Microsoft Fabric

#FABCONSQLCON2026

FABCON
Microsoft Fabric
COMMUNITY CONFERENCE

SQLCON
Microsoft SQL
COMMUNITY CONFERENCE

ATLANTA MARCH 16 - 20, 2026

Enterprise Security In Fabric

Sarab Dua, Bodhisatva Gautam

Thursday, March 19th, 2026
Time: 8:00 – 9:00 AM,
Room: B213 – B214

Microsoft Fabric

The unified data platform for AI transformation

Databases

Data Factory

Analytics

Real-Time Intelligence

Power BI

Fabric IQ

Fabric Platform

Copilot

OneLake

Admin & Governance

Shipped

aka.ms/FabricSecurityWhitepaper

Network Security

GA

Entra conditional access

Service tags

Enterprise data gateway

VNET Data Gateway Support with Private Links for Dataflows Gen2 and Semantic Models

Private endpoint, tenant level

Shortcuts for ADLS Gen2 in VNET

Spark connectivity to Azure data services in a VNET

Private endpoint, workspace level

Workspace IP Firewall

Outbound Access Protection

Data Security

GA

Workspace roles

SQL Object-level security

SQL Column-level security

SQL Row-level security

SQL Dynamic data mailling

SQL granular permissions

Lockbox

Customer Managed Keys

Governance

GA

Information protection

Sensitivity labels

Purview Audit

Endorsement

Lineage

Impact analysis

Domains & Sub Domains

Metadata scanning

Resiliency

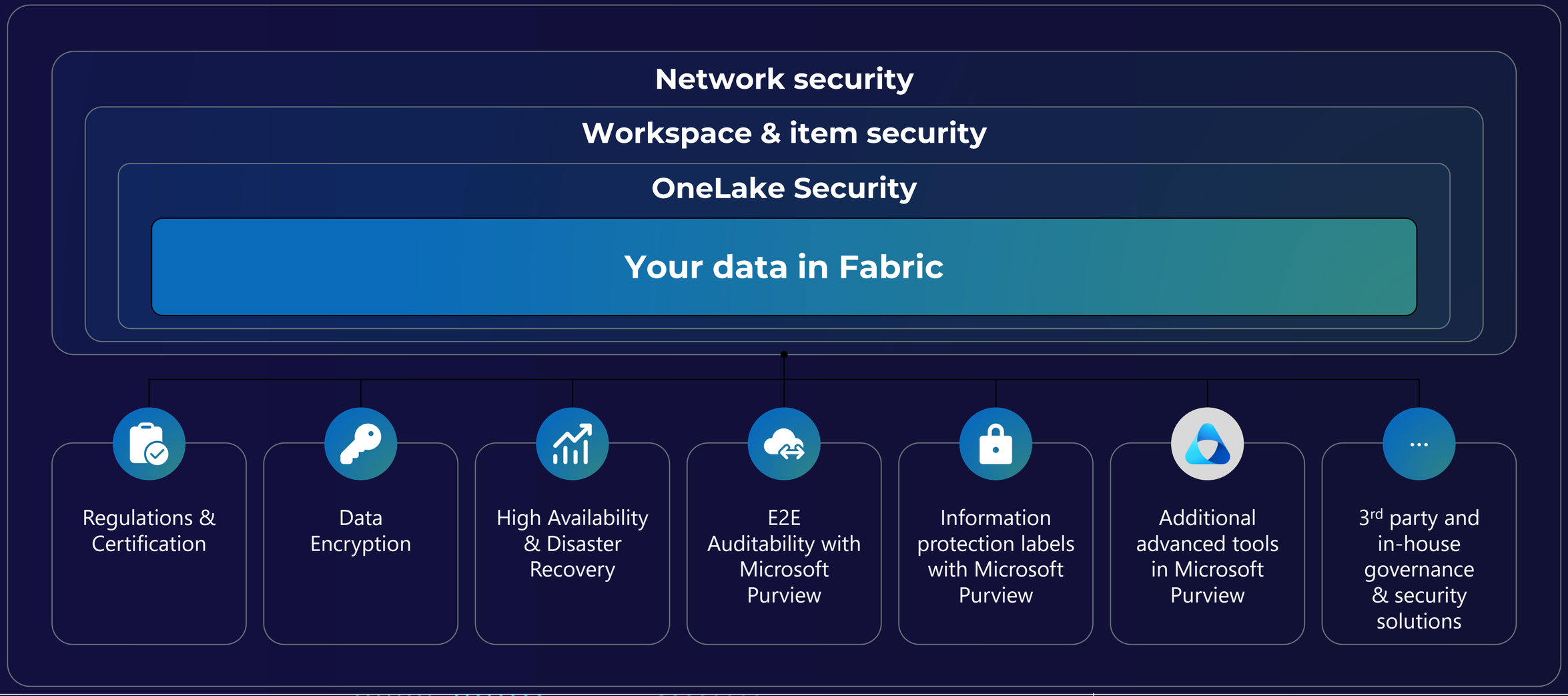
Purview data catalog

Public preview

Admin Monitoring and Insights

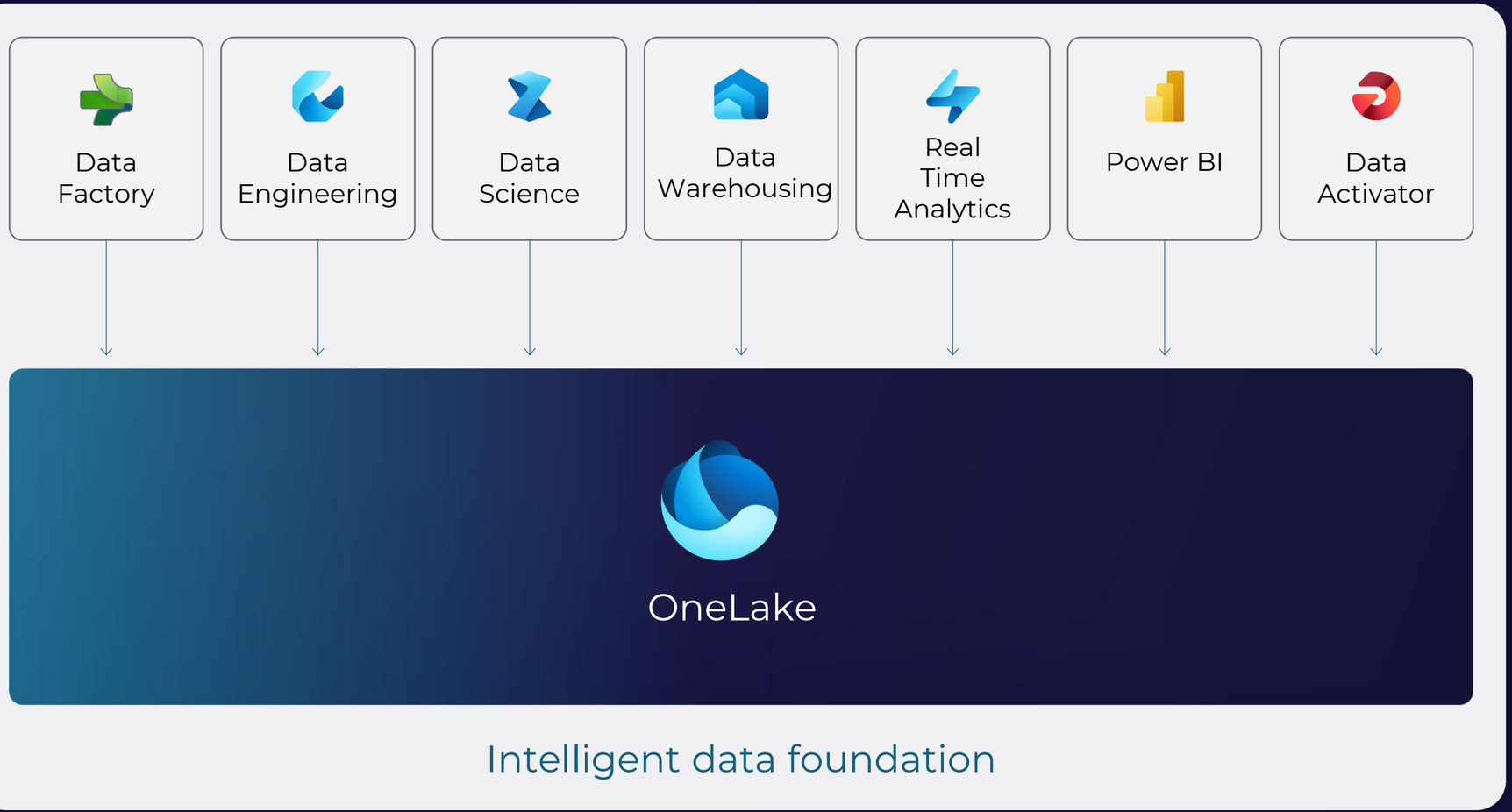
Fabric Monitoring

Security layers in Microsoft Fabric



Network Security in Fabric

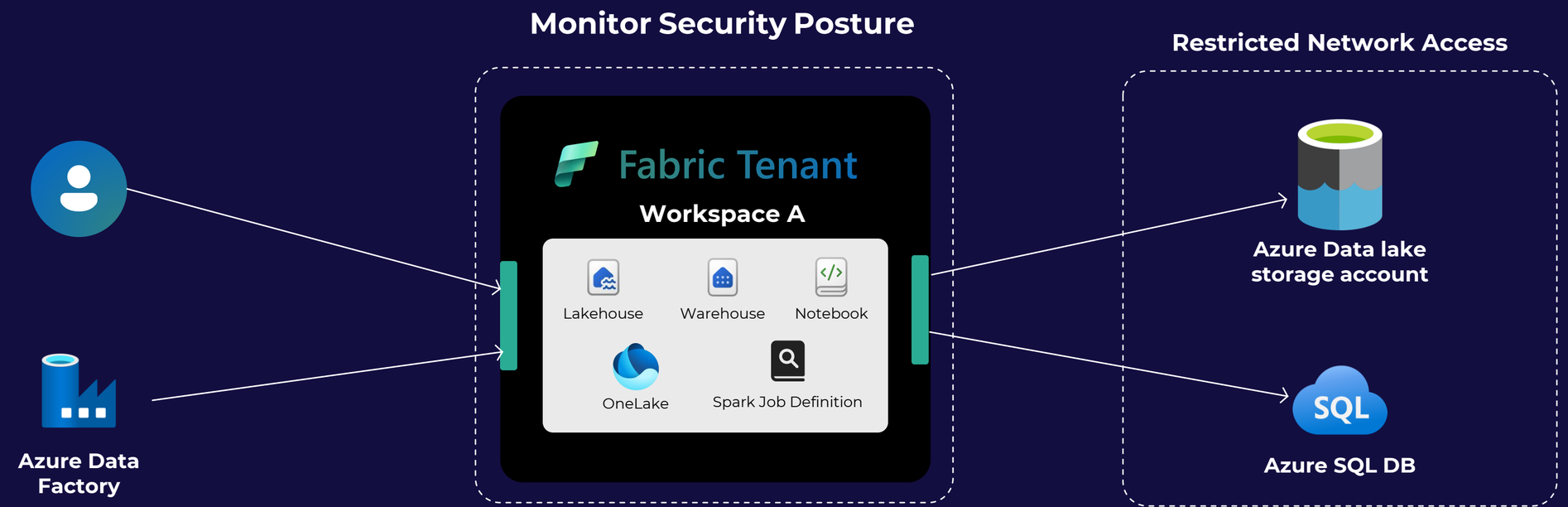
Microsoft Fabric – Secure By default



What it means:

1. All internal communications between the experiences happens through MS backbone network
2. Traffic in and from Fabric is encrypted by TLS 1.2 or more
3. Endpoints and access are protected using Entra

Common Network Security Requirements



Secure access to your data in Fabric (Fabric Inbound)

Restrict Outbound access from Fabric

Securely connect from Fabric to your protected data (Fabric Outbound)

Common Network Security Requirements

- Secure access to your data in Fabric
- Securely connect to your data in cloud or on-premises
- Restrict Outbound access from Fabric
- Monitor & Audit security configuration

Common Network Security Requirements

Secure access to your data in Fabric

- Entra Conditional Access Policies
- Tenant Level Private Link
- Workspace Level Private Link
- Workspace IP Firewall **Generally available now!**
- Resource Instance Rules **Coming Soon!**

Connect securely from Fabric to on-premises/cloud data-sources

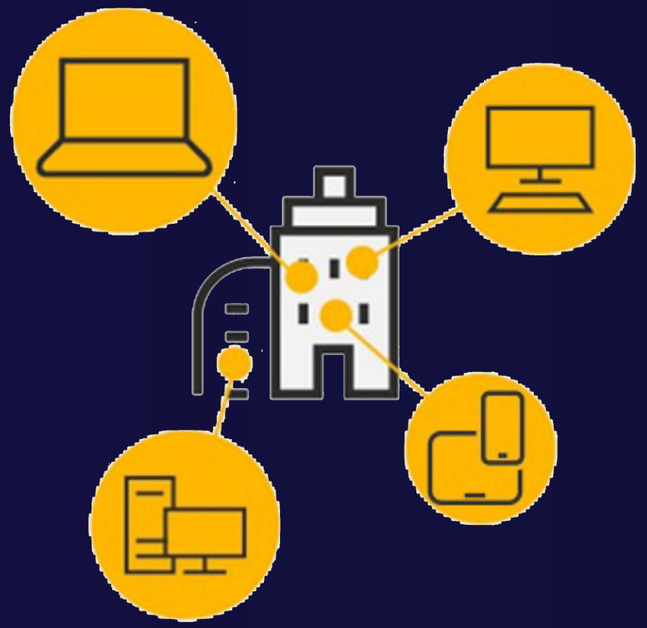
---

Restrict Outbound access from Fabric

Monitor & Audit security configuration

Inbound protection options

Perimeter Network Security



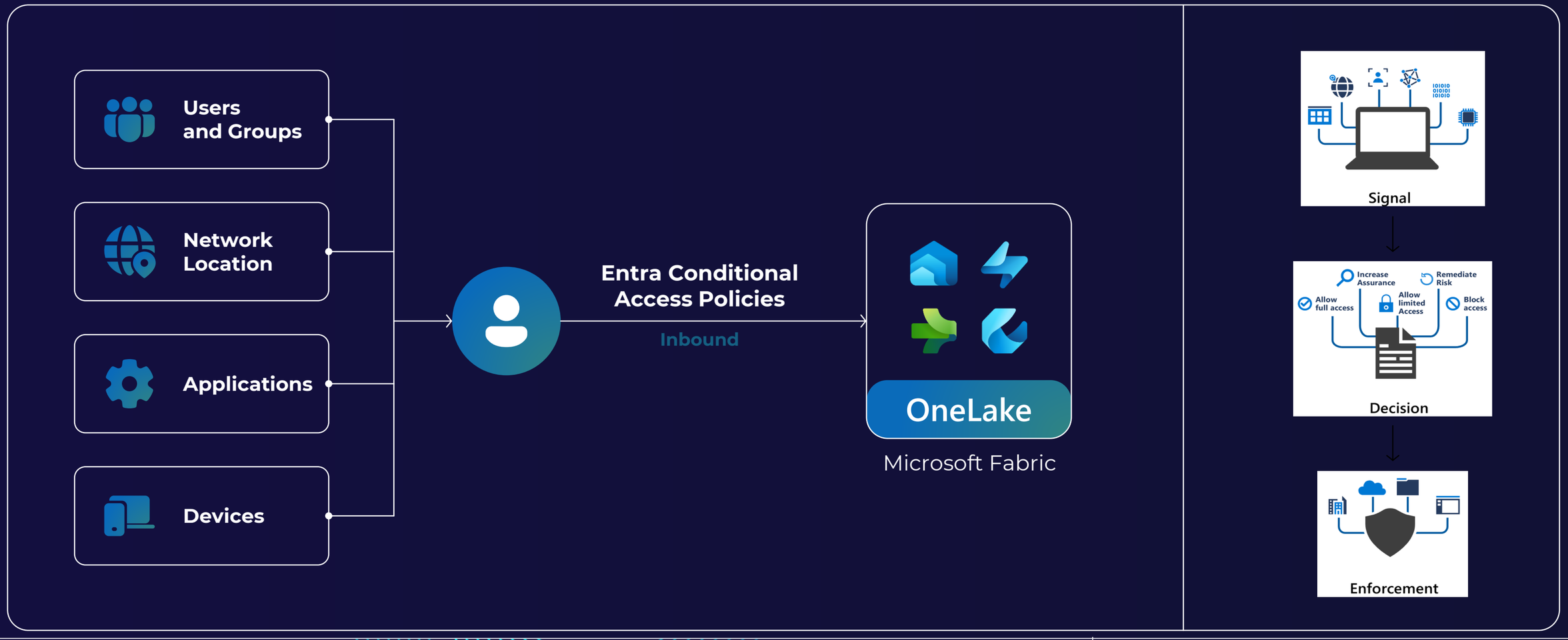
From limited known locations

Zero Trust Approach

to unknown locations

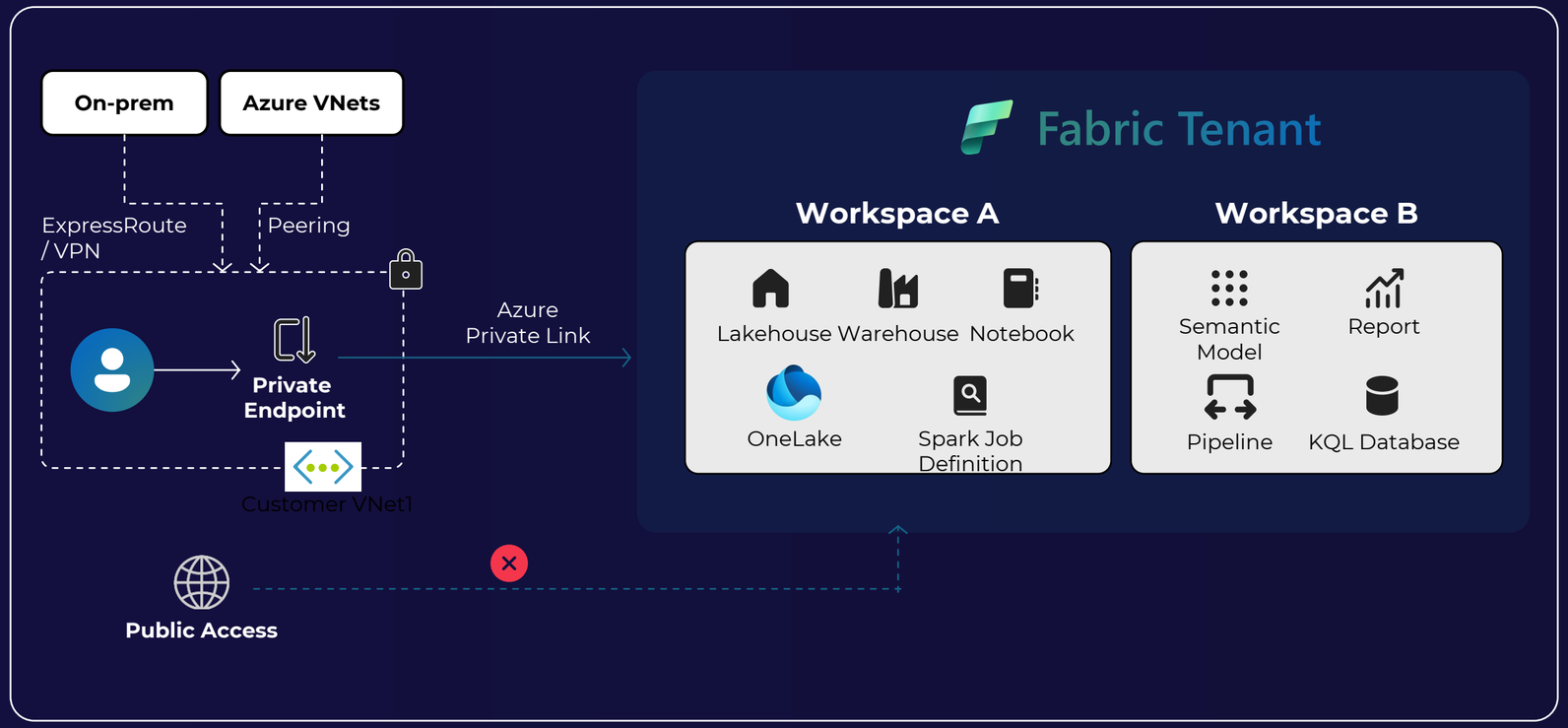
Conditional Access Policies

Decisions – Block, Grant, Require MFA



Private Link for a Fabric Tenant

Perimeter Network Security for your tenant

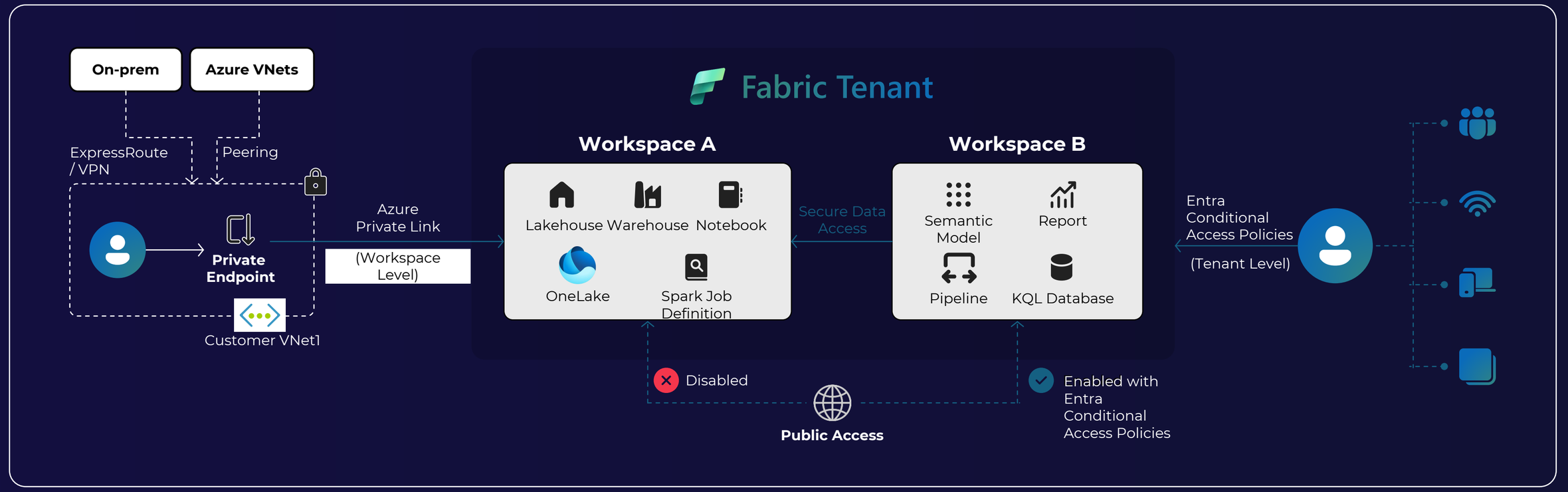


What it means:

1. Fabric is inaccessible from the public internet
2. Every user needs to connect to the private network to gain access

Workspace Private Link for Fabric

Perimeter Network Security for your workspace



Selected workspaces can be protected using Private Links and closed from public internet.

Create a secure connection between public and private workspaces using private data access.

Public workspaces can be secured using Entra policies or IP filtering to use Power BI.

Workspace Private Link

Expanded Workload Coverage

Generally available


Lakehouse


Notebook


Pipeline


CopyJob


Dataflow Gen2


SQL Endpoint


Environment


OneLake Shortcuts


Spark Jobs


Mirrored SQL


Event Stream


EventHouse


Variable library


ML experiment


ML Model


Mounted Data Factory


Warehouse


Mirrored CosmosDB

Public preview

Coming Soon


Activator

Up Next


PowerBI Reports

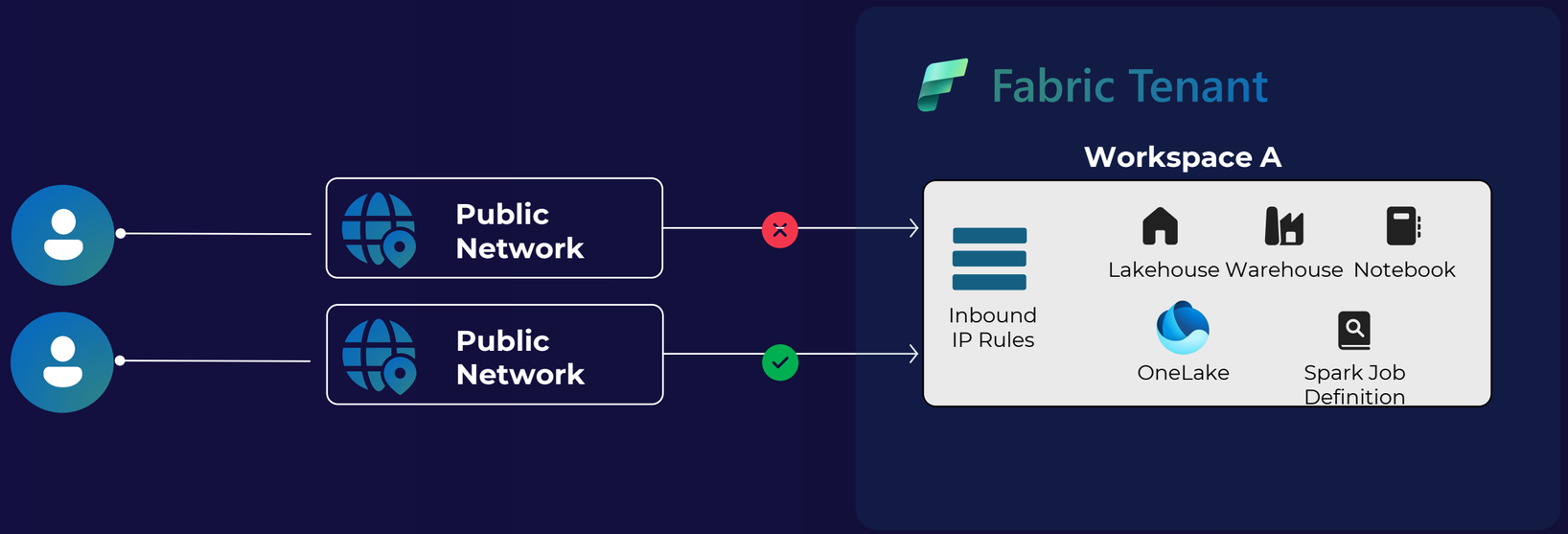

CosmosDB


Semantic Model

Generally Available now!

Workspace IP Firewall for Fabric

Network Security for Fabric workspace from specific IP ranges



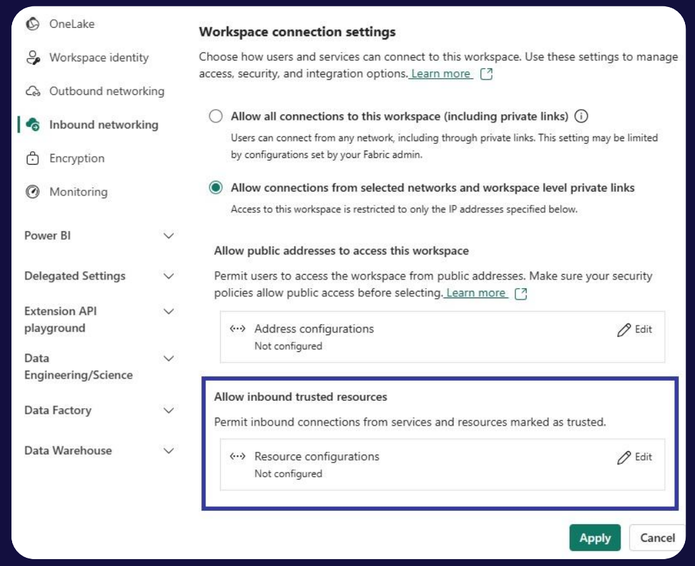
What it means:

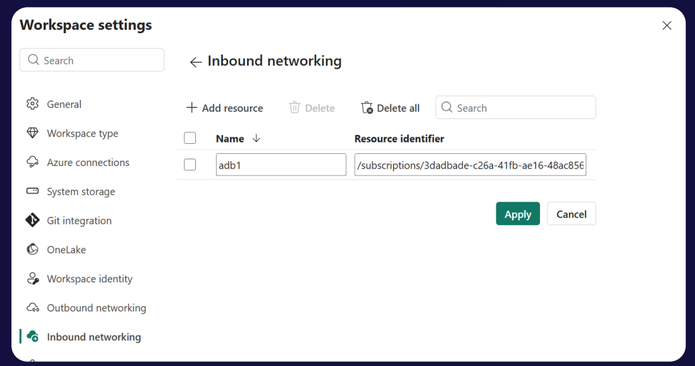
1. Fabric workspace is accessible only from specific public IP or IP ranges
2. Simple setup

Coming Soon!

Workspace Resource Instance Rules

Secure Inbound access to Fabric Workspaces from Cloud Resources





Allows trusted Azure resources to access OneLake by resource identity

Secure inbound access without public internet exposure

Works with Private Link and IP firewall

Keeps environments locked down while preserving critical Azure integrations

Tenant admin enables; workspace admins manage allowed resources

Common Network Security Requirements

Secure access to your data in Fabric

Connect securely from Fabric to on-premises/cloud data-sources

- Data Gateways (On-prem and Vnet)
- Trusted Access
- Managed Private Endpoint

Restrict Outbound access from Fabric

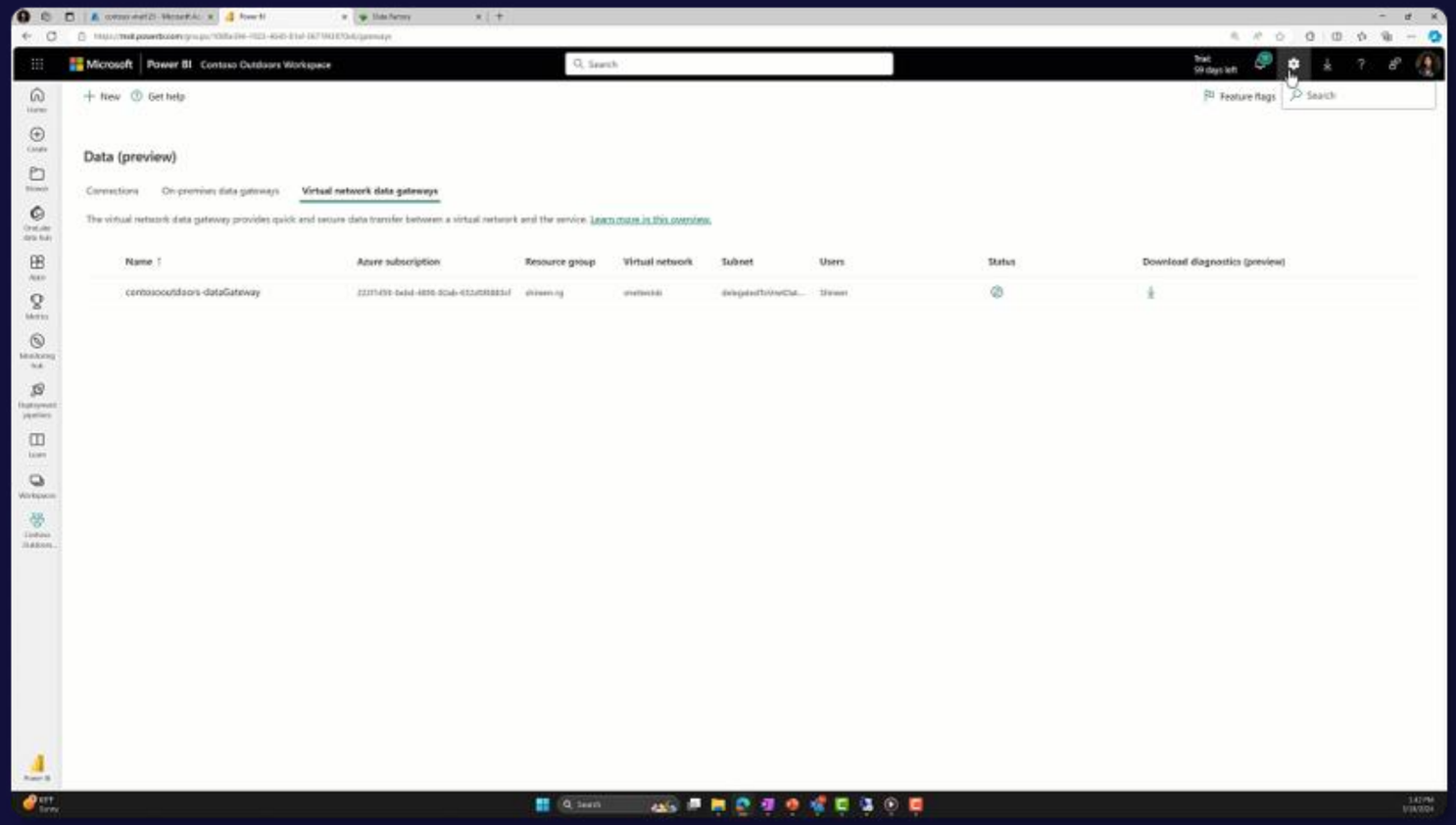
Monitor & Audit security configuration

VNet & On Prem Gateways

Secure connectivity to your Azure and private data services

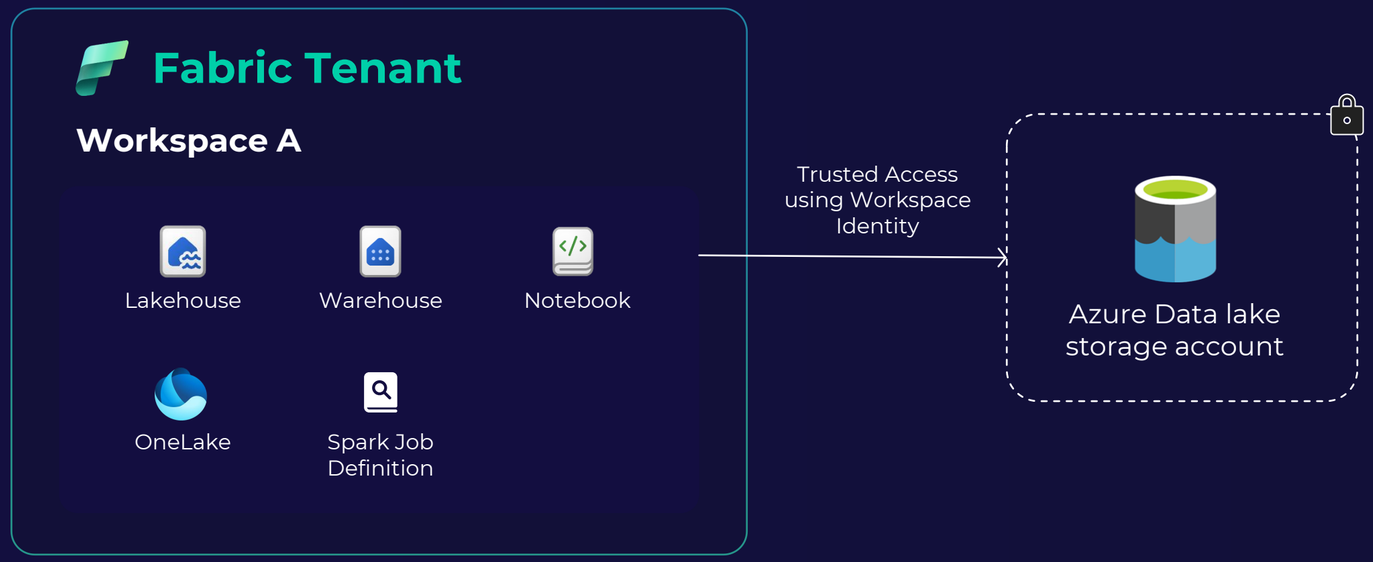
VNet Gateways enable network security compliant access to secured resources

On Prem Gateways enable line of sight to on-prem data sources



Trusted Workspace Access

Secure access to firewall-enabled ADLS Gen 2 Storage accounts



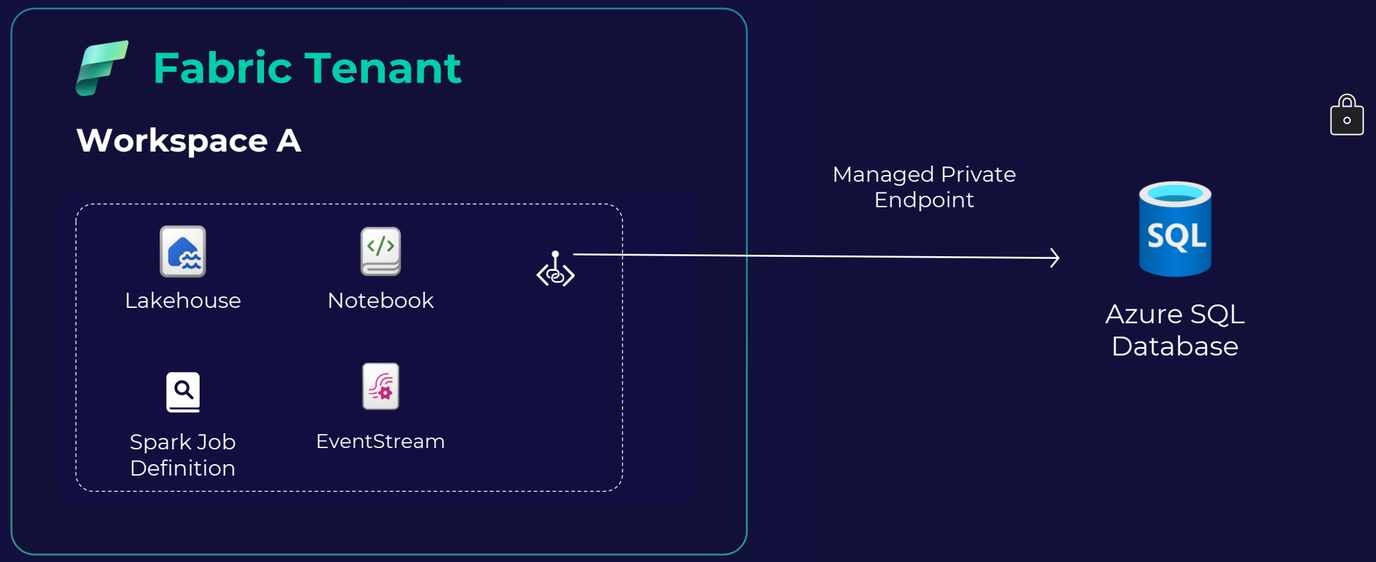
What it means:

1. Use Fabric workspace Identity to securely access ADLS Gen 2 storage accounts via storage resource instance rules

2. Supports OneLake shortcuts, pipelines, T-SQL Copy Statements, Semantic Models with Import Mode, AzCopy

Managed Private Endpoints

Secure access to Azure Resources from Spark and Event stream



1. Secure private access to Azure PaaS services

2. Supports Data Engineering Workloads (Spark, Notebooks, Lakehouse) and Eventstream

Common Network Security Requirements

Secure access to your data in Fabric

Connect securely from Fabric to on-premises/cloud data-sources

Restrict Outbound access from Fabric
- Workspace Outbound Access Protection

Monitor & Audit security configuration

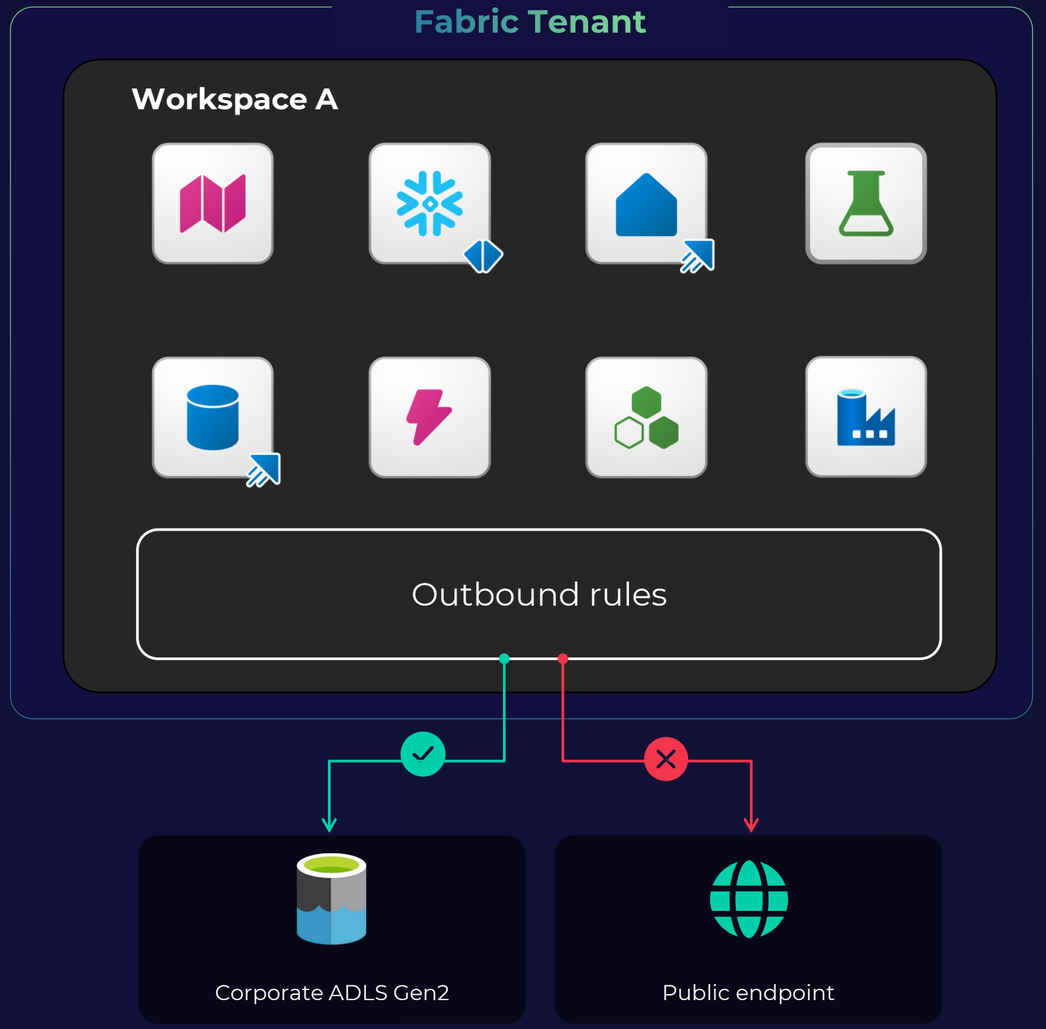
Workspace Outbound Access Protection

To prevent data exfiltration over network

Workspace level control to restrict outbound access to public network

Restrict outbound connections to permitted destinations only

Use in conjunction with other security features to achieve robust Data Exfiltration Protection



Outbound Access Protection

Expanded Workload Coverage

Generally available

Lakehouse

Notebook

SQL Endpoint

Spark Jobs

Coming Soon

Pipeline

CopyJob

Dataflow Gen2

OneLake Shortcuts

Mirrored Databases

Warehouse

Public preview

Coming Soon

PowerBI Reports

Semantic Model

Up Next

Real Time Intelligence

Data Science

Use both outbound and inbound to achieve better DEP

DEP = OAP + inbound security

Inbound security features like private link allow you to restrict who can access your data and from where, reducing risks of data exfiltration

+

Outbound security make sure that malicious users cannot exfiltrate data

Common Network Security Requirements

Secure access to your data in Fabric

Connect securely from Fabric to on-premises/cloud data-sources

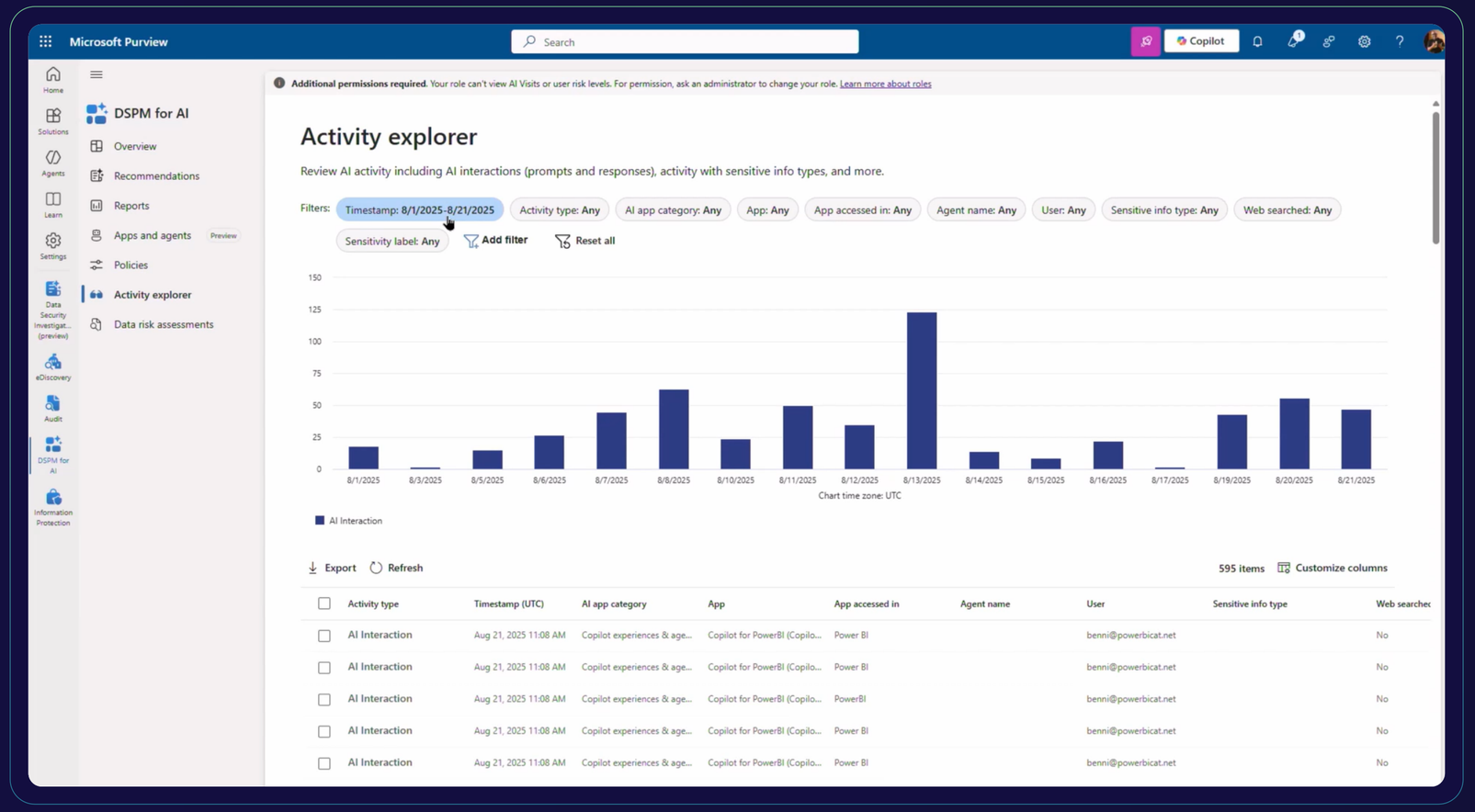
Restrict Outbound access from Fabric

Monitor & Audit security configuration

- Tenant-level APIs for Network Security configuration monitoring
- Audit events in Purview

Networking Audit Information in Purview

Manage audit events for your entire data estate from a single pane



Outbound access protection enabled/disabled events

Events for Managed Private Endpoints creation/deletion

Managed VNet provisioned/removed

VNet data gateway proxy created/updated

Preview

Tenant Level APIs for Network Security Config monitoring

Monitor & Audit workspaces for reporting and compliance

```
GET https://api.fabric.microsoft.com/v1/admin/workspaces/networking/communicationpolicies
```


```
{
  "value": [
    {
      "workspaceId": "fa9ad228-3e6b-44d4-b5f4-e275f337afa9",
      "inbound": {
        "publicAccessRules": {
          "defaultAction": "Deny"
        }
      },
      "outbound": {
        "publicAccessRules": {
          "defaultAction": "Deny"
        },
        "connections": {
          "defaultAction": "Deny",
          "rules": [
            {
              "connectionType": "SQL",
              "defaultAction": "Deny",
              "allowedEndpoints": [
                {
                  "hostNamePattern": "*.microsoft.com"
                }
              ]
            },
            {
              "connectionType": "lakehouse",
              "defaultAction": "Deny",
              "allowedWorkspaces": [
                {
                  "workspaceId": "91c5ae74-e82d-4dd3-bfeb-6b1814030123"
                }
              ]
            },
            {
              "connectionType": "Maria DB",
              "defaultAction": "Allow"
            }
          ]
        },
        "gateways": {
          "defaultAction": "Deny",
          "allowedGateways": [
            {
              "id": "17d8929d-ab32-46d1-858b-fdea74e93bf2"
            }
          ]
        },
        "git": {
          "defaultAction": "Deny"
        }
      }
    }
  ],
  "continuationUri": "https://api.fabric.microsoft.com/v1/admin/workspaces/networking/communicationpolicies?c
  "continuationToken": "eyJHYXN0U2VlbkNvbmS1Y3Rpb25JZCI6NX0=
}
```


List all workspaces that have inbound or outbound access protection enabled in the tenant

List inbound and outbound rules configured for each workspace

Verify that workspace network policies align with organizational security requirements

Enable automated security audits, compliance checks, and reporting workflows

Common Network Security Requirements

Secure access to your data in Fabric

- Entra Conditional Access Policies
- Tenant Level Private Link
- Workspace Level Private Link
- Workspace IP Firewall **Generally available now!**
- Resource Instance Rules **Coming Soon!**

Connect securely from Fabric to on-premises/cloud data-sources

- Data Gateways (On-prem and Vnet)
- Trusted Access
- Managed Private Endpoint

Restrict Outbound access from Fabric

- Workspace Outbound Access Protection

Monitor & Audit security configuration

- Tenant-level APIs for Network Security configuration monitoring
- Audit events in Purview

Demo

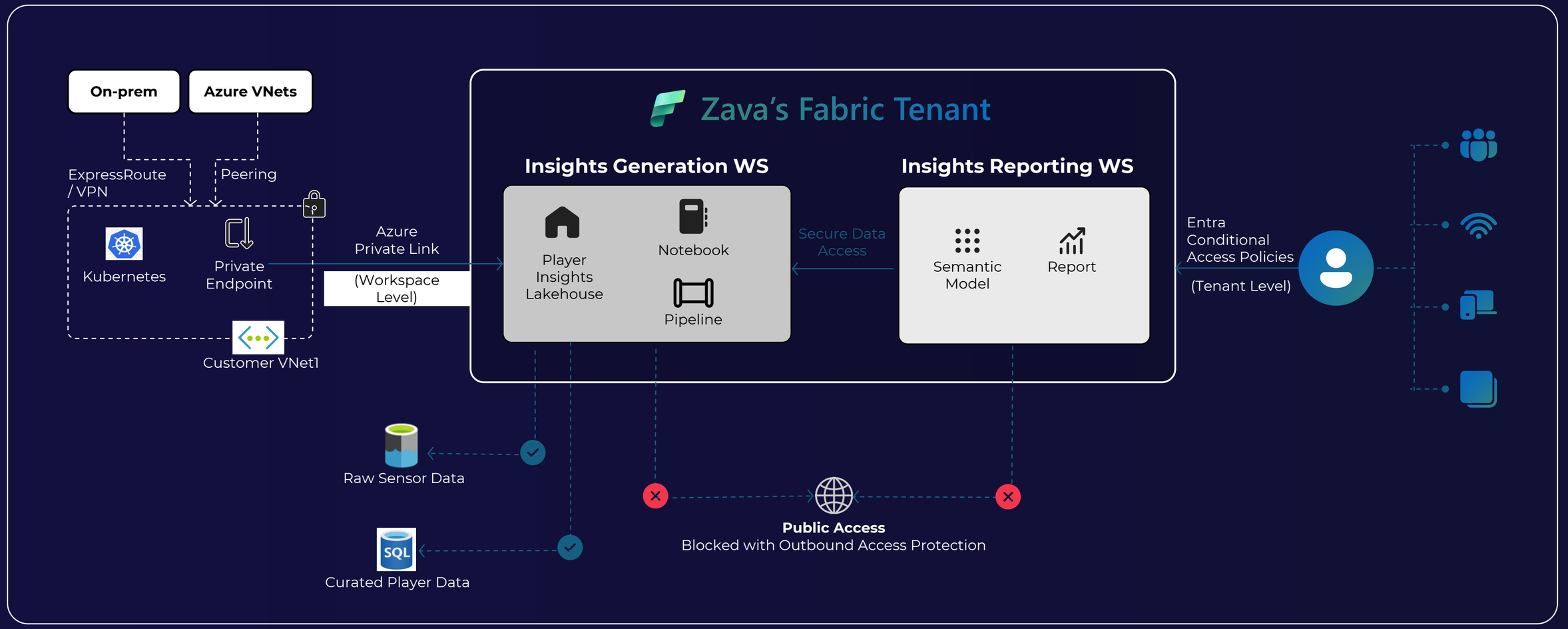
Network Security in Microsoft Fabric

Network Security - Demo

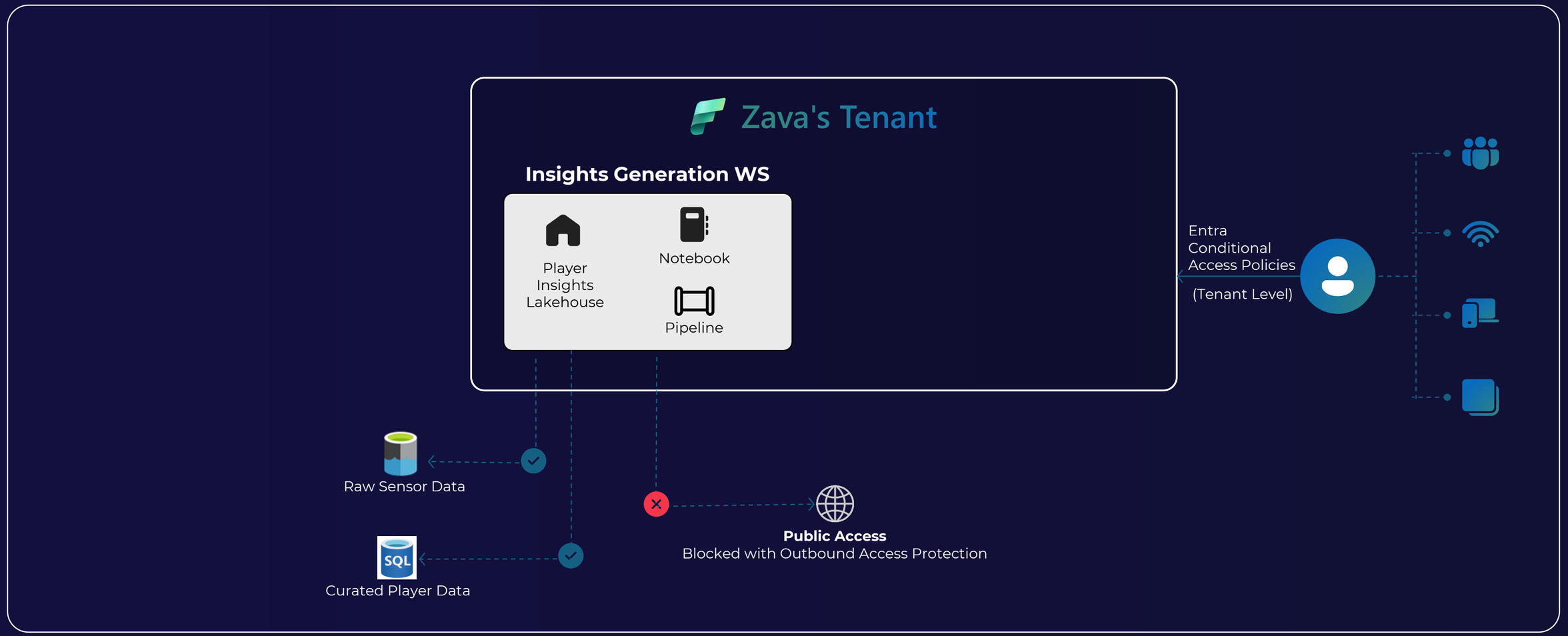
Zava's Soccer Analytics with Microsoft Fabric

Comprehensive data insights powering players performance analysis

Zava's Soccer Analytics



Step 1 : Securing Insights Generation Workspace



Conditional Access | Overview

Microsoft Entra ID

Overview
Policies
Deleted Policies
Insights and reporting
Diagnose and solve problems
Manage
Monitoring
Troubleshooting + Support

Create new policy | Create new policy from templates | Refresh | Got feedback?

Conditional Access for agents, now in preview, is part of Microsoft Agent 365, the control plane for agents. Get early access to Agent 365 via the Frontier program. Learn more

Getting started | Overview | Coverage | Tutorials

Policy Summary

Agent Identities

There are 0 agent identities in your tenant

See all unprotected sign-ins

See all policies protecting agents

Policy Snapshot

4 Enabled 1 Report-only 0 Off

View all policies

Users

3 users signed in during the last 7 days without any policy coverage

See all unprotected sign-ins

Devices

0% of sign-ins in the last 7 days were from unmanaged or non-compliant devices

See all noncompliant devices

See all unmanaged devices

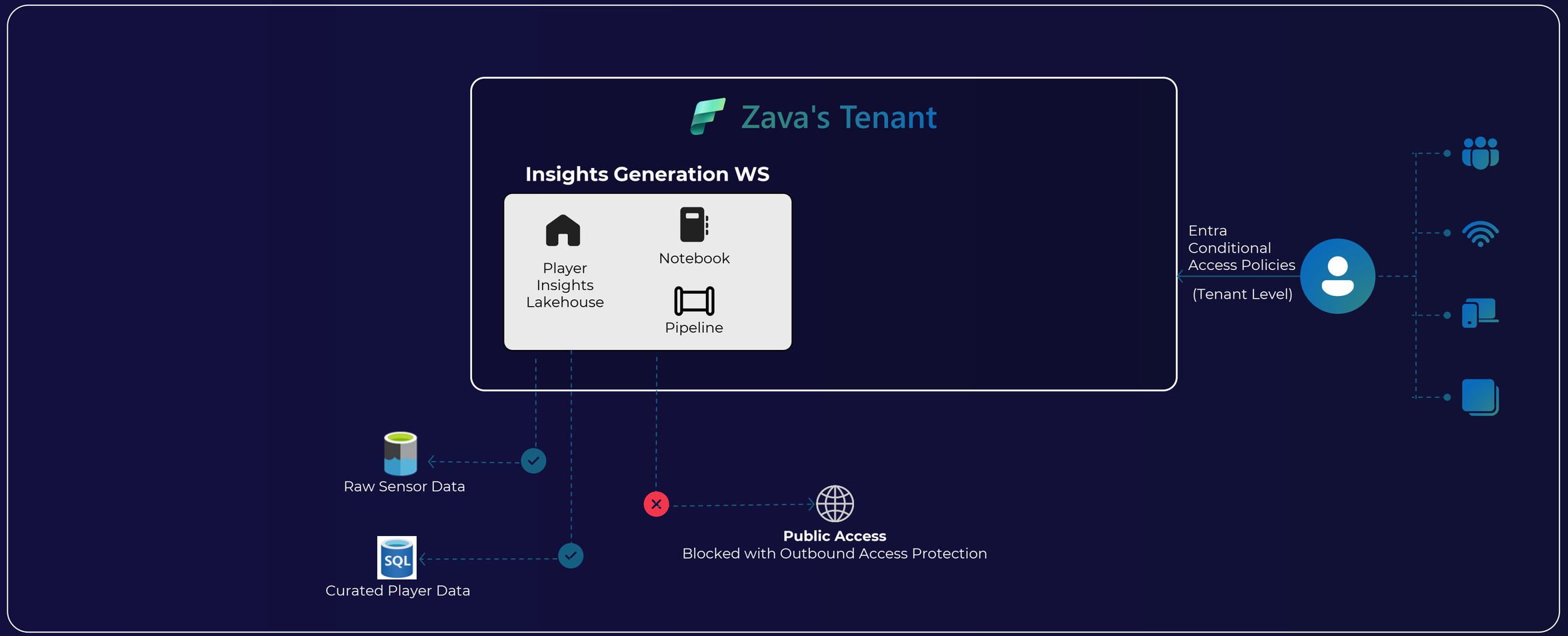
Applications

Browse a list of applications that are not protected by your policies.

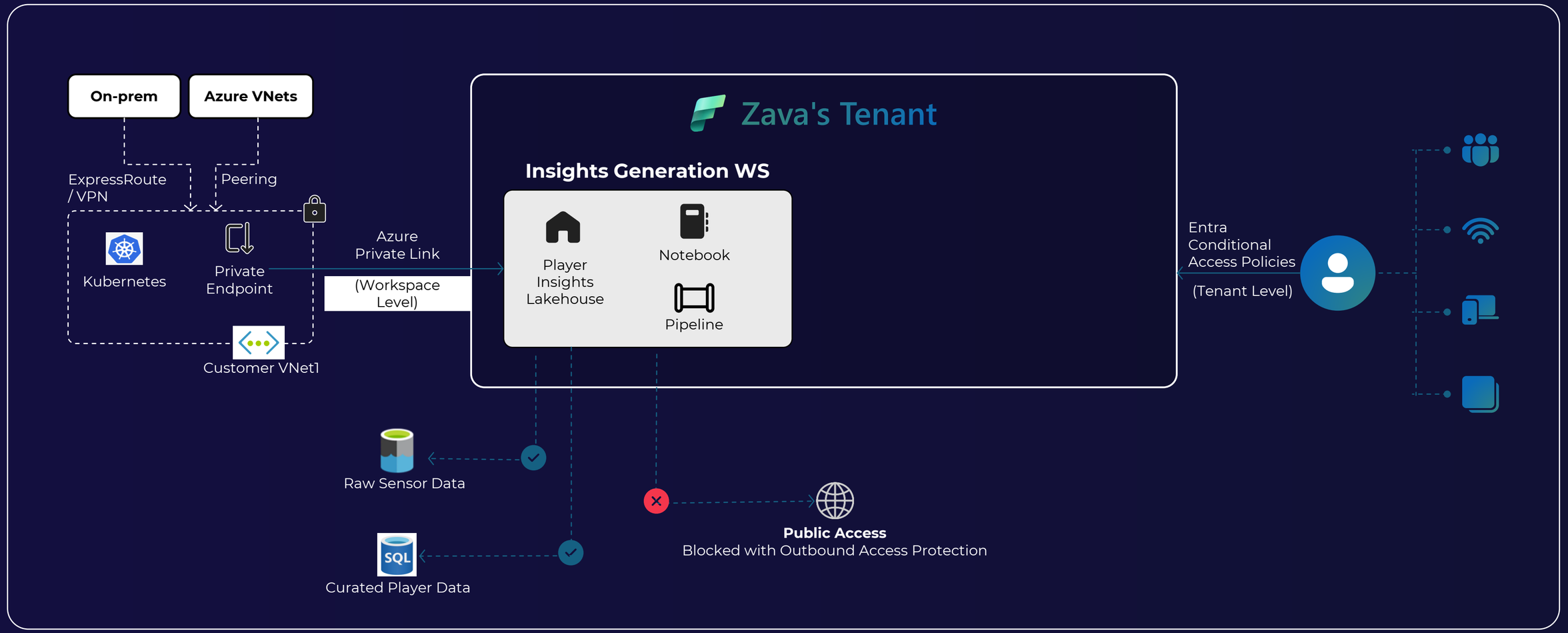
View top unprotected apps

Add or remove favorites by pressing Ctrl+Shift+F

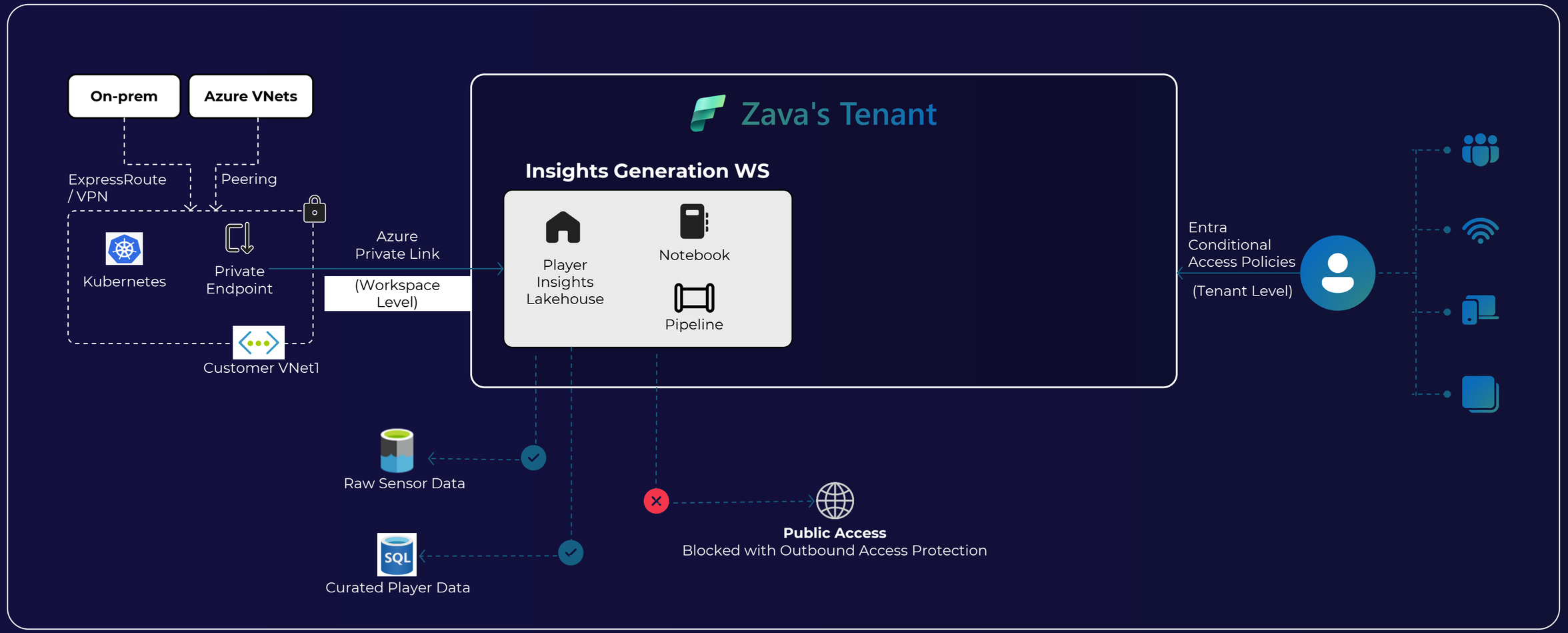
Step 1 : Securing Insights Generation Workspace



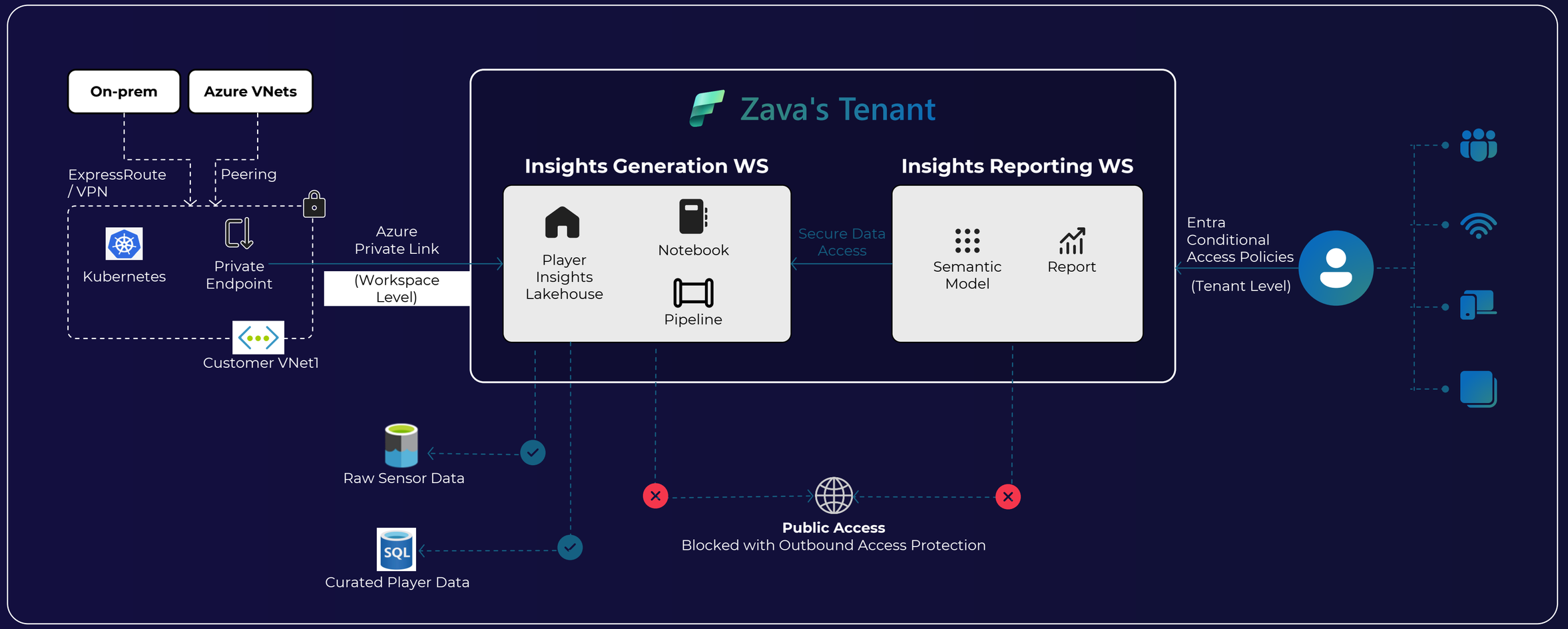
Step 2: Create private connection from Kubernetes to Insights Generation Workspace



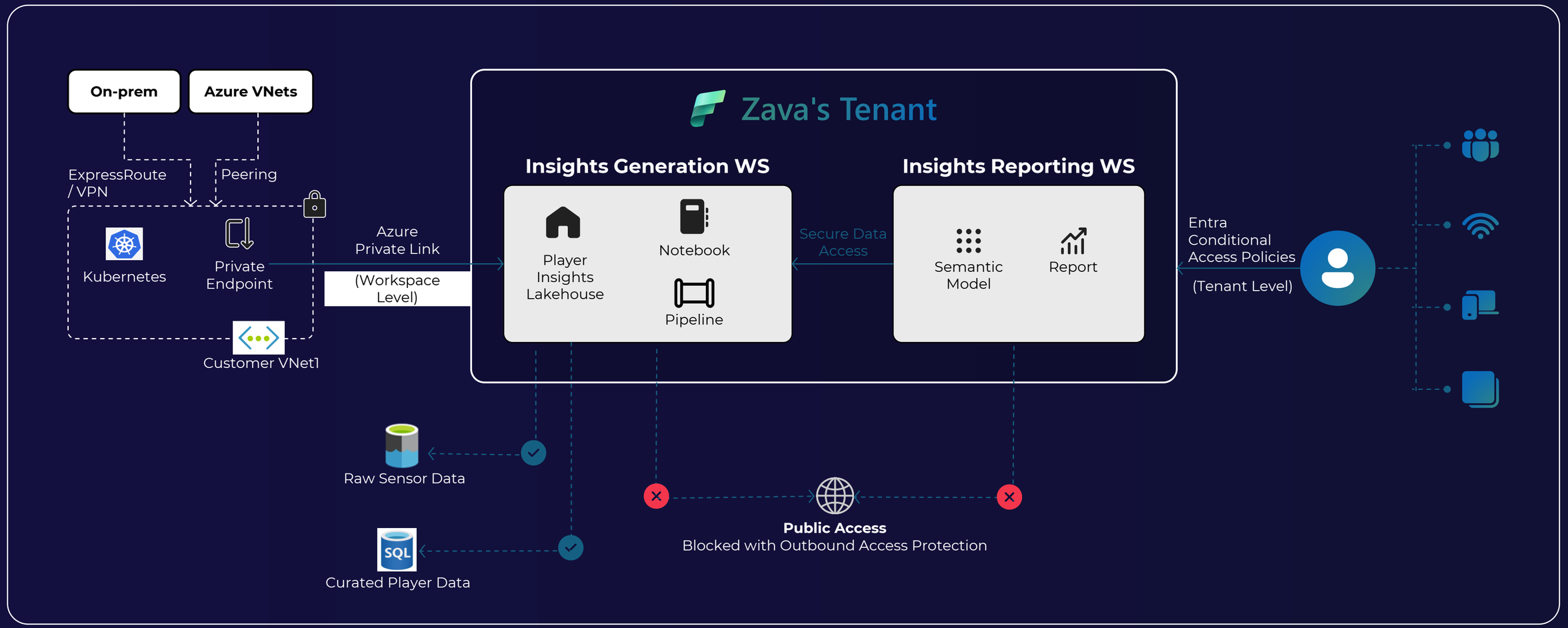
Step 2: Create private connection from Kubernetes to Insights Generation Workspace



Step3 : Securing outbound connection from Reporting Workspace

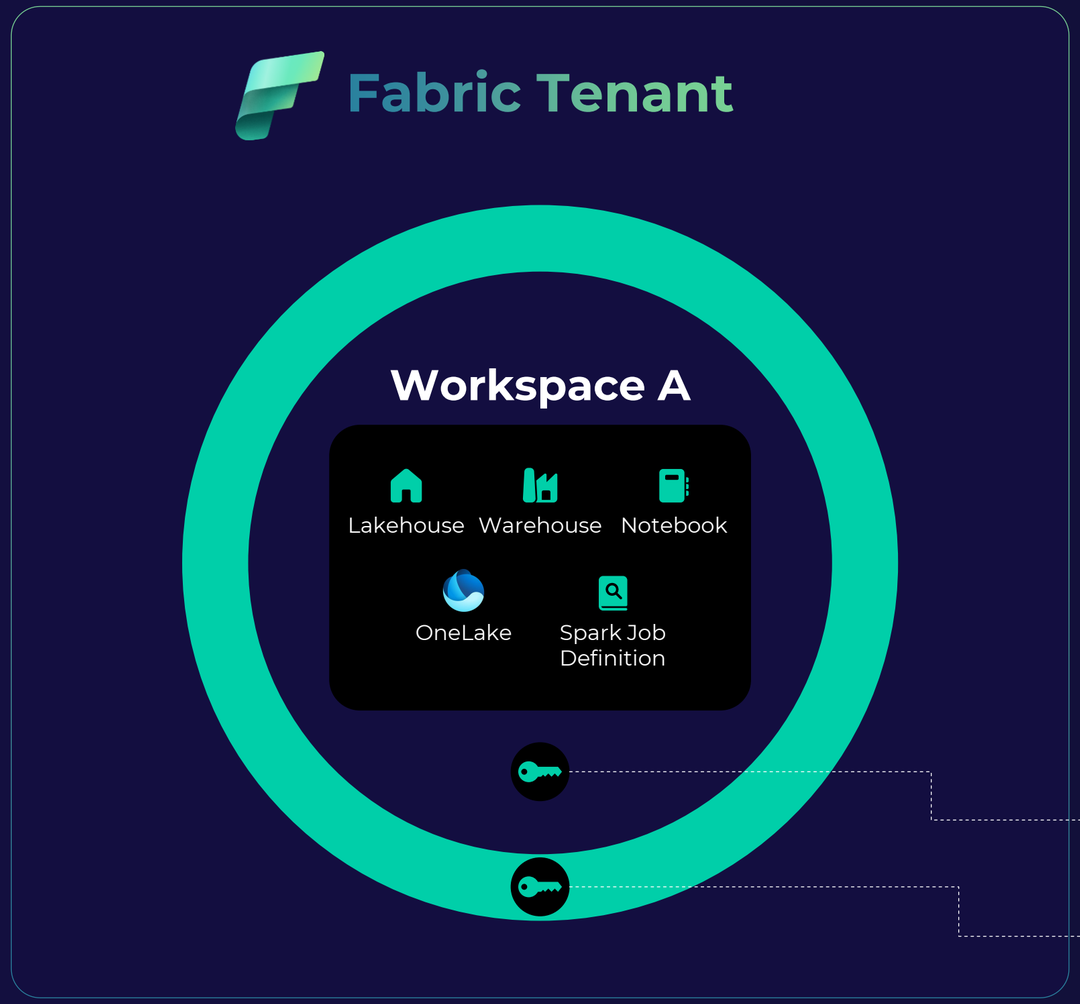


Step3 : Securing outbound connections from Reporting Workspace



Data Security

Customer Managed Keys in Fabric



All data at rest is encrypted by default by Fabric

Use your own encryption keys to encrypt data in Fabric at the workspace-level to meet additional compliance requirements

New

Capacities with Power BI's BYOK–enabled can now also turn on CMK for their workspaces

Customer Managed Keys

Expanded Workload Coverage

Generally available


Lakehouse


Notebook


Pipeline


CopyJob


Dataflow Gen2


Warehouse


Environment


OneLake Shortcuts


Spark Jobs


ML Model


ML experiment


Mirrored Databases

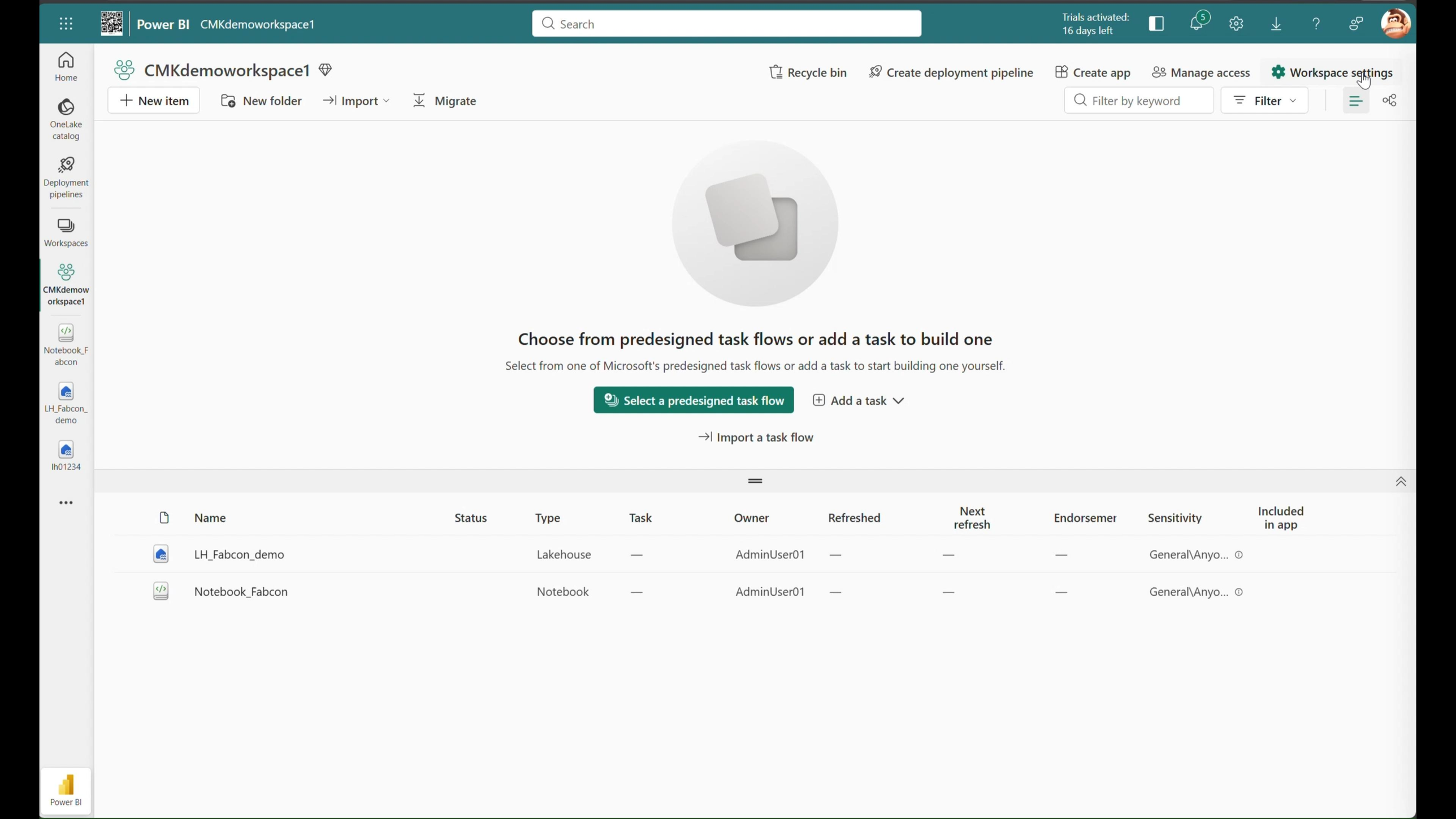
New!

SQL Database

What's next?


Semantic Model


CosmosDB


Power BI
CMKdemoworkspace1
Search
Trials activated:
16 days left
Home
OneLake catalog
Deployment pipelines
Workspaces
CMKdemoworkspace1
Notebook_Fabcon
LH_Fabcon_demo
lh01234
Power BI
CMKdemoworkspace1
Recycle bin
Create deployment pipeline
Create app
Manage access
Workspace settings
New item
New folder
Import
Migrate
Filter by keyword
Filter
Choose from predesigned task flows or add a task to build one
Select from one of Microsoft's predesigned task flows or add a task to start building one yourself.
Select a predesigned task flow
Add a task
Import a task flow
Name
Status
Type
Task
Owner
Refreshed
Next refresh
Endorsemer
Sensitivity
Included in app
LH_Fabcon_demo
Lakehouse
AdminUser01
General\Anyo...
Notebook_Fabcon
Notebook
AdminUser01
General\Anyo...

Workload support matrix

- Easy reference for which security features are supported across which workloads

https://aka.ms/fabric_security_feature_support_matrix

Workload	Item type	Workspace private links	Customer managed keys	Outbound access protection
Data Engineering	Lakehouse	✓	✓	✓
	Lakehouse Shortcut	✓	-	Preview
	Lakehouse SQL Endpoint	✓	✓	✓
	Notebook	✓	✓	✓
	Spark Job Definition	✓	✓	✓
	Environment	✓	✓	✓
	Lakehouse with Schema	-	✓	✓
	Spark Connectors for SQL Data Warehouse	-	-	-
Data Factory	Default Semantic Model	✓	-	✓
	Pipeline	✓	✓	Preview
	Dataflow Gen1	-	-	-
	Dataflow Gen2	-	✓	Preview
	Copy Job	✓	✓	Preview
	Mounted Azure Data Factory	✓	-	-
	Vnet data gateway	✓	-	Preview
	On-premises data gateway: Pipeline/Copy Job	✓	-	Preview
	On-premises data gateway: Dataflow Gen2	-	-	Preview
	Data Workflow	-	-	-

Compliance

Meet data residency requirements with Microsoft Fabric

42+
Available Azure regions

300+
Total Azure datacenters

+ many more Fabric compliance certifications

Compliance in Microsoft Fabric

Fabric is a core Microsoft Online Service

Fabric supports a wide range of compliance standards

- GDPR
- EUDB
- ISO certifications ISO 27001, 27701, 27017, 27018
- HIPAA, HITRUST compliant
- SOX compliant
- SOC 1, SOC 2, Type 2
- FedRamp for Commercial Cloud

Certifications in Microsoft Fabric

Nov 15, 2023

Microsoft Fabric GA

Dec 15, 2023

ISO 27001, 27701, 27017, 27018

Jan 31, 2024

HIPAA

Feb 1, 2024

Australian IRAP

May 1, 2024

SOC 1 & 2Type 2, SOX

CSA STAR

Sep 3, 2024

HITRUST

Nov 1, 2024

FedRAMP Certification on Azure commercial

Jan 2025

PCI DSS

May 2025

K-ISMS

Check out the following sessions on security and monitoring

Enhancing resiliency in Fabric via Item Recovery, Item Identity Architecture and more	Thursday, March 19	10:10 AM – 11:10 AM	C102
Enforce your governance and security regulations in Fabric	Thursday, March 19	11:30 AM – 12:30 PM	C102
Govern, manage, and protect your data in Microsoft Fabric	Thursday, March 19	02:00 PM – 03:00 PM	C202-C204
Microsoft Fabric Security: Best Practices for Network, Data and Governance	Thursday, March 19	04:15 PM – 05:15 PM	C111-C112

Thank you!