FABRIC FORTRESSES

SETTING UP MICROSOFT FABRIC FOR YOUR ENTERPRISE NEEDS

Sam Debruyn

fabric FEBRUARY

Who am I?

Sam Debruyn

📍 Heist-op-den-Berg, BE

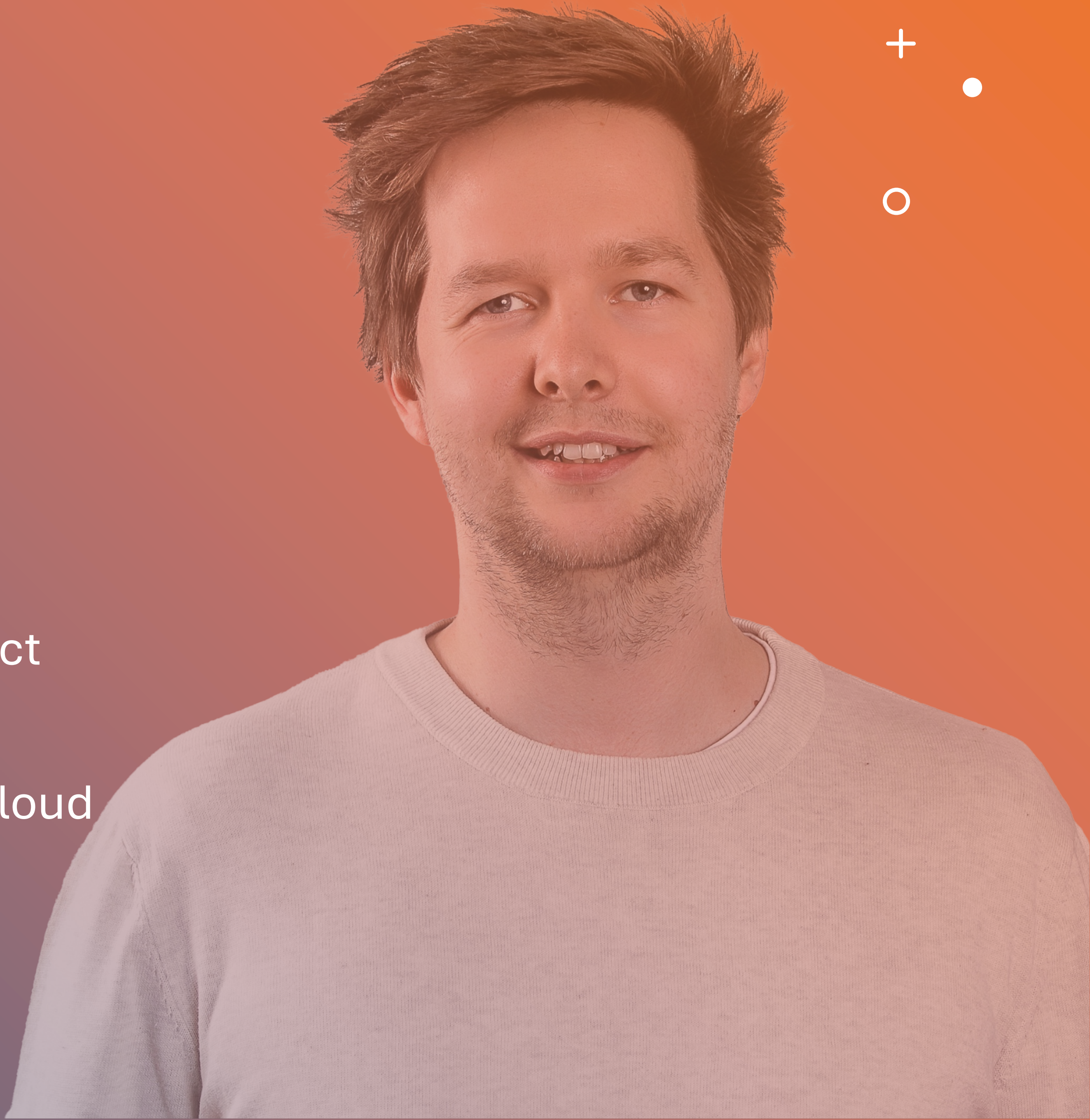
💼 Consultant / Data & Cloud Architect

5️⃣ years in data

🔟 years in software / architecture / cloud

🫶 Fabric, Azure, modern data stack

MVP Microsoft® Most Valuable Professional



Thank you to our Fabric February Friends!

twoday

bouvet

sopra steria

DATAmasterminds

ADVANCING ANALYTICS

Evidi

Profisee
Master Data Management

Tabular Editor

KURANT

Fraktal

CluedIn

Dufrain
THE DATA COMPANY

#FabricFebruary

fabric
FEBRUARY

What we'll talk about

Context & Concepts
Security (concepts)
More security (networking)
Even more security (auth)
Monitoring
Resiliency

Enterprise context

- Problems at scale
  - 🚀Automation is key
- Risks increase
  - More (sensitive) data
  - More ways to access that data
  - More weak links
  - Ageing: solutions must be maintained
- Less “playground” mentality, proper processes in place
- ⌛ Things take more time
- 💰Less focus on lowest possible cost as a decision maker

Security common practices

Defense in depth

Assume breach

Least privilege

Zero trust

Proper patch management

Security awareness

Logging, monitoring, auditing

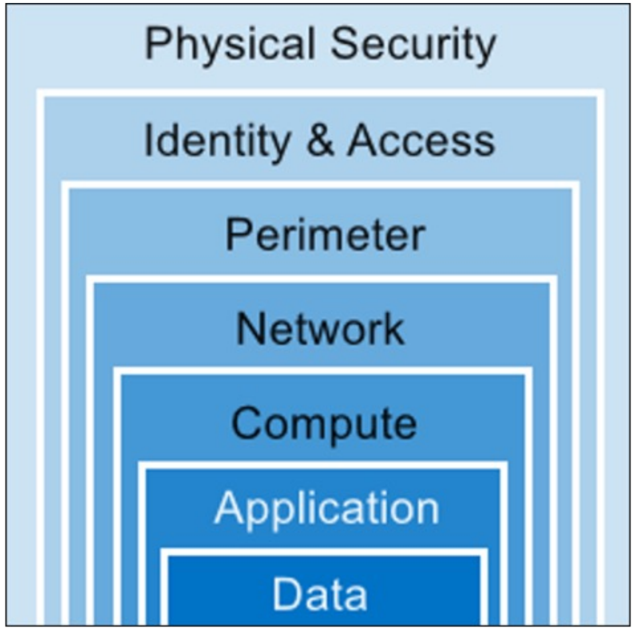
Minimize technical debt

…

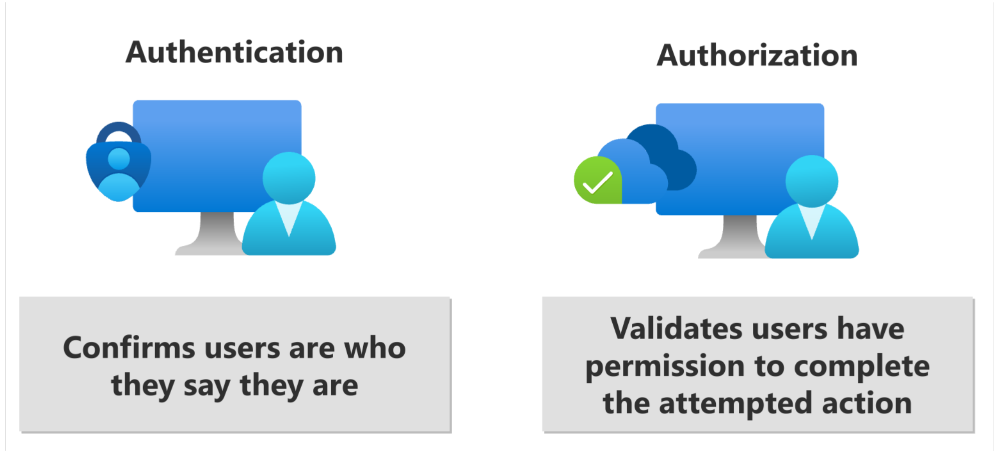
Defense in depth

Think of security in terms of **layers**

Assume Breach and *Zero Trust* so every layer should provide full protection by its own without dependencies on other layers



Authentication / authorization



Authentication

Confirms users are who they say they are

Authorization

Validates users have permission to complete the attempted action

Authentication factors: ways to prove who you are

E.g. email, password, multi-factor app, biometrics, ...

Networking primer: public vs. private networking

The DNS (Domain Name System) translates every domain into an IP address

3 private IP ranges:

10.0.0.0 – 10.255.255.255

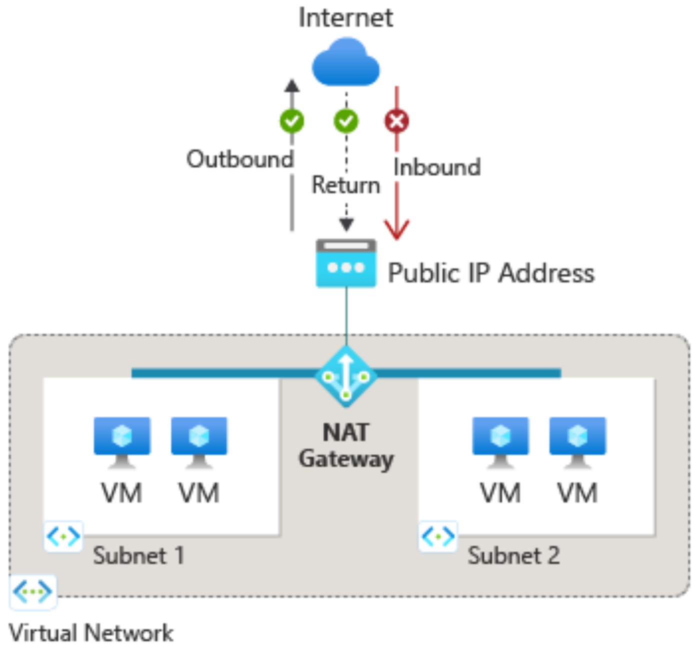
172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Every other IP address is deemed to be publicly accessible

E.g. the address 10.1.2.3 will only be accessible within our own network. The address 11.1.2.3 will be globally accessible.

Private services can be exposed through NAT (Network Address Translation) and port forwarding.



Networking primer

➡️ Incoming traffic / ingress

Everything reaching a certain service from outside.

E.g. users connecting to a Power BI dashboard is incoming traffic from the perspective of Power BI.

Protecting this is a safeguard for security failures on the authentication side.

Outgoing traffic / egress ➡️

Connections made from inside the network to the internet.

E.g. when you load data from a public CSV file, your Fabric instance makes an outgoing connection.

Protecting this is a safeguard to avoid data exfiltration.

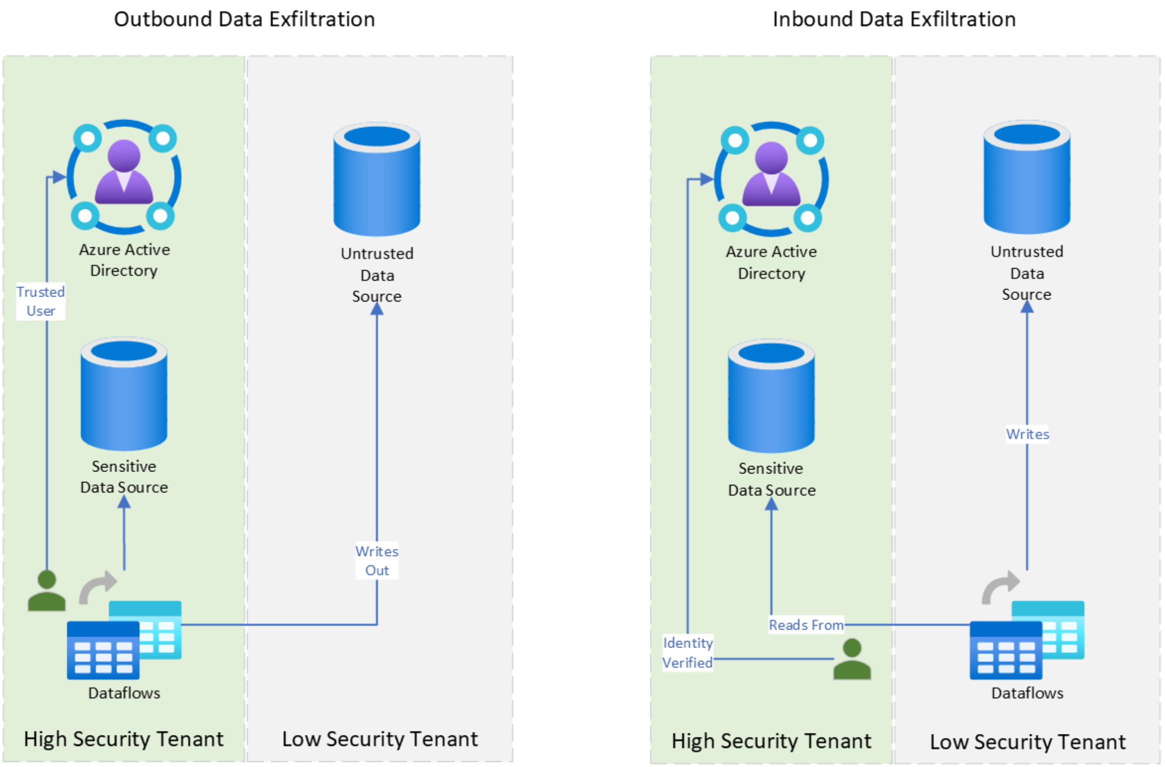
Data Exfiltration Protection (DEP)

Data exfiltration is unauthorized transfer of (sensitive) data from your environment to an unapproved entity.

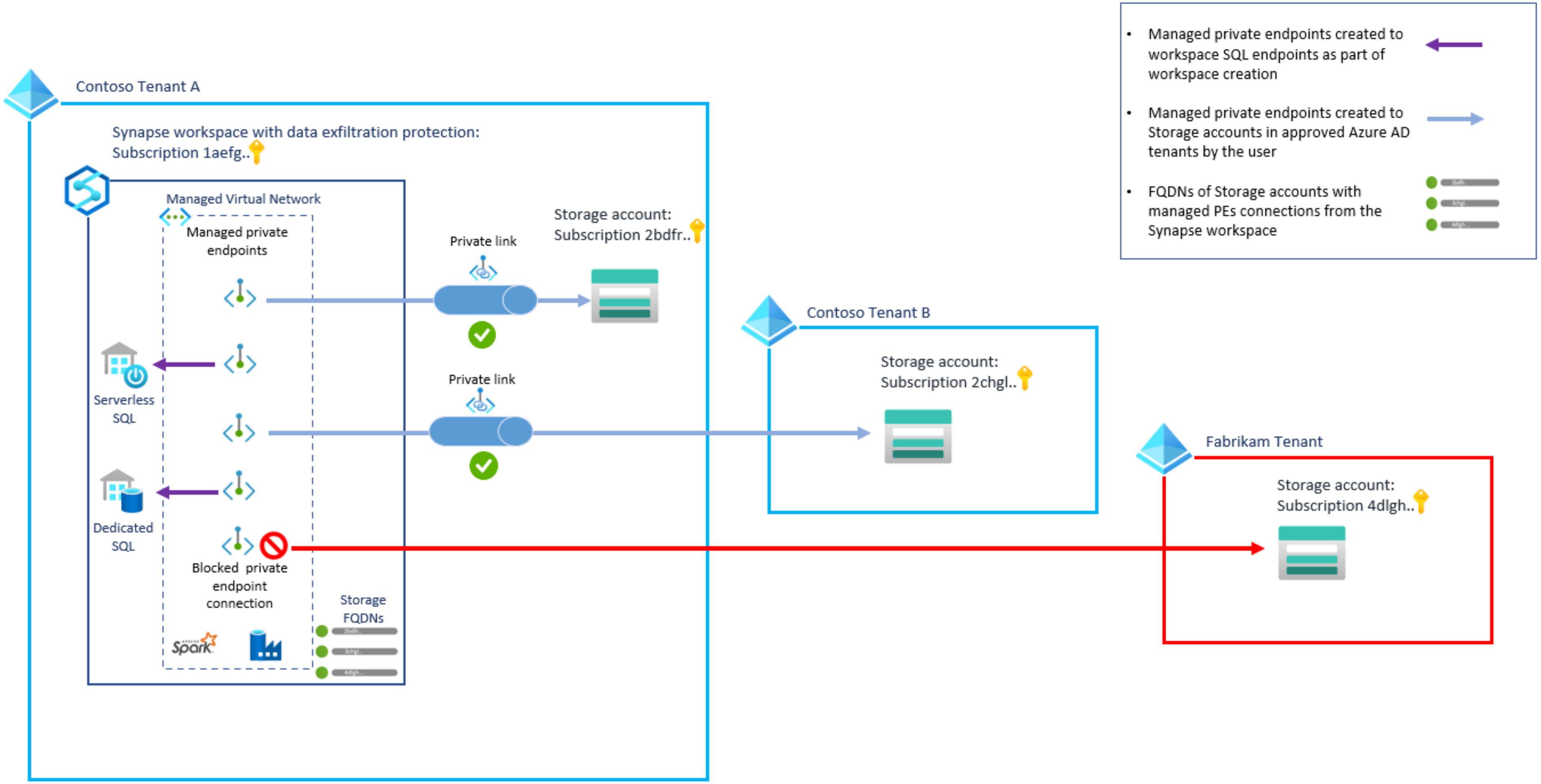
When a malicious user has gained access to your data, they usually want to copy/move your data to their own systems or make it publicly available.

DEP detects and monitors egress traffic to block any unauthorized movement of data.

Data Exfiltration Protection (DEP)



Data Exfiltration Protection (DEP)

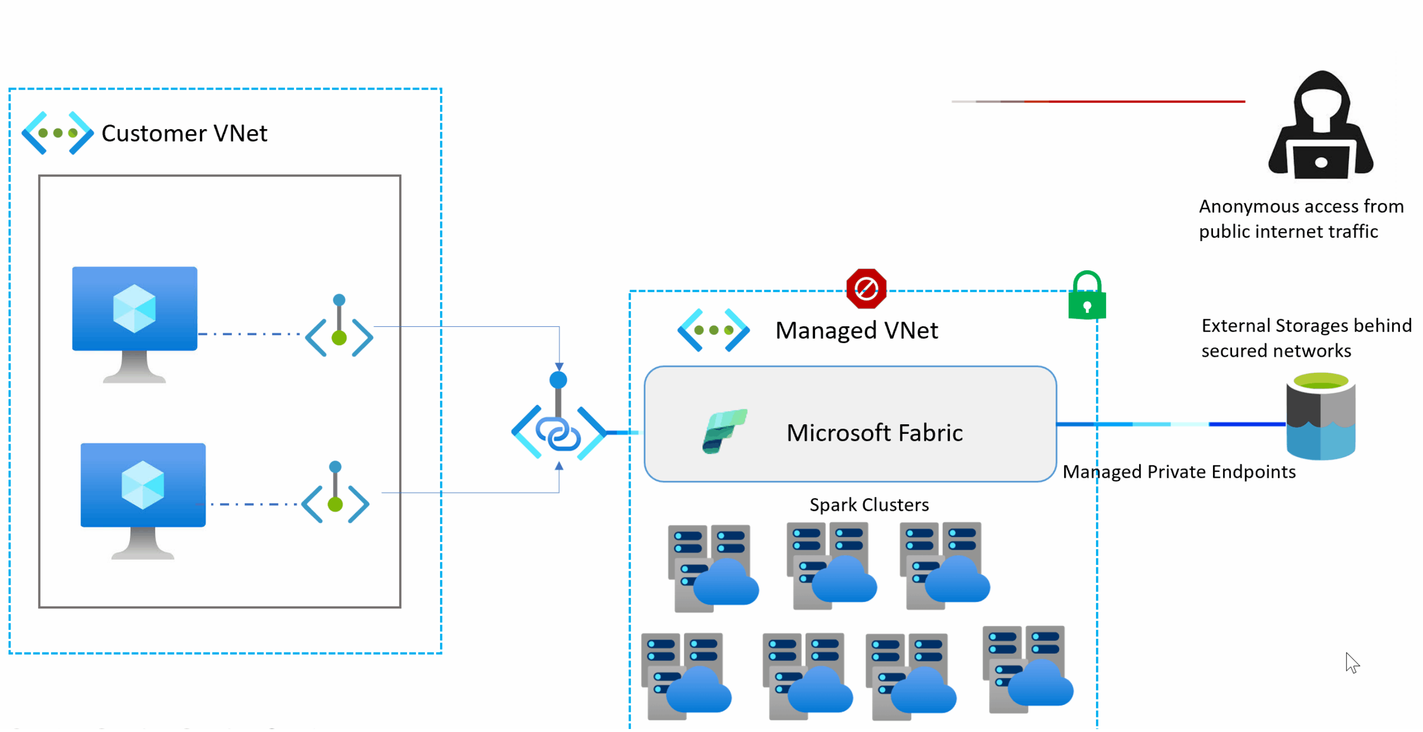


- Managed private endpoints created to workspace SQL endpoints as part of workspace creation
- Managed private endpoints created to Storage accounts in approved Azure AD tenants by the user
- FQDNs of Storage accounts with managed PEs connections from the Synapse workspace

Private networking in Fabric: incoming traffic

Default: public access 🔓

Tenant admins can enable private networking and disable public networking 🔐


Customer VNet
Anonymous access from public internet traffic
Managed VNet
External Storages behind secured networks
Microsoft Fabric
Managed Private Endpoints
Spark Clusters

Enabling private networking in Fabric

✅ Prerequisite: private network with DNS configured

1️⃣ Private Link Service

2️⃣ Provisioning Private Endpoints

3️⃣ Disabling public access

Private networking in Microsoft Fabric: outgoing traffic

Network traffic to storage accounts or SQL databases

⚠️ Comes with limitations for now

🔗 https://learn.microsoft.com/en-us/fabric/security/security-managed-private-endpoints-overview

Authentication & authorization

Microsoft Entra ID

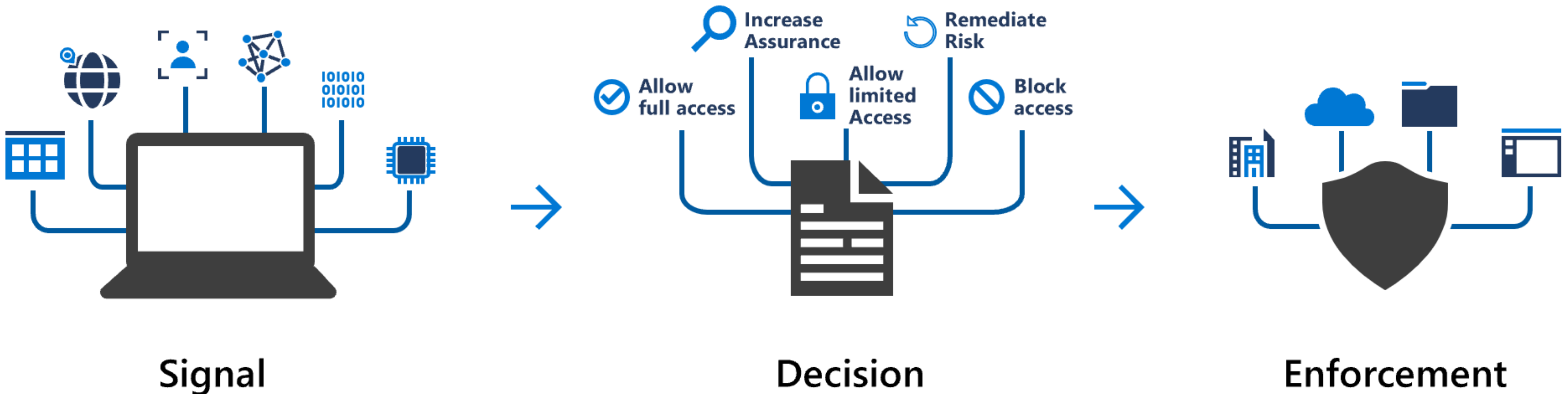
Leverage all features and functionalities of a proven system

👉 Assign permissions in Fabric to Entra ID Groups

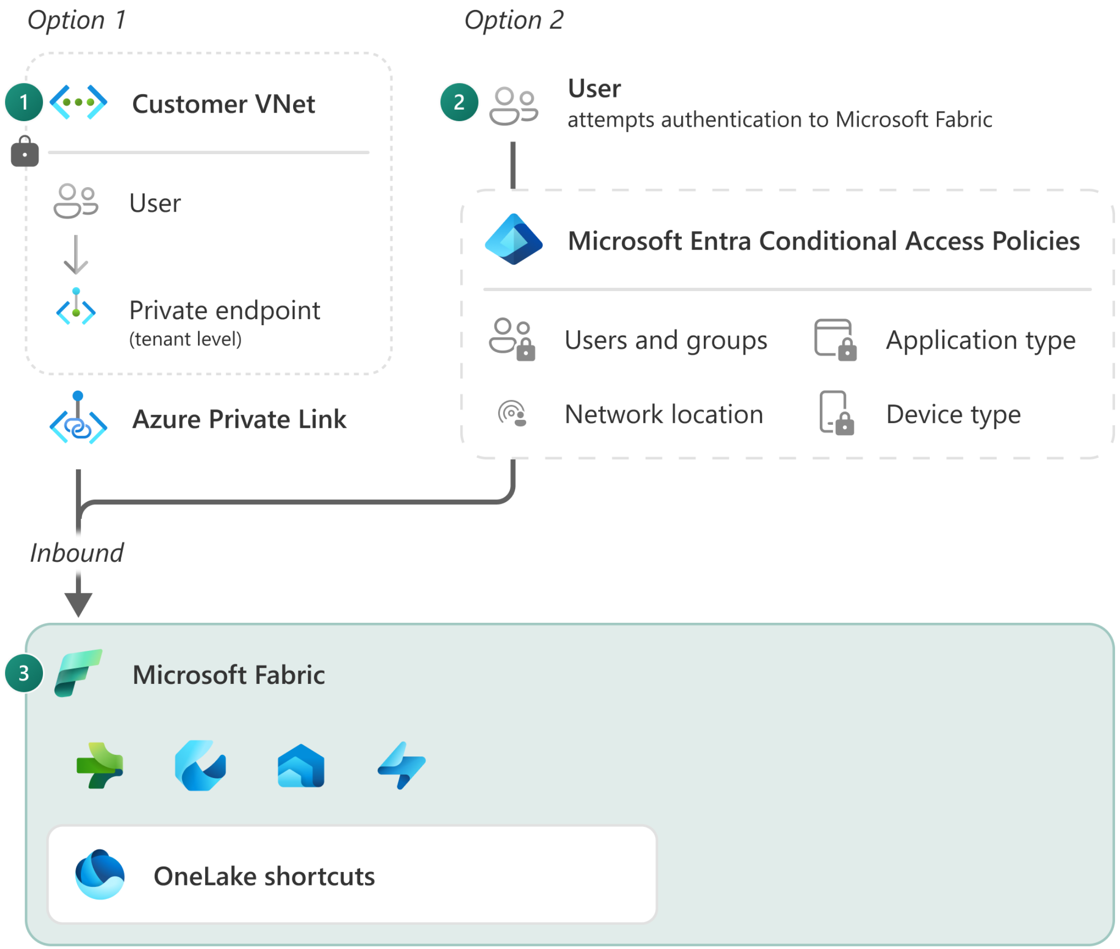
Microsoft Entra ID Conditional Access

Use signals to determine authentication process:

- E.g. users connected to wi-fi on premises can access without MFA and users connected abroad can only access with MFA



Multiple layers working together



Just-in-time access

Through Entra ID Privileged Identity Management (PIM)

Instead of providing access 24/7, only provide access when needed

💡 Could be a good way to protect sensitive data

Access limited in time

Users can be asked to provide a justification

Optionally let another user approve the access

Workspace Identity & Trusted Access

Avoid linking access to resources (e.g. Azure Storage Accounts used in Shortcuts) to individual users

❓ What if users leaves / account is compromised / …

Service principals are a common solution but still have certain risks:

⚠️ Client secret could be leaked

♻️ Rotation of client secrets is often overlooked / prone to secret leakage

In the Entra ID world, Managed Identities are the solution. In Fabric: **Workspace Identity**

Fabric access controls

Tenant-level: who can use any Fabric feature

Workspace-level: admin/member/contributor/viewer

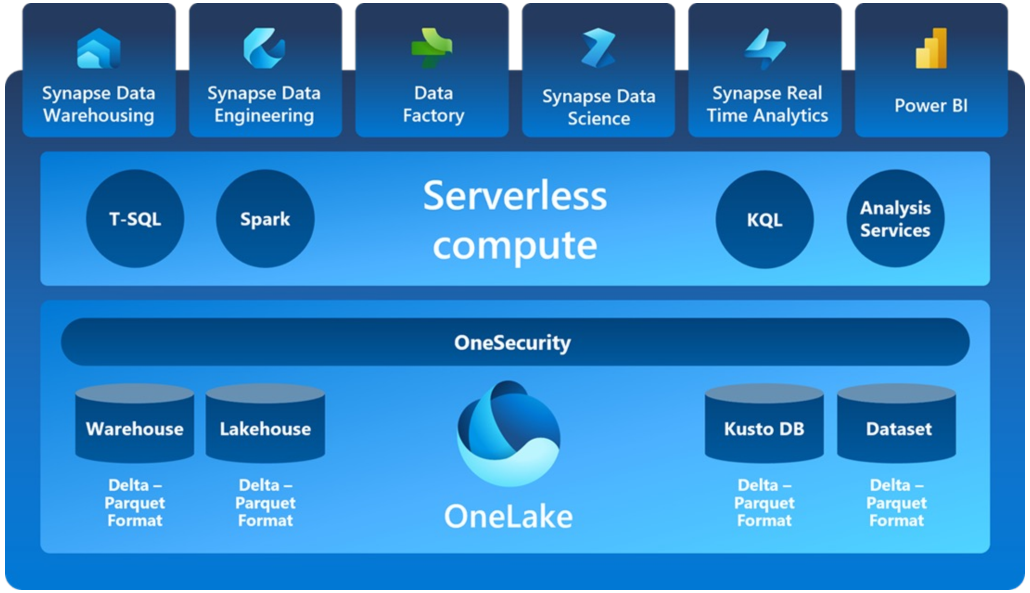
Shared items: single item without Workspace access

read/edit/share/read all with SQL/read all with Spark/build/execute

Row-level security (**RLS**) / column-level security (**CLS**) / object-level security (**OLS**)

Data source **SSO** vs. fixed credential

Fabric endpoints



Fabric UI

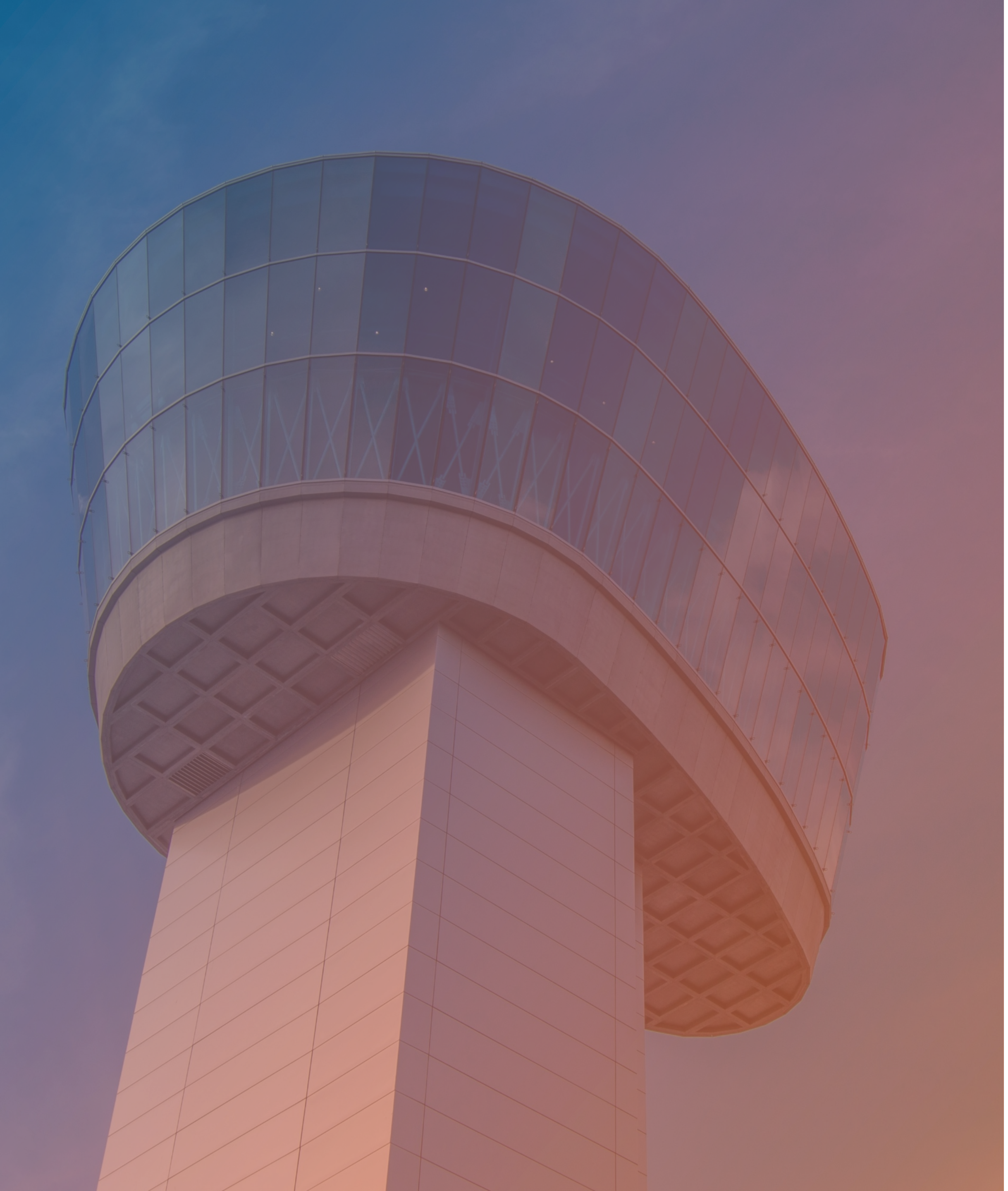
Power BI reports

SQL queries through SQL Analytics Endpoint / Data Warehouse via external tools (SSMS, Azure Data Studio, dbt, Python, ...)

OneLake APIs

Fabric APIs & connectors (e.g. Excel)

...



Monitoring

Power BI audit log

Azure Firewall / 3rd party firewall

Azure PIM access request (with justifications and/or approvals)

Microsoft Purview

Disaster recovery & resiliency

Multiple aspects

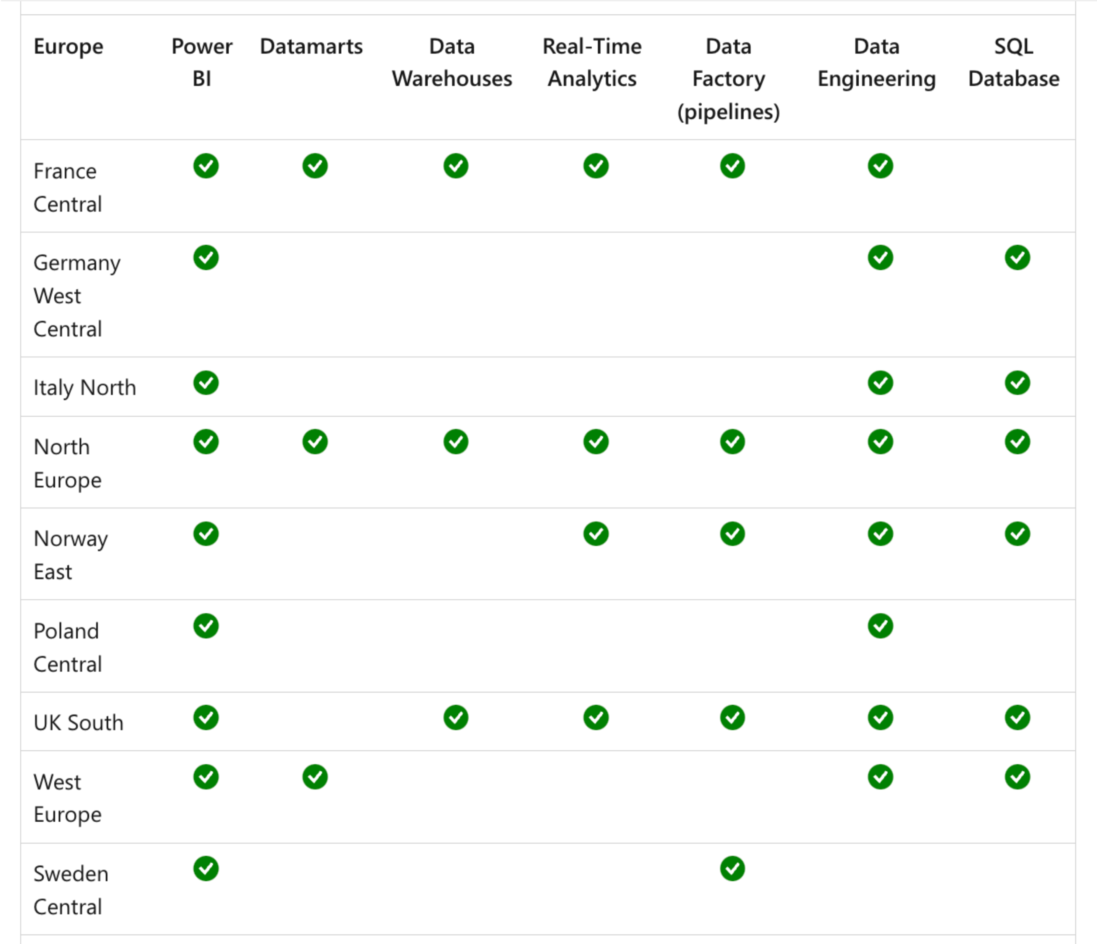
Compute access:

- Less critical
  - E.g. when disaster strikes, maybe a delay on intensive data pipelines is acceptable
- Lakehouses, Data Warehouses, Reports
- No “state” in this layer, so in worst case no data can be processed/accessed

Data access:

- OneLake access
- Storage layer is critical as the worst case is data loss
- OneLake is the ZRS version of ADLS, you might want to check your Shortcut sources as well

Disaster recovery & resiliency: Availability Zones



Europe	Power BI	Datamarts	Data Warehouses	Real-Time Analytics	Data Factory (pipelines)	Data Engineering	SQL Database
France Central	✓	✓	✓	✓	✓	✓	
Germany West Central	✓					✓	✓
Italy North	✓					✓	✓
North Europe	✓	✓	✓	✓	✓	✓	✓
Norway East	✓			✓	✓	✓	✓
Poland Central	✓					✓	
UK South	✓		✓	✓	✓	✓	✓
West Europe	✓	✓				✓	✓
Sweden Central	✓				✓		

Recap

Startup requirements <> enterprise requirements

↗️ Security controls are easily manageable when starting small but can become a challenge at scale

Build security in isolated layers

↗️ Defense in Depth, Least Privilege, Zero Trust, ...

Starting points / recommendations

👉 Assign permissions in Fabric to Entra ID Groups

👉 Private networking

👉 Privileged Identity Management

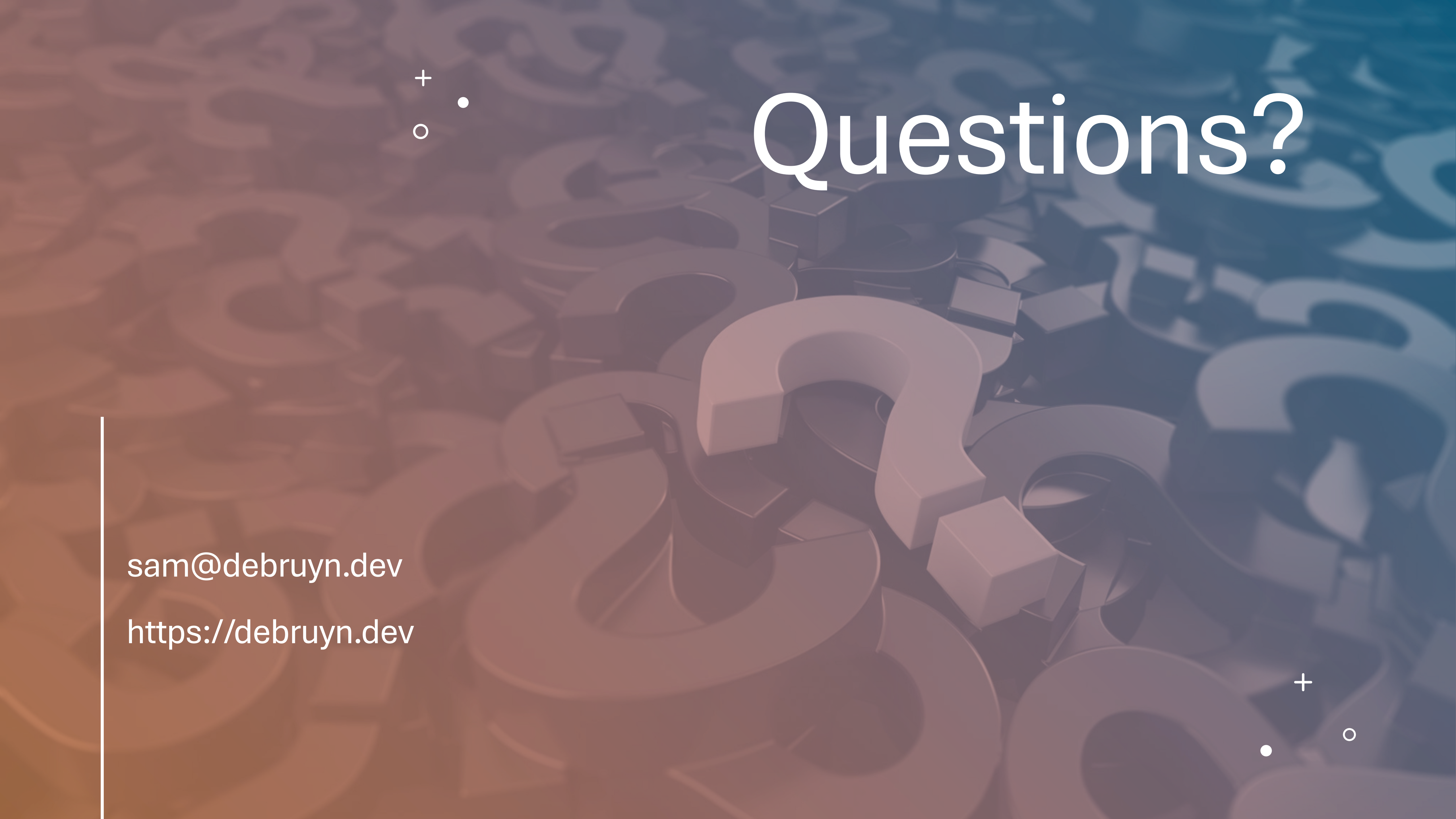
👉 Entra ID Conditional Access

👉 Monitoring through Microsoft Purview

Slides

Slides available at

https://debruyn.dev/ff25



Questions?

sam@debruyn.dev

https://debruyn.dev