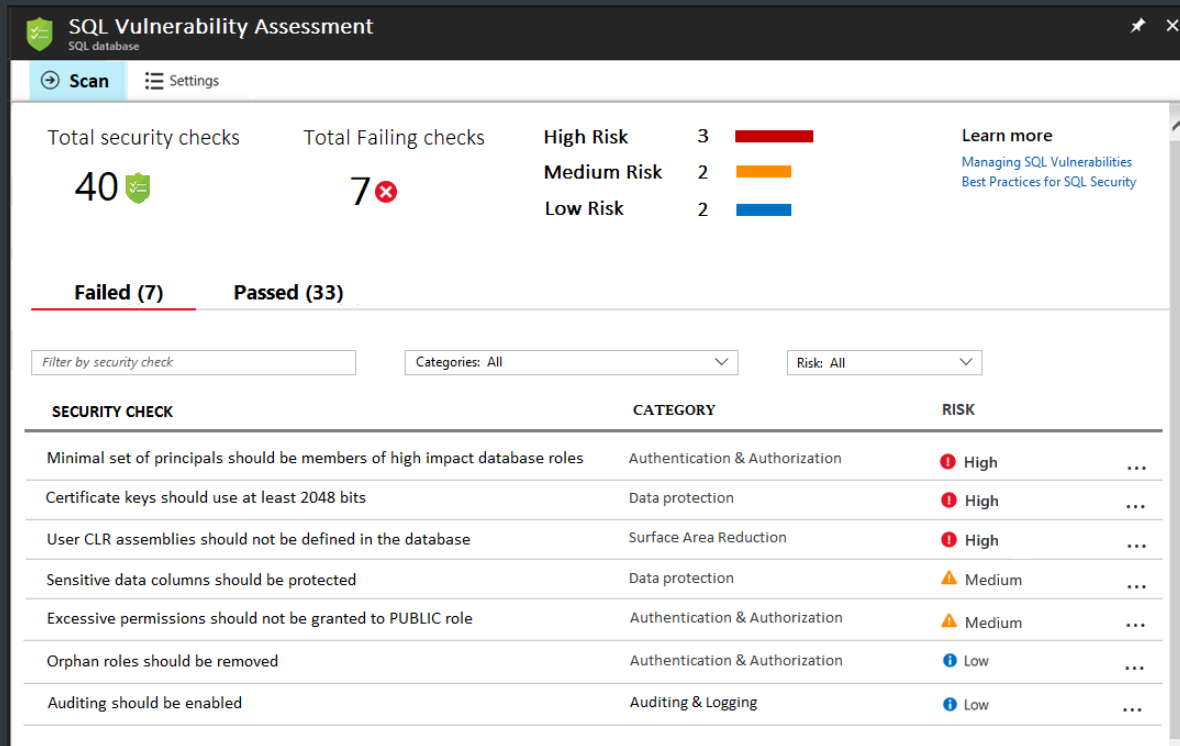
SQL Vulnerability Assessment

Demo – Azure portal

SQL Vulnerability Assessment – for SQL Server!

Demo – SSMS

SQL Data Discovery & Classification

Secure the data, not just the database

- ✓ Automated discovery and classification of sensitive data

- ✓ Labeling (tagging) sensitive data on column level with persistency

- ✓ Audit access to sensitive data

- ✓ Visibility through dashboards & reports

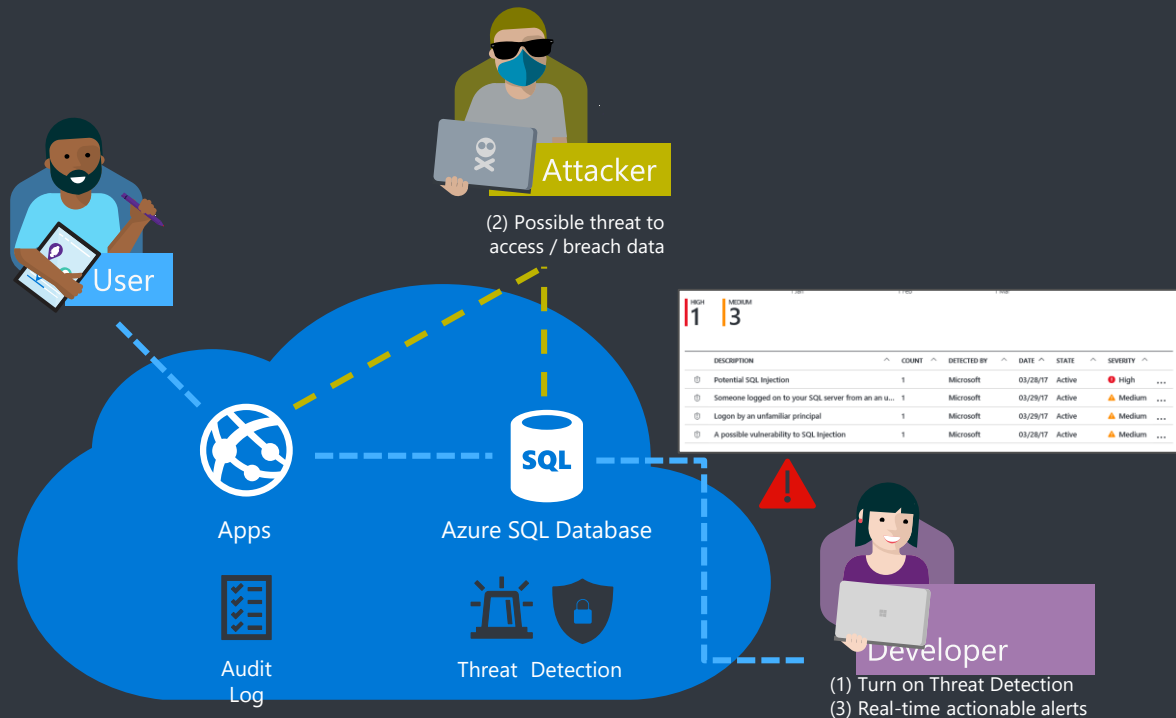- ✓ Hybrid cloud + on-premises
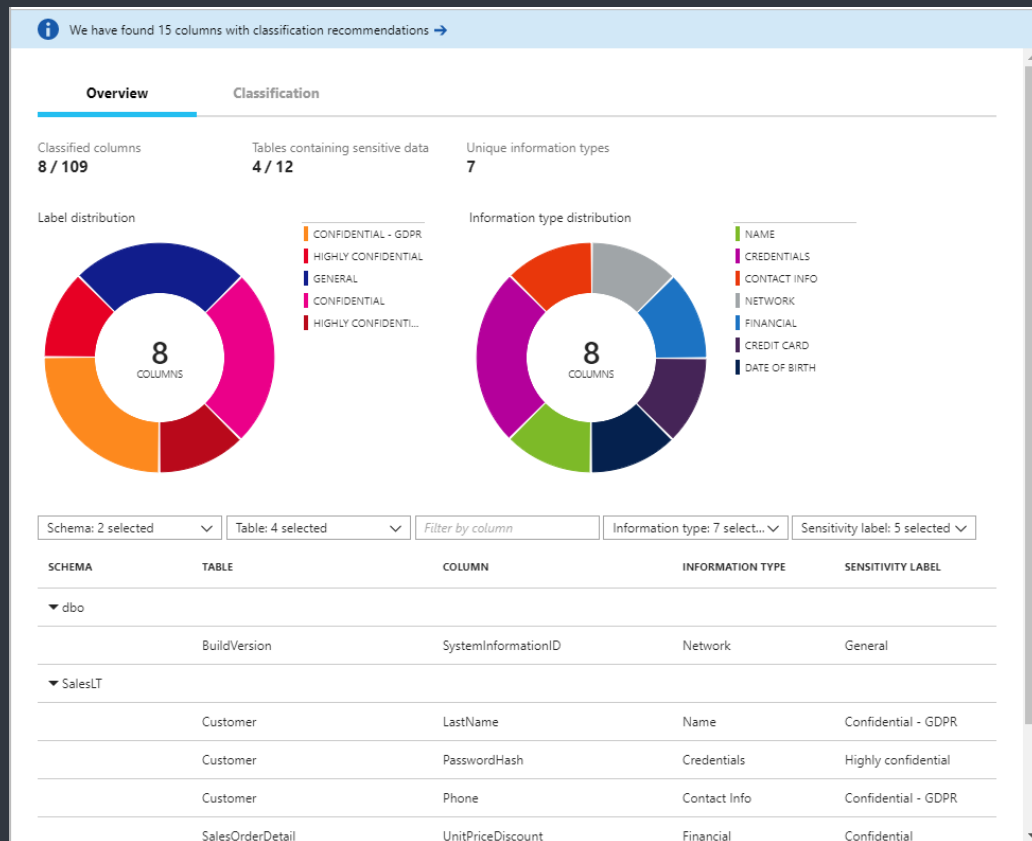
Data Discovery & Classification

Demo

Threat Protection

Advanced Threat Detection

Detect and respond to suspicious database activities

Generally Available

Attacker

(2) Possible threat to access / breach data

User

Apps

Azure SQL Database

Audit Log

Threat Detection

Developer

(1) Turn on Threat Detection
(3) Real-time actionable alerts

HIGH	MEDIUM						
1	3						
DESCRIPTION		COUNT	DETECTED BY	DATE	STATE	SEVERITY	
Potential SQL Injection		1	Microsoft	03/28/17	Active	High	...
Someone logged on to your SQL server from an an u...		1	Microsoft	03/29/17	Active	Medium	...
Logon by an unfamiliar principal		1	Microsoft	03/29/17	Active	Medium	...
A possible vulnerability to SQL Injection		1	Microsoft	03/28/17	Active	Medium	...

✓ Just turn it ON

✓ Detects potential vulnerabilities and SQL injection attacks

✓ Detects unusual behavior activities

✓ Actionable alerts which recommend how to investigate & remediate

*Incurs a charge of $15/server/month , first 60 days for free.

SQL Threat Detection

Demo
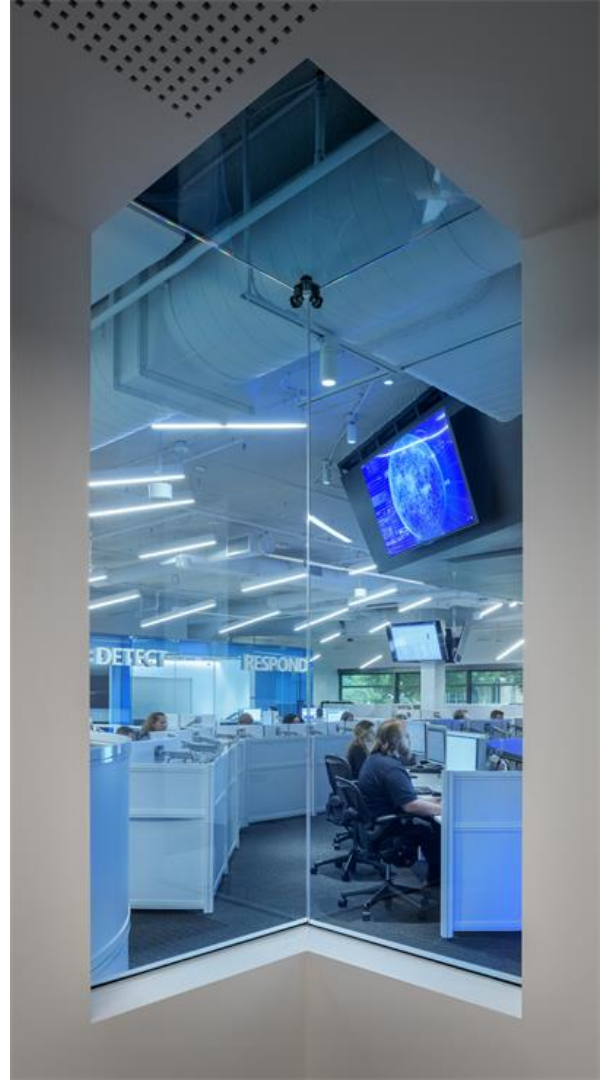
Access Management

Azure Active Directory Authentication

*Enable central identity management for SQL DB*

Central ID Management

- ✓ Helps stop the proliferation of user identities across servers
- ✓ Allows password rotation in a single place
- ✓ **Supports MFA/2FA authentication**

Simplified Permissions management

- ✓ Individual users; Groups; External users w/o Azure AD

Integrated Authentication

- ✓ Integrated Windows auth and single sign-on
- ✓ **Universal/Interactive authentication**
- ✓ Certificate-based authentication
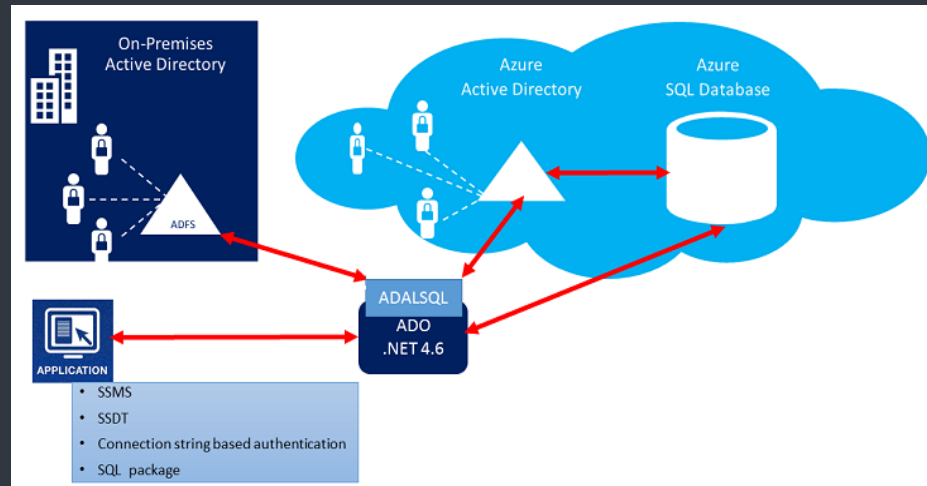
VNET Service Endpoints

Restrict access to your SQL Server from a given VNET/subnet

Extends VNET to SQL PaaS:

✓ An app layer firewall, no messing with IPs

✓ Logical SQL Servers are Restricted to be accessed from specific VNET(s)/Subnet(s)

✓ Routing within the Azure Network

✓ Tunneling is provisioned by Azure – no need to deal with setting up keys, gateways
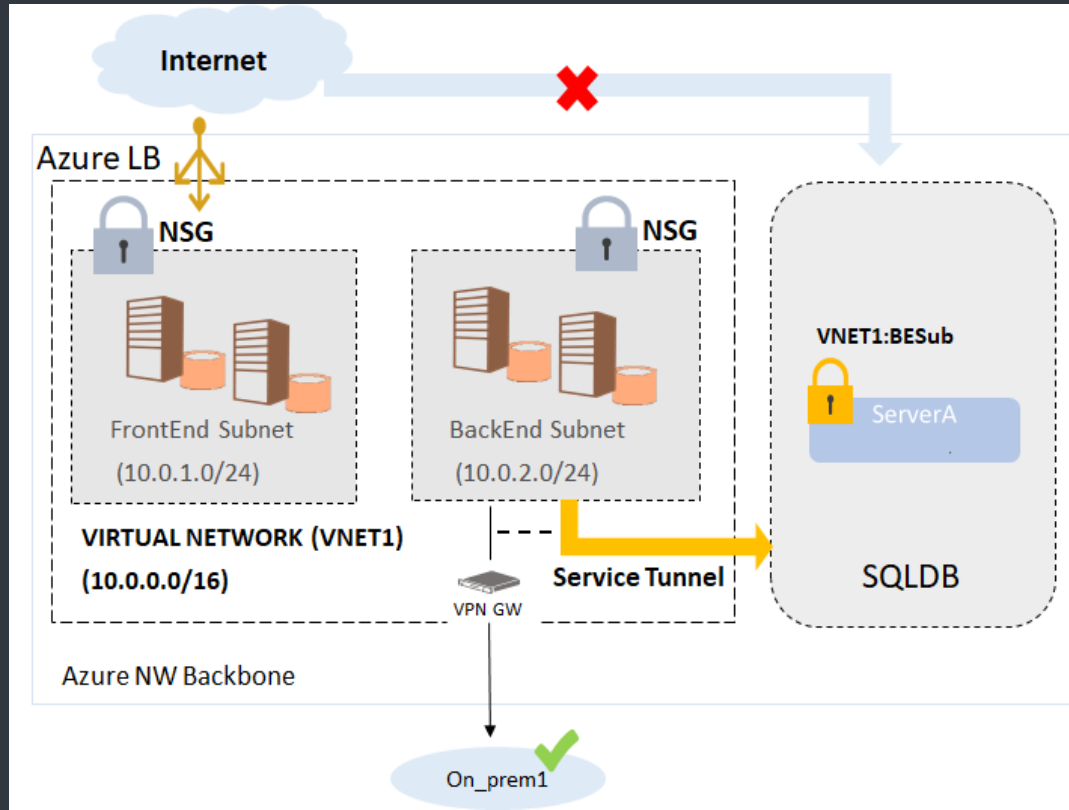
VNET Service Endpoints

Demo

Data Protection

TDE with Bring Your Own Key support

Strengthens customer trust in the cloud and meets compliance requirements that demand separation of key and data management

Encryption-at-rest is on by default

✓ AES-256 encryption encrypts the database, associated backups, and transaction log files at rest

User-controlled TDE protector keys

✓ Stored and managed in Azure Key Vault

✓ Leverage Key Vault's scalability, security, and redundancy

✓ Can be generated by user's own HSM on premise
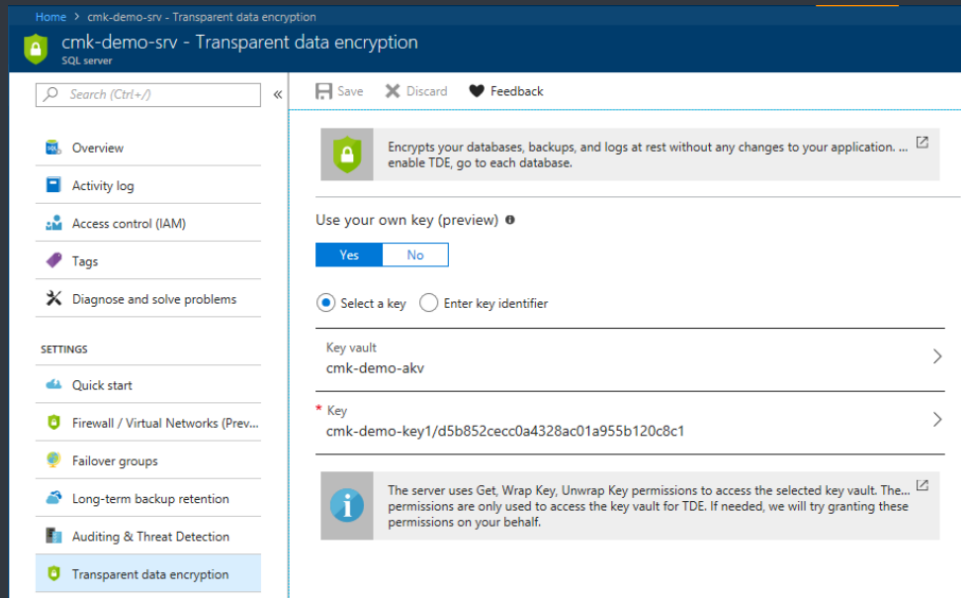
Always Encrypted using Secure Enclaves

*Protects sensitive data in use while **enabling rich computations** and **in-place encryption***
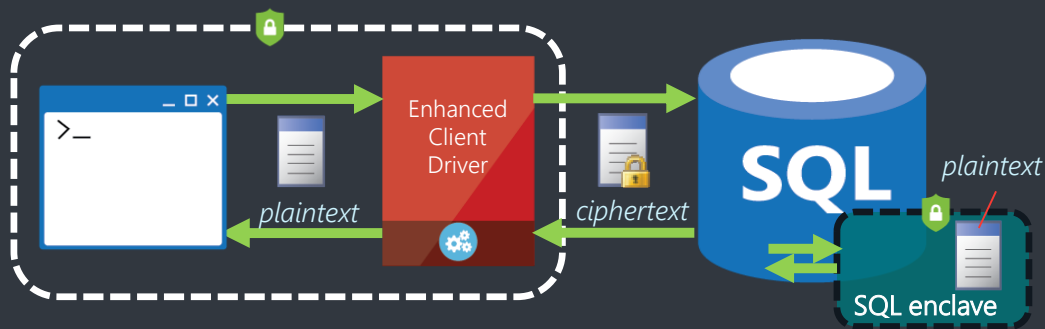
Confidential computing brings secure enclaves to Azure

- Trusted execution environments protecting data in use

- SQL Server Engine delegates operations on encrypted data to the enclave, where the data can be safely decrypted and processed.

- Rich computations on encrypted data!

- In-place encryption and key management, without moving data out of the database
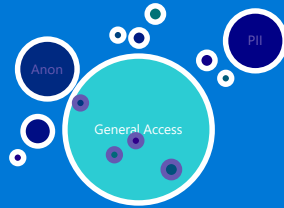
SQL Security Future Goals

| Security By Default | Easy to use & Intelligent Security | Scalable Security Policies | Consistent Security Across Entire SQL Family | Trusted Cloud |

Just like Jimi Hendrix ...

We love to get feedback

Please complete the session feedback forms

sqlbits

SQLBits - It's all about the community...

Please visit Community Corner, we are trying this year to get more people to learn about the SQL Community, equally if you would be happy to visit the community corner we'd really appreciate it.

sqlbits

Thank You

Learn more from Ronit Reger

in /ronit-reger-95b89   ✉ ronitr@microsoft.com

Microsoft