Building a Fortress of Your Fabric Environment: Security Best Practices for Data Engineers

Rate Data Saturday Holland

Review to win

With custom Data Saturdays lego stickers!

Thank you sponsors!

redgate

twintos

wortell

macaw

Your guide in the Era of AI.

Rubicon

Consulting & Technology

ilionx

Data Saturdays

Let’s connect

Erwin de Kreuk

Principal Consultant

Lead Data & AI InSpark

@erwindekreuk.bsky.social

linkedin.com/in/erwindekreuk

erwindekreuk.com

github.com/edkreuk

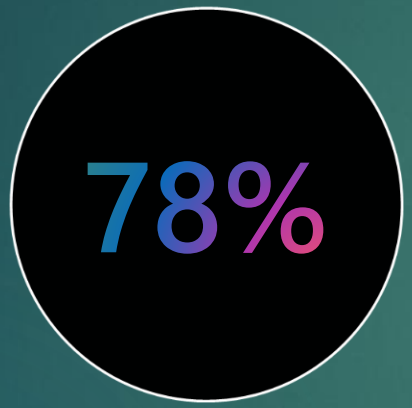
https://sessionize.com/erwin-de-kreuk/

Dutchfabricusergroup.com

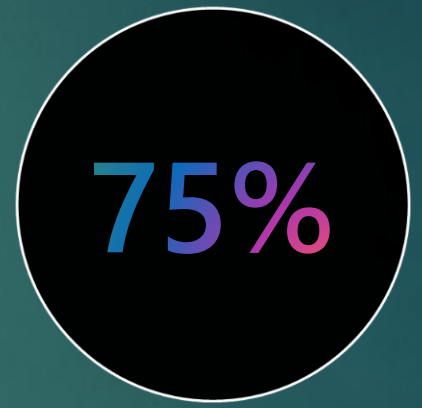
Microsoft® MVP Most Valuable Professional

Cybercriminals are getting more creative just like us

Data culture and AI transformation are happening now



of organizations are implementing or developing a company wide data foundation[1]



of knowledge workers already using AI at work (doubled in the past 6 months)[2]

1. The Alation State of Data Culture Report
2. Microsoft 2024 Work Trend Index Annual Report

Why data security?

Data is most secure if no one can access it.

But…if no one can access data then you can't use it for anything.

* The value of data | World Economic Forum (weforum.org)

Achieving both goals can prove challenging

Ensuring your data is secure

Fostering a data-driven culture

Agenda

Introduction

Challenges

Inbound Connections

Private Links

Outbound connections

Microsoft Purview

Q & A

Fabric Security Whitepaper

Who has ever heard of the Fabric Security Whitepaper?

Only 127 pages

[Microsoft Fabric security white paper - Microsoft Fabric | Microsoft Learn]

Introduction

Security is a top priority for any organization that wants to succeed in the digital age. You need to safeguard your assets from threats and follow your organization's security policies. This whitepaper serves as an end-to-end security overview for Microsoft Fabric. It covers details on how Microsoft secures your data by default as a SaaS service and how you can secure, manage, and govern the data stored in Microsoft Fabric as an organization.

The contents of this whitepaper is created by combining several security related online documents into a single whitepaper for reading convenience. This whitepaper will be updated regularly, but the online documentation will always be up to date. You can find the online documentation here: Microsoft Fabric security - Microsoft Fabric | Microsoft Learn

In the era of AI, **security** and **governance** practices are **prerequisites** for extracting valuable insights from data.[1]

[1]*Chandana Gopal, Research Director, Enterprise Intelligence, IDC*

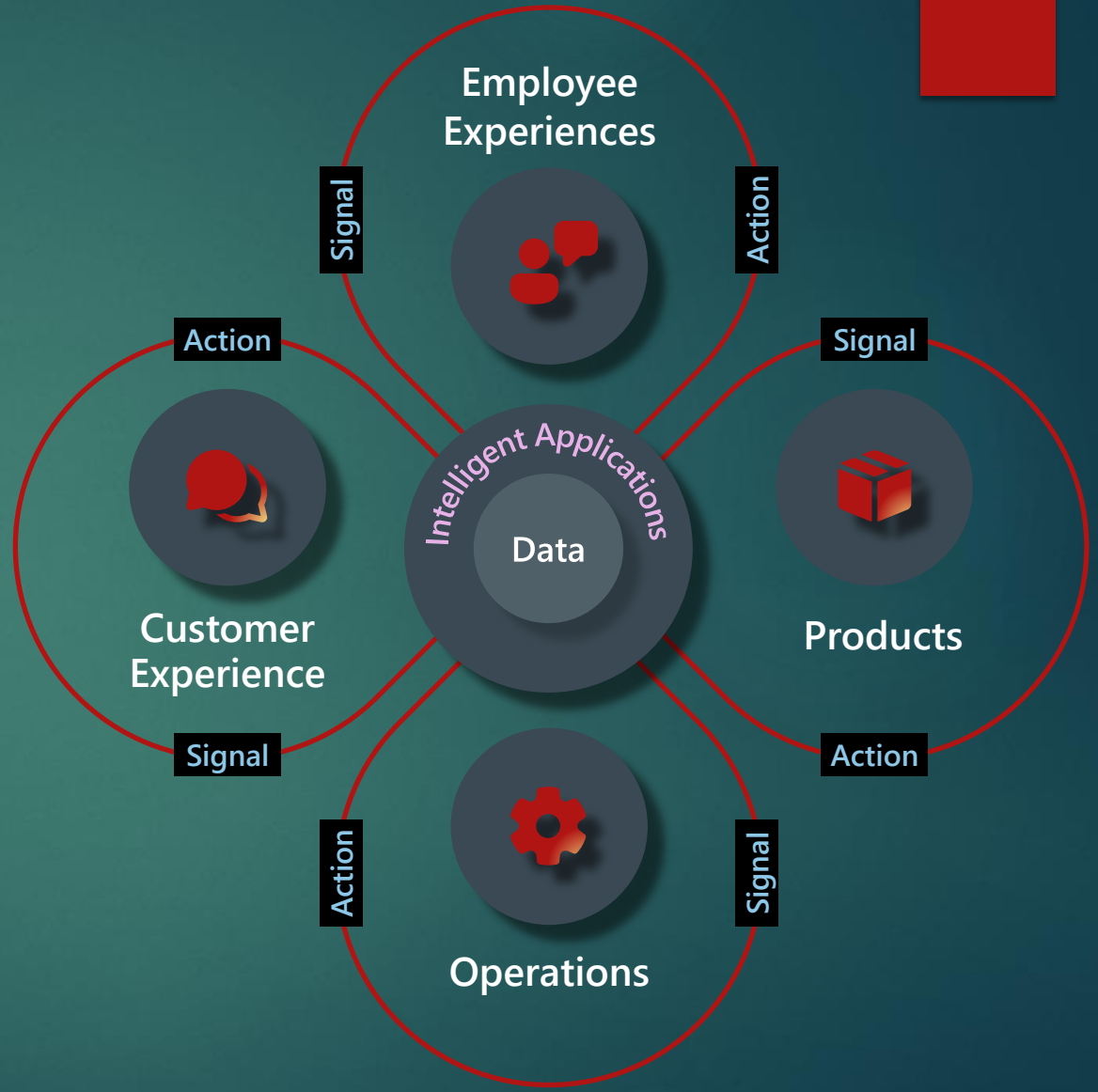
AI is transforming the world

Good AI, needs clean data

Data is the oxygen of our digital transformation

"A new kind of company — we call them insights driven businesses — has formed. They are growing at an average of more than 30% annually"

Forrester Analytics Business Technographics Global Data & Analytics Survey

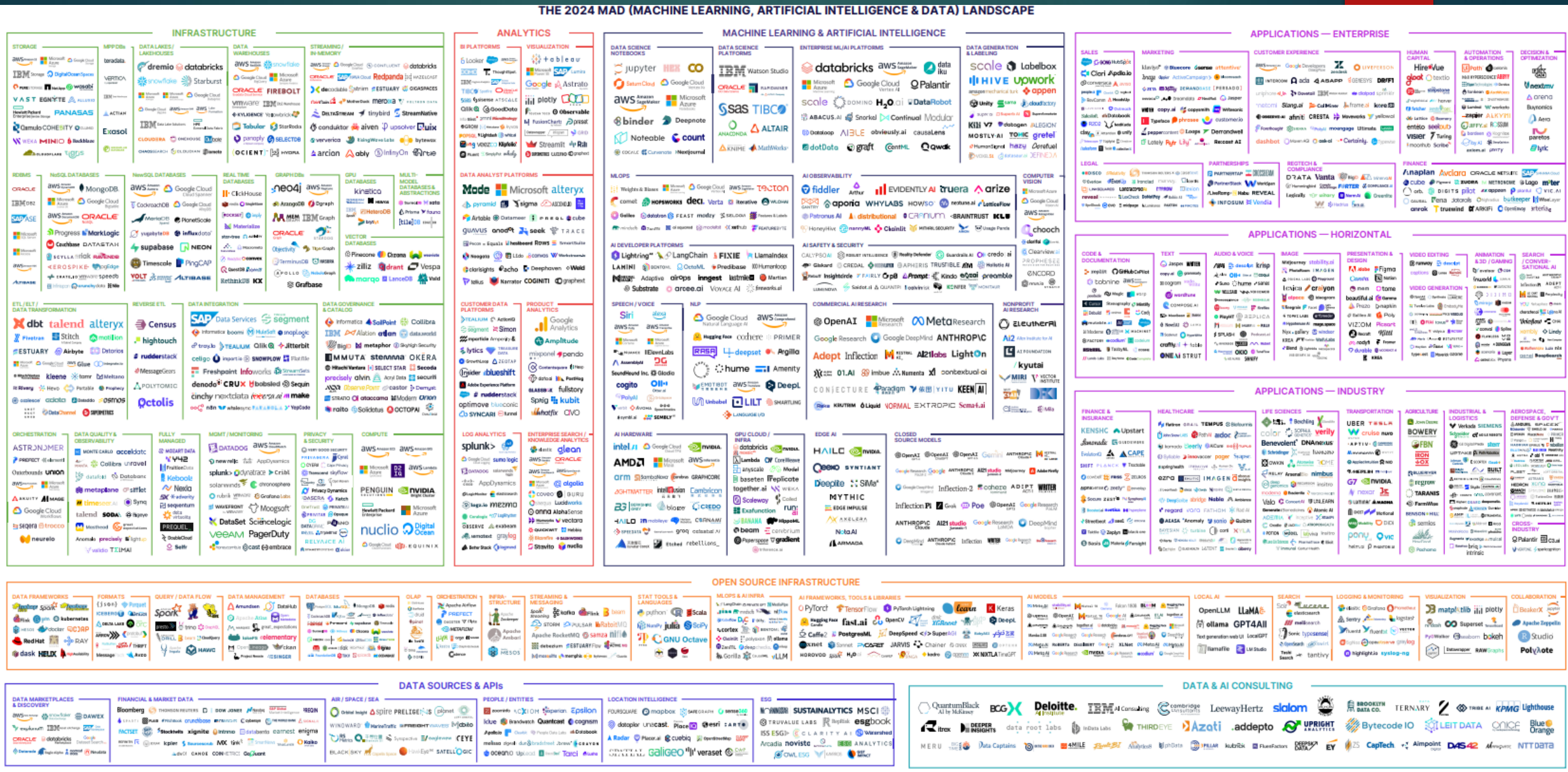


Security : The Cornerstone of Microsoft Fabric

Security is paramount in the digital age, and Microsoft Fabric ensures your data is protected at every stage. By using Fabric, organizations can trust that their data is secure, allowing them to focus on innovation and growth.

How do you translate data into competitive advantage

The 2024 ML, AI, and Data Landscape



Version 1.0 - March 2024 © Matt Turck (@mattturck) , Aman Kabeer (@AmanKabeer11) & FirstMark (@firstmarkcap) Blog post: mattturck.com/MAD2024 Interactive version: MAD.firstmarkcap.com Comments? Email MAD2024@firstmarkcap.com

FIRSTMARK
EARLY STAGE VENTURE CAPITAL

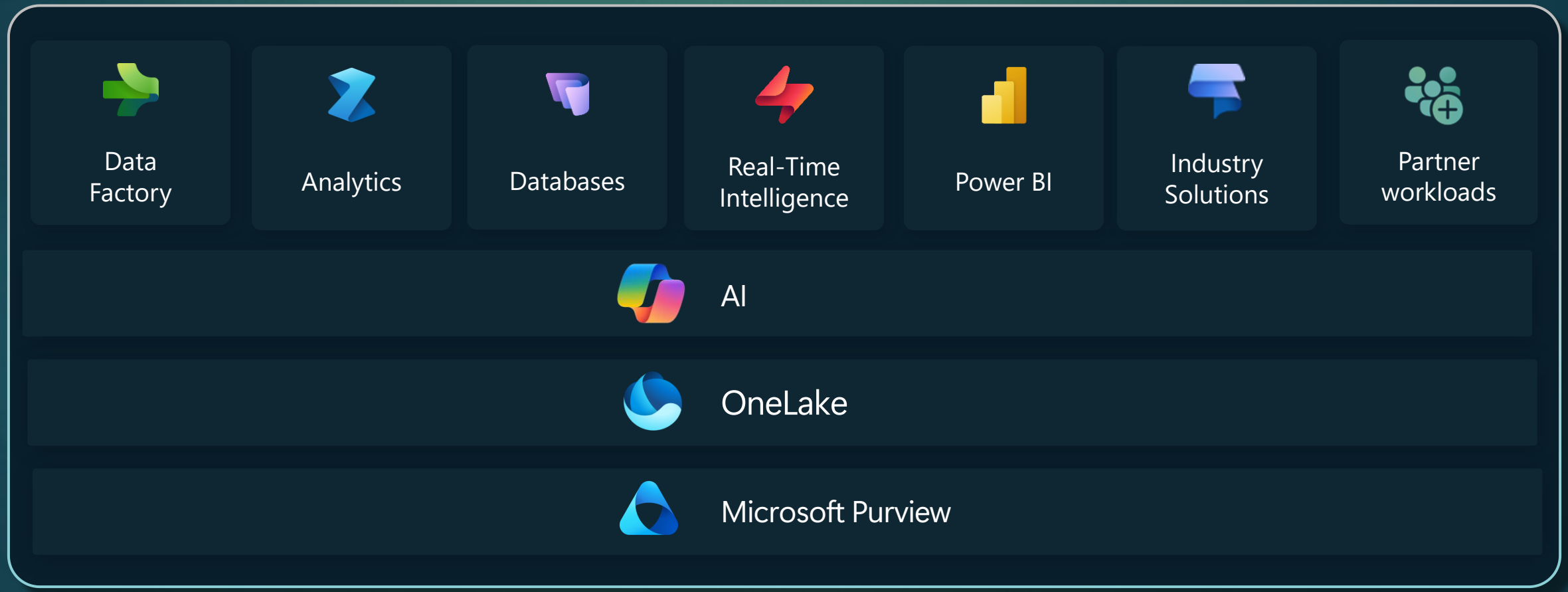
Microsoft Fabric

The unified data platform for AI transformation

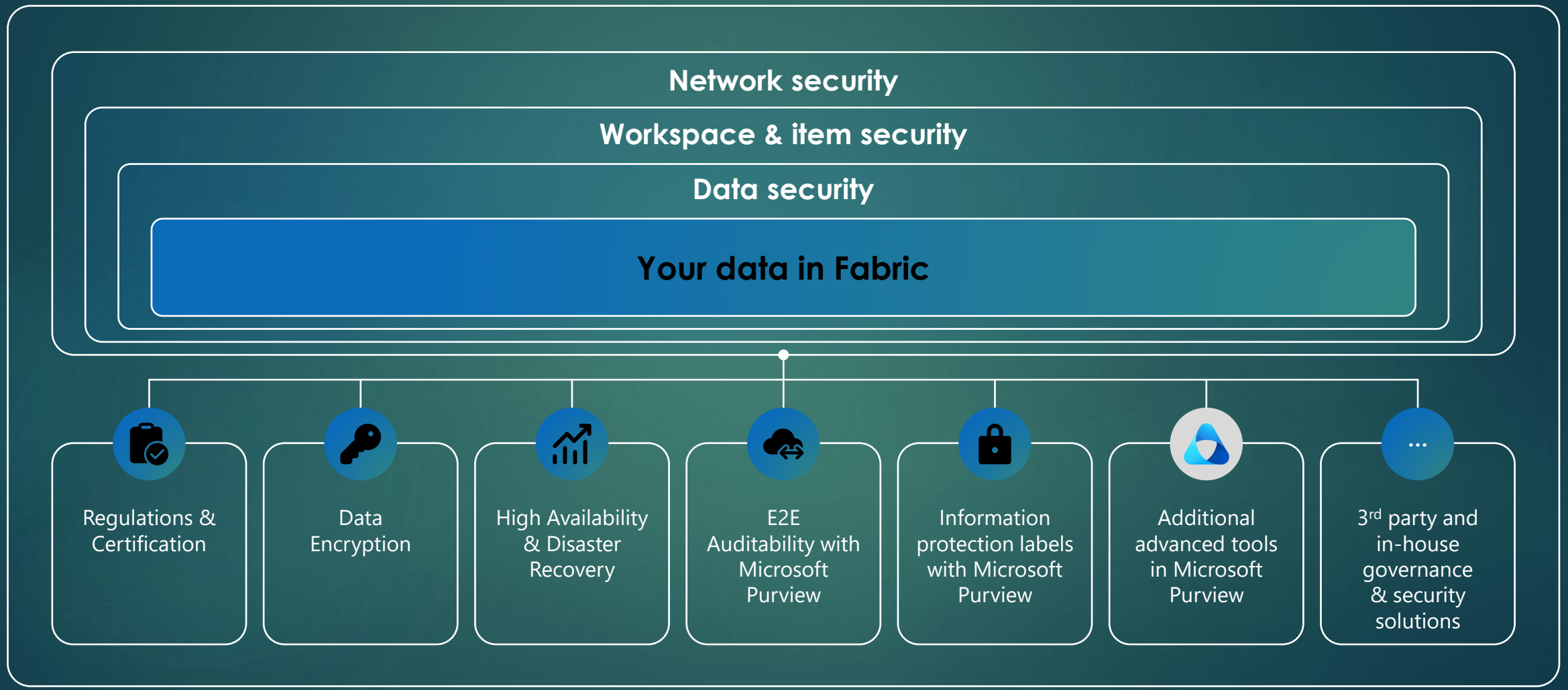
From	To
Isolated component	Unified stack
Single database	All the data
Gen AI Bolted-in	Gen AI built in

Microsoft Fabric

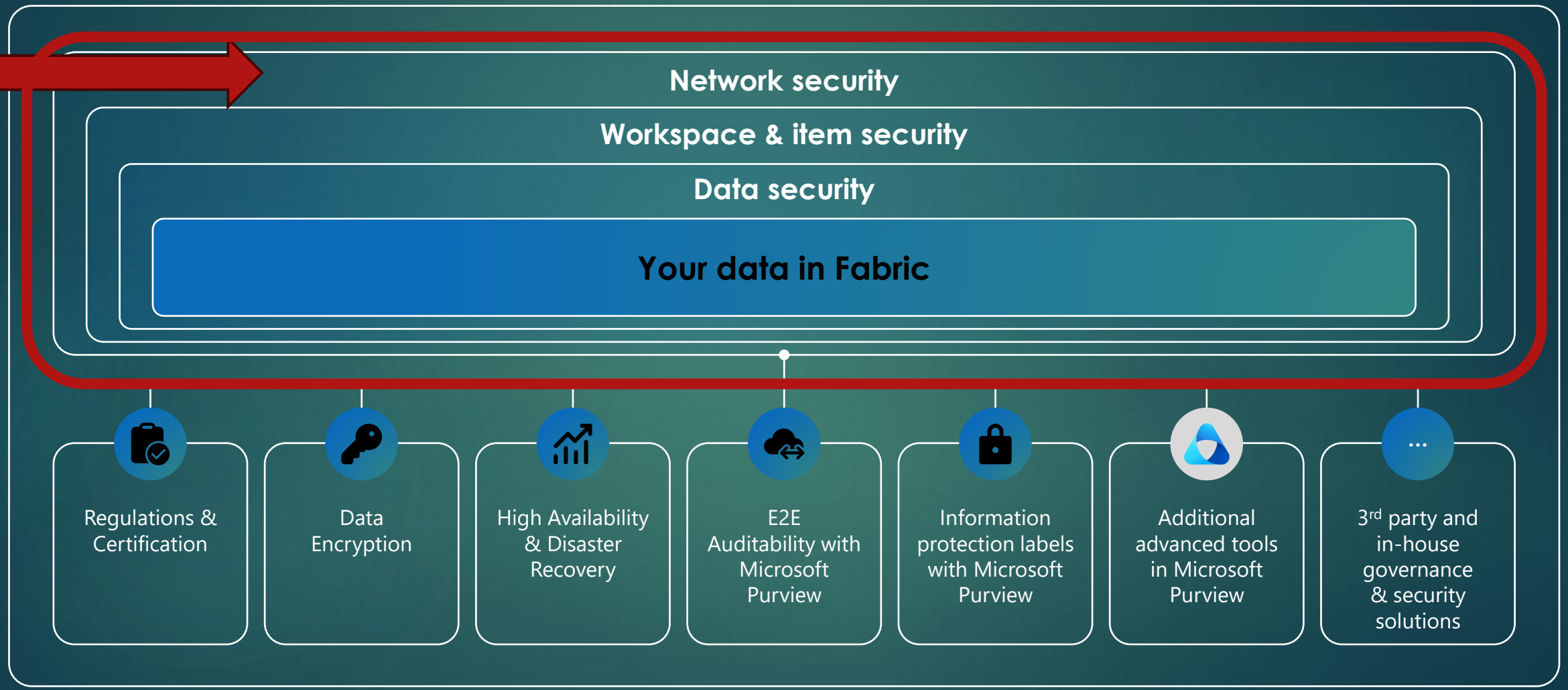
The unified data platform for AI transformation



Security layers in Microsoft Fabric



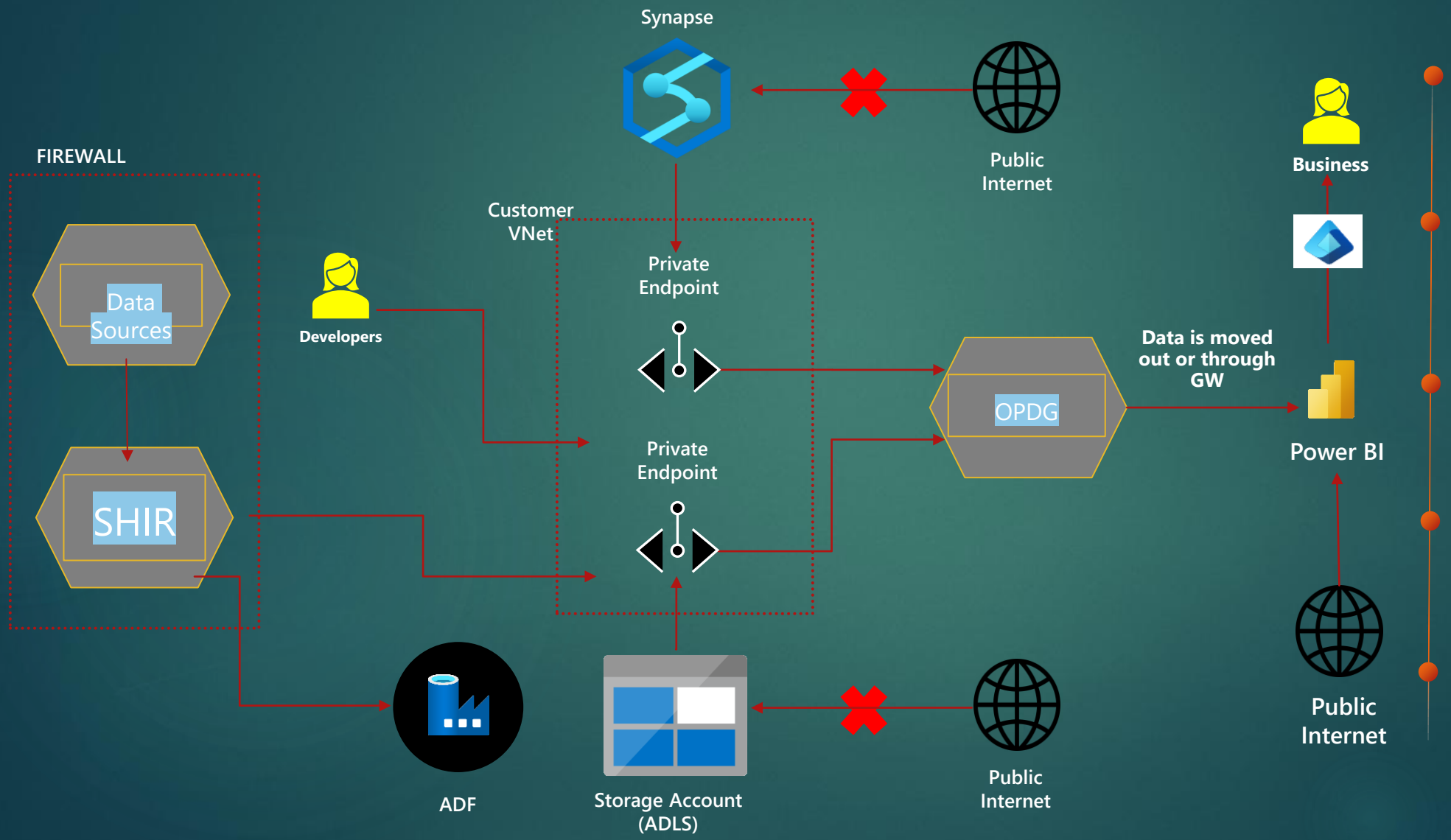
Security layers in Microsoft Fabric



Modern data challenges

- Bring data to the masses, everyone should have access to data to make decisions
- Instant access to the latest data, no copying around
- Modern workforce, anywhere, any device
- At the same time, you need to secure, govern and audit your data to protect customers and the company
- SaaS platforms are designed with these challenges in mind.
- Shift from siloed PaaS to integrated SaaS

Existing PaaS World



PaaS services are disconnected from the Public internet.

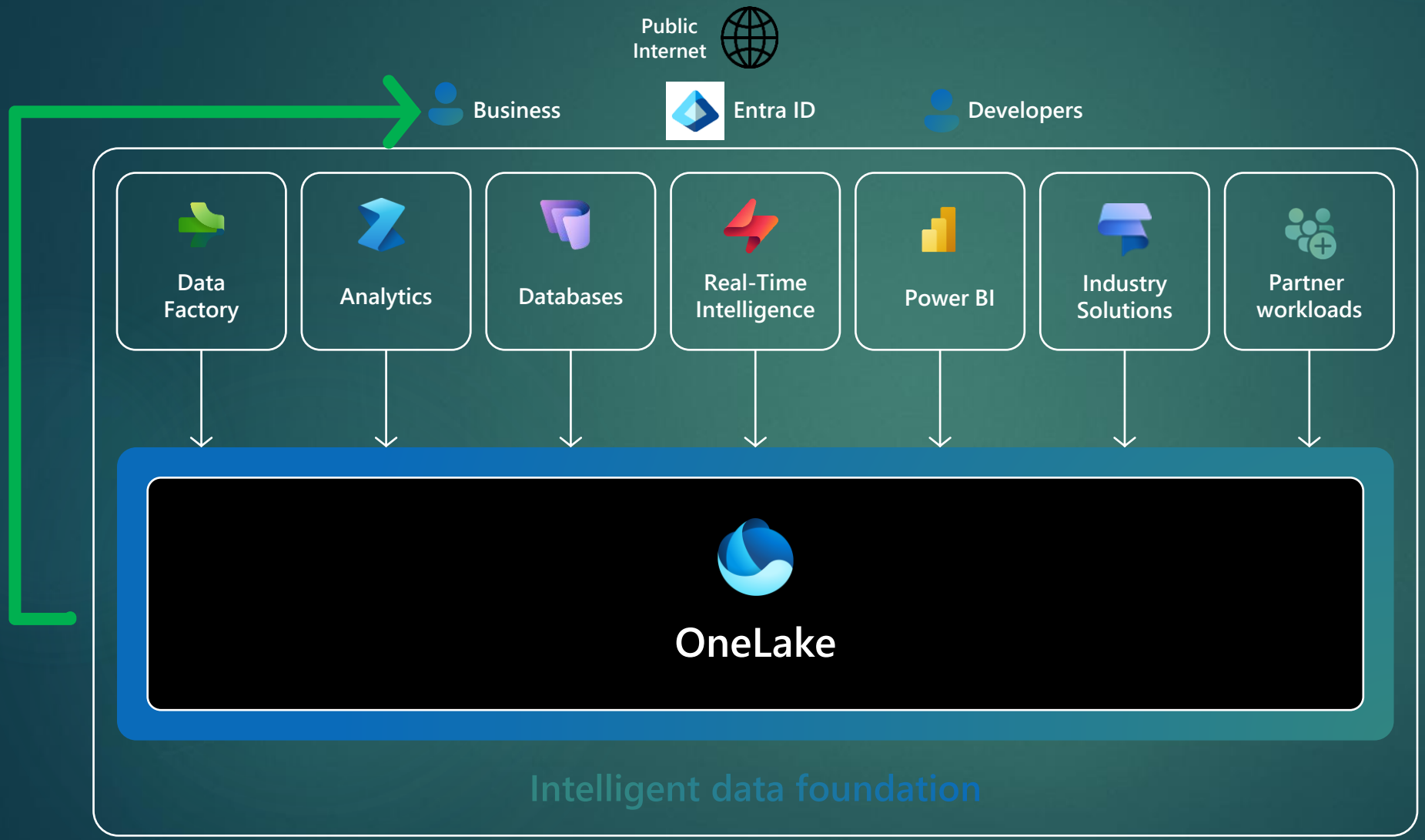
All communications between the services are configured to go through private endpoint

Developers connect to a VPN and connect to the backend services

Data sources are connected through the self-hosted runtime inside the firewall

When the CEO access the data in Power BI Report, the data is imported into Power BI or through the GW with DQ.

Microsoft Fabric – SaaS World



Users connect to the SaaS service from global network

Endpoints and access are protected using Entra ID

All internal communications between the experiences happens through MS backbone network

When the CEO access the data in Power BI Report, the data is fetched directly from the OneLake instantly and securely without copying or moving

Common network security requirements

- Secure access to your data in Fabric (Inbound Protection)
  - Conditional Access Policies
  - Private Link at a Tenant Level
  - Private Link at a Workspace level
  - Workspace IP Firewall
- Restrict outbound access from a Fabric workspace (Outbound Protection)
- Securely connect to data behind a firewall\private link from Fabric (Outbound Access)

Inbound protection options

Perimeter Network Security

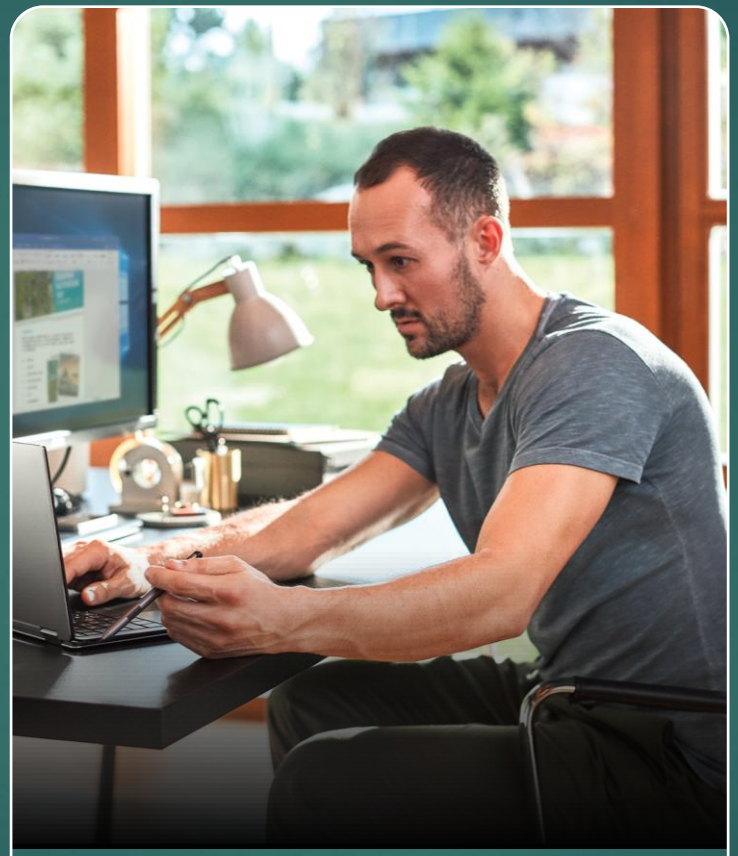
From limited known locations

Zero Trust Approach

to unknown locations

New principles for Zero Trust in today's reality

Verify explicitly



Use least privilege access

Assume breach

Conditional Access Policies

Common Decisions – Block, Grant, Require MFA

Users and Groups

Network Location

Applications

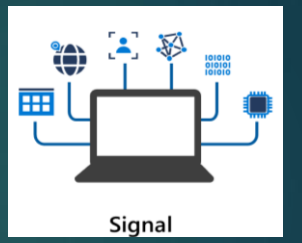
Devices

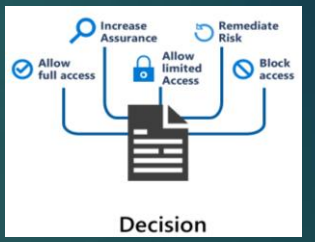
Entra Conditional Access Policies

Inbound

OneLake

Microsoft Fabric





Entra ID Conditional Access

Applications
Protection
Identity Governance
External Identities
Show more
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access

Microsoft Entra

InSpark Labs (InSpark B.V.)

Tenant ID cd004ec9-bc4b-4...
Primary domain insparklab...

399 View users
572 View groups
239 View devices
560 View apps

Erwin de Kreuk

Global Administrator

a79b59b2-3de7-4c48-b6c8-...
View user profile

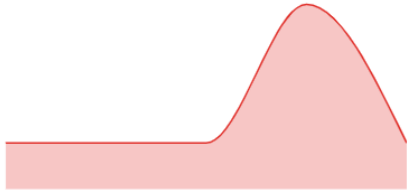
My role assignments 2

High privileged role assignments
Other role assignments

Manage my roles

Users at high risk

8 user detections with risk level "high" in the last 6 months.
Learn more



75% in the last 30 days

View high risk users

Tenant status

Identity Secure Score
77.90%

View recommendations

Microsoft Entra Connect
Enabled

View Entra Connect

Shortcuts

Add | User sign-ins | Audit logs | Authentication Methods | Blocked users | Domain names | Unused service principals | Manage tenants

Named locations | Cross-tenant Access Policies | Tenant restrictions | Risk Based Conditional Access policies | Risky sign-ins | Lifecycle workflows

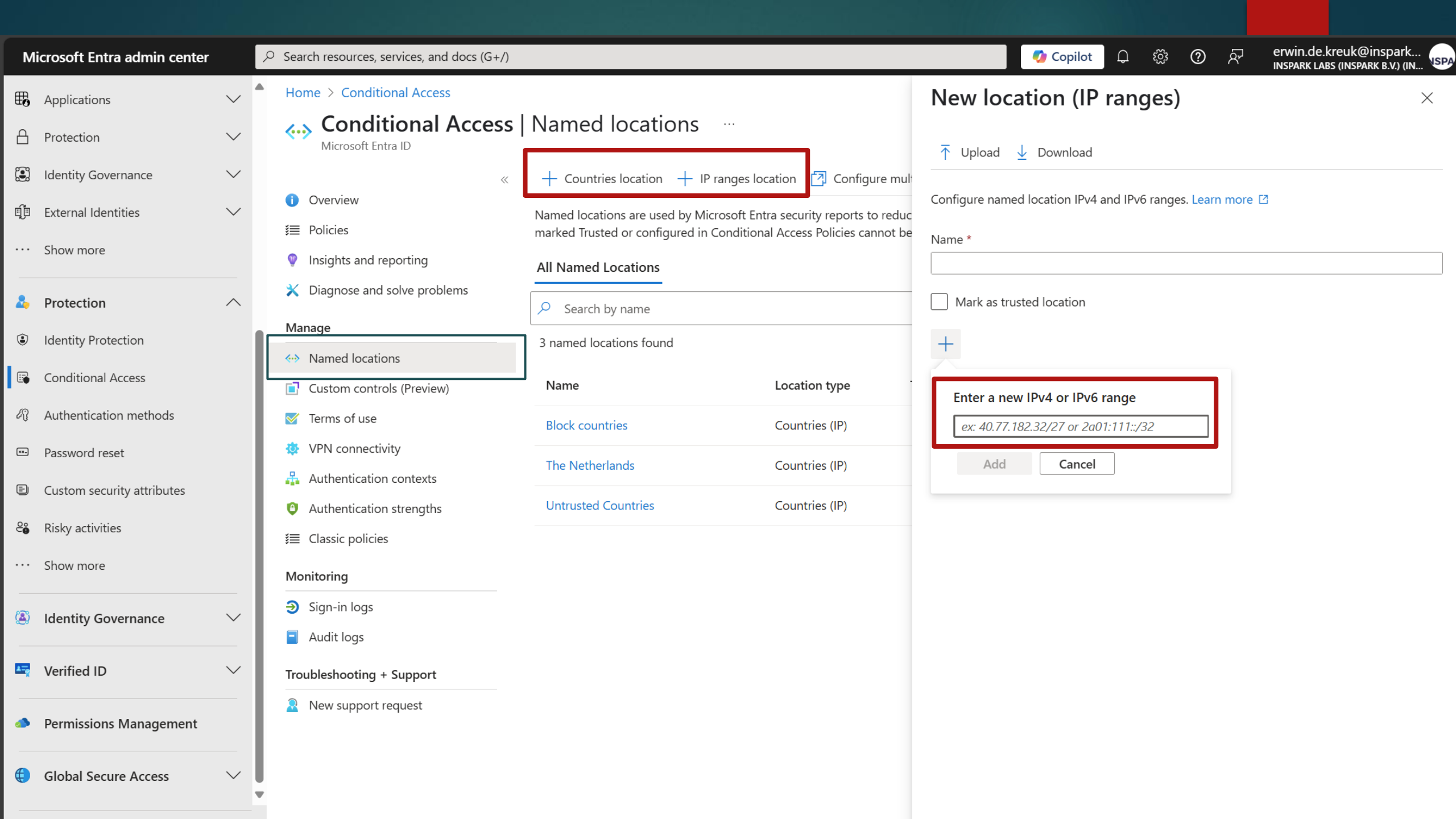
Get the most out of your licenses and subscriptions

Deployment guides

Use these deployment guides to plan, configure and deploy Microsoft Entra capabilities

Microsoft Entra plan

Entra Suite


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
erwin.de.kreuk@inspark...
INSPARK LABS (INSPARK B.V.) (IN...
Applications
Protection
Identity Governance
External Identities
Show more
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Home > Conditional Access
Conditional Access | Named locations
Microsoft Entra ID
Countries location
IP ranges location
Configure mult
Overview
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies
Monitoring
Sign-in logs
Audit logs
Troubleshooting + Support
New support request
Named locations are used by Microsoft Entra security reports to reduc
marked Trusted or configured in Conditional Access Policies cannot be
All Named Locations
Search by name
3 named locations found
Name
Location type
Block countries
Countries (IP)
The Netherlands
Countries (IP)
Untrusted Countries
Countries (IP)
New location (IP ranges)
Upload
Download
Configure named location IPv4 and IPv6 ranges. Learn more
Name *
Mark as trusted location
Enter a new IPv4 or IPv6 range
ex: 40.77.182.32/27 or 2a01:111::/32
Add
Cancel

Applications
Protection
Identity Governance
External Identities
Show more

Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more

Identity Governance
Verified ID
Permissions Management
Global Secure Access

Conditional Access | Overview

Microsoft Entra ID

Overview
Policies
Insights and reporting
Diagnose and solve problems

Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies

Monitoring
Sign-in logs
Audit logs

Troubleshooting + Support
New support request

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

Getting started
Overview
Coverage
Monitoring (Preview)
Tutorials

Policy Summary

Policy Snapshot

23 Enabled 23 Report-only 7 Off

View all policies

Users

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

See all unprotected sign-ins

Devices

100% 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

What's new

The approved client app grant in Conditional Access is retiring in March 2026.

This control will no longer be enforced after March 2026. Update your policy to stay up to date.

Learn more

Named Locations

Microsoft Entra ID now supports IPv6! Update your Named locations with IPv6 ranges.

Learn more

4 policies have a Named Location condition

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

erwin.de.kreuk@inspark...
INSPARK LABS (INSPARK B.V.) (IN...

- Applications
- Protection
- Identity Governance
- External Identities
- Show more

Protection

- Identity Protection
- Conditional Access
- Authentication methods
- Password reset
- Custom security attributes
- Risky activities
- Show more

- **Identity Governance**
- **Verified ID**
- **Permissions Management**
- **Global Secure Access**

Home > Conditional Access | Overview >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users

0 users and groups selected

Target resources

No target resources selected

Network NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Enable policy

Grant

Control access enforcement to block or grant access. Learn more

- Block access
- Grant access

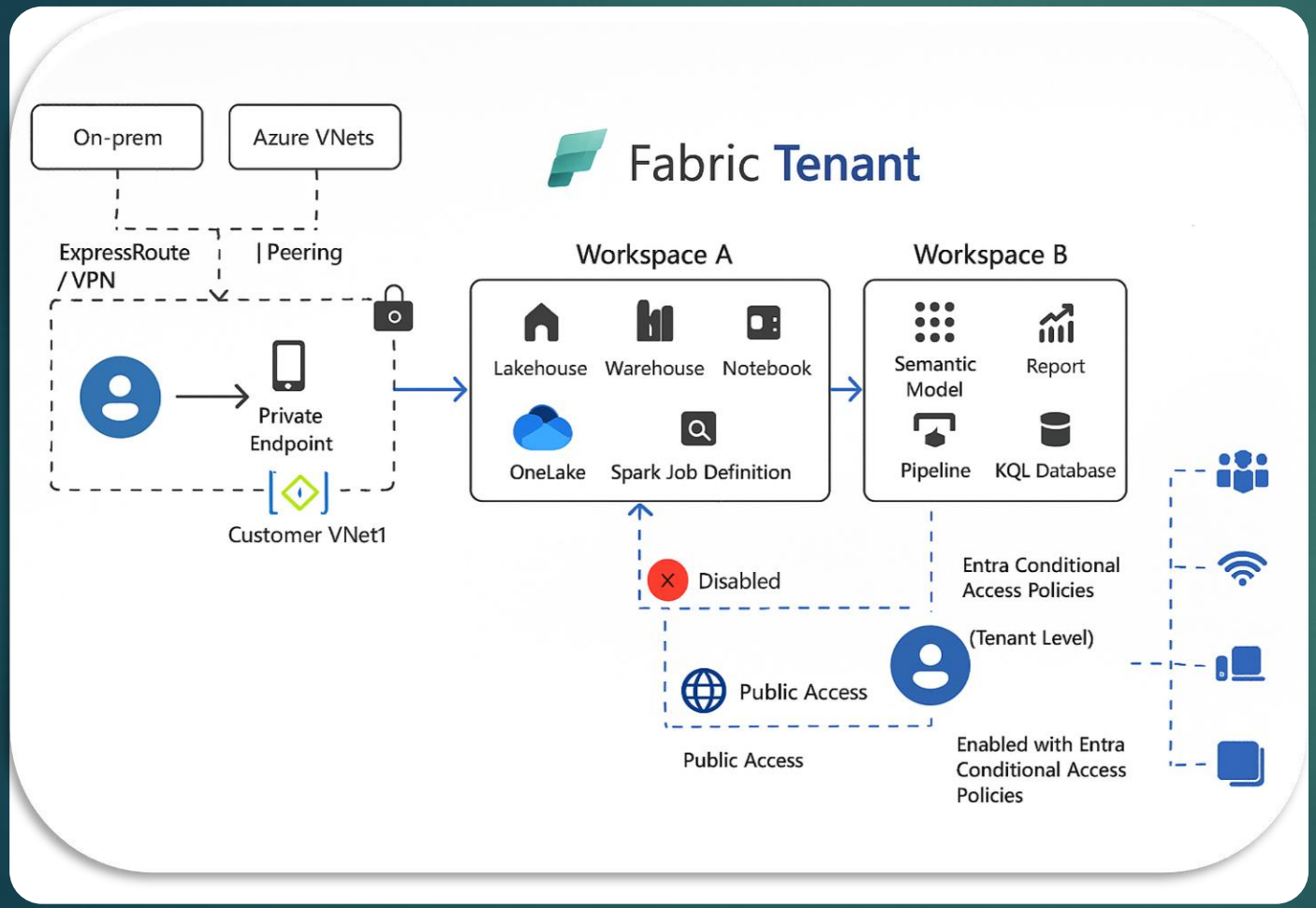
- Require multifactor authentication
- Require authentication strength
- Require device to be marked as compliant
- Require Microsoft Entra hybrid joined device
- Require approved client app
  See list of approved client apps
- Require app protection policy
  See list of policy protected client apps
- Require password change
- All users term of use
- Guests term of use (Jeffrey TEST)

For multiple controls

- Require all the selected controls
- Require one of the selected controls

Private Link for Fabric Tenant

Perimeter Network Security for your tenant



What it means:

1. Fabric is disconnected from the public internet
2. Every users needs to connect to the private network to get access on every device
3. No longer able to load resources locally (slower reports)
4. Increases ExpressRoute bandwidth and added costs for Private Links
5. Several product limitations (like on-prem data gateway)

Private Link for Fabric

Perimeter Network Security for your tenant

Private Link for Fabric (Admin Portal)

Azure **Pri**vate Link

Disabled for the entire organization

Increase security by allowing people to use a **Pri**vate Link to access your Fabric tenant. Someone will need to finish the set-up process in Azure. If that's not you, grant permission to the right person or group by entering their email. Learn More | Set-up instructions

Review the considerations and limitations section before enabling **pri**vate endpoints.

Disabled

This setting applies to the entire organization

Apply Cancel

Block Public Internet Access

Disabled for the entire organization

For extra security, block access to your Fabric tenant via the public internet. This means people who don't have access to the **Pri**vate Link won't be able to get in. Keep in mind, turning this on could take 10 to 20 minutes to take effect. Learn More Set-up instructions

Disabled

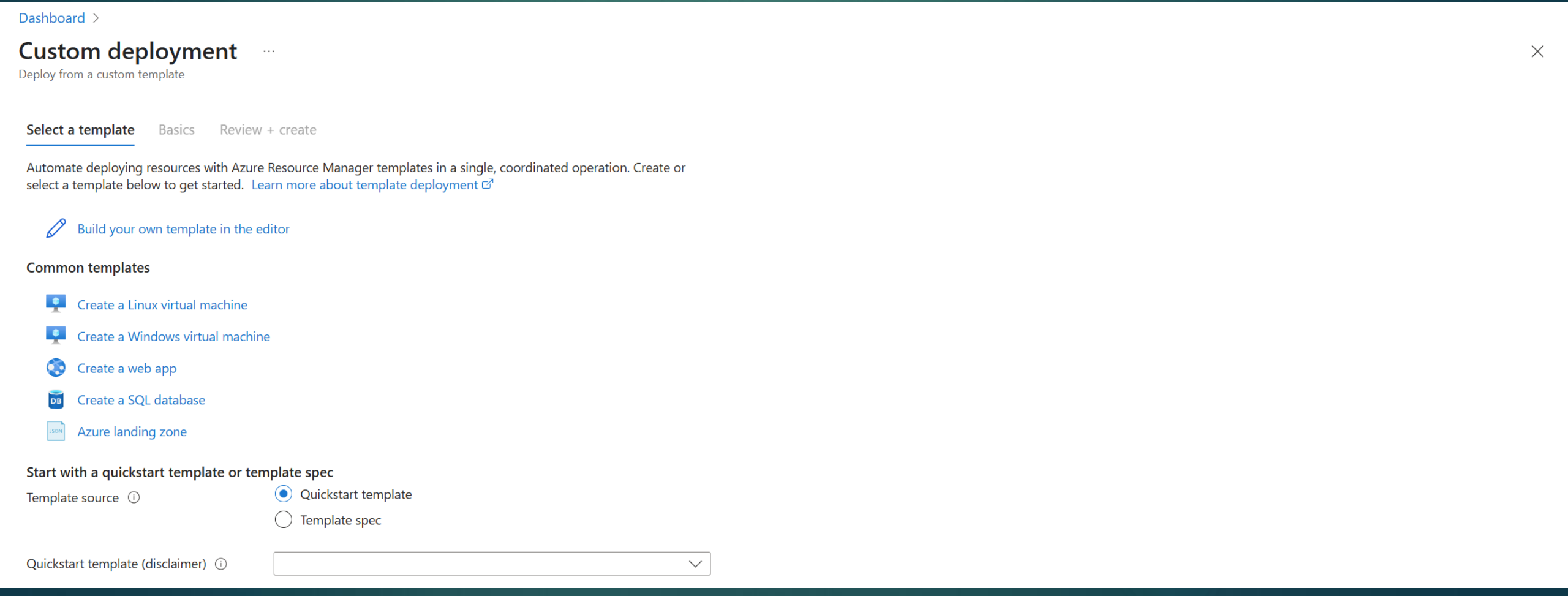
This setting applies to the entire organization

Apply Cancel

Private Link for Fabric

Perimeter Network Security for your tenant

Private Link for Fabric (Azure Portal)



Private Link for Fabric

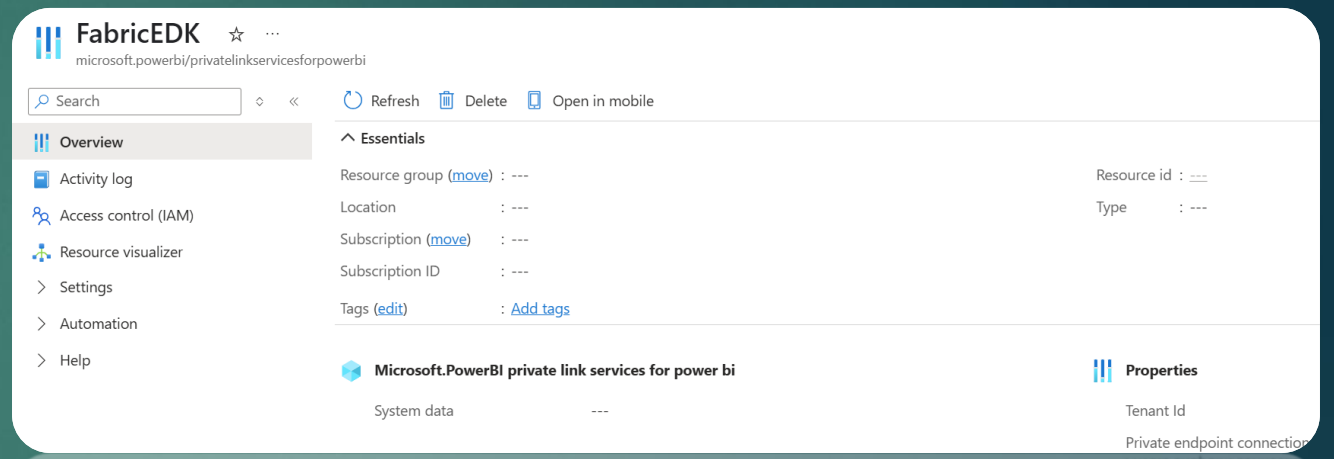
Perimeter Network Security for your tenant

Private Link for Fabric (Azure Portal)

- `<resource-name>` is the name you choose for the Fabric resource.
- `<tenant-object-id>` is your Microsoft Entra tenant ID. See How to find your Microsoft Entra tenant ID.

Copy

```
{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deplo
  "contentVersion": "1.0.0.0",
  "parameters": {},
  "resources": [
      {
          "type":"Microsoft.PowerBI/privateLinkServicesForPowerBI",
          "apiVersion": "2020-06-01",
          "name" : "<resource-name>",
          "location": "global",
          "properties" :
          {
               "tenantId": "<tenant-object-id>"
          }
      }
  ]
}
```

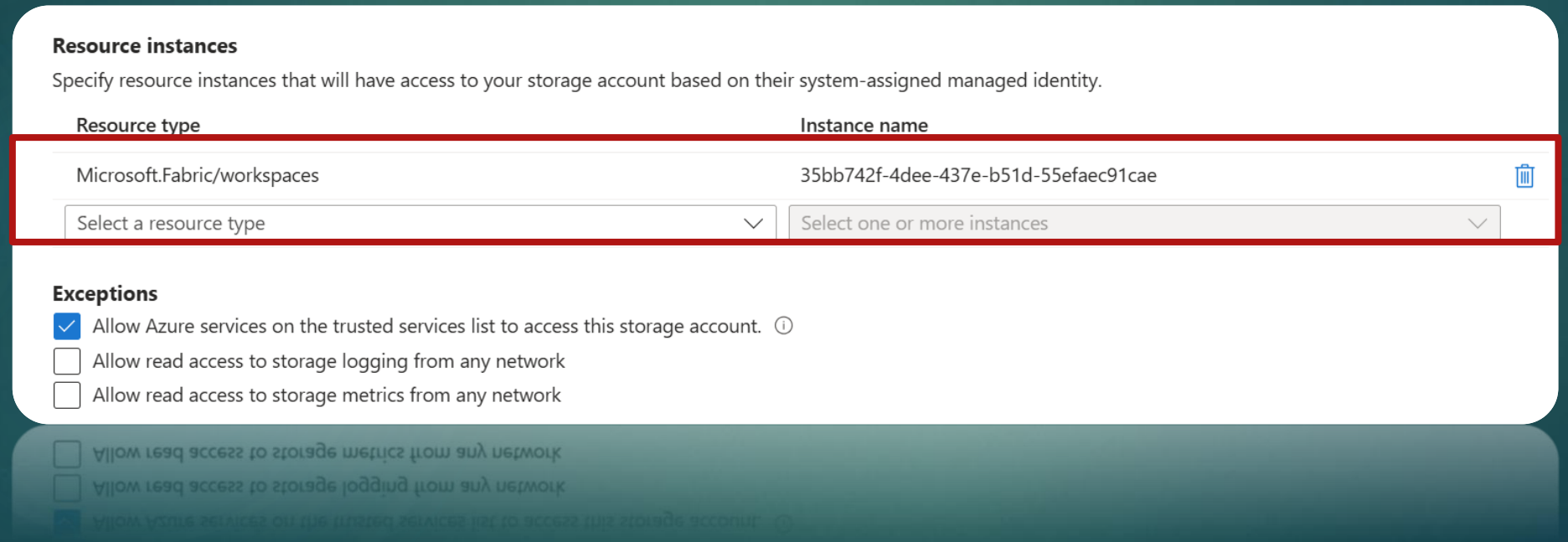


Set up and use private links for secure access to Fabric - Microsoft Fabric | Microsoft Learn

Private Link for Fabric

Perimeter Network Security for your tenant

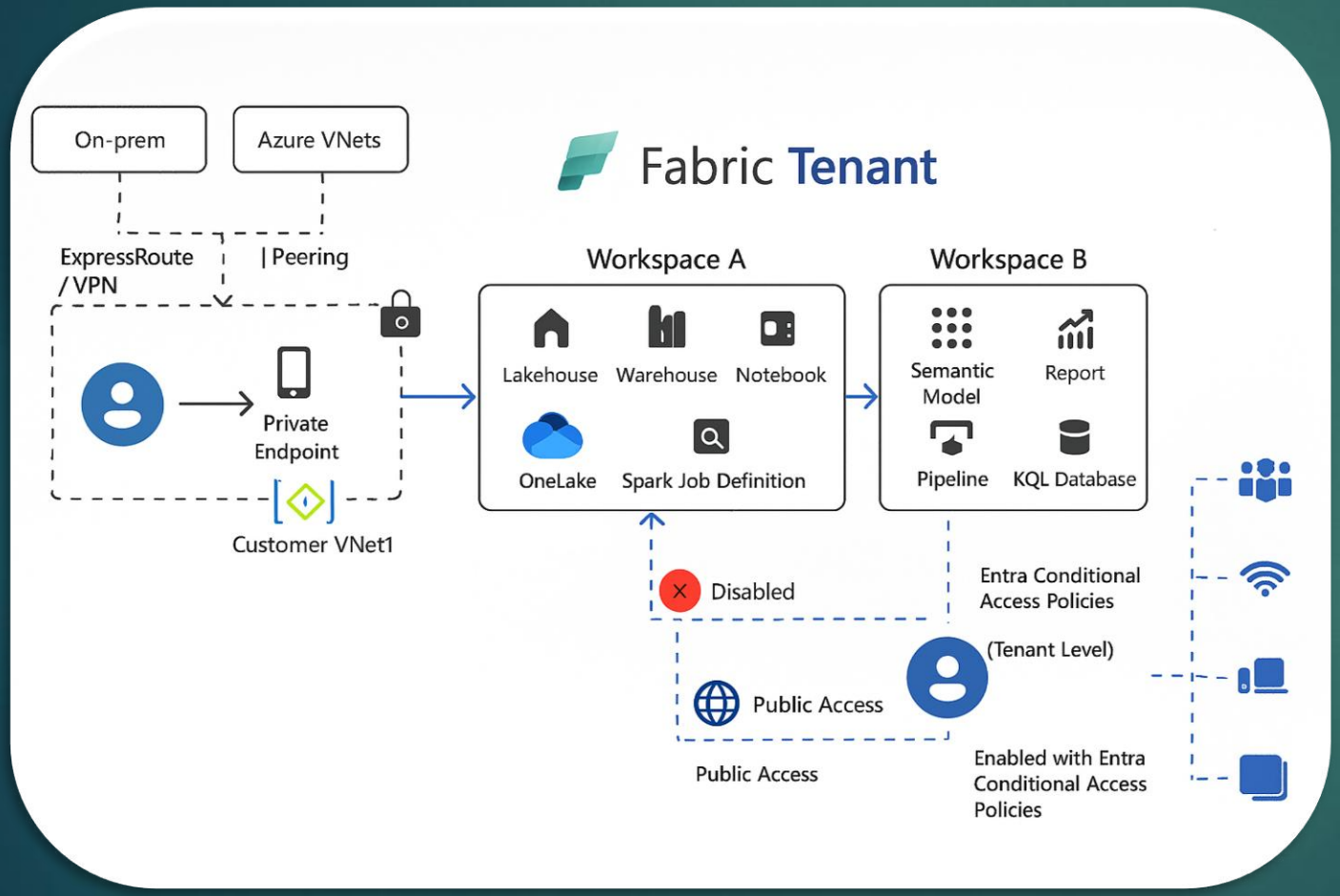
Private Link for Fabric (Azure Portal)



Set up and use private links for secure access to Fabric - Microsoft Fabric | Microsoft Learn

Workspace Private Link for Fabric

Perimeter Network Security for your workspace



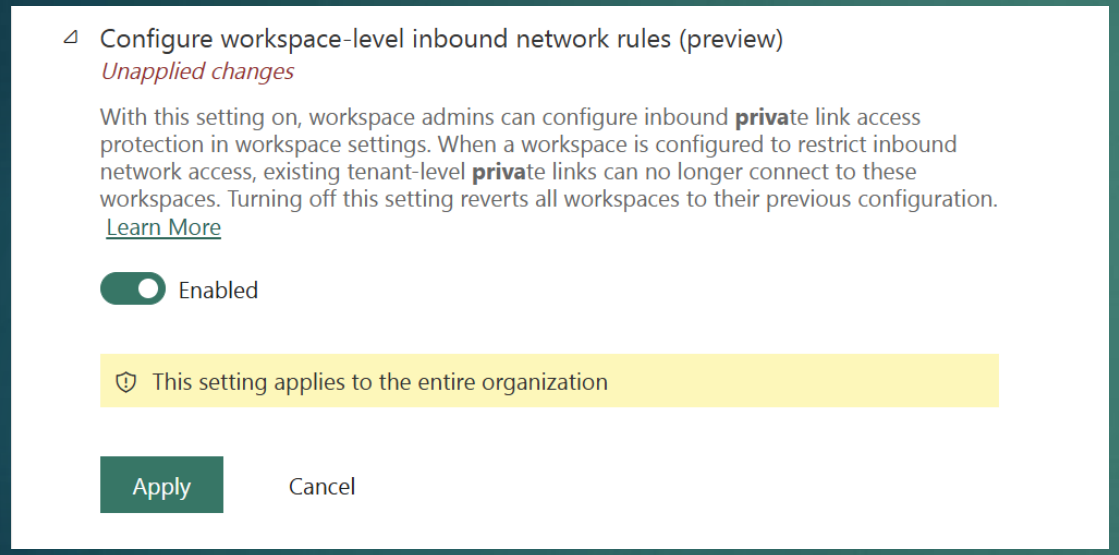
What it means:

1. Selected workspaces can be protected using Private Links and closed from public internet.
2. Create a secure connection between public and private workspaces using private data access.
3. Public workspaces can be secured using Entra policies or IP filtering to use Power BI.

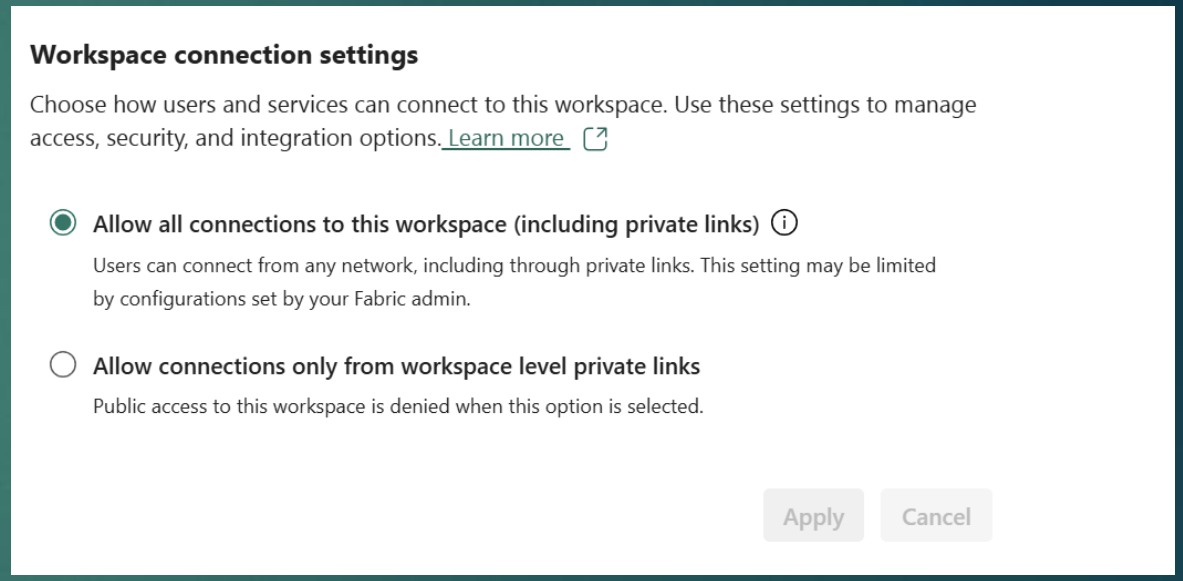
Workspace Private Link for Fabric

Perimeter Network Security for your workspace

Private Link for Workspace (Admin Portal)

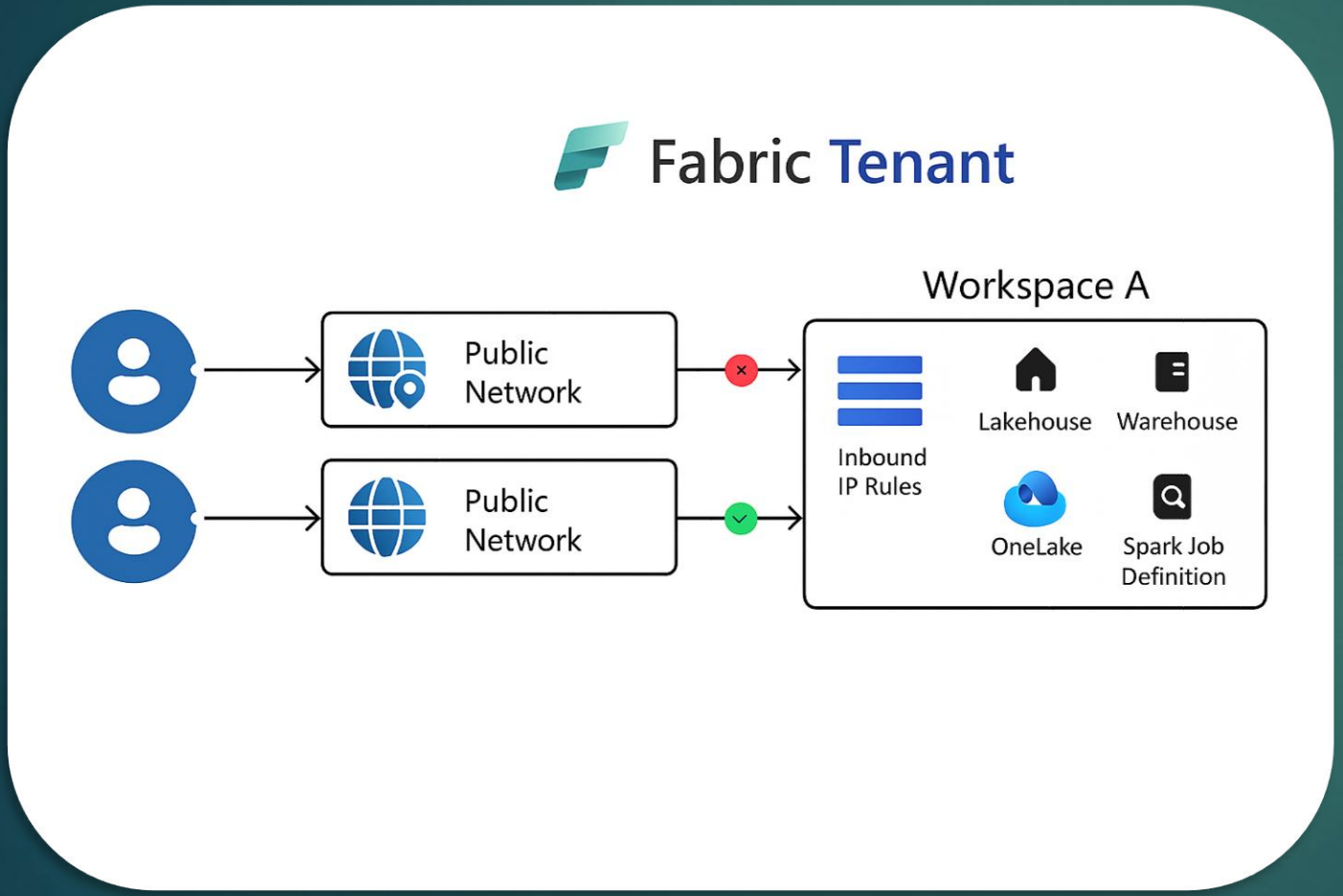


Inbound Netwroking Workspace



Workspace IP Firewall for Fabric

Perimeter Network Security for your workspace



What it means:

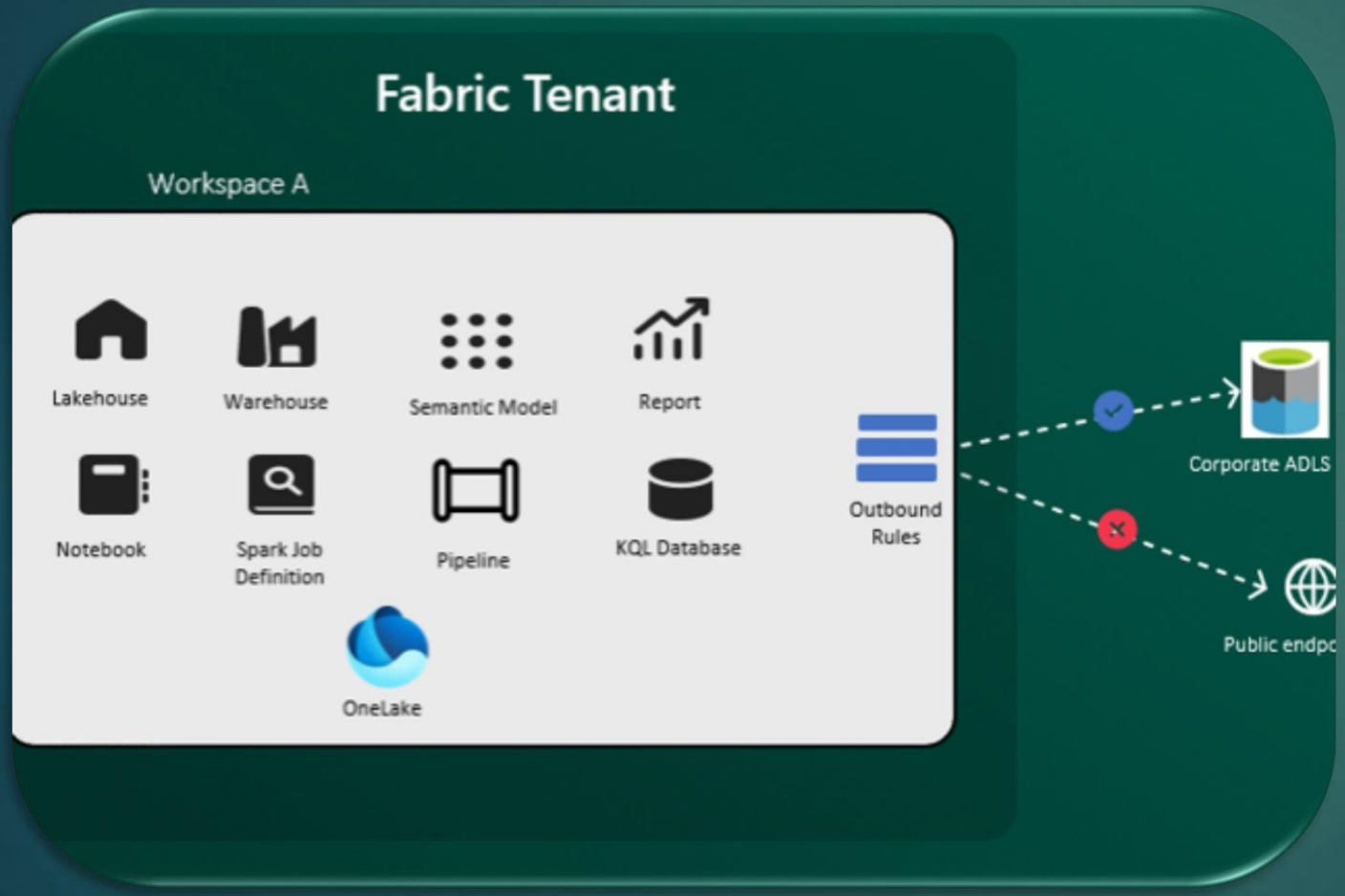
1. Fabric workspace is accesible only form specific public IP or IP Ranges
2. Simple setup.

Fabric Outbound Security

Common network security requirements

- Secure access to your data in Fabric (Inbound Protection)
- Restrict outbound access from a Fabric workspace (Outbound Protection)
  - Outbound Access Policies + Inbound network security features
- Securely connect to data behind a firewall\private link from Fabric (Outbound Access)

Workspace outbound access protection

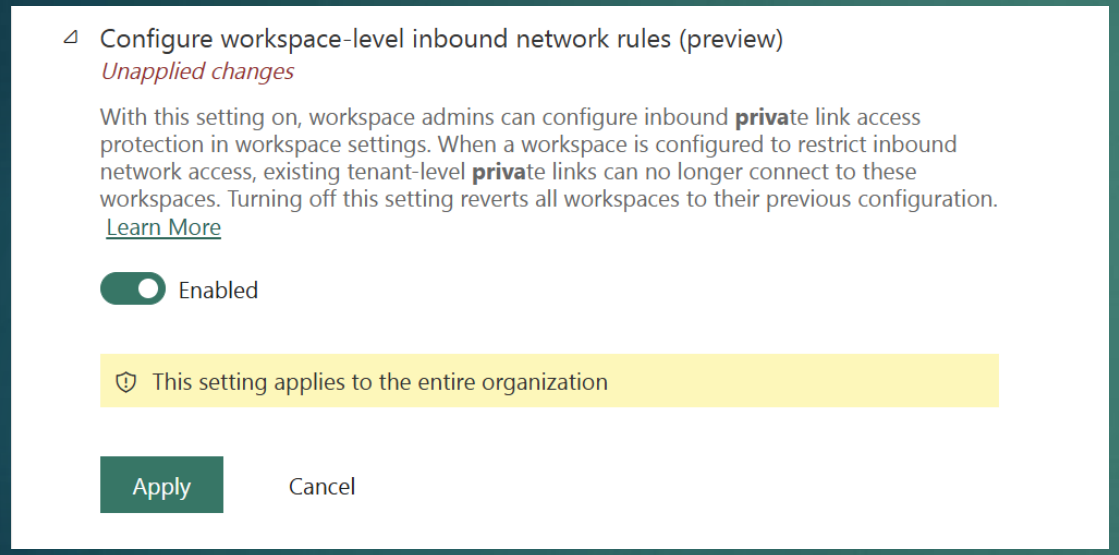


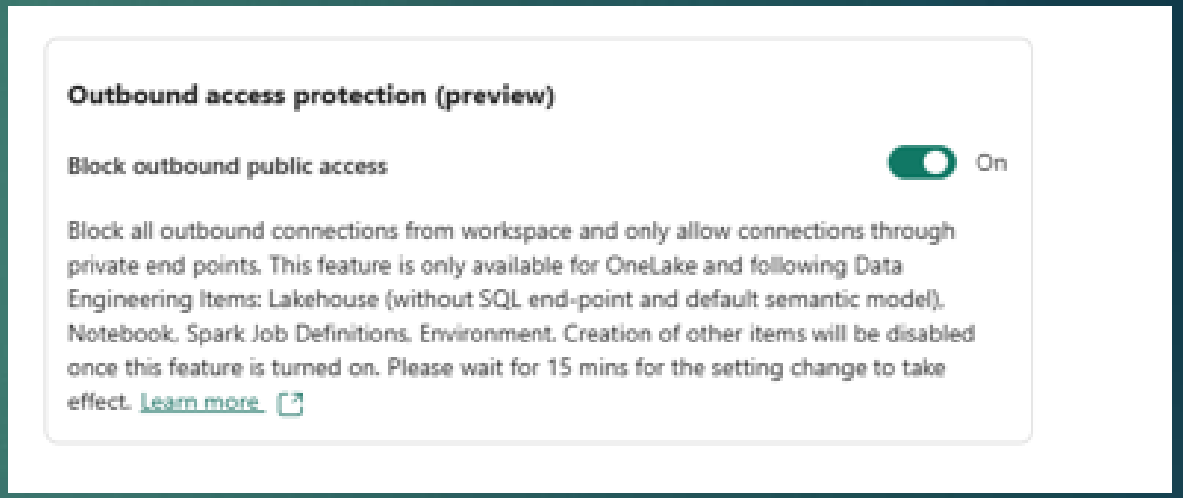
What it means:

1. Workspace level control to restrict outbound access to Public network
2. Restrict outbound connections to permitted destinations only
3. Use in conjunction with other security features to achieve robust outbound control

Workspace outbound access protection

Outbound rules (Admin Portal)





Data Exfiltration Protection

DEP = Outbound + Inbound protection

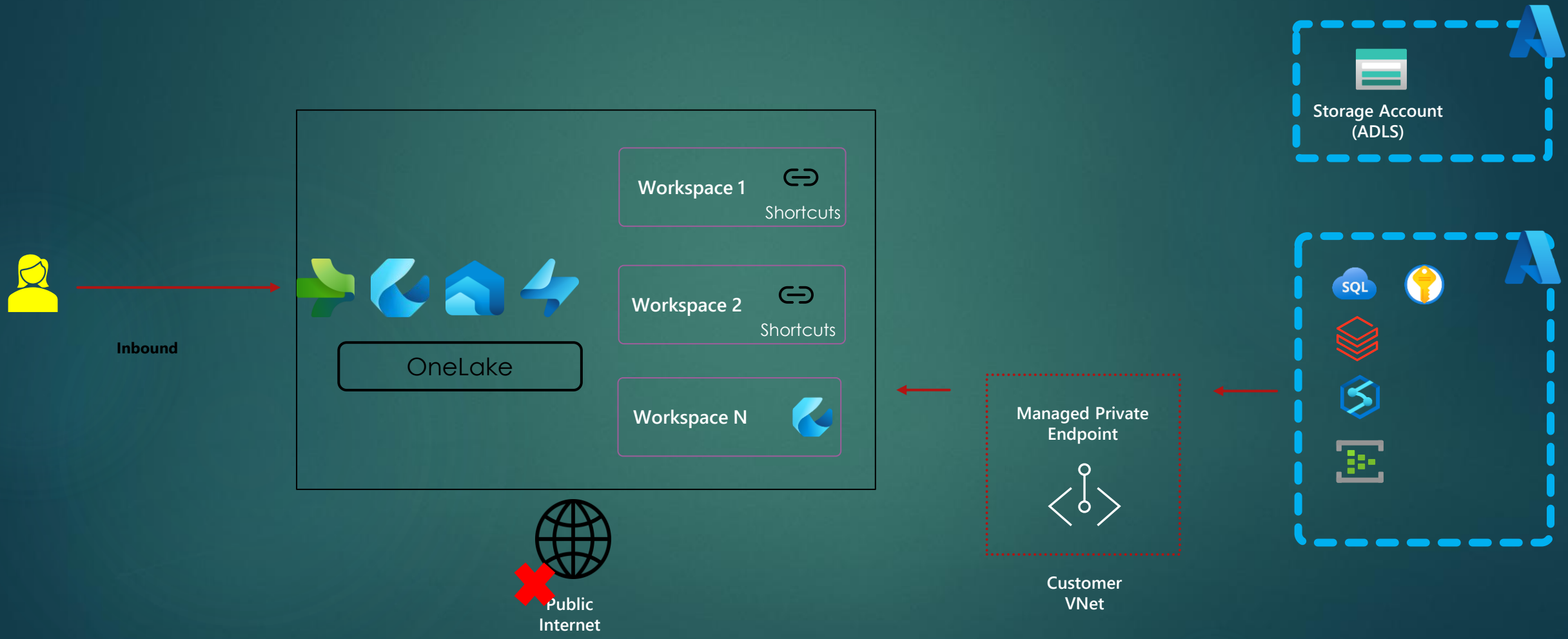
Inbound security features like private link allow you to restrict who can access your data and from where, reducing risks of data exfiltration

Outbound security make sure that malicious users cannot exfiltrate data

Common network security requirements

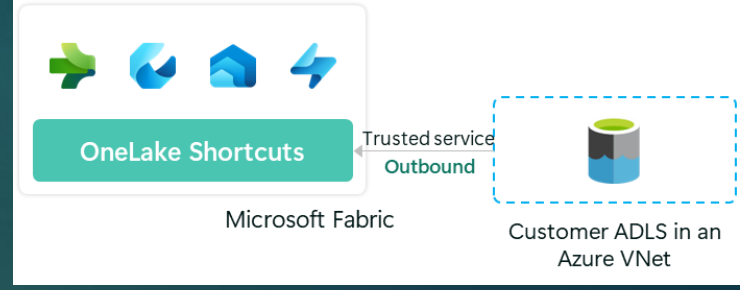
- Secure access to your data in Fabric (Inbound Protection)
- Restrict outbound access from a Fabric workspace (Outbound Protection)
- Securely connect to data behind a firewall\private link from Fabric (Outbound Access)
  - Trusted Access
  - Data Gateways(On-prem and VNet)
  - Managed Private Endpoints

Getting data into Fabric



Create and use managed private endpoints in Microsoft Fabric - Microsoft Fabric | Microsoft Learn

Getting data into Fabric



Trusted Access for Fabric Workspace Identity

Storage Account (ADLS)

Workspace 1
Shortcuts

Workspace 2
Shortcuts

Workspace N

OneLake

Inbound

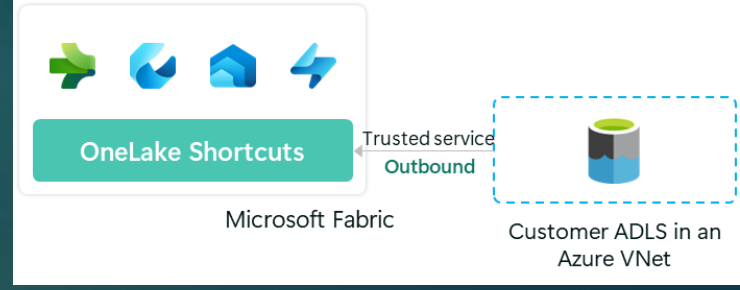
Managed Private Endpoint

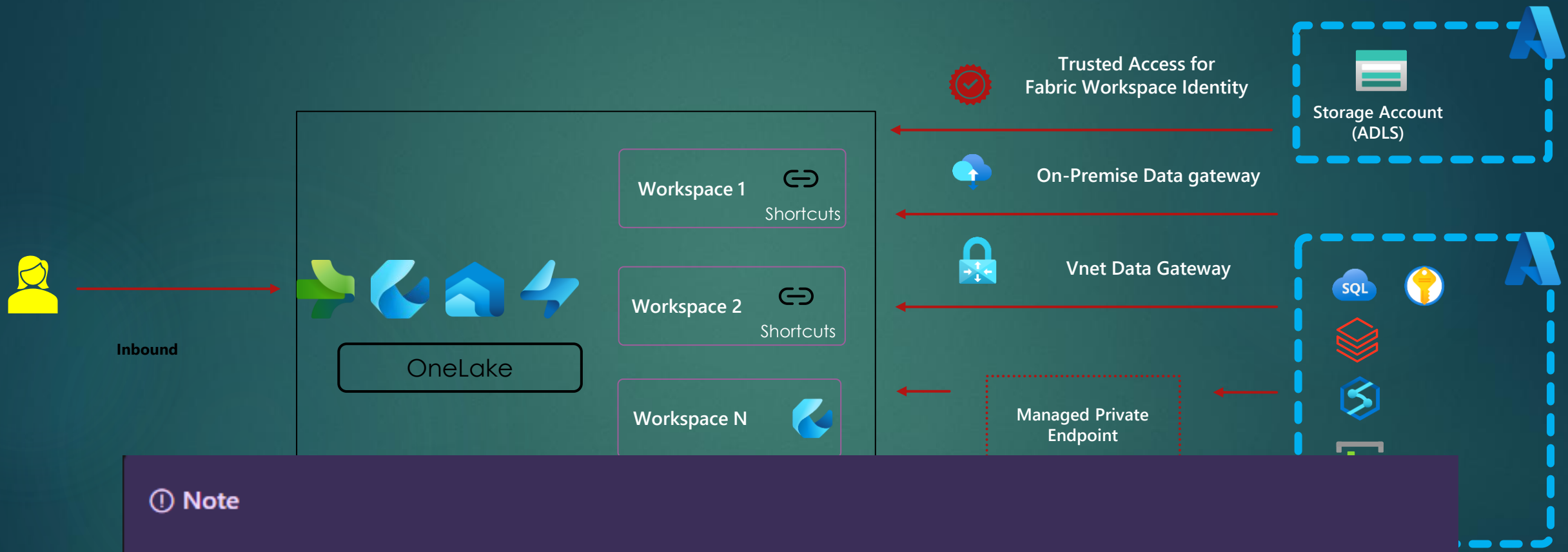
Customer VNet

Public Internet

Trusted workspace access in Microsoft Fabric - Microsoft Fabric | Microsoft Learn

Getting data into Fabric





Note

Trusted workspace access is **generally available**, but can only be used in F SKU capacities. For information about buying a Fabric subscription, see **Buy a Microsoft Fabric subscription**. Trusted workspace access is not supported in Trial capacities.

Create and use managed private endpoints in Microsoft Fabric - Microsoft Fabric | Microsoft Learn

Getting data into Fabric

Storage account name

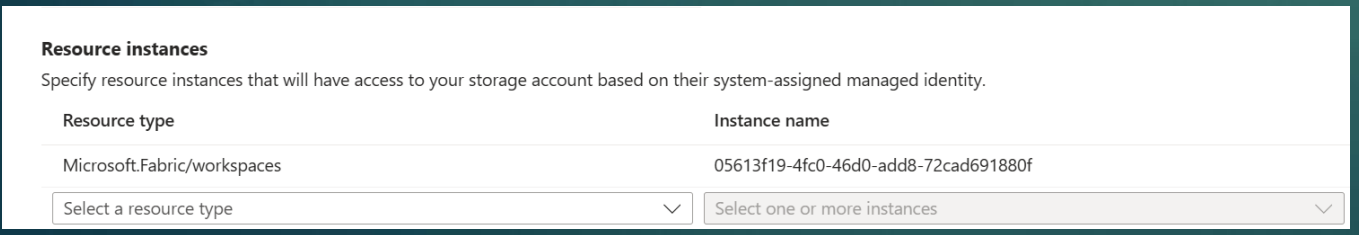
Region

TenantID

WorkspaceId

Leave subscription for workspace as is

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "resources": [
        {
            "type": "Microsoft.Storage/storageAccounts",
            "apiVersion": "2023-01-01",
            "name": "<storage account name>",
            "id": "/subscriptions/<subscription id of storage account>/resourceGroups/<resource group
ame>/providers/Microsoft.Storage/storageAccounts/<storage account name>",
            "location": "<region>",
            "kind": "StorageV2",
            "properties": {
                "networkAcls": {
                    "resourceAccessRules": [
                        {
                            "tenantId": "<tenantid>",
                            "resourceId": "/subscriptions/00000000-0000-0000-0000-
00000000000/resourcegroups/Fabric/providers/Microsoft.Fabric/workspaces/<workspace-id>"
                        }]
                }
            }
        }
    ]
}
```



Common network security requirements

Secure access to your data in Fabric (Inbound Protection)
- Conditional Access Policies
- Private Link at a Tenant Level
- Private Link at a Workspace level
- Workspace IP Firewall

Restrict outbound access from a Fabric workspace (Outbound Protection)
- Outbound Access Policies + Inbound network security features

Securely connect to data behind a firewall\private link from Fabric (Outbound Access)
- Trusted Access
- Data Gateways(On-prem and VNet)
- Managed Private Endpoints

Flexibility with no compromise to **Security**

Workspace Private Link for Fabric

October 1st , 2025

General availability

- Supported: Lakehouse, Shortcut, Notebook, ML experiment/model, Pipeline, Warehouse, Dataflows, Eventstream, Mirrored DB
- Access to WS PL workspaces via API Only

September 30th ,2025

General availability

- Access to WS PL workspaces via Fabric portal and API

Roadmap

General availability +

- Support for more Fabric experiences like Power BI, databases, Data Activator and more.


DEMO

Microsoft Purview

Reshape how you access, manage, and act on data and insights by connecting every data source and analytics service together in Fabric

Keep your data safe and governed with unified data governance, information protection, and risk and compliance solutions

Data ownership	Unmatched security & compliance	Unified governance

Microsoft Purview

Data Security

For information and cybersecurity teams

- Data Loss Prevention
- Insider Risk Management
- Information Protection

Data Governance

For data consumers, data owners, data officers

- Data Discovery
- Data Curation & Management
- Data Estate Health

Risk & Compliance

For risk, compliance, and legal teams

- Data Lifecycle Management
- eDiscovery & Audit
- Communication Compliance

On-prem and multi-cloud

Unstructured & structured data

Across IaaS, and SaaS

Data Security integrations in Fabric

Information Protection

Manual labeling of Fabric assets

Label-based access control for specific users and groups

Downstream inheritance from Lakehouse to other items within a Fabric workspace

Data Loss Prevention

DLP policies to notify users with policy tips when they interact with sensitive data in semantic models and lakehouse.

DLP policies to restrict access to users outside of your organization for semantic models

Insider Risk Management

Detect risky usage signals in PowerBI

Data Security in Fabric

Data Encryption:

- Data in rest
- Data in transit

Column Level encryption

- Presido Home - Microsoft Presidio

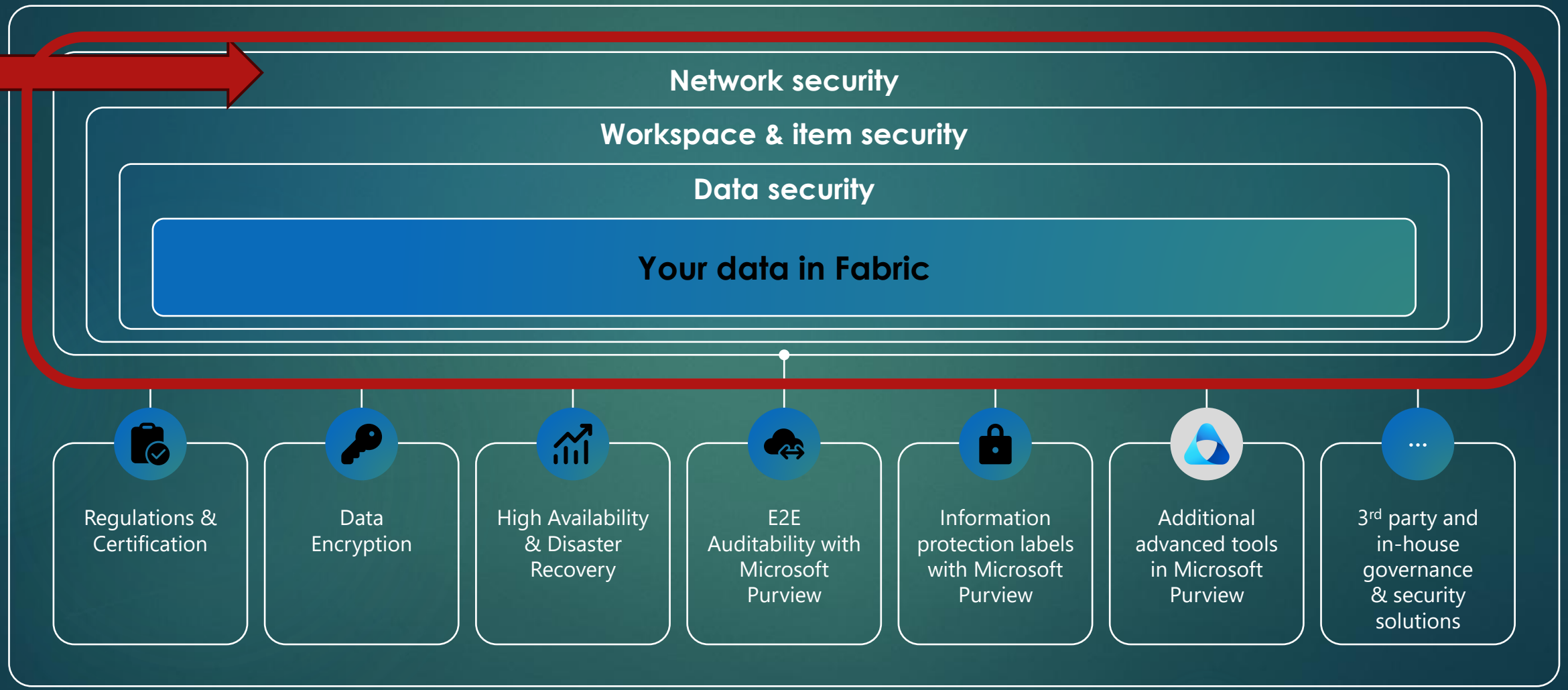
Onelake Security:

- OneLake security overview - Microsoft Fabric | Microsoft Learn

Customer Managed Keys (Preview)

- Customer-managed keys for Fabric workspaces - Microsoft Fabric | Microsoft Learn

Recap


Network security
Workspace & item security
Data security
Your data in Fabric
Regulations & Certification
Data Encryption
High Availability & Disaster Recovery
E2E Auditability with Microsoft Purview
Information protection labels with Microsoft Purview
Additional advanced tools in Microsoft Purview
3rd party and in-house governance & security solutions

Rate Data Saturday Holland

Review to win

With custom Data Saturdays lego stickers!

Let’s connect

Thank you

@erwindekreuk.bsky.social

linkedin.com/in/erwindekreuk

erwindekreuk.com

github.com/edkreuk

https://sessionize.com/erwin-de-kreuk/

Dutchfabricusergroup.com

Microsoft® Most Valuable Professional