Microsoft

Microsoft Data & Analytics

Ankur Mishra | Lana Koprivica

Azure Data & AI

Dec 2020

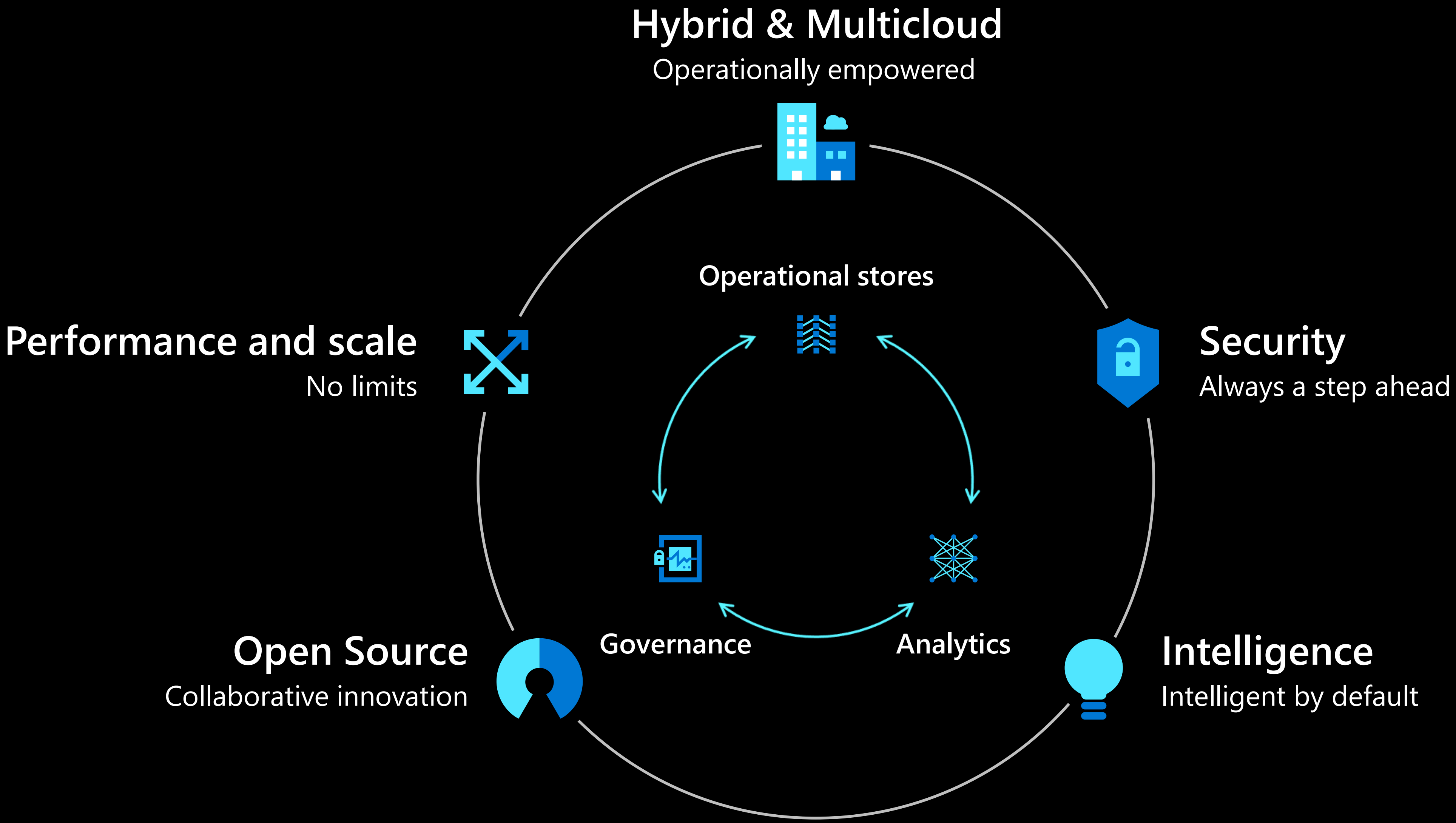
Microsoft Data & Analytics

Ankur Mishra | Lana Koprivica

Azure Data & AI

Dec 2020

Azure Data Product Pillars



Hybrid & Multicloud
Operationally empowered

Performance and scale
No limits

Security
Always a step ahead

Open Source
Collaborative innovation

Intelligence
Intelligent by default

Azure Data Products and Services

Operational stores

SQL Server

Azure SQL DB

Azure SQL DB Edge

Azure Cosmos DB

Azure for PostgreSQL

Azure for MySQL

Azure for MariaDB

Analytics

Azure Synapse Analytics

- Azure HDInsight
- Azure SQL Data Warehouse
- Azure Data Factory
- Azure Data Explorer
- Azure Stream Analytics
- Azure Databricks
- Internal Cosmos

Governance

Azure Purview

Azure Data Share

Azure Synapse Analytics

A single managed service for analytics over your lake, warehouse, or operational stores.

Limitless Scale

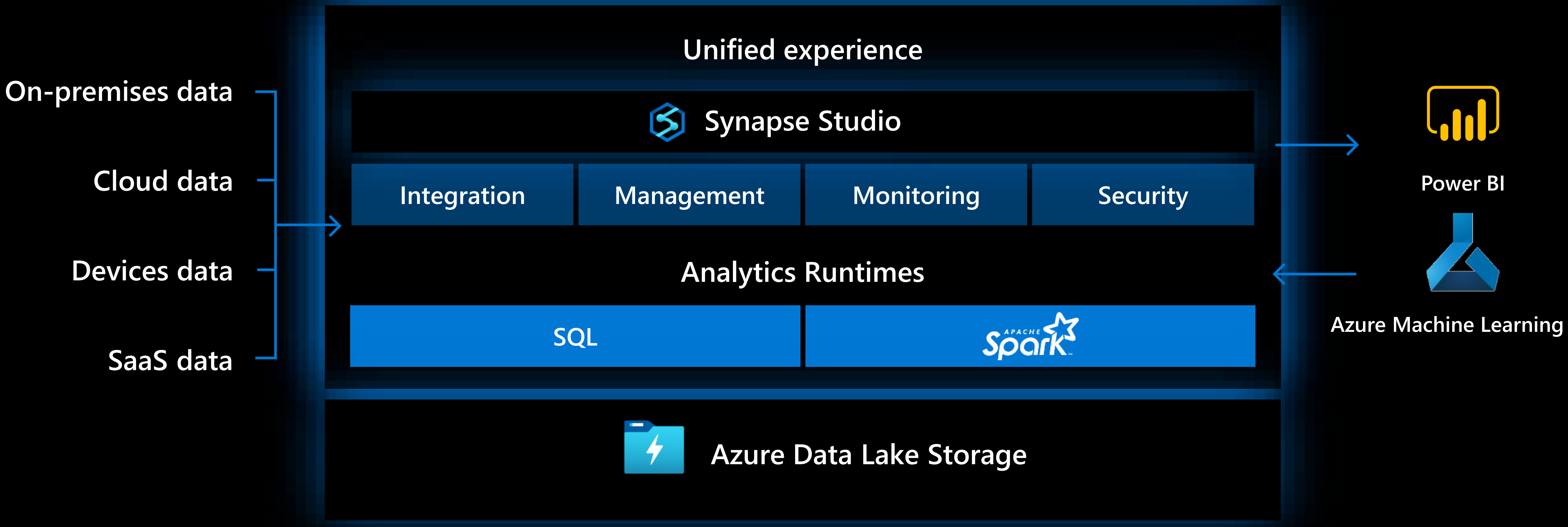
Powerful Insights

Unified Experience

Unmatched Security

Azure Synapse Analytics

Limitless analytics service with unmatched time to insight



On-premises data

Cloud data

Devices data

SaaS data

Unified experience

Synapse Studio

Integration

Management

Monitoring

Security

Analytics Runtimes

SQL

Apache Spark

Azure Data Lake Storage

Power BI

Azure Machine Learning

Microsoft Azure

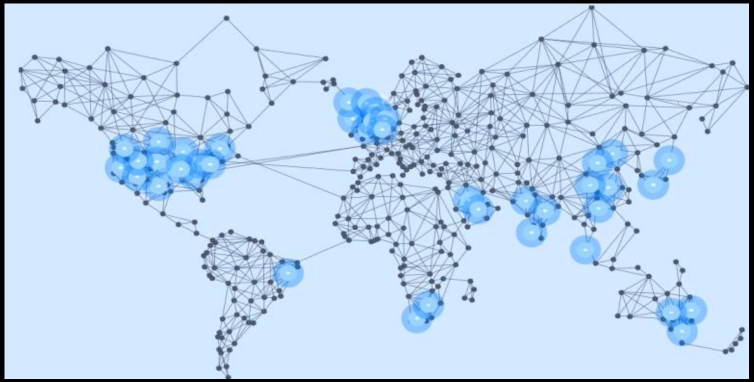
Invent with purpose

Microsoft Azure

Be future ready | Build on your terms | Operate hybrid seamlessly | Trust your cloud

Azure Fundamentals

Global



60+ Azure regions

Largest geographical footprint of any cloud provider with more than **60+** Azure regions

Secure

Microsoft Cyber Defense Operations Center

>3,500 full-time security professionals

6.5 trillion global signals daily

$1 billion annual cybersecurity investment

Compliant

92 Compliance offerings

GLOBAL

- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- ISO 22301:2012
- ISO/IEC 27701:2019
- ISO 9001:2015
- ISO 20000-1:2011
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CIS Benchmark
- CSA STAR Certification
- CSA STAR Attestation
- CSA STAR Self-Assessment
- WCAG 2.0 (ISO 40500:2012)

U.S. GOVT

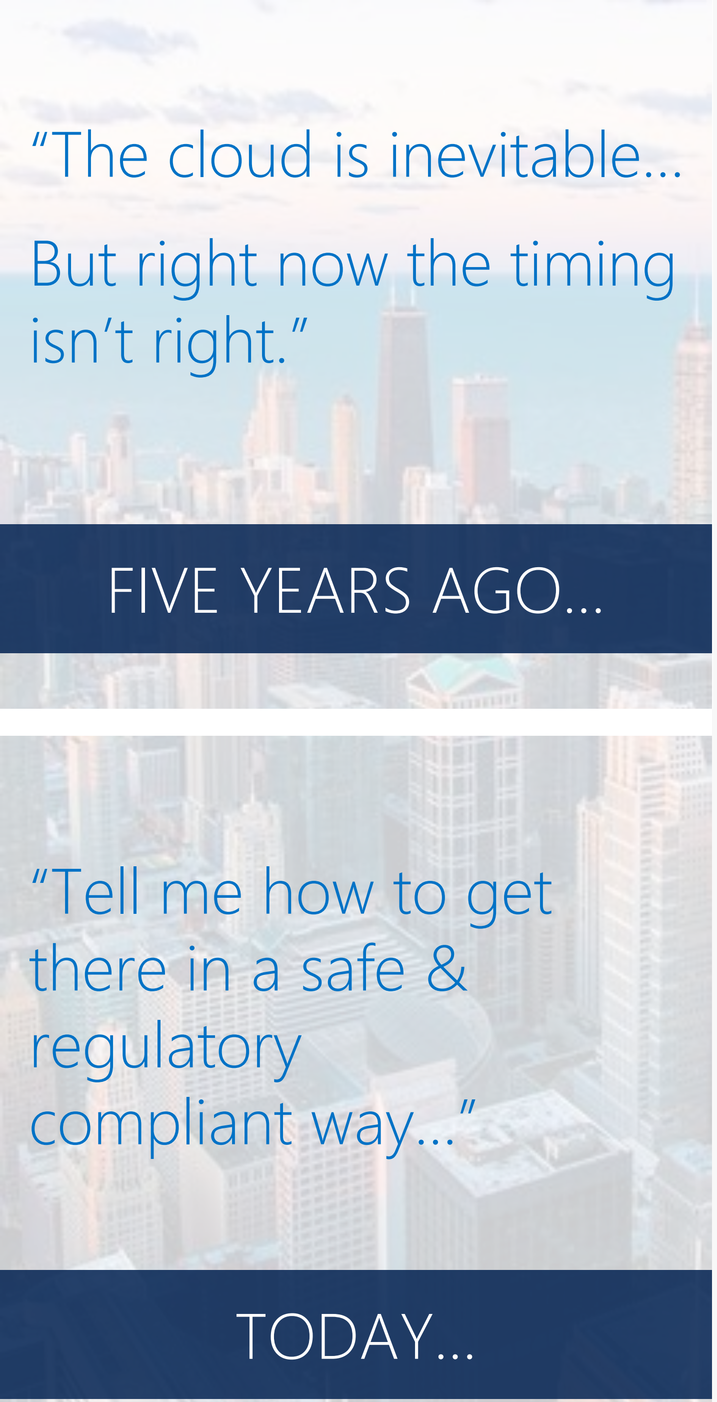
- FedRAMP High
- FedRAMP Moderate
- EAR
- ITAR
- DoD DISA SRG Level 5
- DoD DISA SRG Level 4
- DoD DISA SRG Level 2
- DFARS
- DoE 10 CFR Part 810
- NIST SP 800-171
- NIST CSF
- Section 508 VPATs
- FIPS 140-2
- CJIS
- IRS 1075
- CNSSI 1253

INDUSTRY

- PCI DSS Level 1
- GLBA (US)
- FFIEC (US)
- Shared Assessments (US)
- SEC 17a-4 (US)
- CFTC 1.31 (US)
- FINRA 4511 (US)
- SOX (US)
- 23 NYCRR 500 (US)
- OSFI (Canada)
- FCA + PRA (UK)
- APRA (Australia)
- FINMA (Switzerland)
- FSA (Denmark)
- RBI + IRDAI (India)
- MAS + ABS (Singapore)
- NBB + FSMA (Belgium)
- AFM + DNB (Netherlands)
- AMF + ACPR (France)
- KNF (Poland)
- European Banking Authority (EBA)
- FISC (Japan)
- HIPAA BAA (US)
- HITRUST Certification
- GxP (FDA 21 CFR Part 11)
- MARS-E (US)
- NHS IG Toolkit (UK)
- NEN 7510:2011 (Netherlands)
- FERPA (US)
- CDSA
- MPAA (US)
- FACT (UK)
- DPP (UK)

REGIONAL

- Argentina PDPA
- Australia IRAP Unclassified
- Australia IRAP PROTECTED
- Canada Privacy Laws
- China GB 18030:2005
- China DJCP (MLPS) Level 3
- China TRUCS / CCCPPF
- EU EN 301 549
- EU ENISA IAF
- EU Model Clauses
- EU – US Privacy Shield
- GDPR
- Germany C5
- Germany IT-Grundschutz workbook
- India MeitY
- Japan CS Mark Gold
- Japan My Number Act
- Netherlands BIR 2012
- New Zealand Gov CIO Framework
- Singapore MTCS Level 3
- Spain ENS High
- Spain DPA
- UK Cyber Essentials Plus
- UK G-Cloud
- UK PASF



"The cloud is inevitable…

But right now the timing isn't right."

FIVE YEARS AGO…

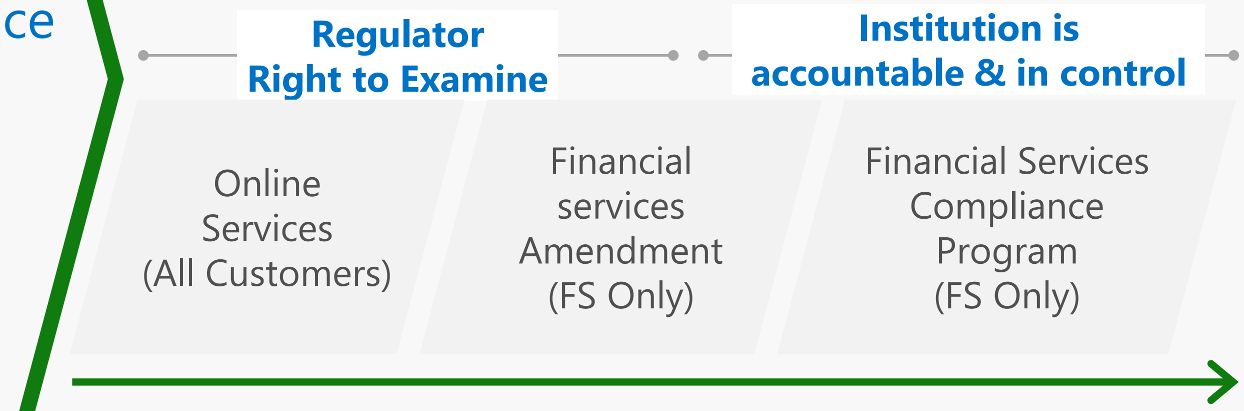
"Tell me how to get there in a safe & regulatory compliant way…"

TODAY…

Leading edge regulatory compliance capabilities empowering financial services

Over 120 financial services regulators engaged in last 5 years

FDIC
EUROPEAN CENTRAL BANK
EUROSYSTEM



Regulator Right to Examine

Institution is accountable & in control

Online Services (All Customers)

Financial services Amendment (FS Only)

Financial Services Compliance Program (FS Only)

Customers are moving!

90% of the G-SIFI financial institutions

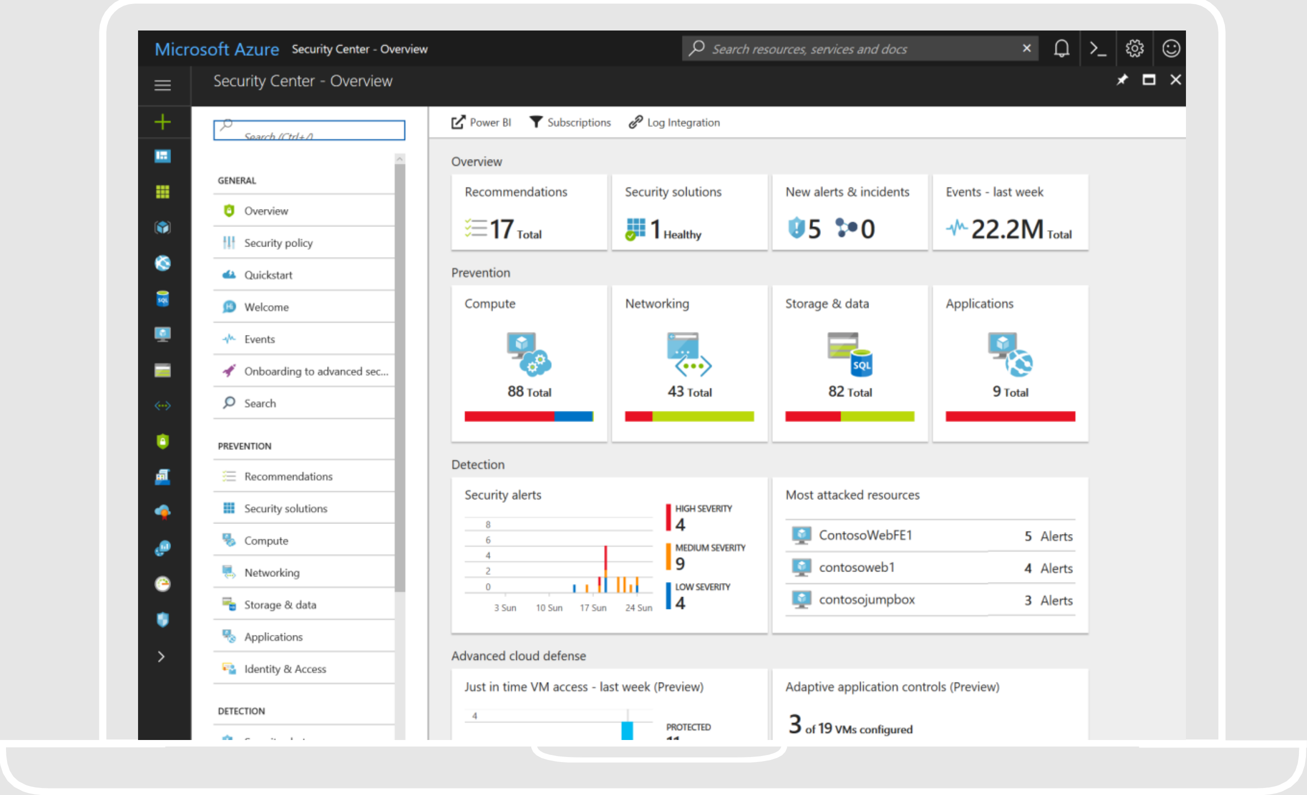
are now using the Microsoft Cloud…

Azure Security Center

Protection through best practices

Detect threats and attacks

Remediate issues



Overview

Recommendations	Security solutions	New alerts & incidents	Events - last week
17 Total	1 Healthy	5 0	22.2M Total

Prevention

Compute	Networking	Storage & data	Applications
88 Total	43 Total	82 Total	9 Total

Detection

Security alerts

HIGH SEVERITY 4

MEDIUM SEVERITY 9

LOW SEVERITY 4

Most attacked resources

ContosoWebFE1	5 Alerts
contosoweb1	4 Alerts
contosojumpbox	3 Alerts

Advanced cloud defense

Just in time VM access - last week (Preview)

Adaptive application controls (Preview)

3 of 19 VMs configured

Governance

Data governance is interdisciplinary

Data Management

Data Engineering

Data Stewardship

Chief Data Officer

Data Discovery

What data do I have?

Where did the data originate?

Can I trust it?

Data Governance

What's my exposure to risk?

Is my usage compliant?

How do I control access to my data?

Data Compliance

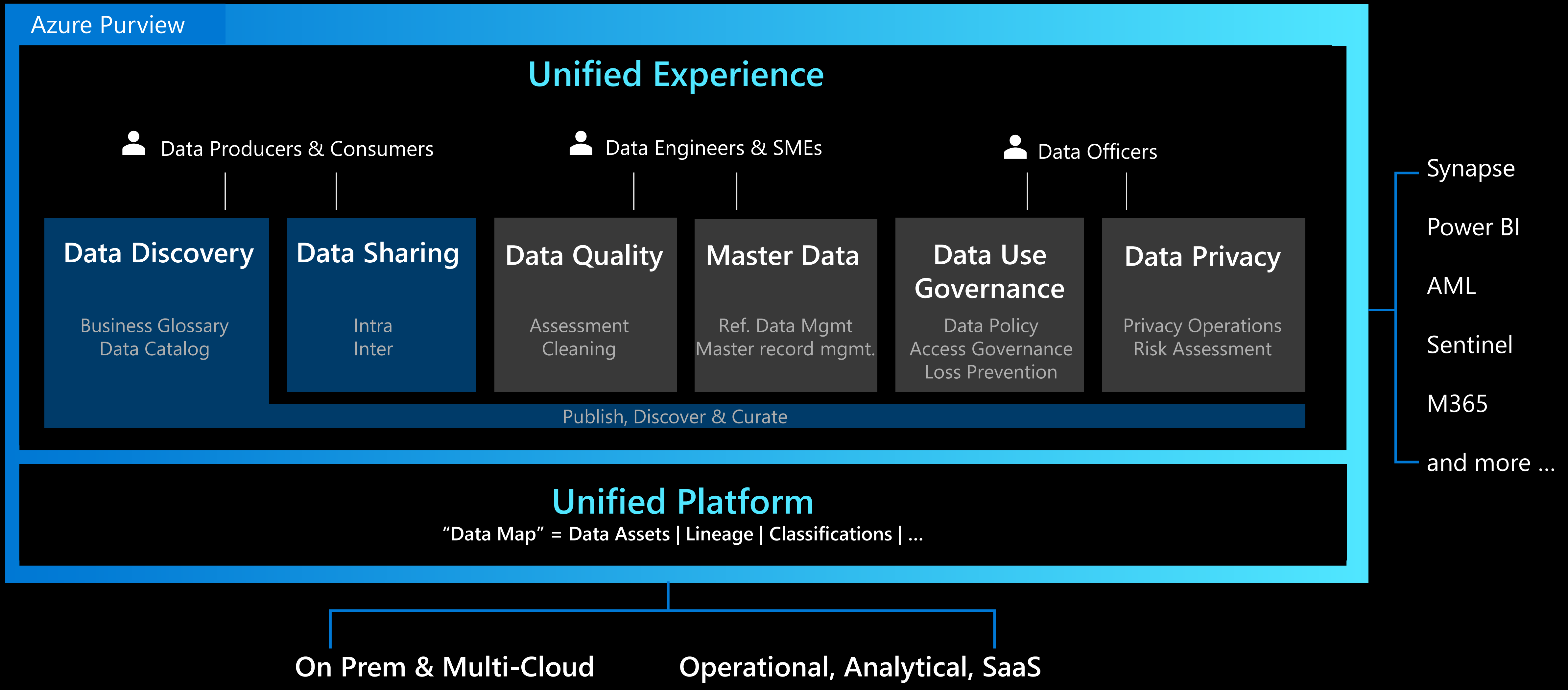
Data Security

Data Policy

Data Governance

A unified approach to data governance

■ Roadmap



Azure Purview

Unified Experience

Data Producers & Consumers

Data Engineers & SMEs

Data Officers

Data Discovery
Business Glossary
Data Catalog

Data Sharing
Intra
Inter

Data Quality
Assessment
Cleaning

Master Data
Ref. Data Mgmt
Master record mgmt.

Data Use Governance
Data Policy
Access Governance
Loss Prevention

Data Privacy
Privacy Operations
Risk Assessment

Publish, Discover & Curate

Unified Platform

“Data Map” = Data Assets | Lineage | Classifications | ...

Synapse

Power BI

AML

Sentinel

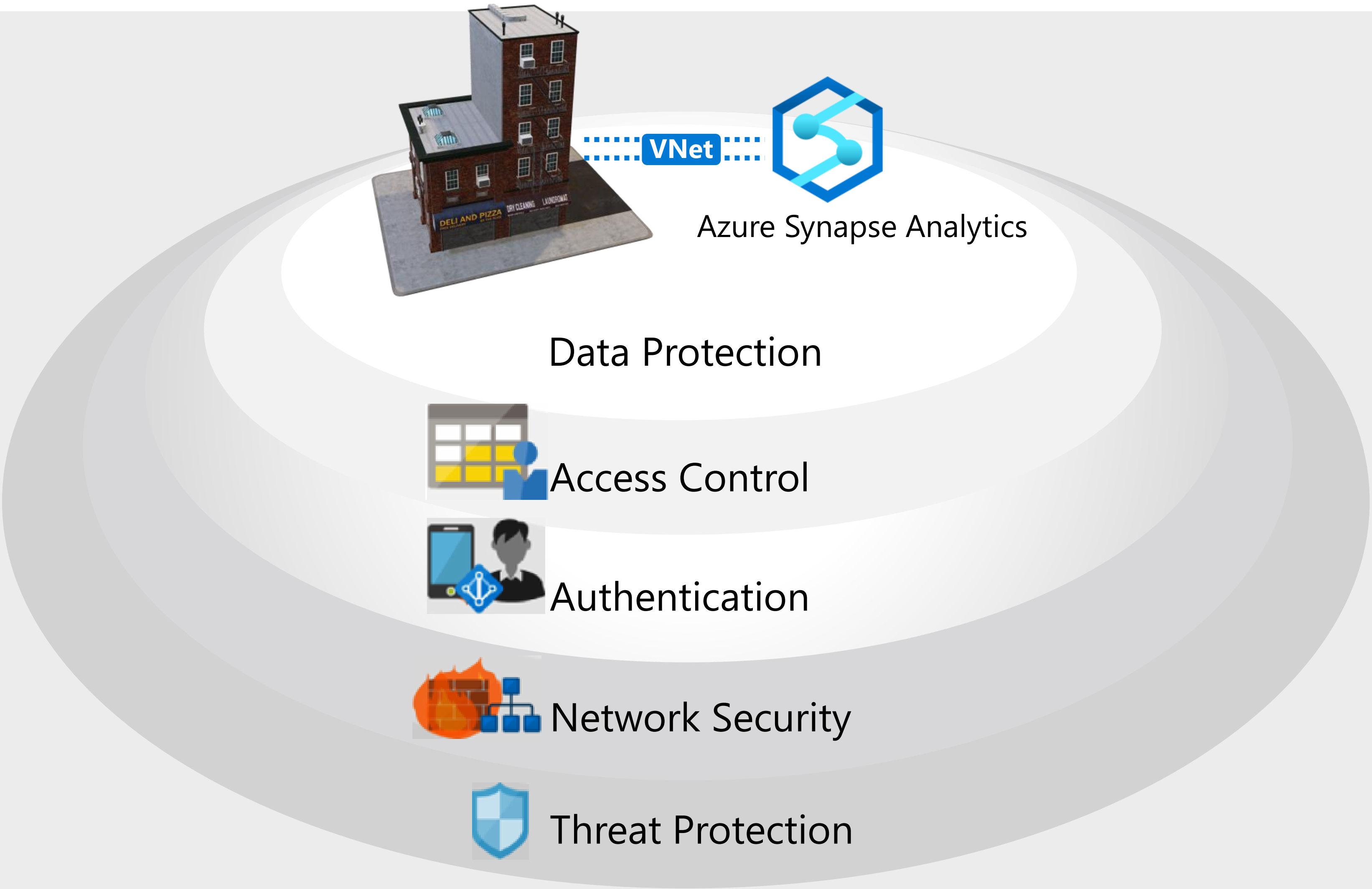
M365

and more ...

On Prem & Multi-Cloud

Operational, Analytical, SaaS

Enterprise-grade security



Defense-in-Depth

Industry-leading compliance

- ISO 27001
- SOC 1 Type 2
- SOC 2 Type 2
- PCI DSS Level 1
- Cloud Controls Matrix
- ISO 27018
- Content Delivery and Security Association
- Shared Assessments
- FedRAMP JAB P-ATO
- HIPAA / HITECH
- FIPS 140-2
- 21 CFR Part 11
- FERPA
- DISA Level 2
- CJIS
- IRS 1075
- ITAR-ready
- Section 508 VPAT
- European Union Model Clauses
- EU Safe Harbor
- United Kingdom G-Cloud
- China Multi Layer Protection Scheme
- China GB 18030
- China CCCPPF
- Singapore MTCS Level 3
- Australian Signals Directorate
- New Zealand GCIO
- Japan Financial Services
- ENISA IAF

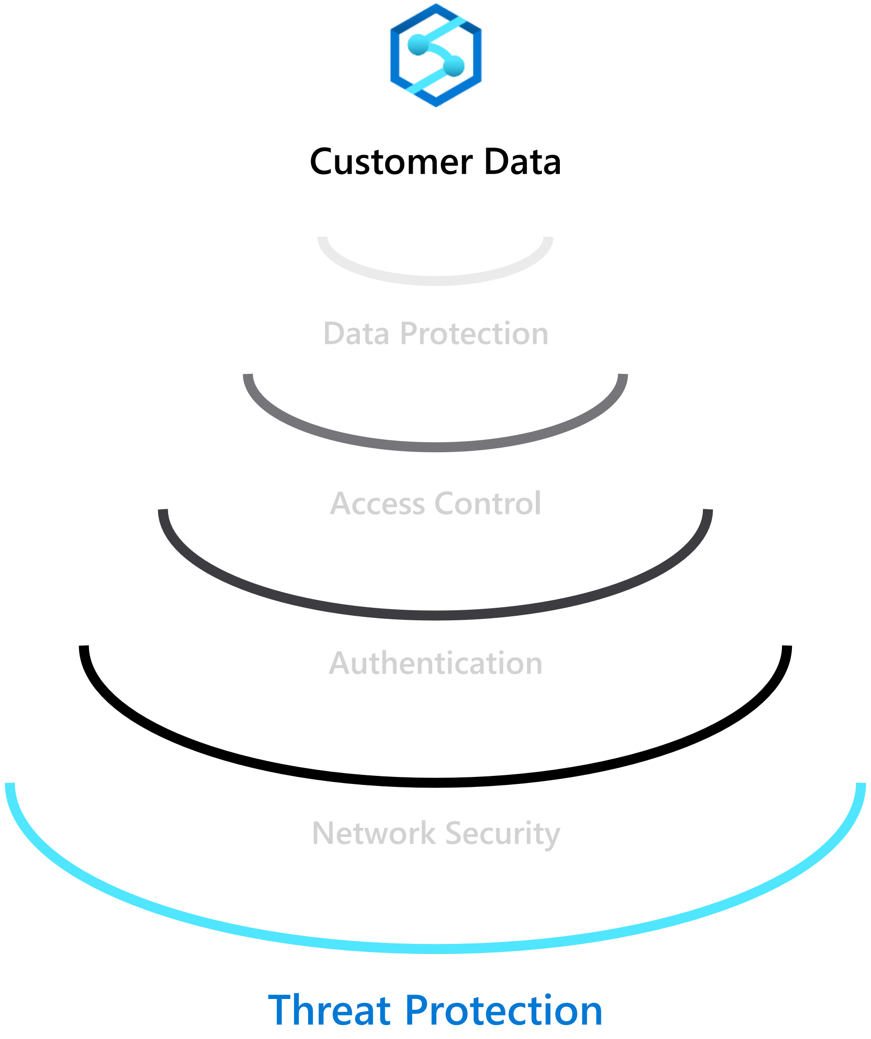
Threat Protection - Business requirements

How do we enumerate and track potential SQL vulnerabilities?

To mitigate any security misconfigurations before they become a serious issue.

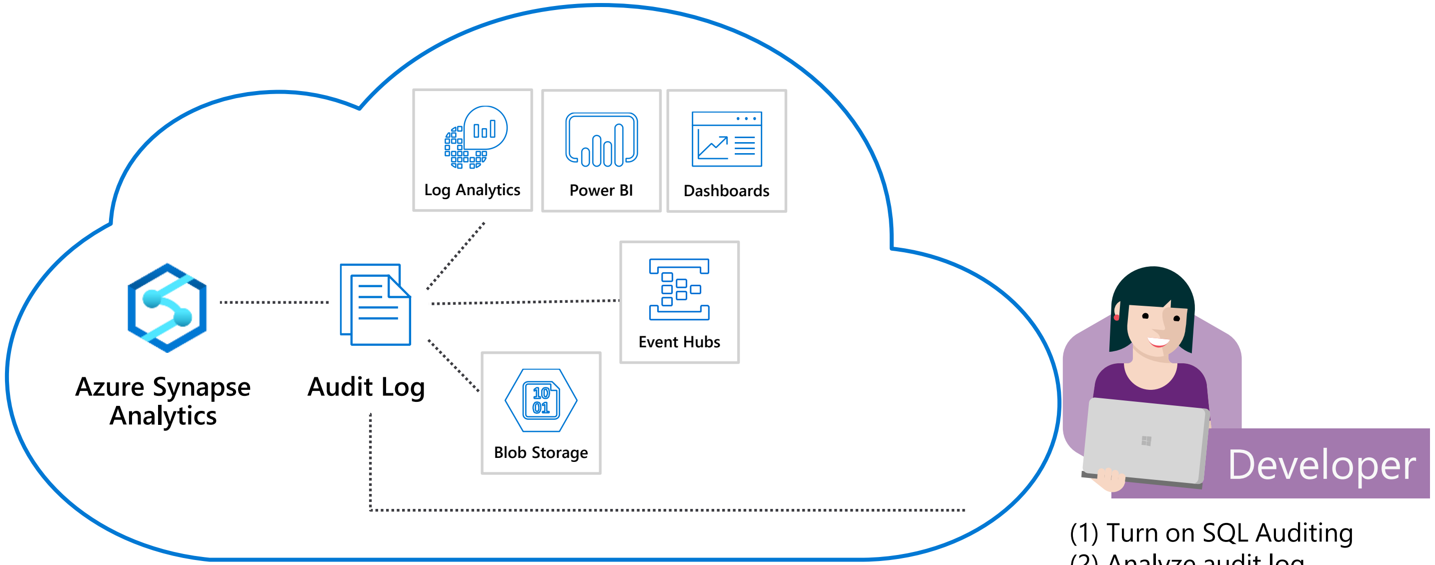
How do we discover and alert on suspicious database activity?

To detect and resolve any data exfiltration or SQL injection attacks.

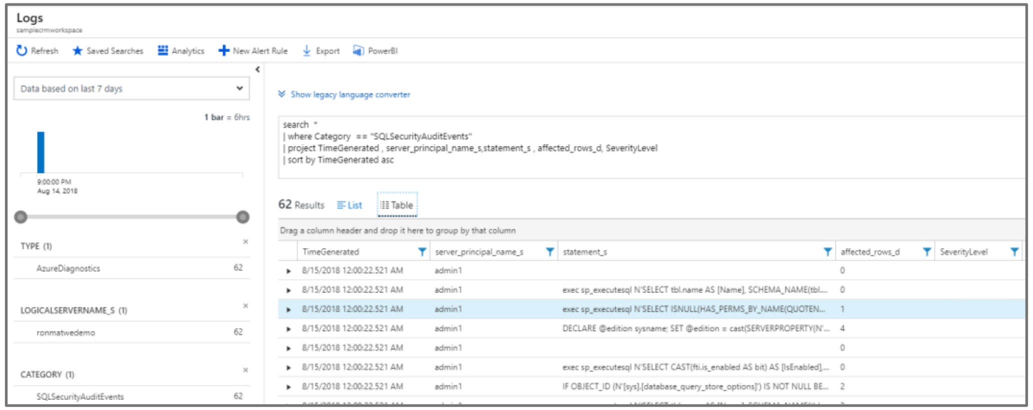


SQL auditing in Azure Log Analytics and Event Hubs

Gain insight into database audit log



(1) Turn on SQL Auditing
(2) Analyze audit log



```
search *
| where Category == "SQLSecurityAuditEvents"
| project TimeGenerated , server_principal_name_s,statement_s , affected_rows_d, SeverityLevel
| sort by TimeGenerated asc
```

TYPE (1)

AzureDiagnostics	62

LOGICALSERVERNAME_S (1)

ronmatwedemo	62

CATEGORY (1)

SQLSecurityAuditEvents	62

62 Results

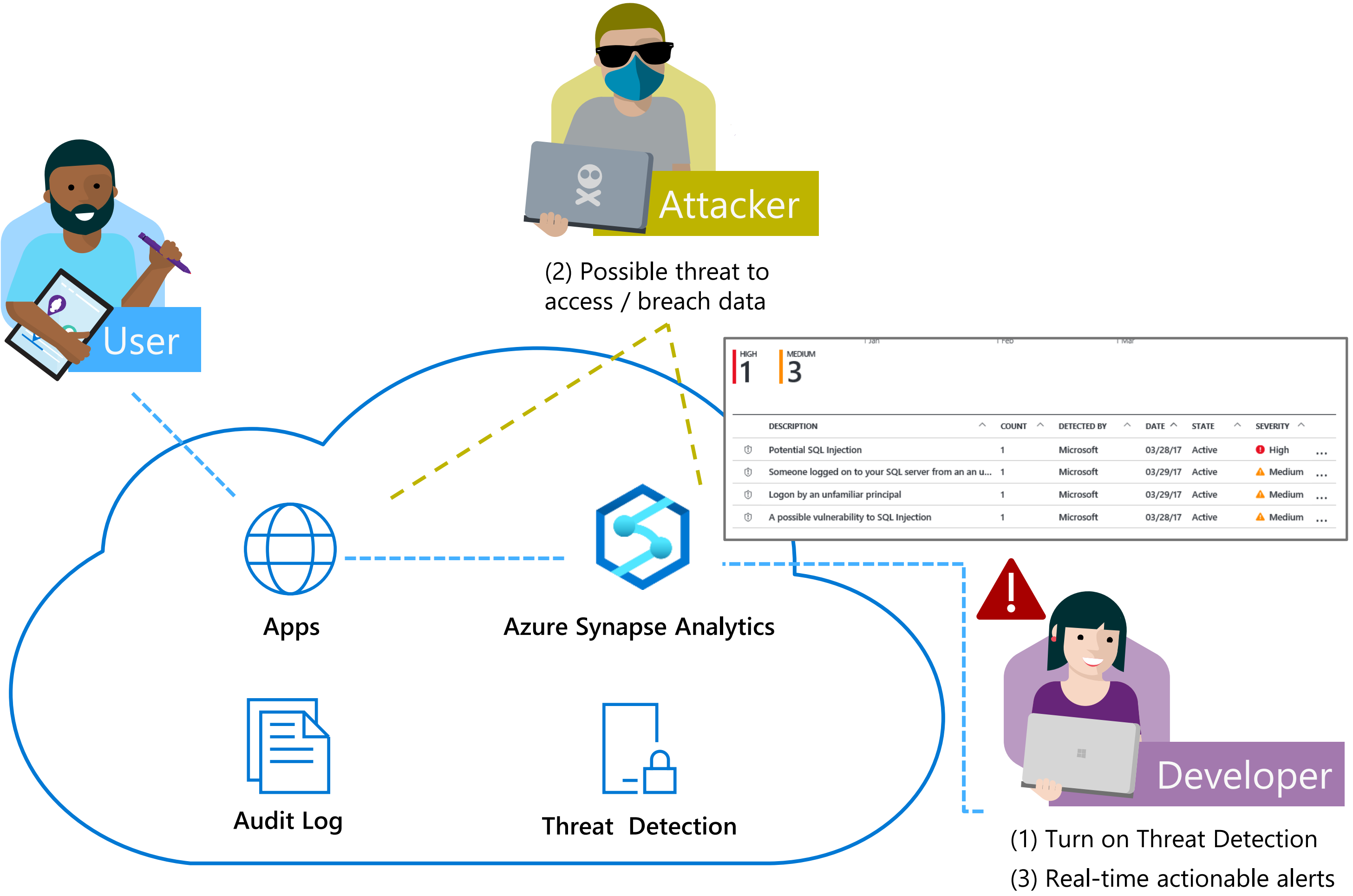
Drag a column header and drop it here to group by that column

TimeGenerated	server_principal_name_s	statement_s	affected_rows_d	SeverityLevel
8/15/2018 12:00:22.521 AM	admin1		0	
8/15/2018 12:00:22.521 AM	admin1	exec sp_executesql N'SELECT tbl.name AS [Name], SCHEMA_NAME(tbl....	0	
8/15/2018 12:00:22.521 AM	admin1	exec sp_executesql N'SELECT ISNULL(HAS_PERMS_BY_NAME(QUOTEN...	1	
8/15/2018 12:00:22.521 AM	admin1	DECLARE @edition sysname; SET @edition = cast(SERVERPROPERTY(N'...	4	
8/15/2018 12:00:22.521 AM	admin1		0	
8/15/2018 12:00:22.521 AM	admin1	exec sp_executesql N'SELECT CAST(fti.is_enabled AS bit) AS [IsEnabled],...	0	
8/15/2018 12:00:22.521 AM	admin1	IF OBJECT_ID (N'[sys].[database_query_store_options]') IS NOT NULL BE...	2	

- ✓ Configurable via audit policy
- ✓ SQL audit logs can reside in
  - Azure Storage account
  - Azure Log Analytics
  - Azure Event Hubs
- ✓ Rich set of tools for
  - Investigating security alerts
  - Tracking access to sensitive data

SQL threat detection

Detect and investigate anomalous database activity


Attacker
(2) Possible threat to access / breach data
User
Apps
Azure Synapse Analytics
Audit Log
Threat Detection
Developer
(1) Turn on Threat Detection
(3) Real-time actionable alerts

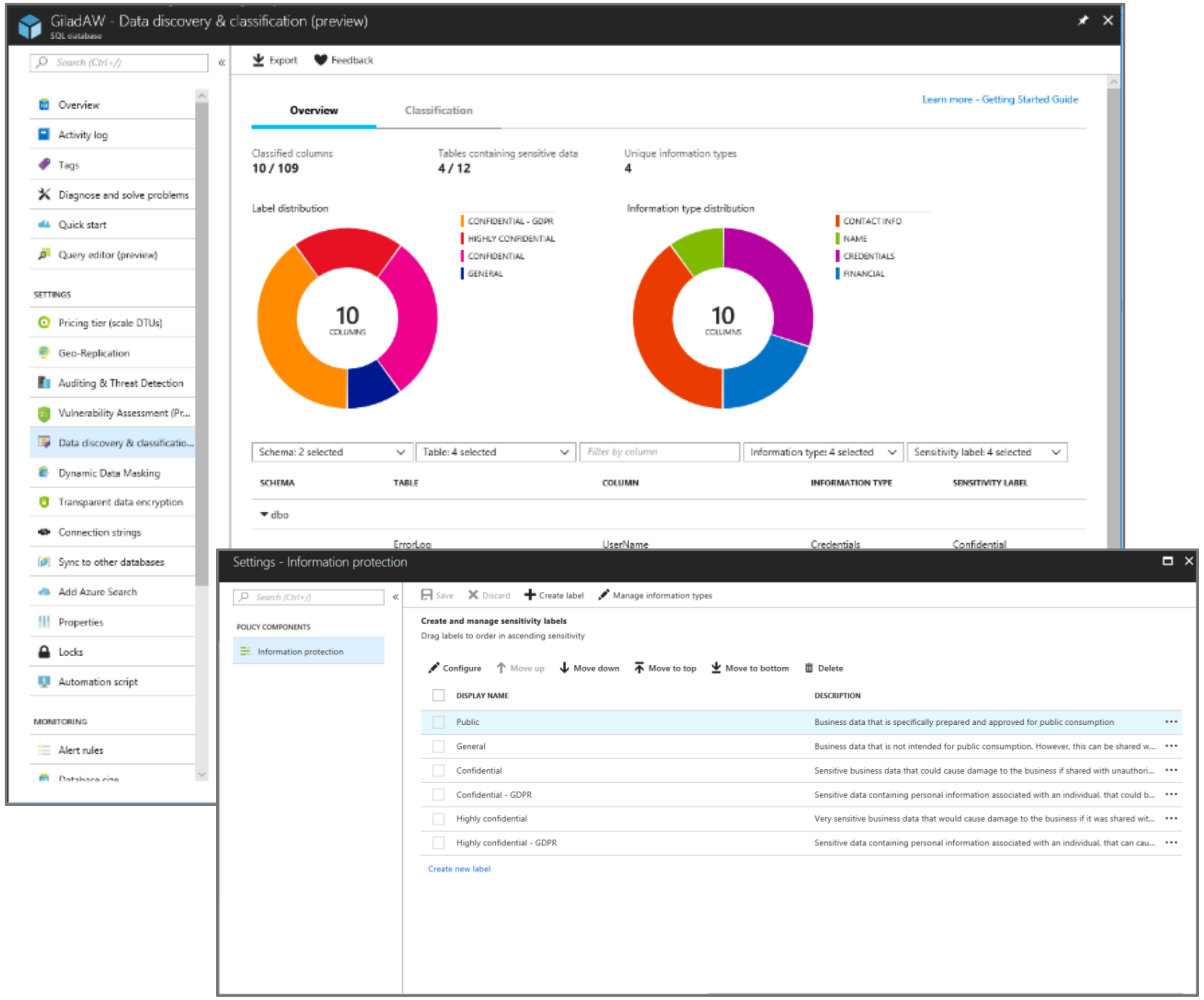
HIGH 1 MEDIUM 3

	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	...

- ✓ Detects potential SQL injection attacks
- ✓ Detects unusual access & data exfiltration activities
- ✓ Actionable alerts to investigate & remediate
- ✓ View alerts for your entire Azure tenant using Azure Security Center

SQL Data Discovery & Classification

Discover, classify, protect and track access to sensitive data



Classified columns
10 / 109

Tables containing sensitive data
4 / 12

Unique information types
4

Schema: 2 selected | Table: 4 selected | Filter by column | Information type: 4 selected | Sensitivity label: 4 selected

SCHEMA	TABLE	COLUMN	INFORMATION TYPE	SENSITIVITY LABEL
dbo				
	ErrorLog	UserName	Credentials	Confidential

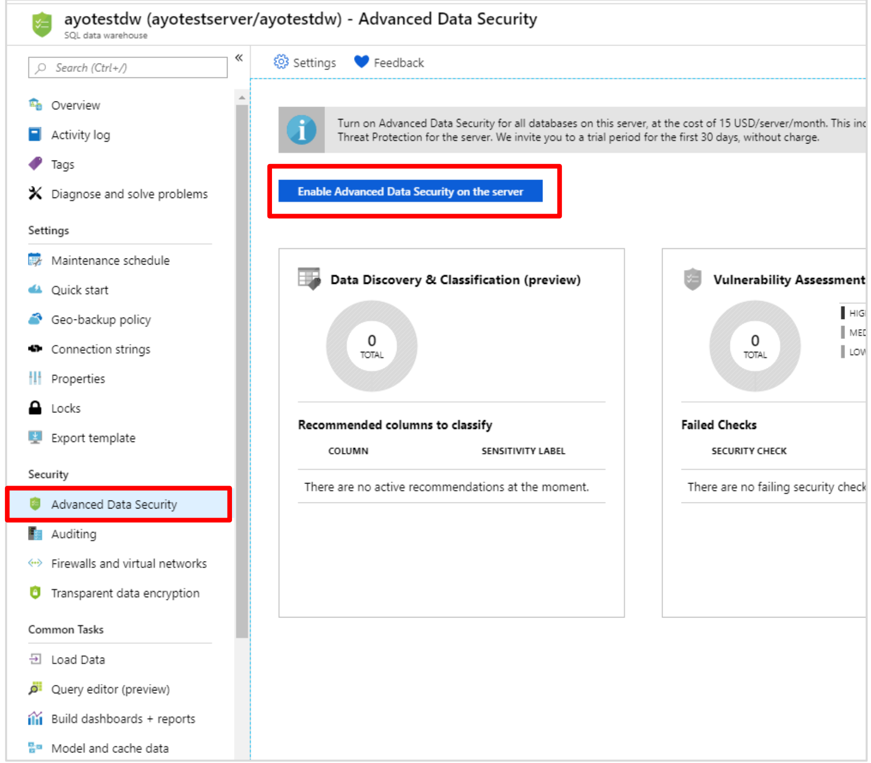
Create and manage sensitivity labels
Drag labels to order in ascending sensitivity

	DISPLAY NAME	DESCRIPTION
□	Public	Business data that is specifically prepared and approved for public consumption
□	General	Business data that is not intended for public consumption. However, this can be shared w...
□	Confidential	Sensitive business data that could cause damage to the business if shared with unauthori...
□	Confidential - GDPR	Sensitive data containing personal information associated with an individual, that could b...
□	Highly confidential	Very sensitive business data that would cause damage to the business if it was shared wit...
□	Highly confidential - GDPR	Sensitive data containing personal information associated with an individual, that can cau...

- ✓ Automatic discovery of columns with sensitive data
- ✓ Add persistent sensitive data labels
- ✓ Audit and detect access to the sensitive data
- ✓ Manage labels for your entire Azure tenant using Azure Security Center

SQL Data Discovery & Classification - setup

Step 1: Enable Advanced Data Security on the logical SQL Server



Turn on Advanced Data Security for all databases on this server, at the cost of 15 USD/server/month. This inc
Threat Protection for the server. We invite you to a trial period for the first 30 days, without charge.

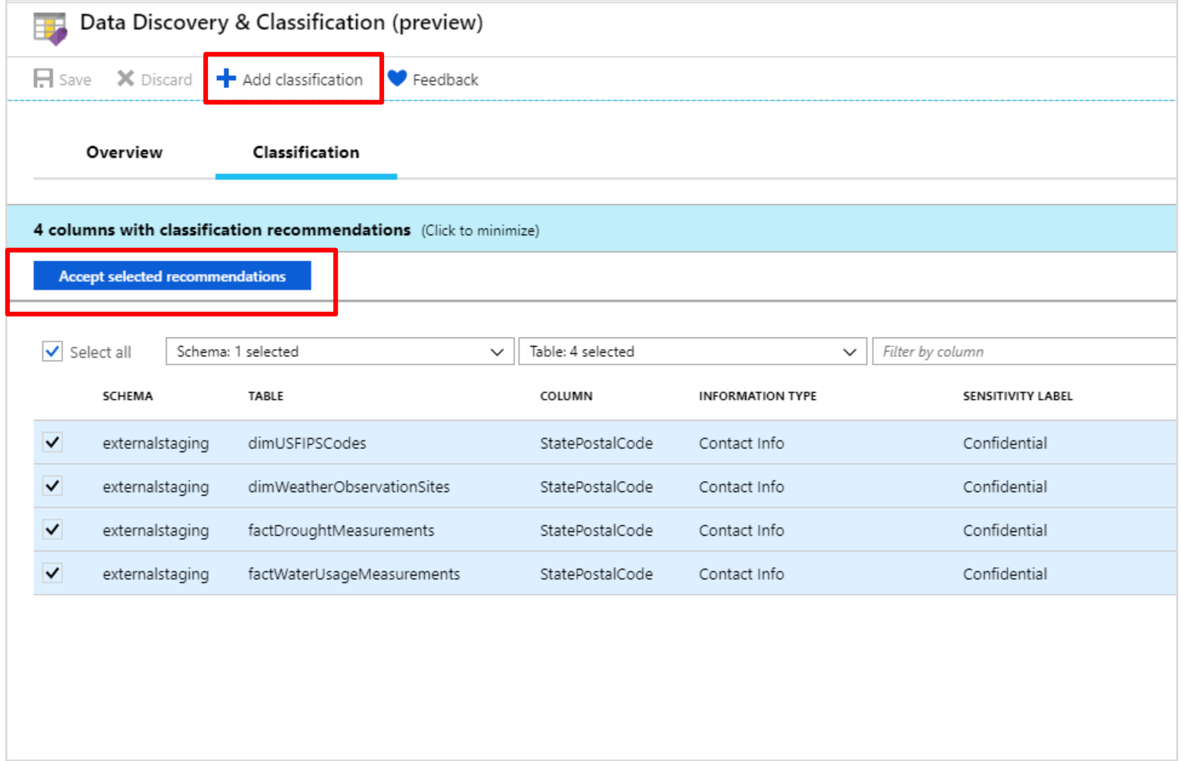
Recommended columns to classify

COLUMN	SENSITIVITY LABEL
There are no active recommendations at the moment.	

Failed Checks

SECURITY CHECK
There are no failing security check

Step 2: Use recommendations and/or manual classification to classify all the sensitive columns in your tables

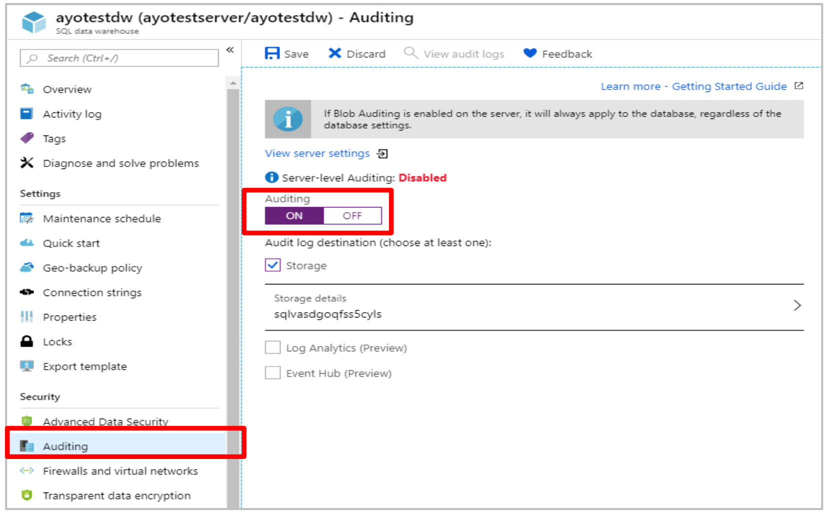


4 columns with classification recommendations (Click to minimize)

	SCHEMA	TABLE	COLUMN	INFORMATION TYPE	SENSITIVITY LABEL
☑	externalstaging	dimUSFIPSCodes	StatePostalCode	Contact Info	Confidential
☑	externalstaging	dimWeatherObservationSites	StatePostalCode	Contact Info	Confidential
☑	externalstaging	factDroughtMeasurements	StatePostalCode	Contact Info	Confidential
☑	externalstaging	factWaterUsageMeasurements	StatePostalCode	Contact Info	Confidential

SQL Data Discovery & Classification – audit sensitive data access

Step 1: Configure auditing for your target Data warehouse. This can be configured for just a single data warehouse or all databases on a server.



If Blob Auditing is enabled on the server, it will always apply to the database, regardless of the database settings.

Server-level Auditing: Disabled

Auditing: ON OFF

Audit log destination (choose at least one):

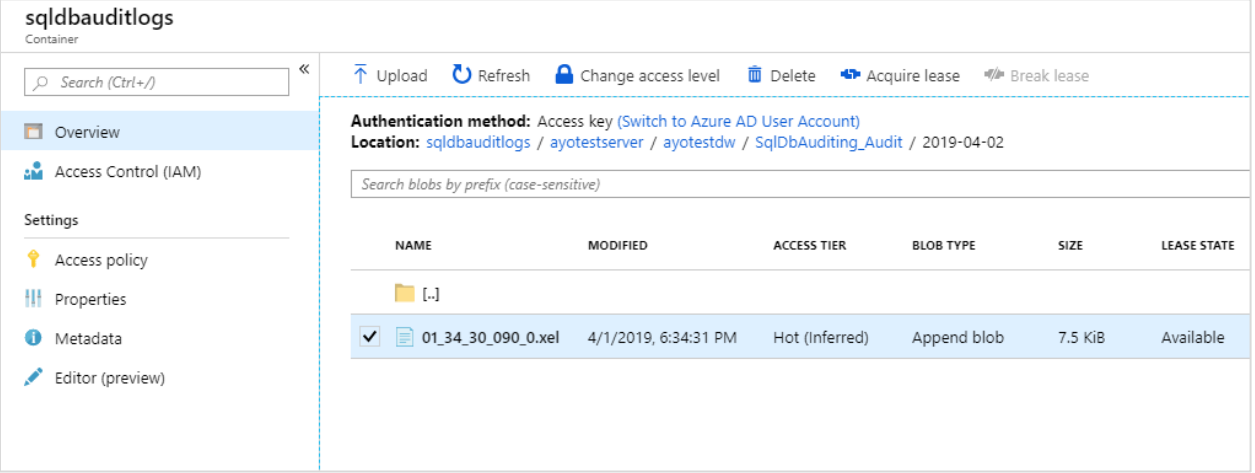
☑ Storage

Storage details: sqlvasdgoqfss5cyls

☐ Log Analytics (Preview)

☐ Event Hub (Preview)

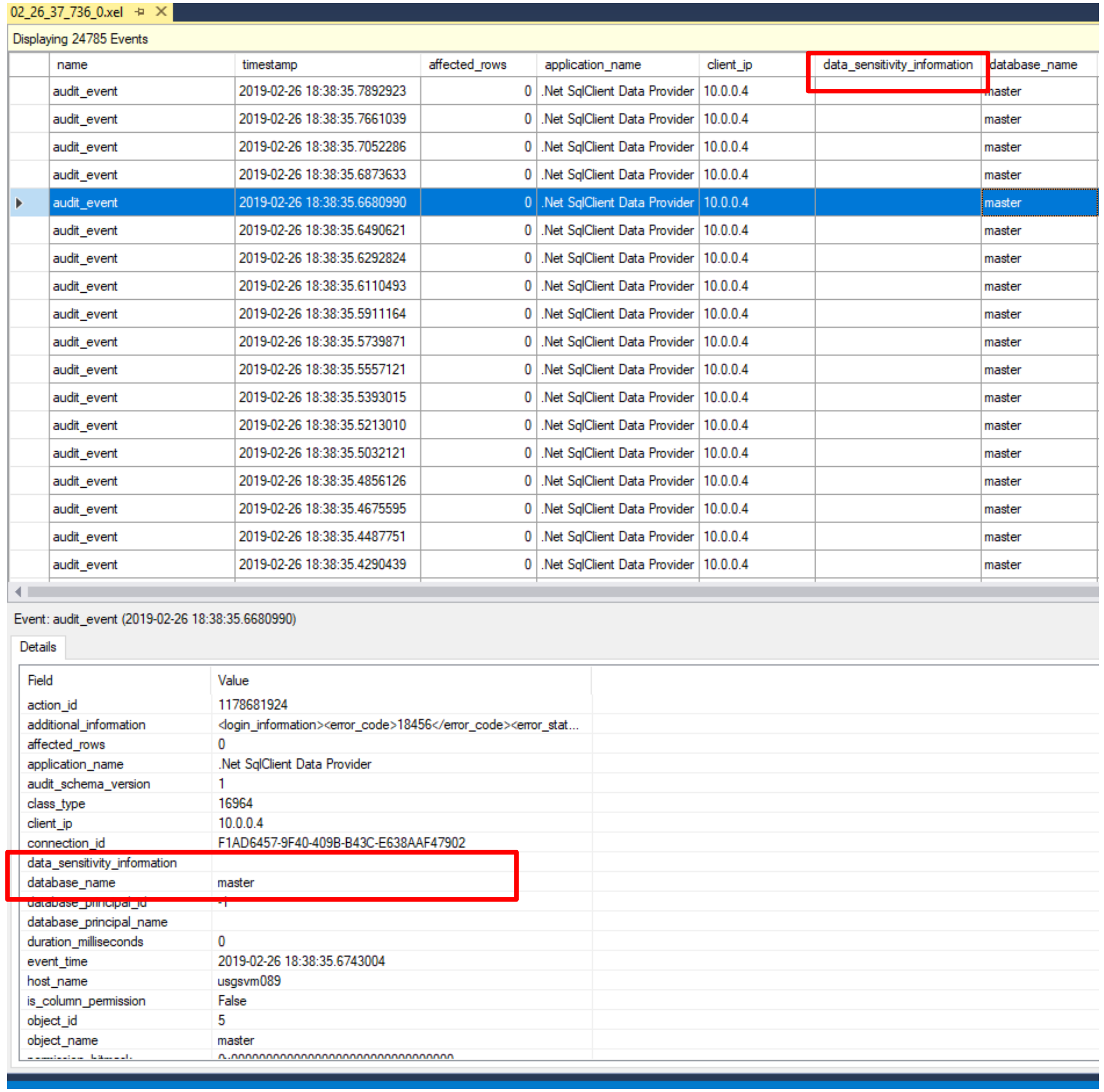
Step 2: Navigate to audit logs in storage account and download 'xel' log files to local machine.



Authentication method: Access key (Switch to Azure AD User Account)
Location: sqldbauditlogs / ayotestserver / ayotestdw / SqlDbAuditing_Audit / 2019-04-02

	NAME	MODIFIED	ACCESS TIER	BLOB TYPE	SIZE	LEASE STATE
	[..]					
☑	01_34_30_090_0.xel	4/1/2019, 6:34:31 PM	Hot (Inferred)	Append blob	7.5 KiB	Available

Step 3: Open logs using extended events viewer in SSMS. Configure viewer to include 'data_sensitivity_information' column



Displaying 24785 Events

name	timestamp	affected_rows	application_name	client_ip	data_sensitivity_information	database_name
audit_event	2019-02-26 18:38:35.7892923	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.7661039	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.7052286	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.6873633	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.6680990	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.6490621	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.6292824	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.6110493	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.5911164	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.5739871	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.5557121	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.5393015	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.5213010	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.5032121	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.4856126	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.4675595	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.4487751	0	.Net SqlClient Data Provider	10.0.0.4		master
audit_event	2019-02-26 18:38:35.4290439	0	.Net SqlClient Data Provider	10.0.0.4		master

Event: audit_event (2019-02-26 18:38:35.6680990)

Details

Field	Value
action_id	1178681924
additional_information	<login_information><error_code>18456</error_code><error_stat...
affected_rows	0
application_name	.Net SqlClient Data Provider
audit_schema_version	1
class_type	16964
client_ip	10.0.0.4
connection_id	F1AD6457-9F40-409B-B43C-E638AAF47902
data_sensitivity_information	
database_name	master
database_principal_id	-1
database_principal_name	
duration_milliseconds	0
event_time	2019-02-26 18:38:35.6743004
host_name	usgsvm089
is_column_permission	False
object_id	5
object_name	master
permission_bitmask	0x00000000000000000000000000000000

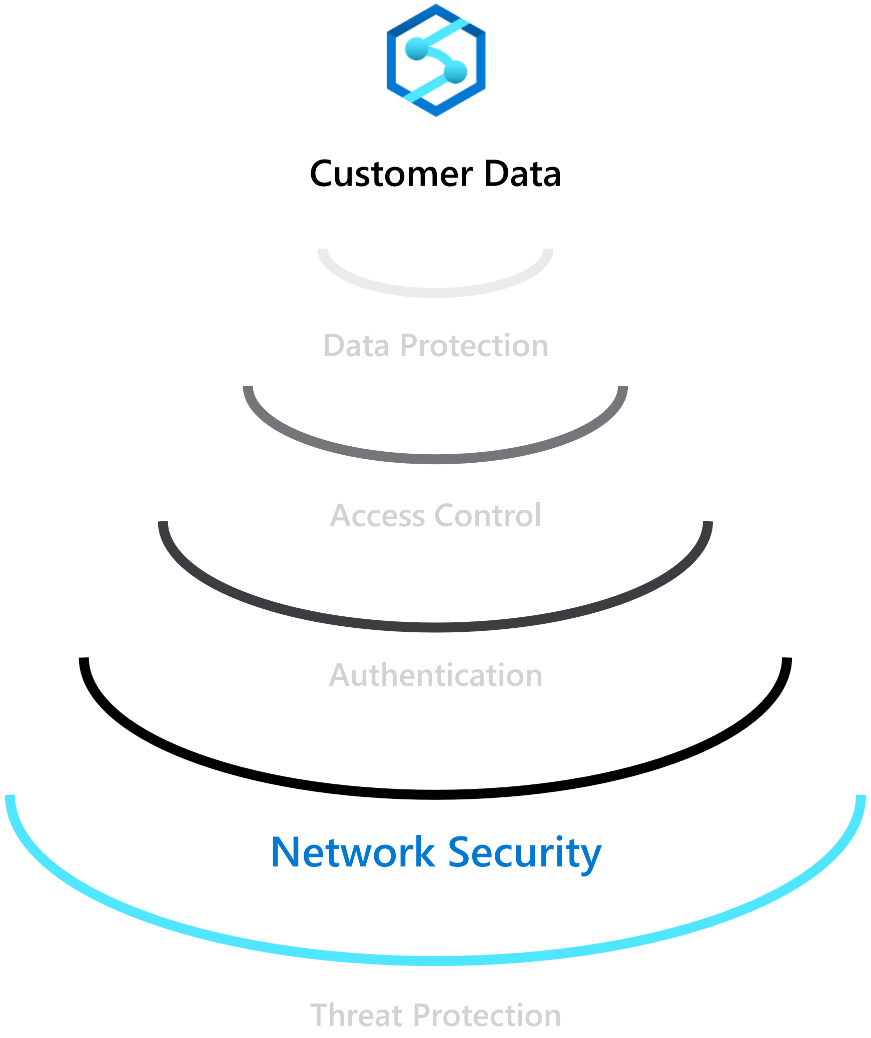
Network Security - Business requirements

How do we implement network isolation?

Data at different levels of security needs to be accessed from different locations.

How do we achieve separation?

Disallowing access to entities outside the company's network security boundary.

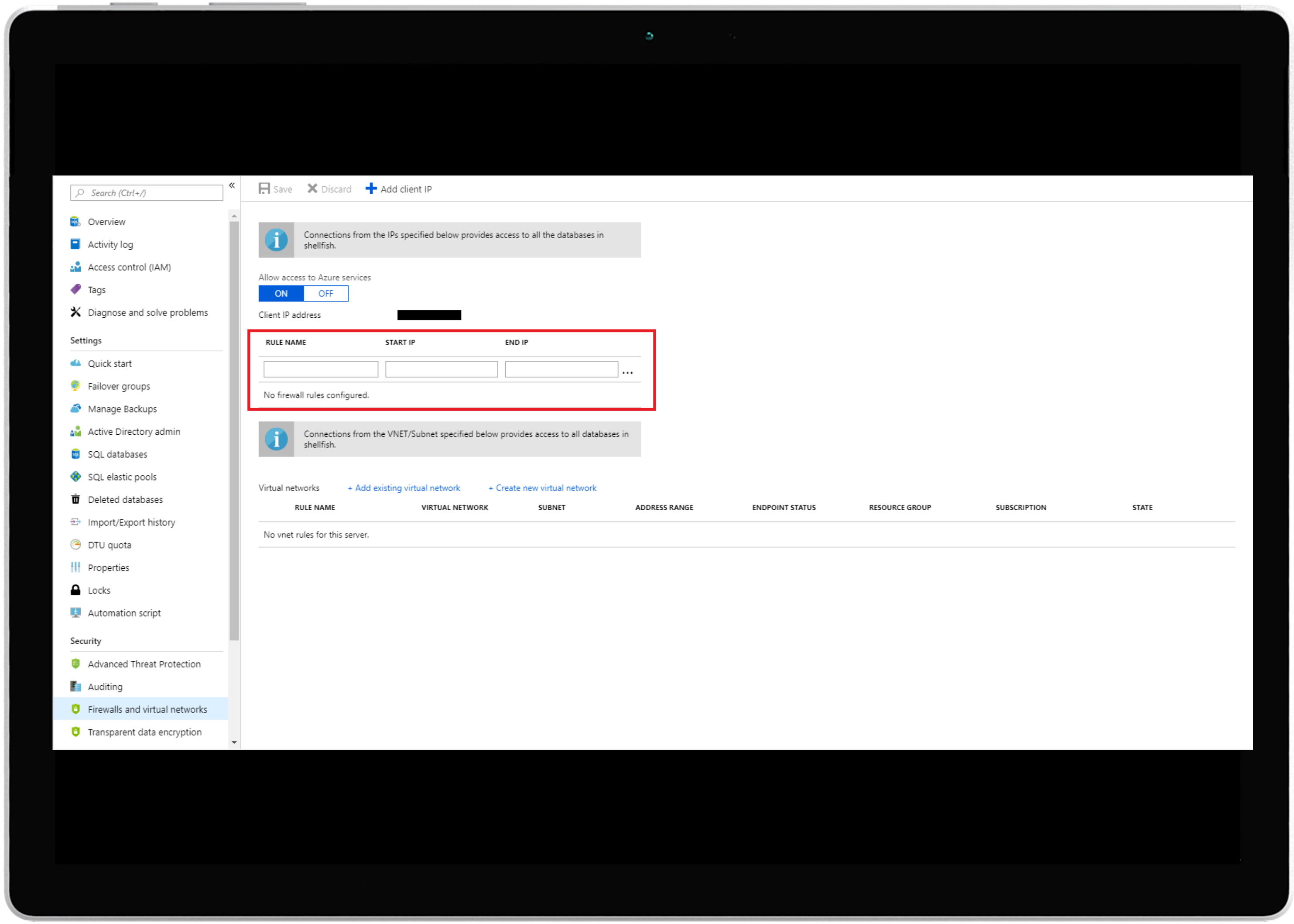


Firewall configuration on the portal

By default, Azure blocks all external connections to port 1433

Configure with the following steps:

Azure Synapse Analytics Resource:
Server name > Firewalls and virtual networks



Connections from the IPs specified below provides access to all the databases in shellfish.

Allow access to Azure services

[ON] OFF

Client IP address [redacted]

RULE NAME	START IP	END IP

No firewall rules configured.

Connections from the VNET/Subnet specified below provides access to all databases in shellfish.

Virtual networks + Add existing virtual network + Create new virtual network

RULE NAME	VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION	STATE

No vnet rules for this server.

Firewall configuration using REST API

Managing firewall rules through REST API must be authenticated.

For information, see Authenticating Service Management Requests.

Server-level rules can be created, updated, or deleted using REST API.

To create or update a server-level firewall rule, execute the PUT method.

To remove an existing server-level firewall rule, execute the DELETE method.

To list firewall rules, execute the GET.

```
PUT
https://management.azure.com/subscriptions/{subscriptionI
d}/resourceGroups/{resourceGroupName}/providers/Microsoft
.Sql/servers/{serverName}/firewallRules/{firewallRuleName
}?api-version=2014-04-01REQUEST BODY
{
  "properties": {
    "startIpAddress": "0.0.0.3",
    "endIpAddress": "0.0.0.3"
  }
}

DELETE
https://management.azure.com/subscriptions/{subscriptionI
d}/resourceGroups/{resourceGroupName}/providers/Microsoft
.Sql/servers/{serverName}/firewallRules/{firewallRuleName
}?api-version=2014-04-01

GET
https://management.azure.com/subscriptions/{subscriptionI
d}/resourceGroups/{resourceGroupName}/providers/Microsoft
.Sql/servers/{serverName}/firewallRules/{firewallRuleName
}?api-version=2014-04-01
```

Firewall configuration using PowerShell/T-SQL

Windows PowerShell Azure cmdlets

New-AzureRmSqlServerFirewallRule

Get-AzureRmSqlServerFirewallRule

Set-AzureRmSqlServerFirewallRule

Transact SQL

sp_set_firewall_rule

sp_delete_firewall_rule

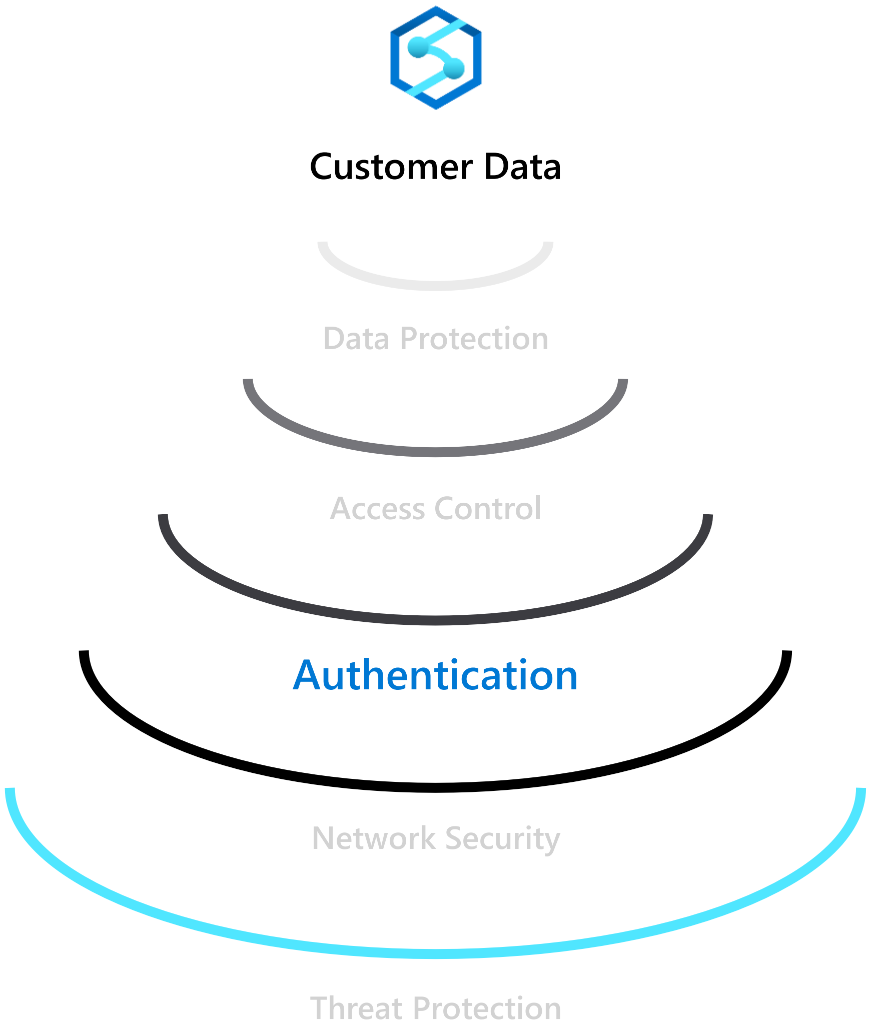
```
# PS Allow external IP access to SQL DW
PS C:\> New-AzureRmSqlServerFirewallRule
         -ResourceGroupName "myResourceGroup" `
         -ServerName $servername `
         -FirewallRuleName "AllowSome"
         -StartIpAddress "0.0.0.0"
         -EndIpAddress "0.0.0.0“

-- T-SQL Allow external IP access to SQL DW
EXECUTE sp_set_firewall_rule
         @name = N'ContosoFirewallRule’,
         @start_ip_address = '192.168.1.1’,
         @end_ip_address = '192.168.1.10'
```

Authentication - Business requirements

How do I configure Azure Active Directory with Azure Synapse Analytics?

I want additional control in the form of multi-factor authentication

How do I allow non-Microsoft accounts to be able to authenticate?



Customer Data

Data Protection

Access Control

Authentication

Network Security

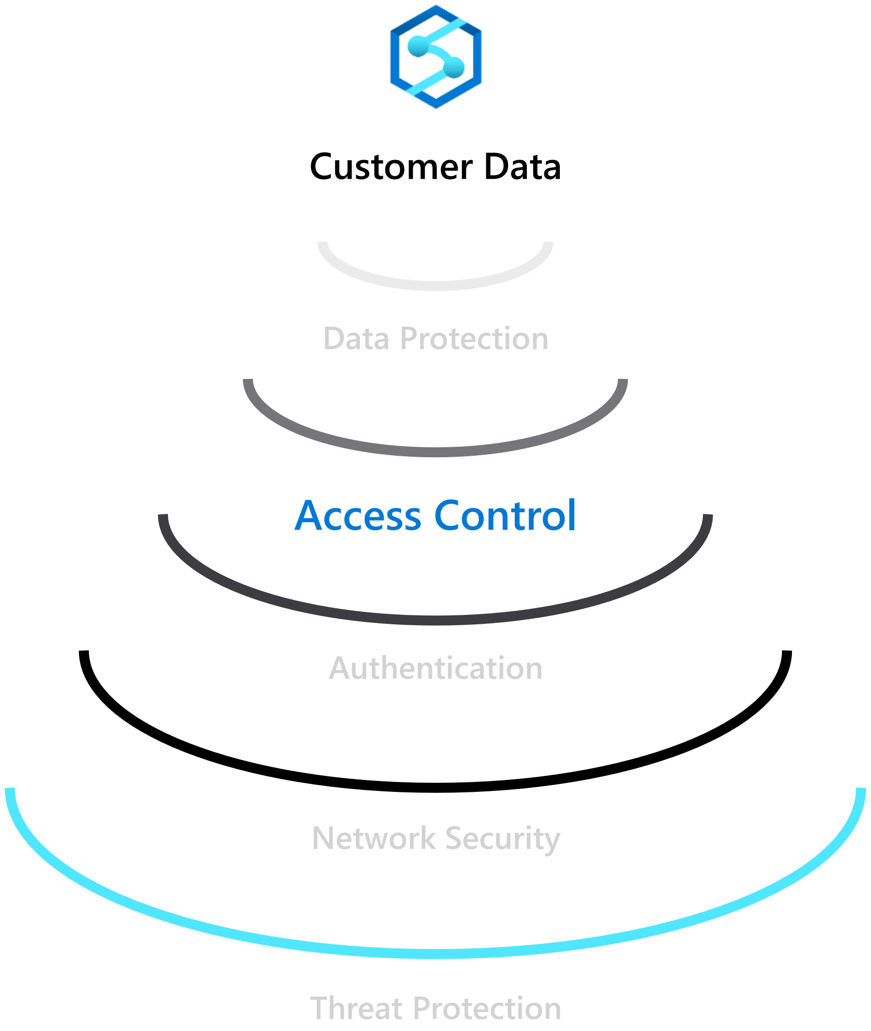
Threat Protection

Access Control - Business requirements

How do I restrict access to sensitive data to specific database users?

How do I ensure users only have access to relevant data?

For example, in a hospital only medical staff should be allowed to see patient data that is relevant to them—and not every patient’s data.



Object-level security (tables, views, and more)

Overview

GRANT controls permissions on designated tables, views, stored procedures, and functions.

Prevent unauthorized queries against certain tables.

Simplifies design and implementation of security at the database level as opposed to application level.

```
-- Grant SELECT permission to user RosaQdM on table Person.Address in the AdventureWorks2012 database
GRANT SELECT ON OBJECT::Person.Address TO RosaQdM;
GO
-- Grant REFERENCES permission on column BusinessEntityID in view HumanResources.vEmployee to user Wanida
GRANT REFERENCES(BusinessEntityID) ON OBJECT::HumanResources.vEmployee to Wanida with GRANT OPTION;
GO
-- Grant EXECUTE permission on stored procedure HumanResources.uspUpdateEmployeeHireInfo to an application role called Recruiting11
USE AdventureWorks2012;
GRANT EXECUTE ON OBJECT::HumanResources.uspUpdateEmployeeHireInfo TO RECRUITING 11;
GO
```

Row-level security (RLS)

Overview

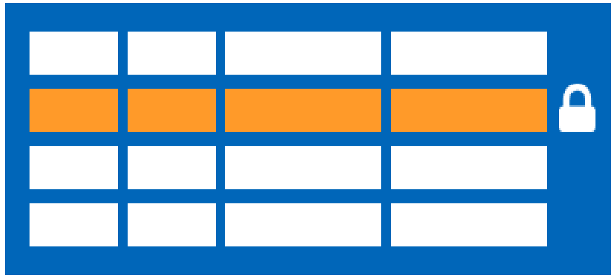
Fine grained access control of specific rows in a database table.

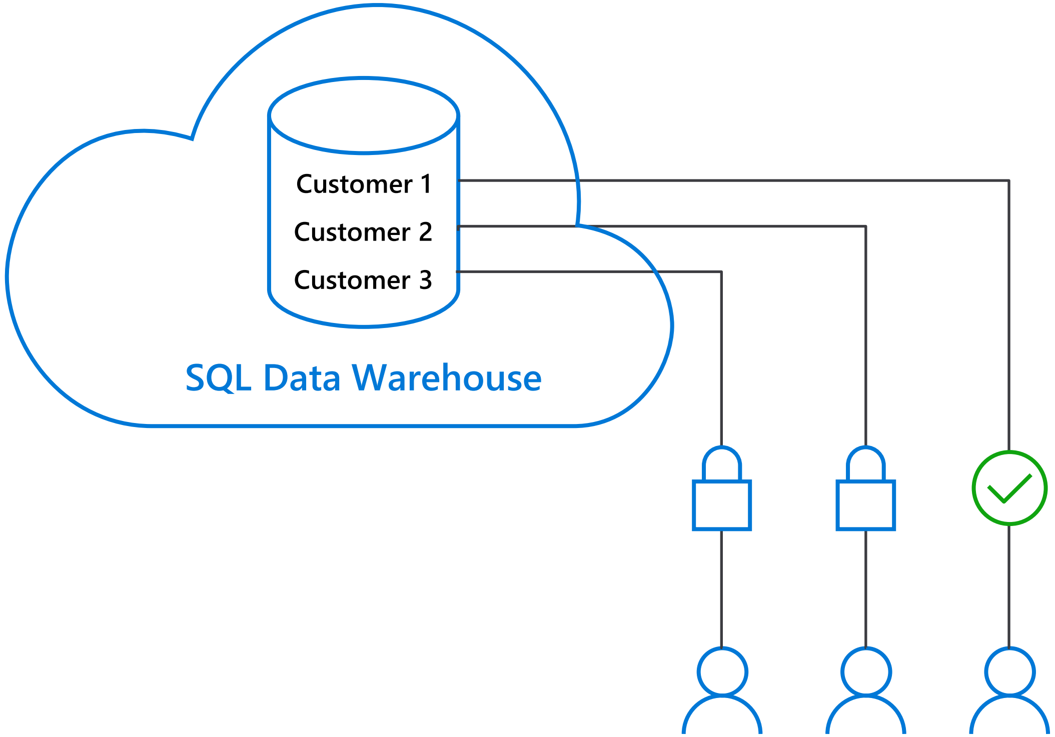
Help prevent unauthorized access when multiple users share the same tables.

Eliminates need to implement connection filtering in multi-tenant applications.

Administer via SQL Server Management Studio or SQL Server Data Tools.

Easily locate enforcement logic inside the database and schema bound to the table.





Row-level security

Creating policies

Filter predicates silently filter the rows available to read operations (SELECT, UPDATE, and DELETE).

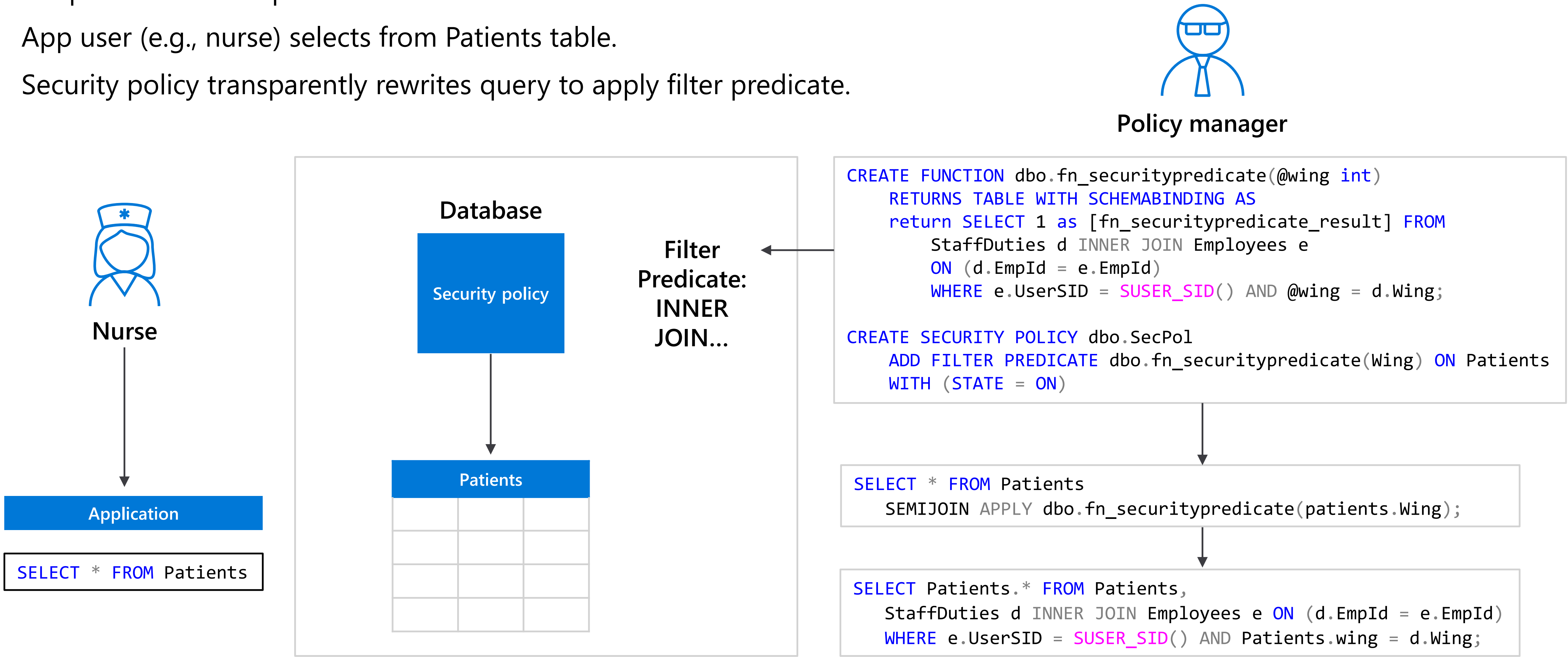
The following examples demonstrate the use of the CREATE SECURITY POLICY syntax

```sql
-- The following syntax creates a security policy with a filter predicate for the Customer table
CREATE SECURITY POLICY [FederatedSecurityPolicy]
ADD FILTER PREDICATE [rls].[fn_securitypredicate]([CustomerId])
ON [dbo].[Customer];

-- Create a new schema and predicate function, which will use the application user ID stored in CONTEXT_INFO to filter rows.
CREATE FUNCTION rls.fn_securitypredicate (@AppUserId int)
RETURNS TABLE
WITH SCHEMABINDING
AS
RETURN (
SELECT 1 AS fn_securitypredicate_result
WHERE
DATABASE_PRINCIPAL_ID() = DATABASE_PRINCIPAL_ID('dbo') -- application context
AND CONTEXT_INFO() = CONVERT(VARBINARY(128), @AppUserId));
GO
```

Row-level security

Three steps:

1. Policy manager creates filter predicate and security policy in T-SQL, binding the predicate to the patients table.
2. App user (e.g., nurse) selects from Patients table.
3. Security policy transparently rewrites query to apply filter predicate.



```
SELECT * FROM Patients
```

```
CREATE FUNCTION dbo.fn_securitypredicate(@wing int)
    RETURNS TABLE WITH SCHEMABINDING AS
    return SELECT 1 as [fn_securitypredicate_result] FROM
        StaffDuties d INNER JOIN Employees e
        ON (d.EmpId = e.EmpId)
        WHERE e.UserSID = SUSER_SID() AND @wing = d.Wing;

CREATE SECURITY POLICY dbo.SecPol
    ADD FILTER PREDICATE dbo.fn_securitypredicate(Wing) ON Patients
    WITH (STATE = ON)
```

```
SELECT * FROM Patients
   SEMIJOIN APPLY dbo.fn_securitypredicate(patients.Wing);
```

```
SELECT Patients.* FROM Patients,
   StaffDuties d INNER JOIN Employees e ON (d.EmpId = e.EmpId)
   WHERE e.UserSID = SUSER_SID() AND Patients.wing = d.Wing;
```

Column-level security

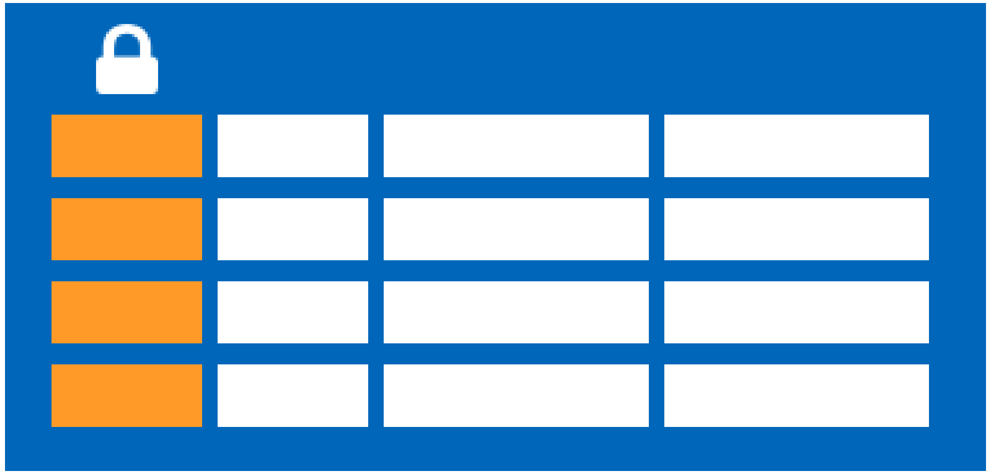
Overview

Control access of specific columns in a database table based on customer's group membership or execution context.

Simplifies the design and implementation of security by putting restriction logic in database tier as opposed to application tier.

Administer via GRANT T-SQL statement.

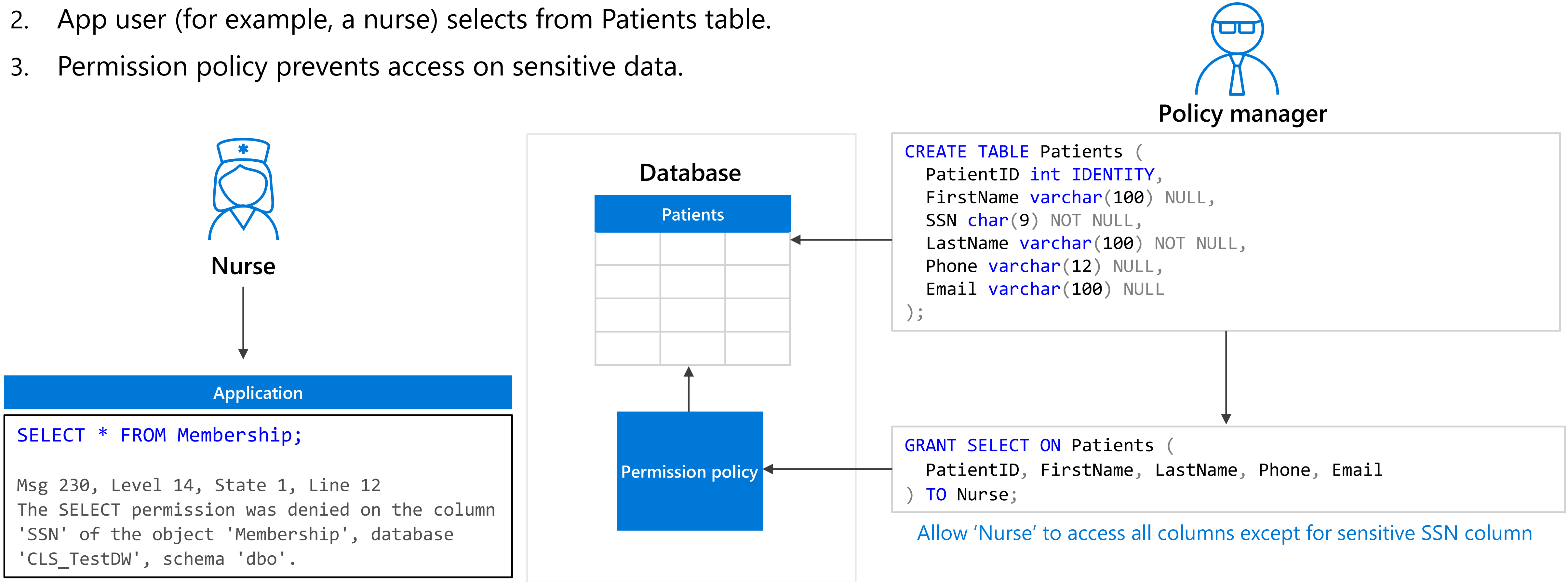
Both Azure Active Directory (AAD) and SQL authentication are supported.



Column-level security

Three steps:

1. Policy manager creates permission policy in T-SQL, binding the policy to the Patients table on a specific group.
2. App user (for example, a nurse) selects from Patients table.
3. Permission policy prevents access on sensitive data.



```
CREATE TABLE Patients (
  PatientID int IDENTITY,
  FirstName varchar(100) NULL,
  SSN char(9) NOT NULL,
  LastName varchar(100) NOT NULL,
  Phone varchar(12) NULL,
  Email varchar(100) NULL
);
```

```
GRANT SELECT ON Patients (
  PatientID, FirstName, LastName, Phone, Email
) TO Nurse;
```

Allow 'Nurse' to access all columns except for sensitive SSN column

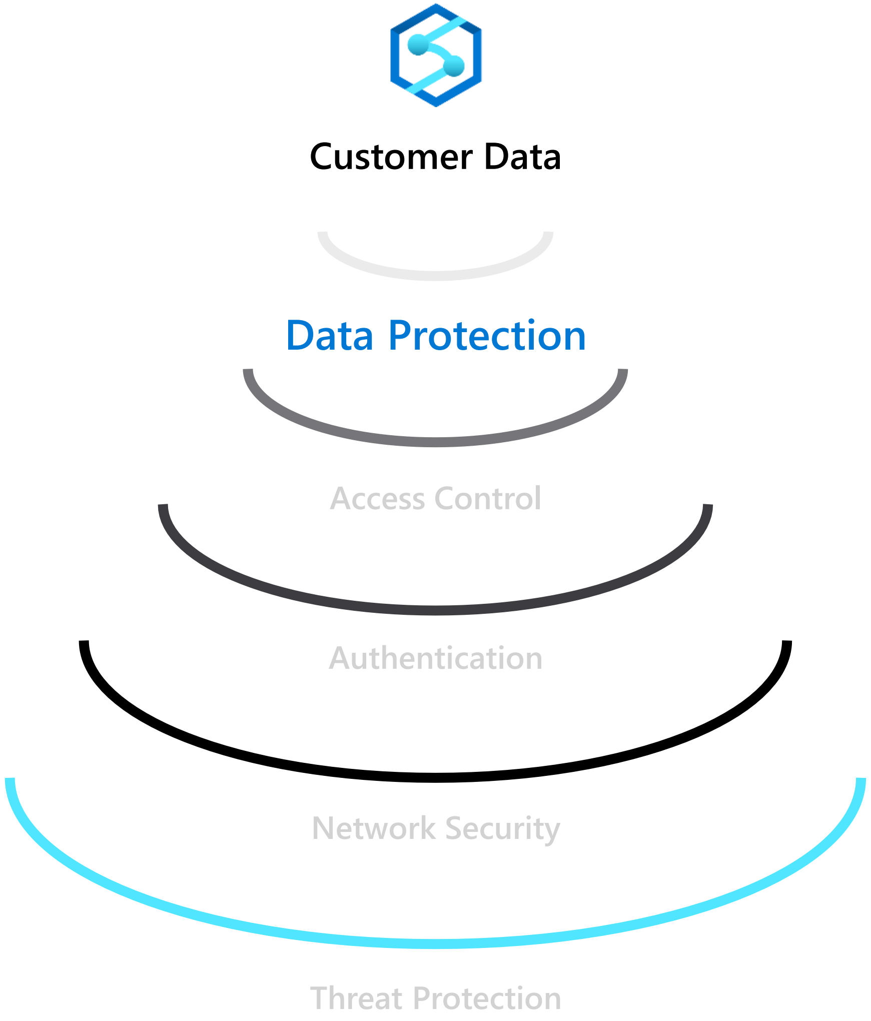
```
SELECT * FROM Membership;

Msg 230, Level 14, State 1, Line 12
The SELECT permission was denied on the column
'SSN' of the object 'Membership', database
'CLS_TestDW', schema 'dbo'.
```

Queries executed as 'Nurse' will fail if they include the SSN column

Data Protection - Business requirements

How do I protect sensitive data against unauthorized (high-privileged) users?

What key management options do I have?



Customer Data

Data Protection

Access Control

Authentication

Network Security

Threat Protection

Dynamic Data Masking

Overview

Prevent abuse of sensitive data by hiding it from users

Easy configuration in new Azure Portal

Policy-driven at table and column level, for a defined set of users

Data masking applied in real-time to query results based on policy

Multiple masking functions available, such as full or partial, for various sensitive data categories (credit card numbers, SSN, etc.)

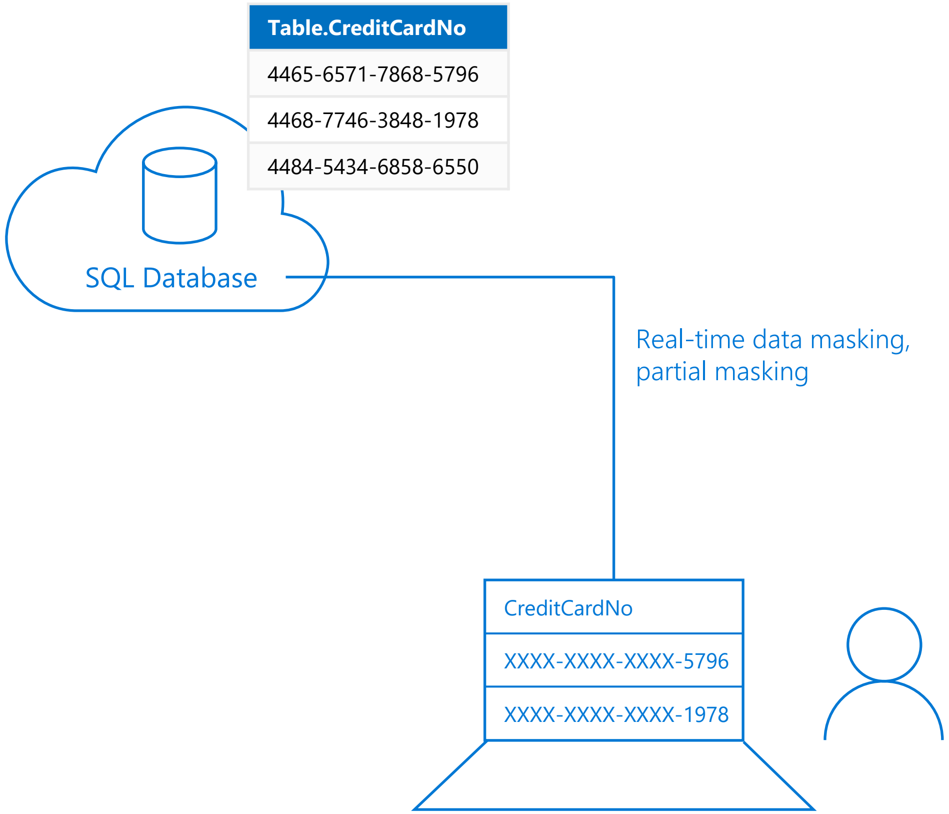


Table.CreditCardNo
4465-6571-7868-5796
4468-7746-3848-1978
4484-5434-6858-6550

CreditCardNo
XXXX-XXXX-XXXX-5796
XXXX-XXXX-XXXX-1978

Column Level Encryption

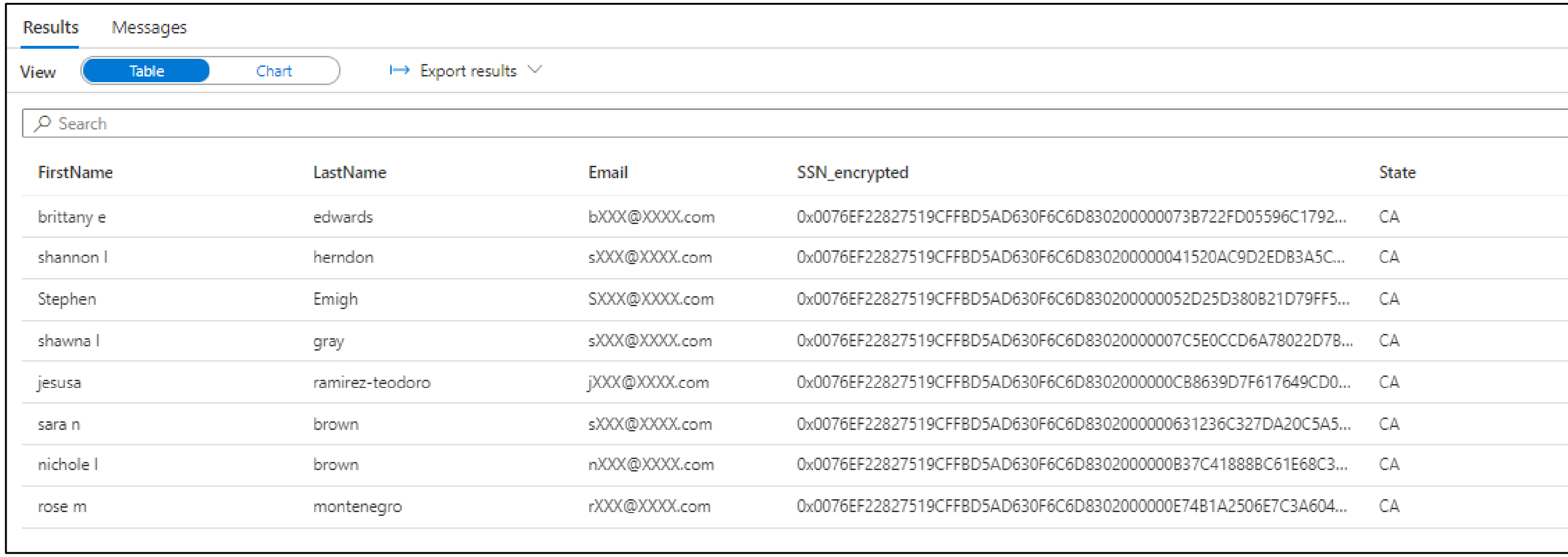
Overview

It helps to implement fine-grained protection of sensitive data within a table in dedicated SQL pool.

The data in CLE enforced columns is encrypted on disk. User need to use DECRYPTBYKEY function to decrypt it.

5 step process to set up CLE

1. Create master key
2. Create certificate
3. Configure symmetric key for encryption
4. Encrypt the column data
5. Close symmetric key



FirstName	LastName	Email	SSN_encrypted	State
brittany e	edwards	bXXX@XXXX.com	0x0076EF22827519CFFBD5AD630F6C6D830200000073B722FD05596C1792...	CA
shannon l	herndon	sXXX@XXXX.com	0x0076EF22827519CFFBD5AD630F6C6D830200000041520AC9D2EDB3A5C...	CA
Stephen	Emigh	SXXX@XXXX.com	0x0076EF22827519CFFBD5AD630F6C6D830200000052D25D380B21D79FF5...	CA
shawna l	gray	sXXX@XXXX.com	0x0076EF22827519CFFBD5AD630F6C6D83020000007C5E0CCD6A78022D7B...	CA
jesusa	ramirez-teodoro	jXXX@XXXX.com	0x0076EF22827519CFFBD5AD630F6C6D8302000000CB8639D7F617649CD0...	CA
sara n	brown	sXXX@XXXX.com	0x0076EF22827519CFFBD5AD630F6C6D8302000000631236C327DA20C5A5...	CA
nichole l	brown	nXXX@XXXX.com	0x0076EF22827519CFFBD5AD630F6C6D8302000000B37C41888BC61E68C3...	CA
rose m	montenegro	rXXX@XXXX.com	0x0076EF22827519CFFBD5AD630F6C6D8302000000E74B1A2506E7C3A604...	CA

Dynamic Data Masking

Three steps

1. Security officer defines dynamic data masking policy in T-SQL over sensitive data in the Employee table. The security officer uses the built-in masking functions (default, email, random)

2. The app-user selects from the Employee table

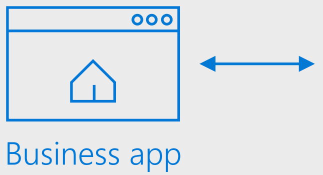
3. The dynamic data masking policy obfuscates the sensitive data in the query results for non-privileged users

Security officer

1

```
ALTER TABLE [Employee]
ALTER COLUMN [SocialSecurityNumber]
ADD MASKED WITH (FUNCTION = 'DEFAULT()')

ALTER TABLE [Employee]
ALTER COLUMN [Email]
ADD MASKED WITH (FUNCTION = 'EMAIL()')

ALTER TABLE [Employee]
ALTER COLUMN [Salary]
ADD MASKED WITH (FUNCTION = 'RANDOM(1,20000)')

GRANT UNMASK to admin1
```

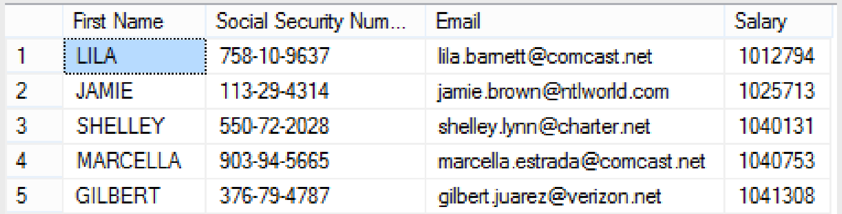
2



```
SELECT [First Name],
       [Social Security Number],
       [Email],
       [Salary]
FROM   [Employee]
```

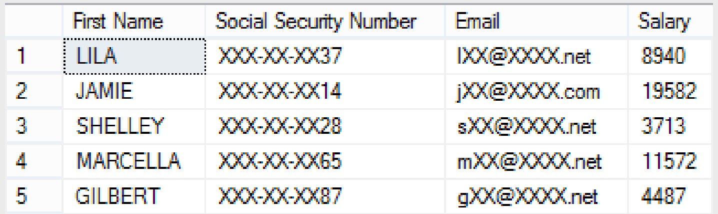
3

Non-masked data (admin login)



	First Name	Social Security Num...	Email	Salary
1	LILA	758-10-9637	lila.barnett@comcast.net	1012794
2	JAMIE	113-29-4314	jamie.brown@ntlworld.com	1025713
3	SHELLEY	550-72-2028	shelley.lynn@charter.net	1040131
4	MARCELLA	903-94-5665	marcella.estrada@comcast.net	1040753
5	GILBERT	376-79-4787	gilbert.juarez@verizon.net	1041308

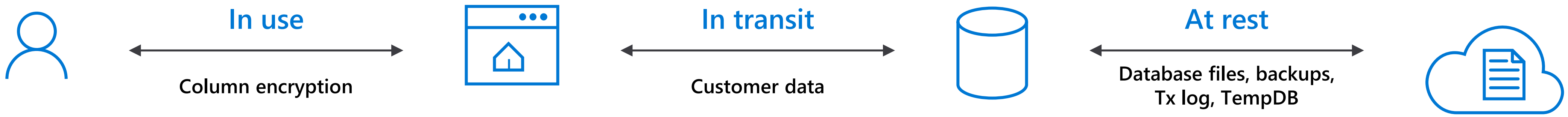
Masked data (admin1 login)



	First Name	Social Security Number	Email	Salary
1	LILA	XXX-XX-XX37	lXX@XXXX.net	8940
2	JAMIE	XXX-XX-XX14	jXX@XXXX.com	19582
3	SHELLEY	XXX-XX-XX28	sXX@XXXX.net	3713
4	MARCELLA	XXX-XX-XX65	mXX@XXXX.net	11572
5	GILBERT	XXX-XX-XX87	gXX@XXXX.net	4487

Types of data encryption

Data Encryption	Encryption Technology	Customer Value
In transit	Transport Layer Security (TLS) from the client to the server TLS 1.2	Protects data between client and server against snooping and man-in-the-middle attacks
At rest	Transparent Data Encryption (TDE) for Azure Synapse Analytics	Protects data on the disk User or Service Managed key management is handled by Azure, which makes it easier to obtain compliance



In use

Column encryption

In transit

Customer data

At rest

Database files, backups, Tx log, TempDB

Transparent data encryption (TDE)

Overview

All customer data encrypted at rest

TDE performs real-time I/O encryption and decryption of the data and log files.

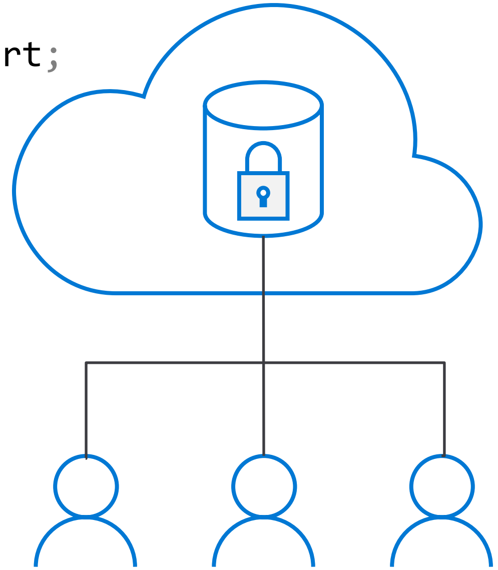
Service OR User managed keys.

Application changes kept to a minimum.

Transparent encryption/decryption of data in a TDE-enabled client driver.

Compliant with many laws, regulations, and guidelines established across various industries.

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
go
CREATE CERTIFICATE MyServerCert WITH SUBJECT = 'My DEK Certificate';
go
USE MyDatabase;
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
GO
ALTER DATABASE MyDatabase
SET ENCRYPTION ON;
GO
```



Transparent data encryption (TDE)

Key Vault

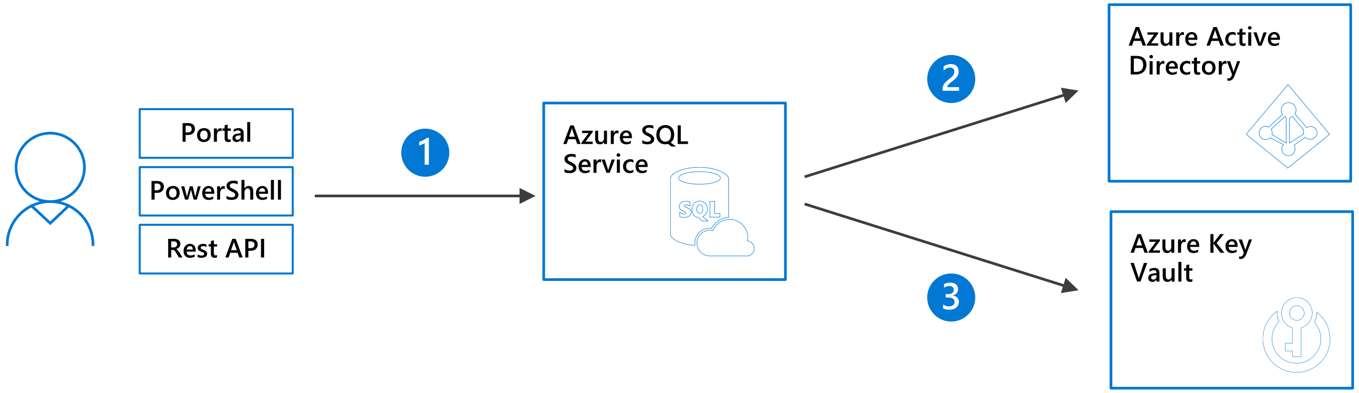
Benefits with User Managed Keys

Assume more control over who has access to your data and when.

Highly available and scalable cloud-based key store.

Central key management that allows separation of key management and data.

Configurable via Azure Portal, PowerShell, and REST API.



1 The Key Vault admin grants vault access to the SQL Database server using its unique Azure Active Directory (AD) identity

2 The server uses its Azure AD identity to authenticate with Azure AD for access to your Key Vault

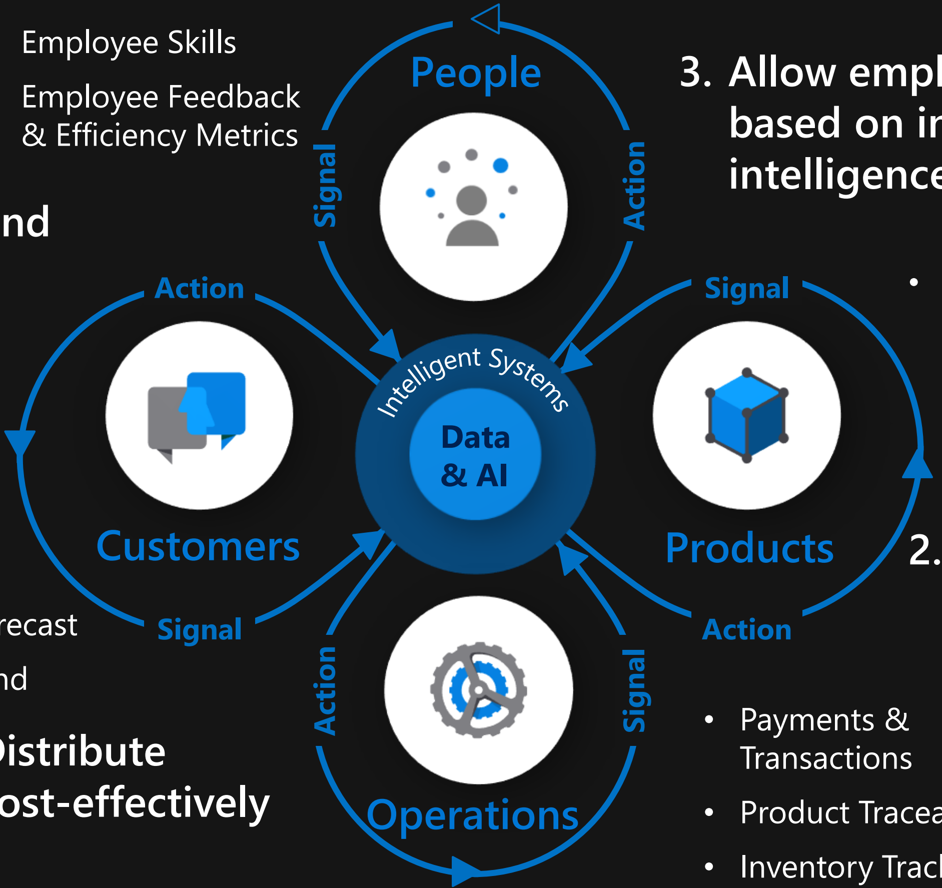
3 The server sends get, wrap key, and unwrap key request to the asymmetric key in key Vault for database encryption key protection.

Microsoft

Q&A | Thank you

Retail Data Platform

In order to create data gravity and build digital feedback loops, we need to bring together data across customer demand, commerce, payments, and distribution



- Employee Skills
- Employee Feedback & Efficiency Metrics

1. Identify, convert, and build long term relationships with customers

- Customer Search Data
- Customer Demand Forecast
- Commerce (in-store and online visits)

3. Allow employees to clientele based on individual customer intelligence

- Product Feedback

2. Manage merchandise decisions and offer personalized pricing / promotions

- Payments & Transactions
- Product Traceability
- Inventory Tracking

4. Distribute cost-effectively