Microsoft

# sqlbits

Welcomes you!

# Azure SQL Database Security

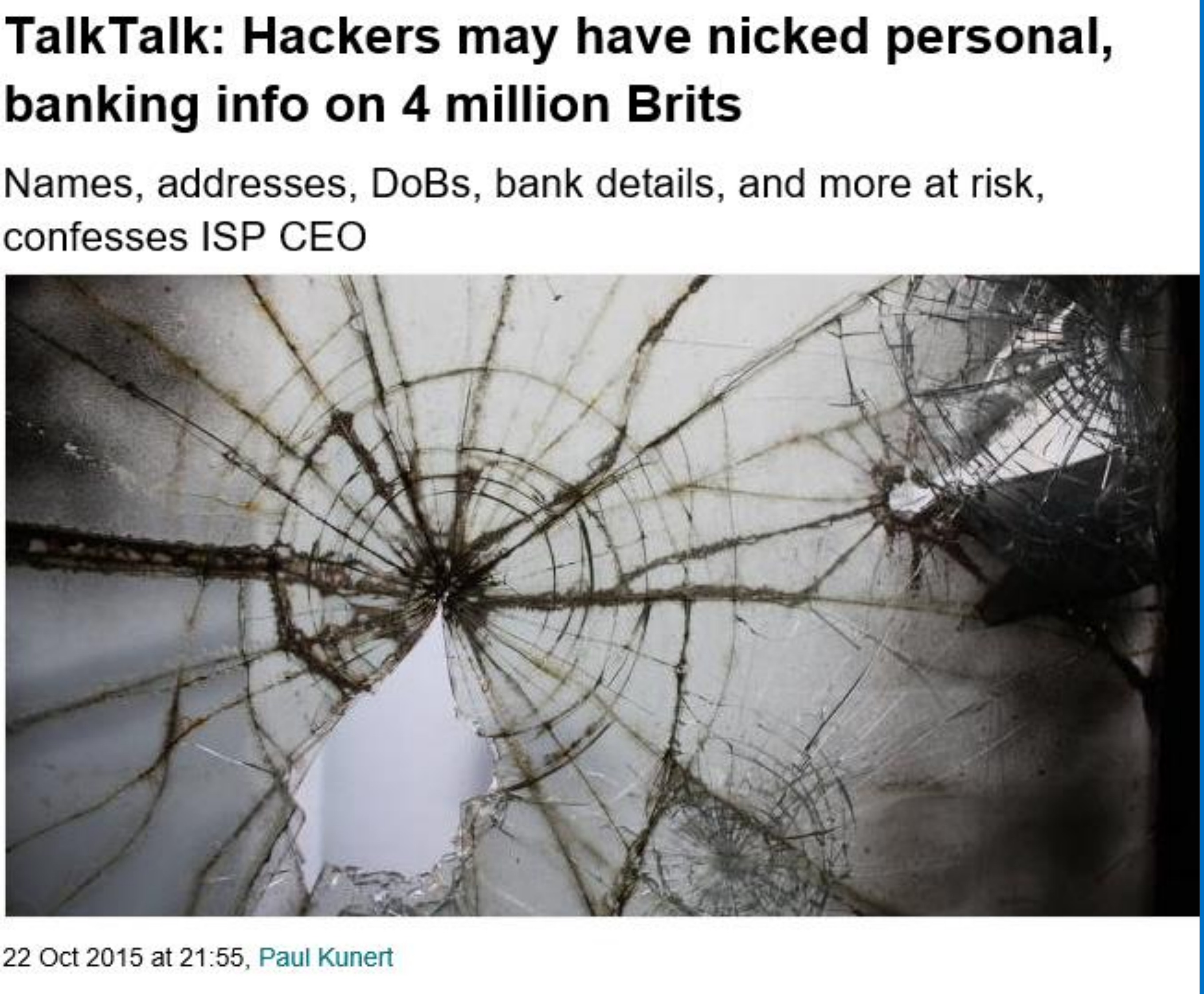
## Securing your data is easier than ever

Ron Matchoro
Senior Program Manager

May 2016

sqlbits Microsoft

# A recent successful data breach



## TalkTalk: Hackers may have nicked personal, banking info on 4 million Brits

Names, addresses, DoBs, bank details, and more at risk, confesses ISP CEO

22 Oct 2015 at 21:55, Paul Kunert

Source: Dennoir/Flickr.com

**DDoS attack on the TalkTalk Web site**

↓

**SQL injection to retrieve data from the database**

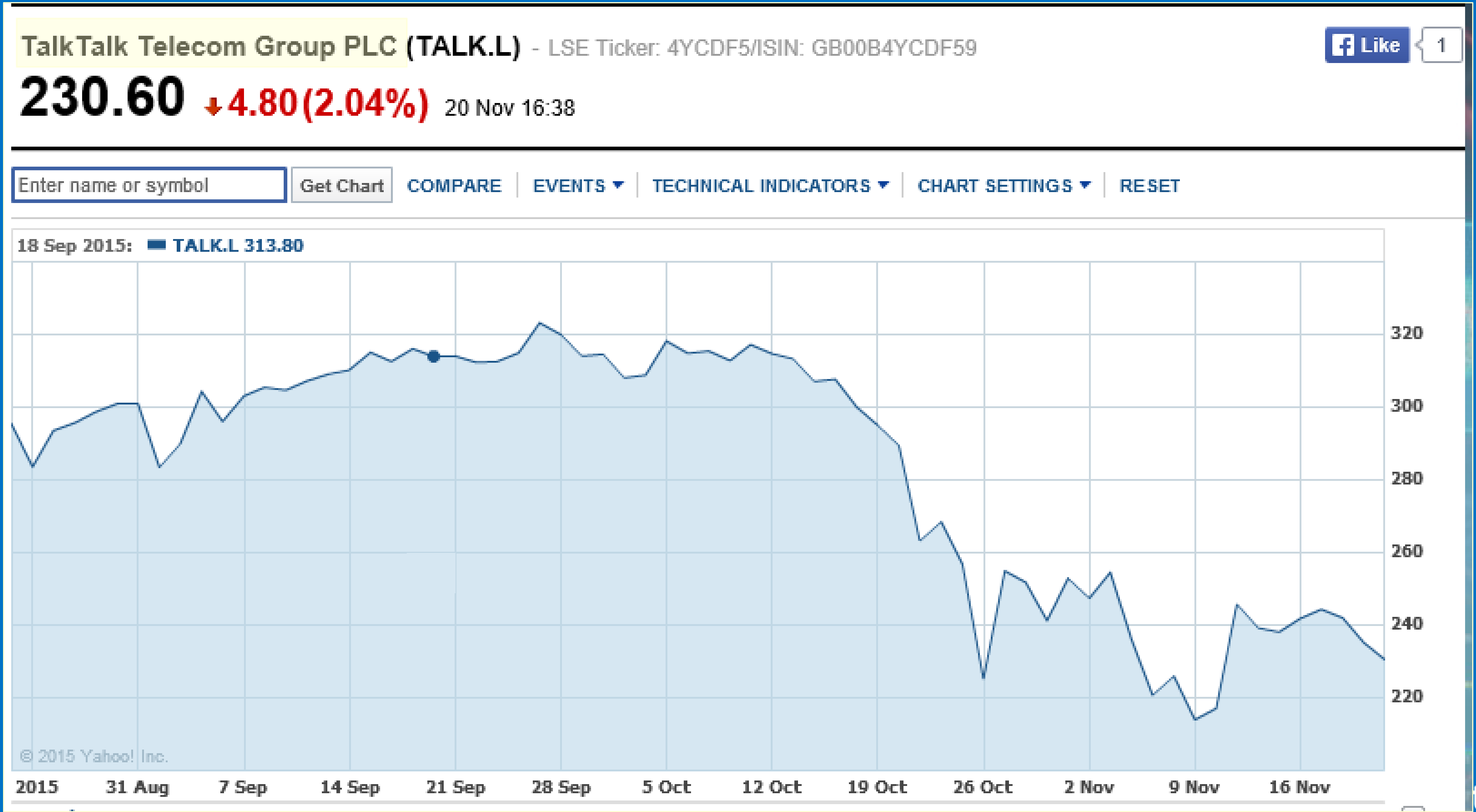
↓

**Customer data breached**

↓

**Received calls demanding ransom**

Attacker
Attacker sends command for his bots to attack bank.
Compromised PC
Compromised PC
Compromised PC
Compromised PC
Compromised PC
Internet



TalkTalk Telecom Group PLC (TALK.L) - LSE Ticker: 4YCDF5/ISIN: GB00B4YCDF59

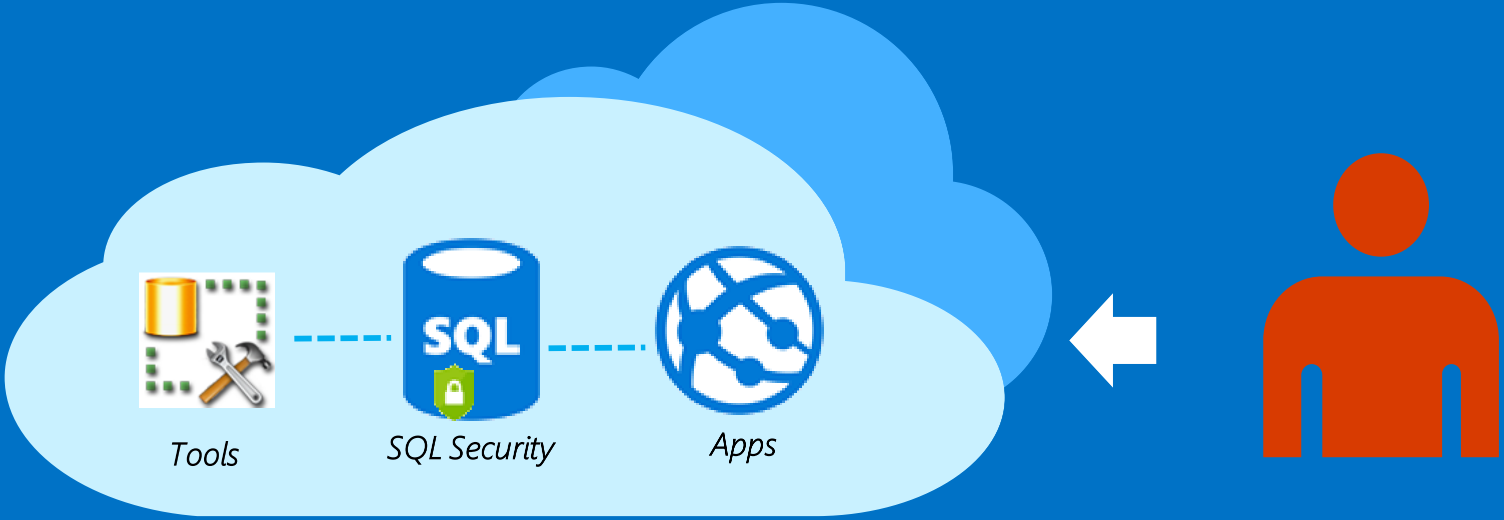
230.60 ↓4.80(2.04%) 20 Nov 16:38

18 Sep 2015: ▬ TALK.L 313.80

# Why SQL Database Security?

"[2014] was the year when so many high-profile organizations met with the nigh inevitability of "the breach" that "cyber" was front and center at the boardroom level."

*Verizon Data Breach Investigation Report 2015*



## SQL Users

- Lack of knowledge
- Lack of time
- Lack of budget
- Lack of methods

## SQL Data

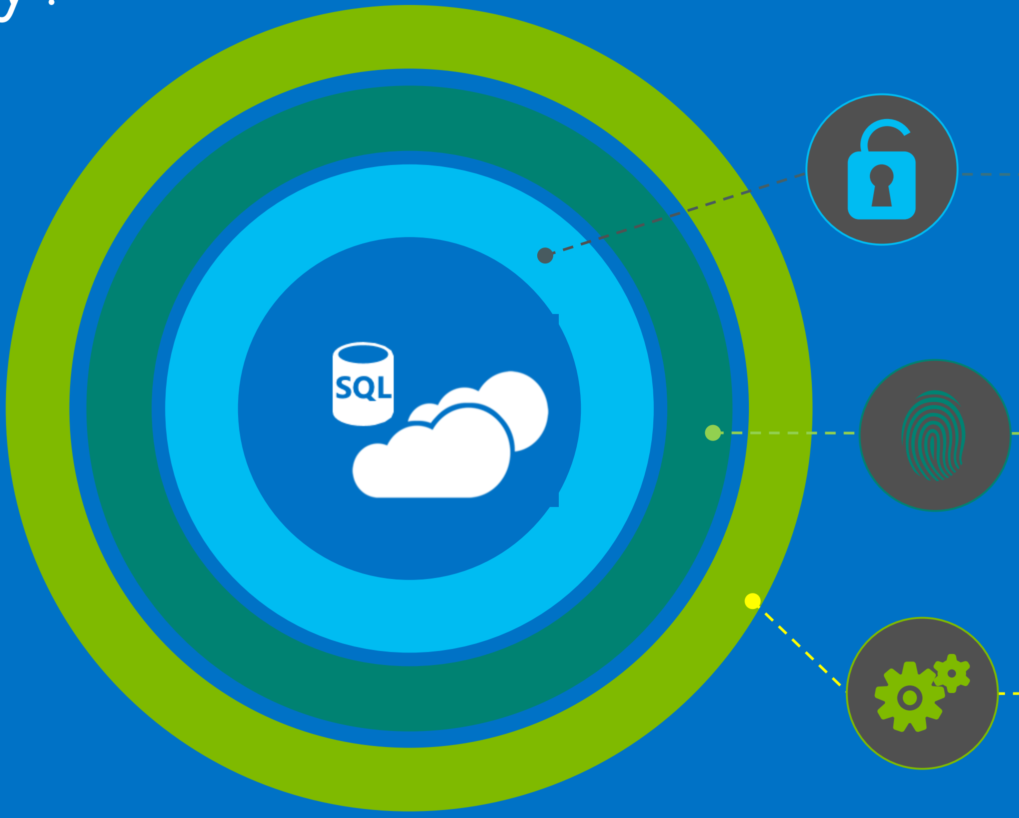
- Personal
- Financial
- Intellectual property

## SQL Threats

- Malicious insider
- SQL injection
- Credential theft
- Password cracking

# Security and Compliance

## Security :



### Protect Data

Encryption in motion :***Transport Layer Security*** (TLS)
Encryption at rest :***Transparent Data Encryption*** (TDE)
Encryption in use (client) : ***Always Encrypted*** *(AE)*

### Control Access

Database Access: :***Azure Active Directory Authentication*** (AAD)
Application Access :***Dynamic Data Masking & Row-Level Security*** (RLS),

### Proactive Monitoring

Tracking & Detecting : ***Auditing*** & ***Threat Detection***

## Compliance: FedRAMP, ISO, HIPPA, PCI, EU Model Clauses , UK G-Cloud

(government) (medial) (payment) (personal) (public sector)

sqlbits Microsoft

# Protect Data

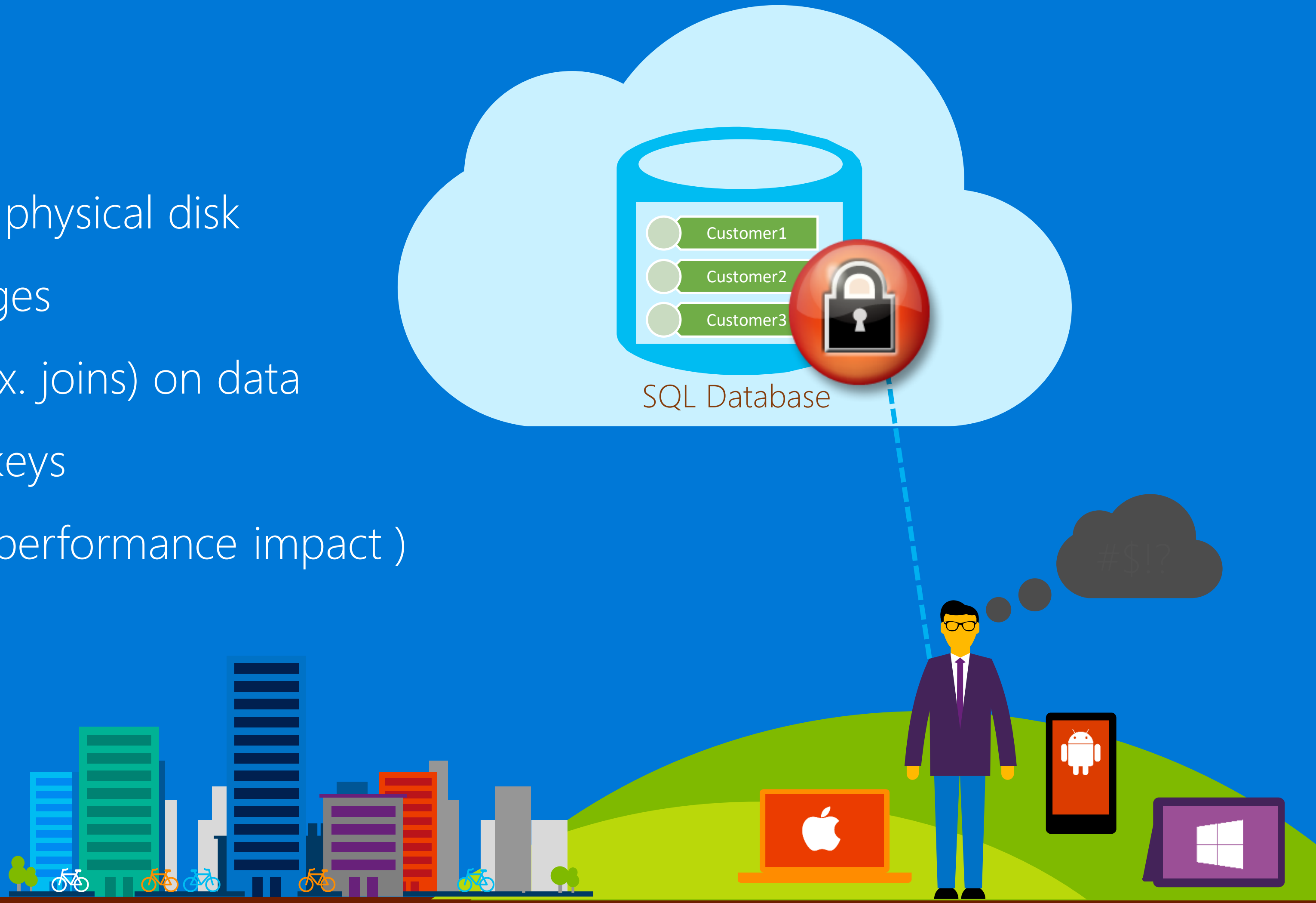
- At-rest : Transparent Data Encryption (TDE)
- In-use : Always Encrypted (AE)

# Transparent Data Encryption

*Protect data on SQL database physical storage*

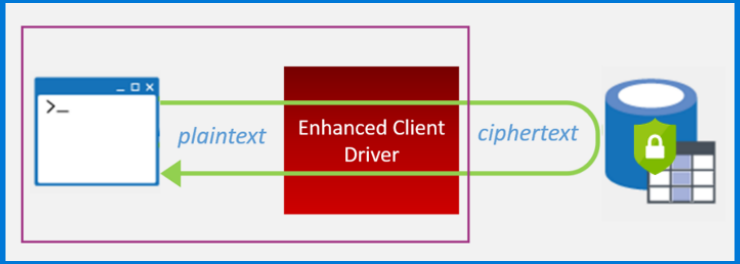
*from unauthorized access,*

- ✓ Server-side encryption of the data on physical disk
- ✓ Simple to Use , Zero application changes
- ✓ Support for all database operations (ex. joins) on data
- ✓ SQL Database service manages your keys
- ✓ AES-NI Hardware Acceleration (2-3% performance impact )



# Always Encrypted

*Protects the highly sensitive data in-use from high privilege SQL users.*



## Client side encryption

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

## Queries on Encrypted Data

Support for equality comparison, incl. join, group by and distinct operators.

## Application Transparency

Minimal application changes via server and client library enhancements.

*Status: Preview*

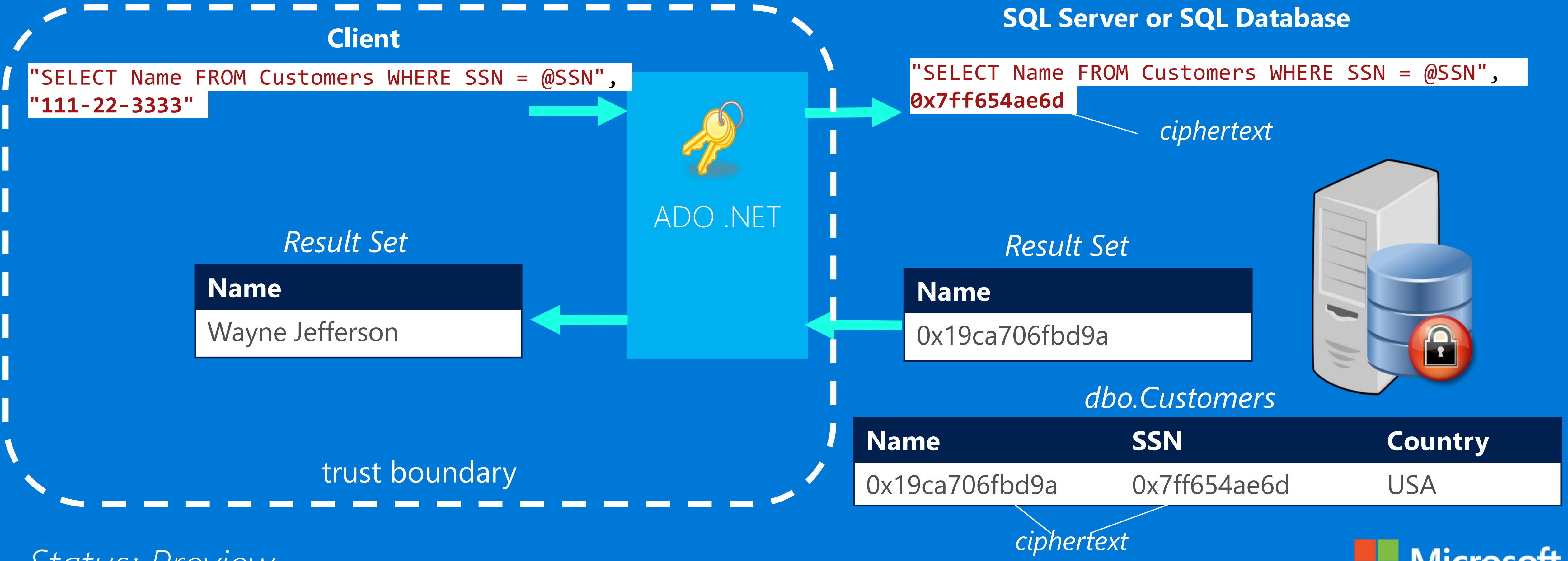
Microsoft

# How Always Encrypted Works

*Protects the highly sensitive data in-use*

*from high privilege SQL users.*

*Encrypted sensitive data and corresponding keys are never seen in plaintext in SQL Server*



**Client**

```
"SELECT Name FROM Customers WHERE SSN = @SSN",
"111-22-3333"
```

ADO .NET

*Result Set*

| Name |
|---|
| Wayne Jefferson |

trust boundary

**SQL Server or SQL Database**

```
"SELECT Name FROM Customers WHERE SSN = @SSN",
0x7ff654ae6d
```

*ciphertext*

*Result Set*

| Name |
|---|
| 0x19ca706fbd9a |

*dbo.Customers*

| Name | SSN | Country |
|---|---|---|
| 0x19ca706fbd9a | 0x7ff654ae6d | USA |

*ciphertext*

*Status: Preview*

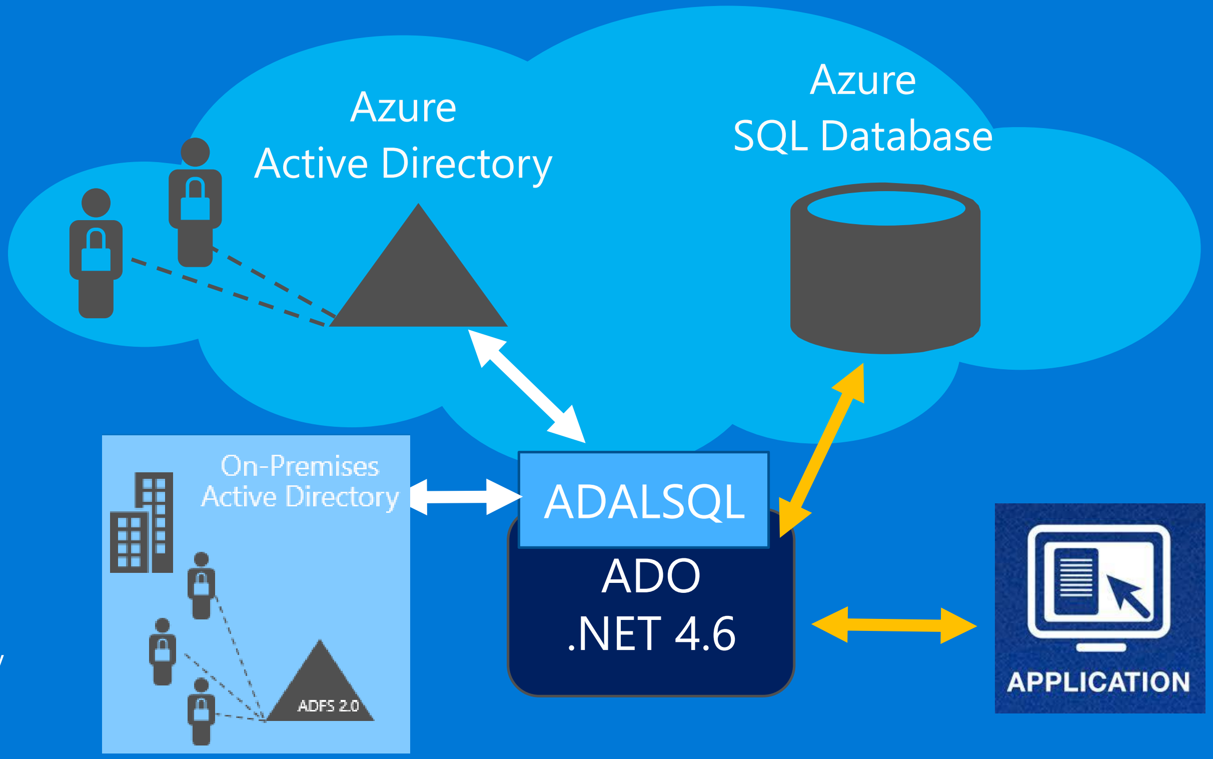
# Control Access

- DB Access: Azure AD Authentication (AAD)
- App Access : Dynamic Data Masking (DDM)
- App Access : Row-level security (RLS)

# Azure Active Directory Authentication

## A central place to *manage users* across services

- ✓ Alternative to SQL Server authentication
- ✓ Simplifies database permission management using external Azure Active Directory groups
- ✓ Allows password rotation in a single place



## *Multiple authentication methods*

- ✓ **Username/password** for Azure AD managed accounts
- ✓ **Single Sign-On** using Integrated Windows authentication , for federated domains which is authenticated via Azure AD
- ✓ **Certificate-based authentication**, in case the certificate registered with Azure Active Directory

*Status: Preview*

Microsoft

# Why Dynamic Data Masking?

Limit the exposure of sensitive data by obfuscating query results for app users and engineer

## Limit Access to Sensitive Data

Protects against unauthorized access to sensitive data in the application, using built-in or custom masking rules. Privileged users can still see unmasked data.

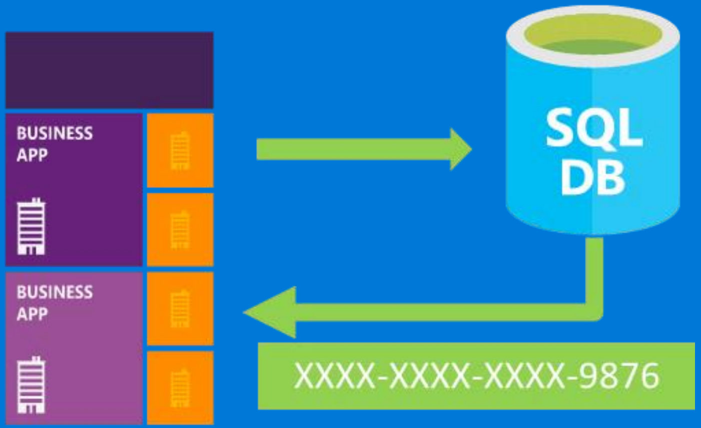
## Application Transparency

Data is masked on-the-fly, underlying data in the database remains intact. Transparent to the application and applied according to user privilege

.

APP Users

Dev Users

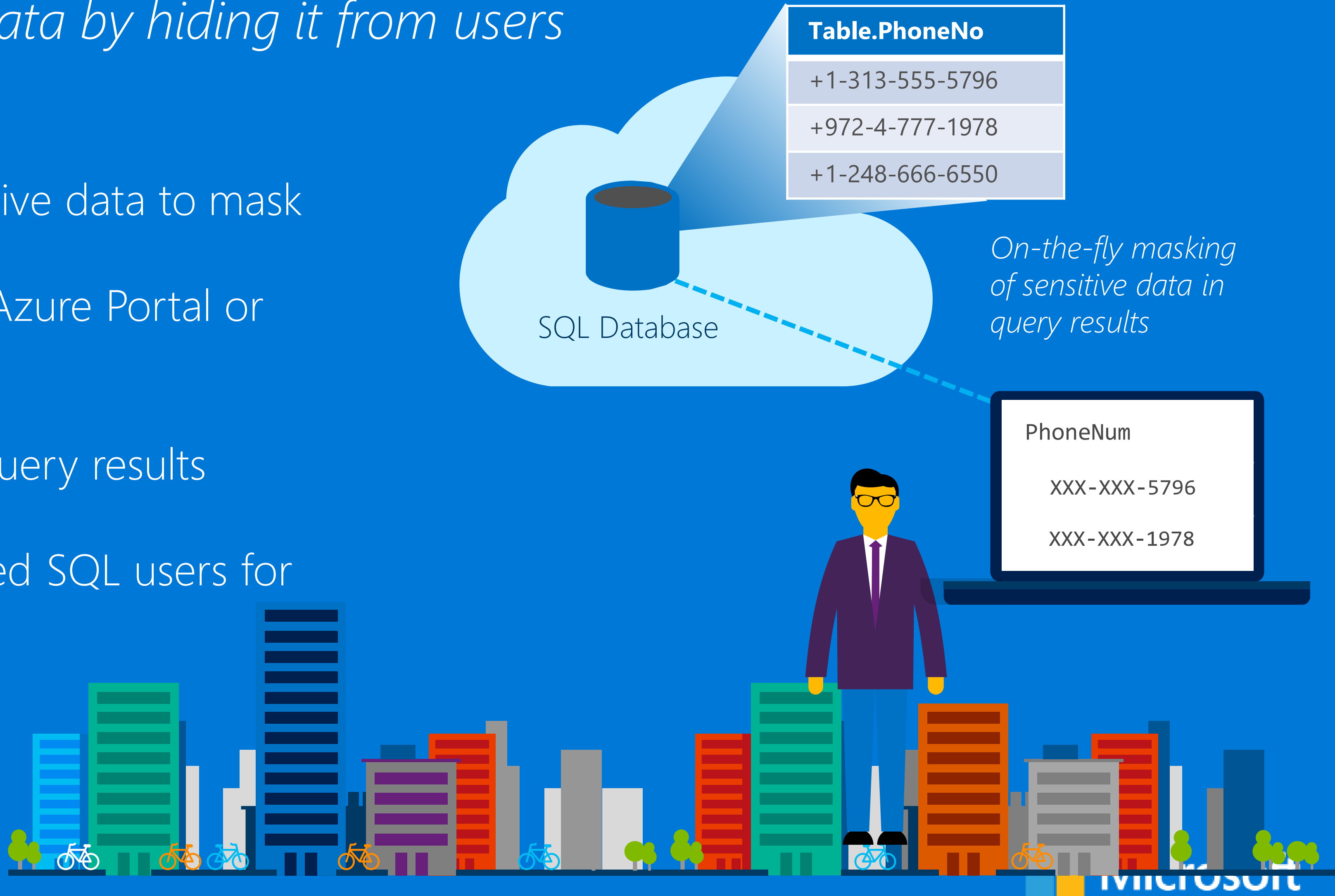


Microsoft

# Dynamic Data Masking

*Limit the exposure of sensitive data by hiding it from users*

- ✓ Auto-discovery of potentially sensitive data to mask
- ✓ Configurable masking policy from Azure Portal or via DDL in the Server
- ✓ On-the-fly obfuscation of data in query results
- ✓ Flexibility to define a set of privileged SQL users for un-masked data access



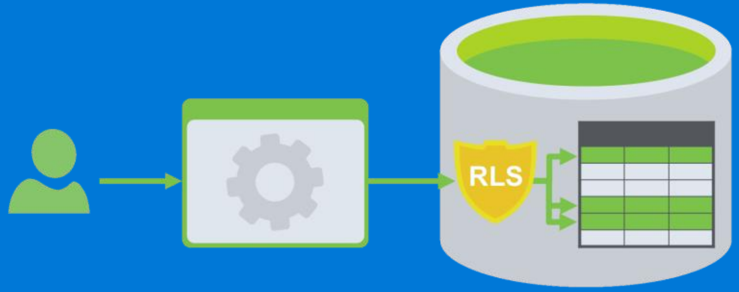
| Table.PhoneNo |
|---|
| +1-313-555-5796 |
| +972-4-777-1978 |
| +1-248-666-6550 |

*On-the-fly masking of sensitive data in query results*

| PhoneNum |
|---|
| XXX-XXX-5796 |
| XXX-XXX-1978 |

# Row-level security

*Centralize your row access logic within the database.*



## Fine-grained Access Control

Control both read- and write-access to specific rows of data in a shared database.
Flexible access criteria (user identity, role/group memberships, connection data, time of day, etc).

## Application Transparency

- RLS works transparently at query time, no app changes needed.
- Reduces application maintenance and code complexity.

# *Proactive Monitoring*

- Tracking :Auditing
- Intelligences insights: Threat Detection (TD)

# Why Auditing & Threat Detection?

*Detect suspicious database activities, gain insight into database events and streamline compliance-related tasks*

## Regulatory Compliance

A strong demand for cloud applications to meet security **standards** recommended by regulating authorities.

(PCI-DSS, SOX, HIPAA)

## Intelligent algorithms

Proprietary algorithms work around the clock to develop a behavioral profile of your database, identifying anomalous activities and potential threats

## Investigate and mitigate

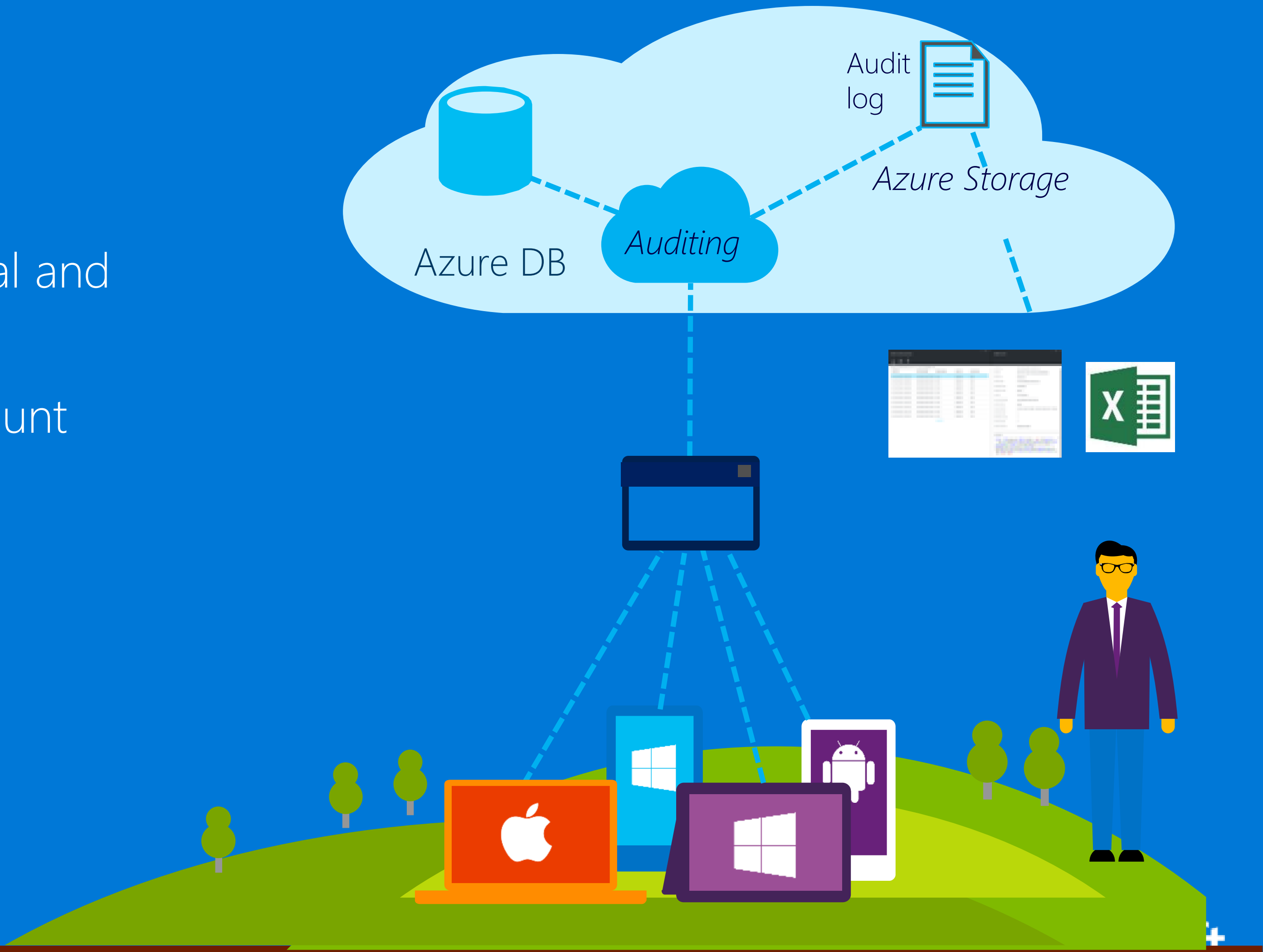
React and respond to threats in real-time, via email alerts and the Azure portal.

Microsoft

# Auditing

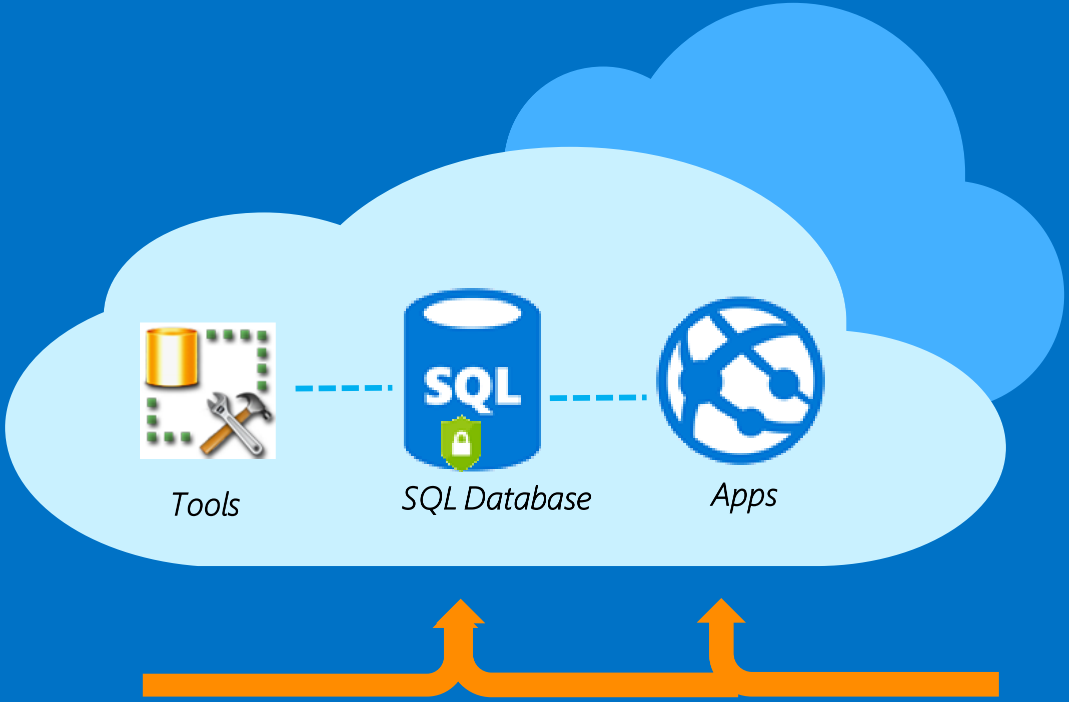
*Gain insight into database events and streamline compliance-related tasks*

- ✓ Configurable audit policy via the Azure portal and standard API
- ✓ Audit logs reside in your Azure Storage account
- ✓ Azure portal viewer and excel templates for analysis of audit log



# Demo

Malicious insider



Tools

SQL Database

Apps

External Attacker

Microsoft

# Azure SQL Database Security

*Securing your data is easier than ever*

## Protect Data

Encrypt the data in-transit , at-rest and in-use

- Transport Layer Security
- Transparent Data Encryption
- Always Encrypted

## Control Access

Limit application &database to sensitive data

- Dynamic Data Masking
- Row-Level Security
- Azure AD Authentication

## Proactive Monitoring

Monitor and track the ongoing database activities

- Auditing
- Threat Detection

Microsoft

Microsoft

sqlbits

# Thank you!

Microsoft