Session Feedback

SQL KONFERENZ 2025



Securing and Automating Your Fabric Real-Time Intelligence Assets

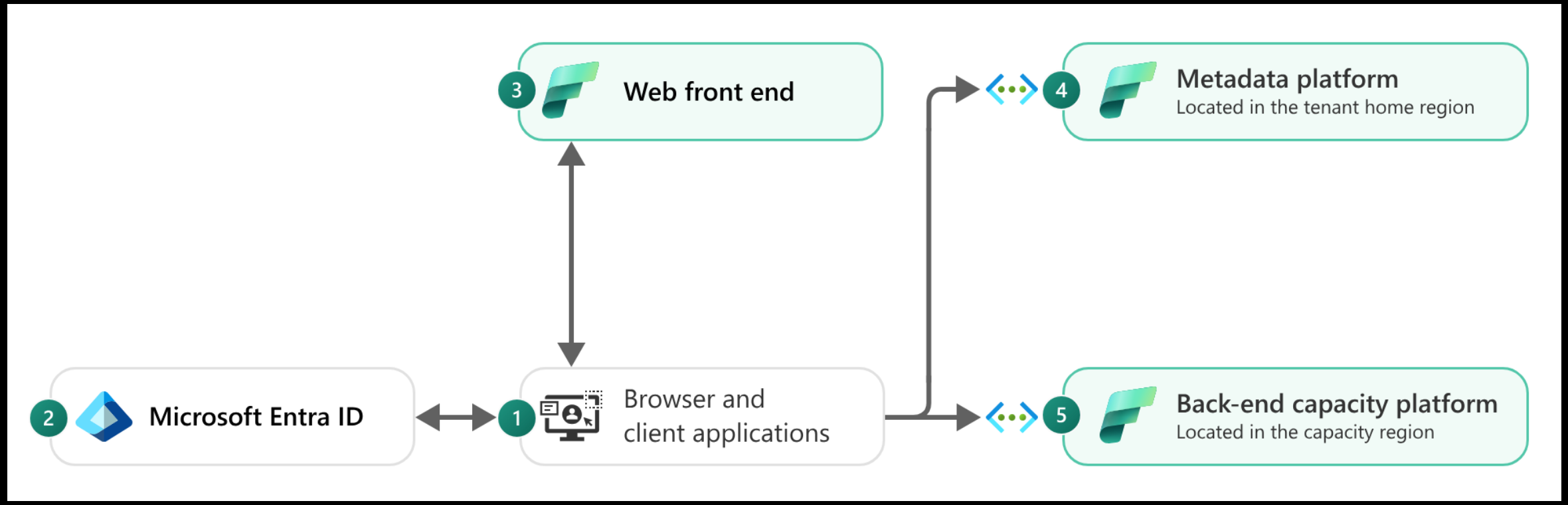
Johan Ludvig Brattås & Rune Ovlien Rakeie

Agenda

- Automation
  - Fabric REST API
  - What is IaC
  - Automation options
- Security
  - Authentication
  - Networking
  - Permission model
  - Compute engine



Fabric architecture



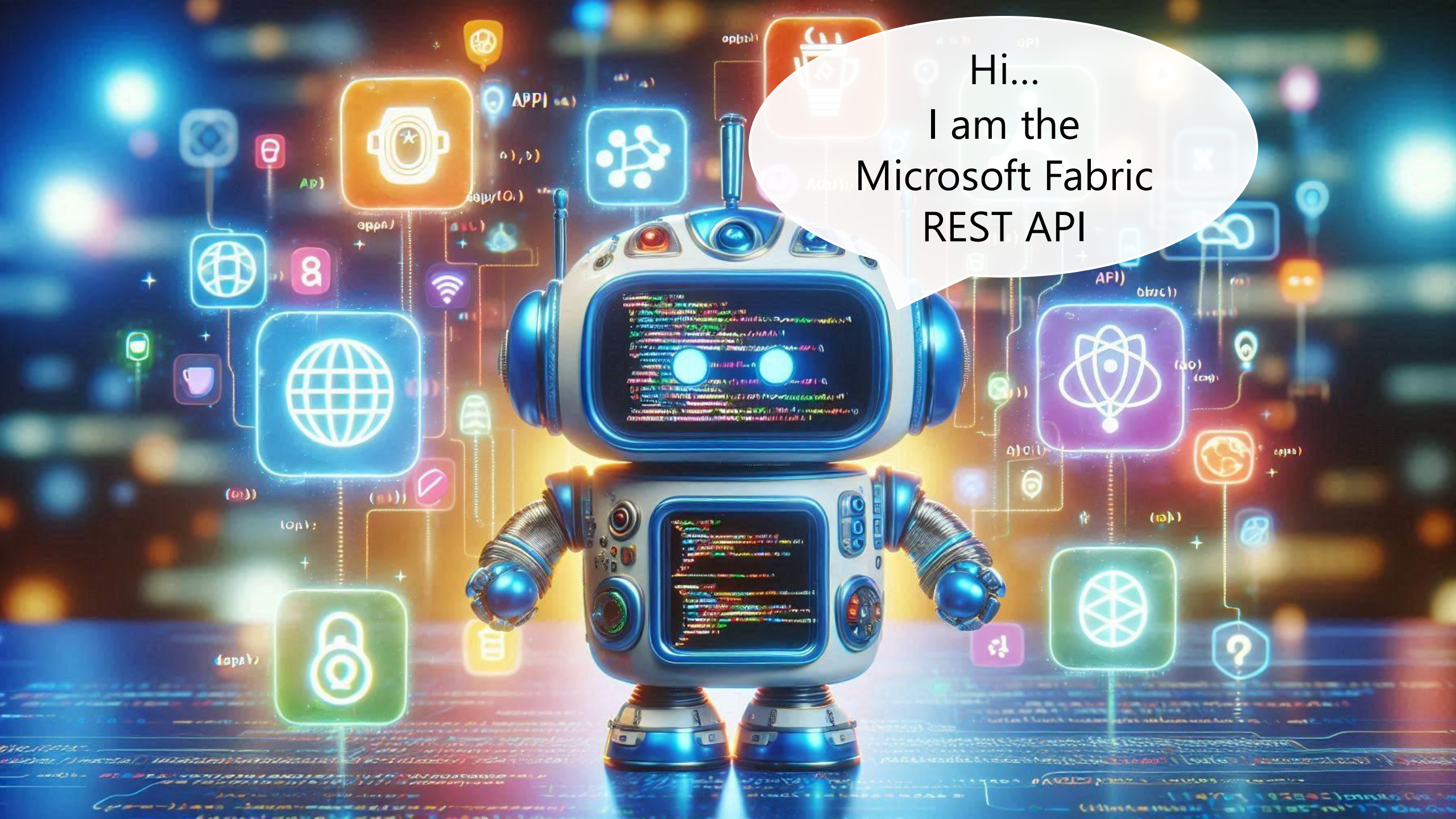
SQL KONFERENZ 2025



Automation

- The core component: APIs
- Infrastructure as Code (IaC)


Preparation
for
Demo


Hi...
I am the
Microsoft Fabric
REST API

What is a REST API anyway?

- **RE**presentational **S**tate **T**ransfer **API**
- **Client-server architecture**
  - Client and server operate independently
- **Stateless**
  - Contains all data necessary to process request
- **Uniform interface**
  - Uses standard HTTP methods (GET, POST, PUT, PATCH, DELETE)
- **Resource based**
  - Everything is a resource, identified by a unique URL



SQL KONFERENZ 2025



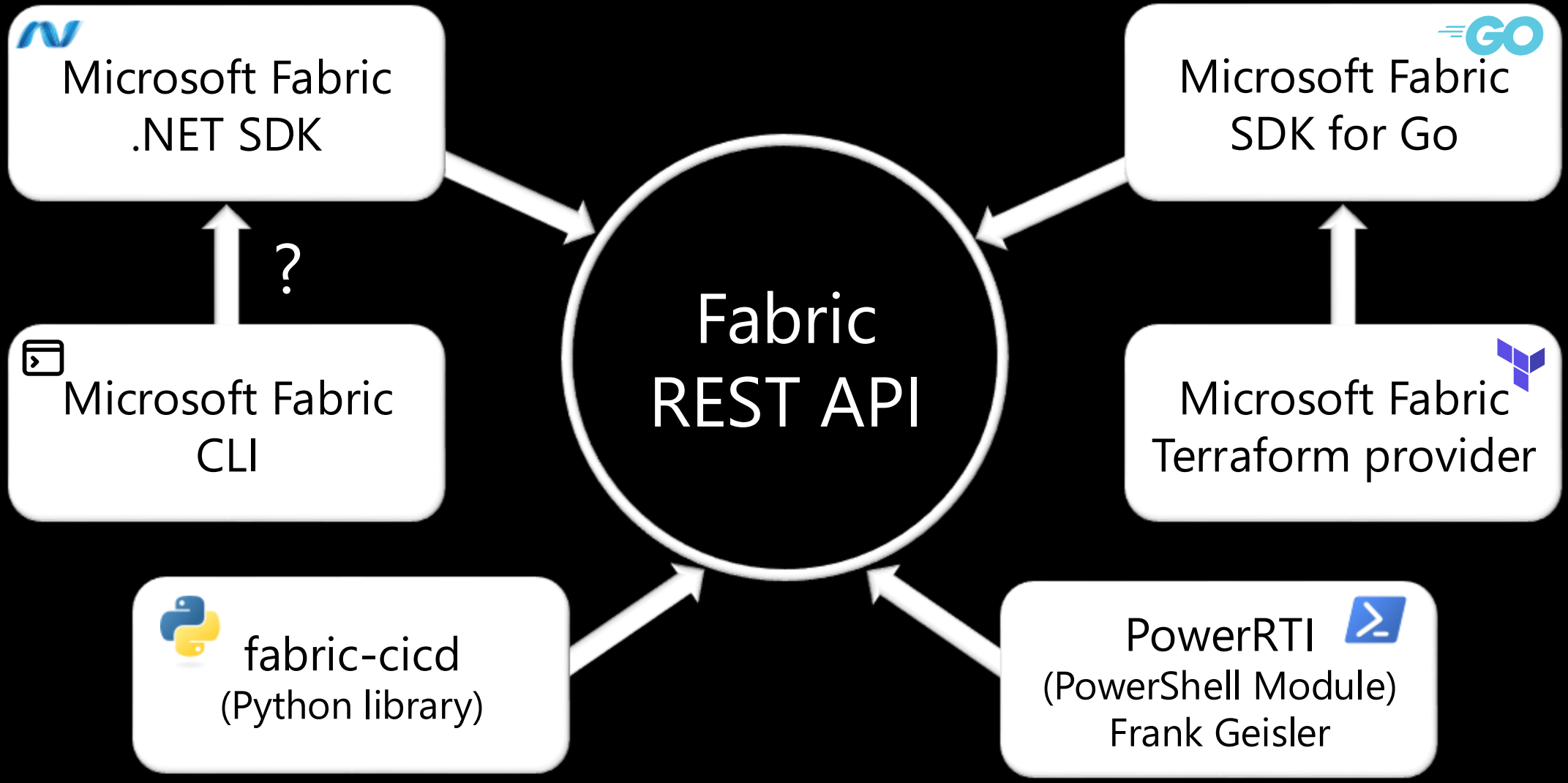
Real-time Intelligence

Fabric REST API supports these items:

- Eventhouse
- KQL Database
- KQL Queryset
- Eventstreams
- Dashboards
- Reflex *(only interactive login)*



Tools and libraries



What is Infrastructure-as-Code?



Manage and provision computing infrastructure through machine-readable configuration files

IaC can be:

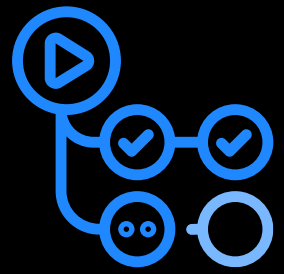
- Versioned
- Automated

Why is IaC important?



Consistency

Identical
Every time



Automation

Full process
Reduce risk
Speed up



Version Control

Track
Revert
Collaborate



Scalability

Easy change
Re-deploy

Icons: https://flaticon.com

IaC - Declarative vs Imperative



Imperative

- Exact instructions
- Step-by-Step
- Specify what to do
- Traditional programming



Declarative

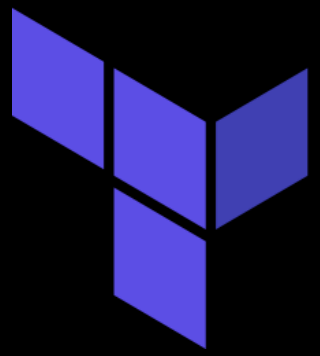
- Declare the desired outcome
- The tool figures out the rest

Icons: https://flaticon.com

PowerShell

- Imperative approach
- Powerful scripting language
- No official PowerShell module yet
- Use the REST APIs and regular az-modules
- For RTI -> module PowerRTI
  - Maintained by Frank Geisler





HashiCorp

Terraform

+ Declarative approach
+ First release July 2014
+ Unified interface across providers
+ Powerful state & change management
+ Modular testing capabilities
+ Downloaded several 100 millions of times
+ 4600 providers + 18000 published modules

- Changed license from MPL 2.0 to BUSL 1.1
- Hashicorp acquired by IBM recently

OpenTofu



- Open Source 🙌🏻
- Very similar feature-wise to Terraform
- Aim of maintaining feature parity with Terraform

What about Bicep?

- Bicep generates ARM
- Does not work with Fabric APIs
- Never will (in current form)

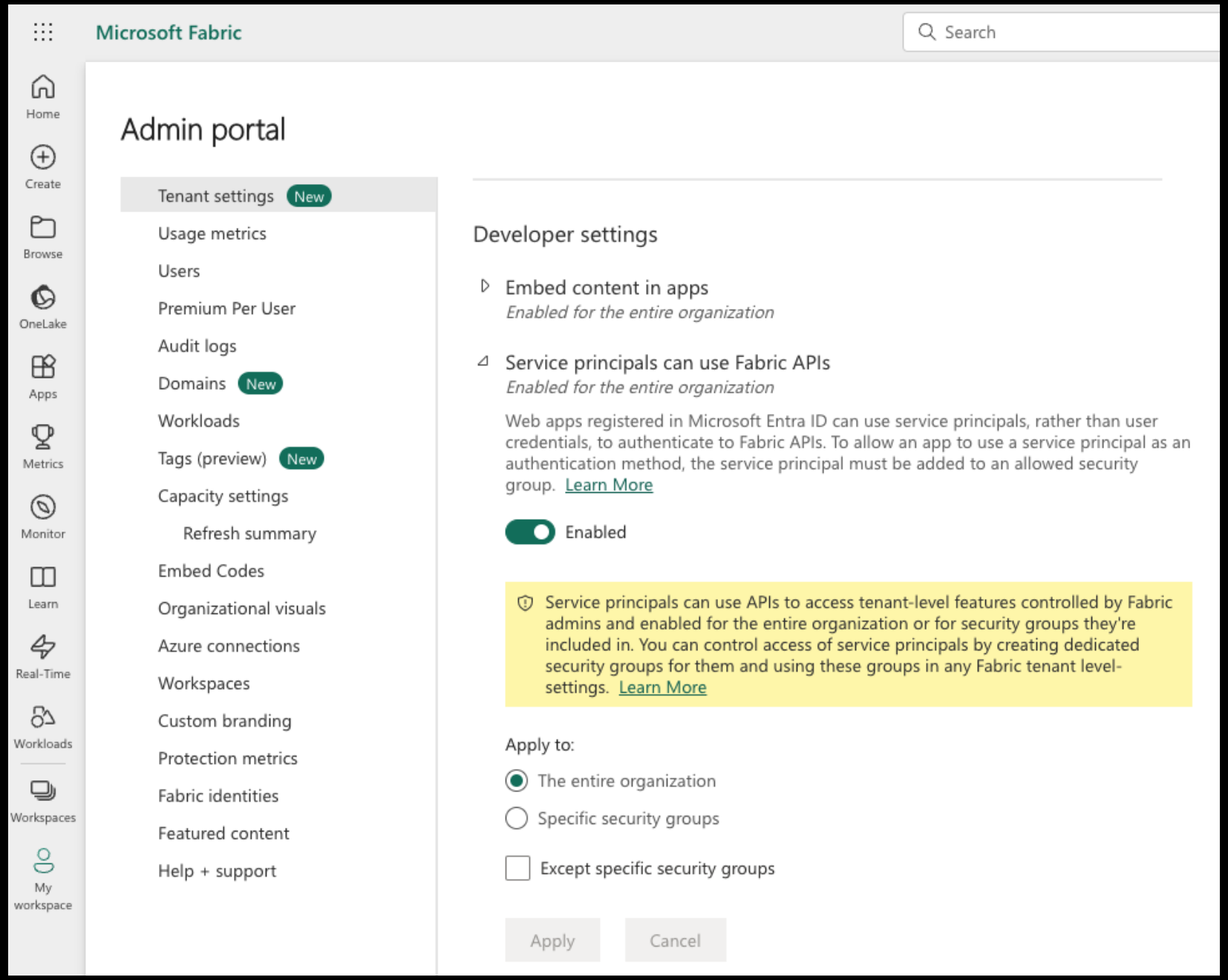


...however, you can provision Fabric capacities

Authentication for Fabric REST API

- User credentials (interactive)
- Service Principal
  - with Client Certificate
  - with Client Secret
  - Managed Identity (MSI)
  - with OpenID Connect (OIDC) aka Workload Identity Federation




Microsoft Fabric
Search
Home
Create
Browse
OneLake
Apps
Metrics
Monitor
Learn
Real-Time
Workloads
Workspaces
My workspace
Admin portal
Tenant settings New
Usage metrics
Users
Premium Per User
Audit logs
Domains New
Workloads
Tags (preview) New
Capacity settings
Refresh summary
Embed Codes
Organizational visuals
Azure connections
Workspaces
Custom branding
Protection metrics
Fabric identities
Featured content
Help + support
Developer settings
Embed content in apps
Enabled for the entire organization
Service principals can use Fabric APIs
Enabled for the entire organization
Web apps registered in Microsoft Entra ID can use service principals, rather than user credentials, to authenticate to Fabric APIs. To allow an app to use a service principal as an authentication method, the service principal must be added to an allowed security group. Learn More
Enabled
Service principals can use APIs to access tenant-level features controlled by Fabric admins and enabled for the entire organization or for security groups they're included in. You can control access of service principals by creating dedicated security groups for them and using these groups in any Fabric tenant level-settings. Learn More
Apply to:
The entire organization
Specific security groups
Except specific security groups
Apply
Cancel


Demo

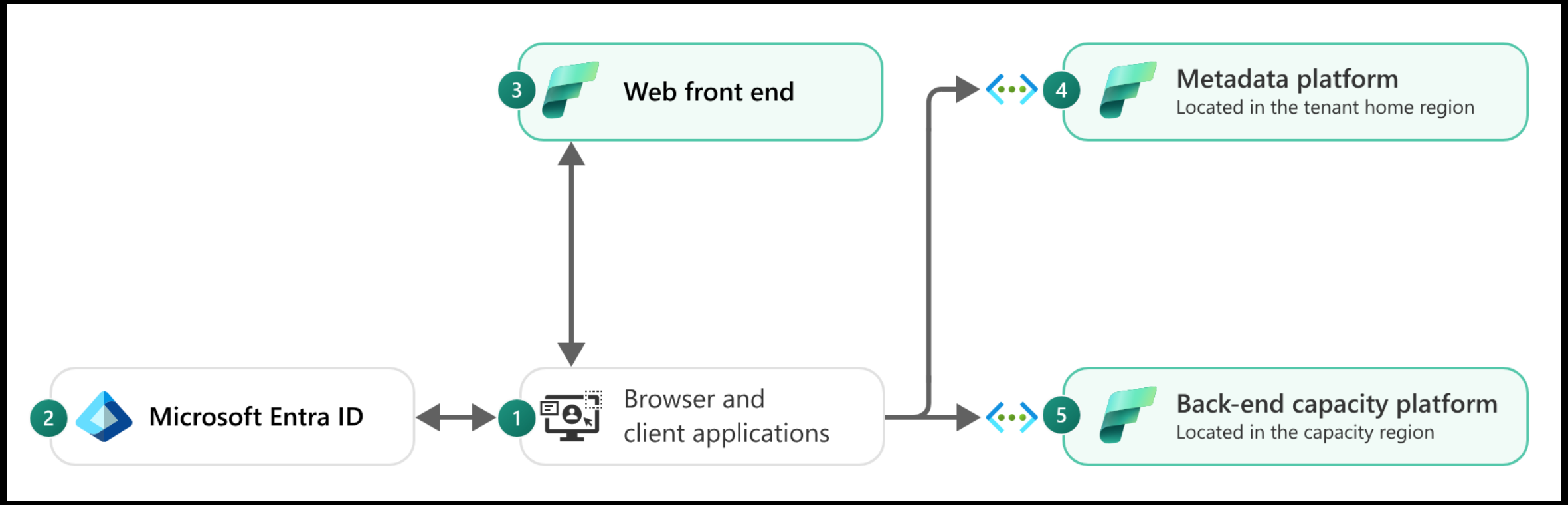
SQL
KONFERENZ
2025



Security

- Authentication
- Networking
- Permission model
- Compute engine

Fabric Security architecture



Authentication

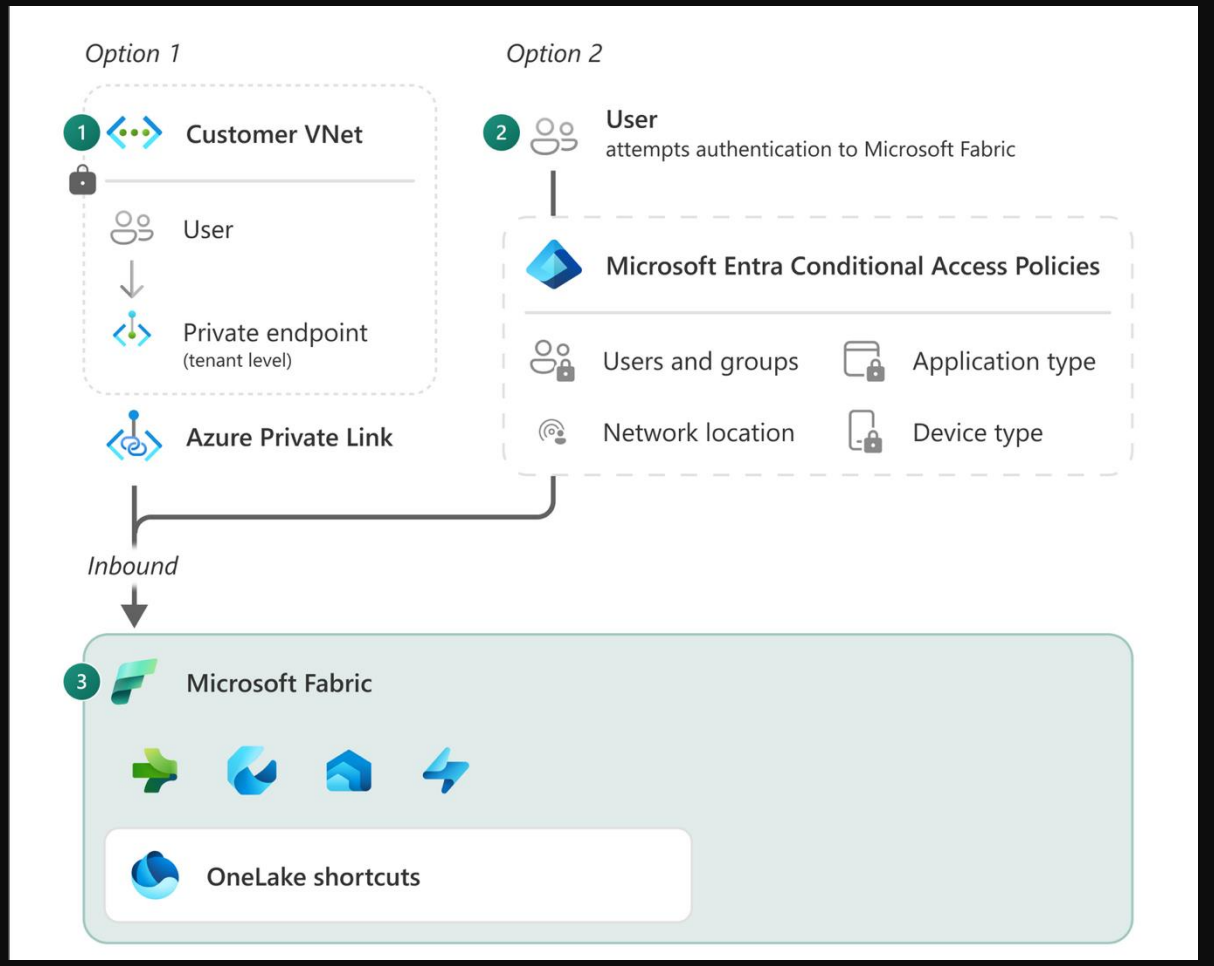
- Handled by Entra ID (AAD)
- Security groups
- SSO with user name (e-mail)



Networking

Inbound

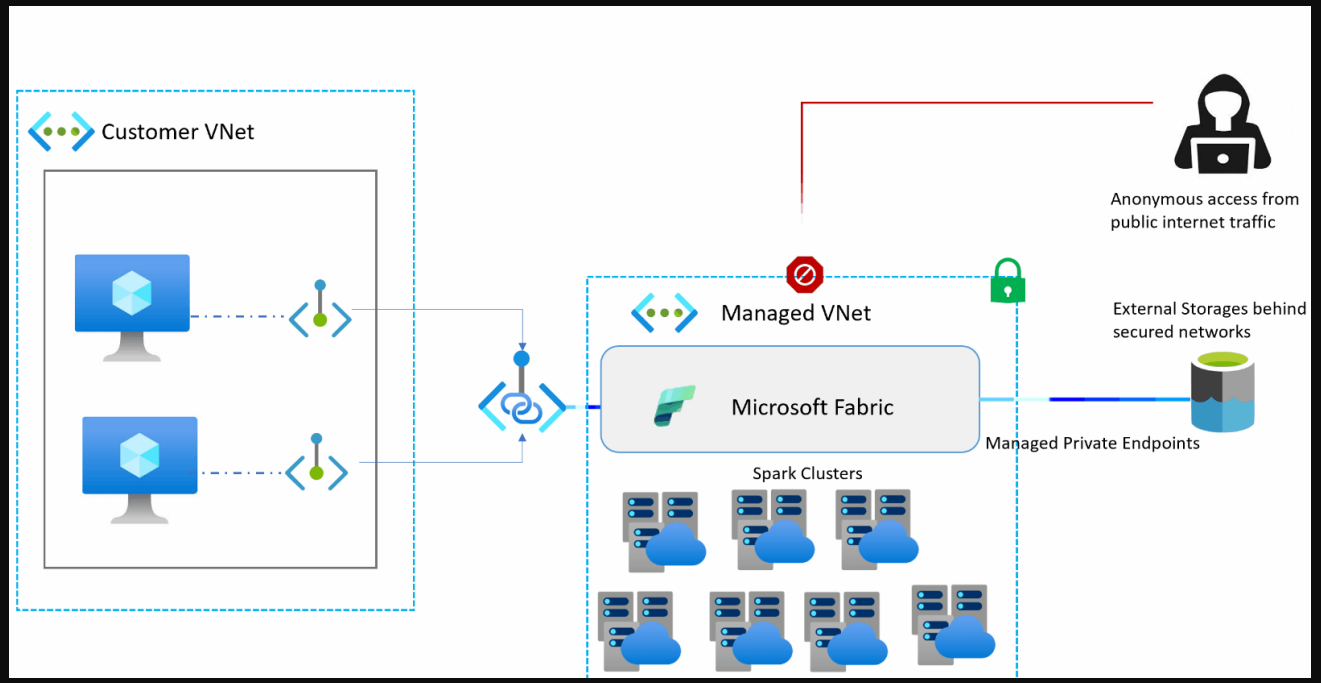
- Private link
- Conditonal Access (Entra)
- On-prem Data Gateways



Networking

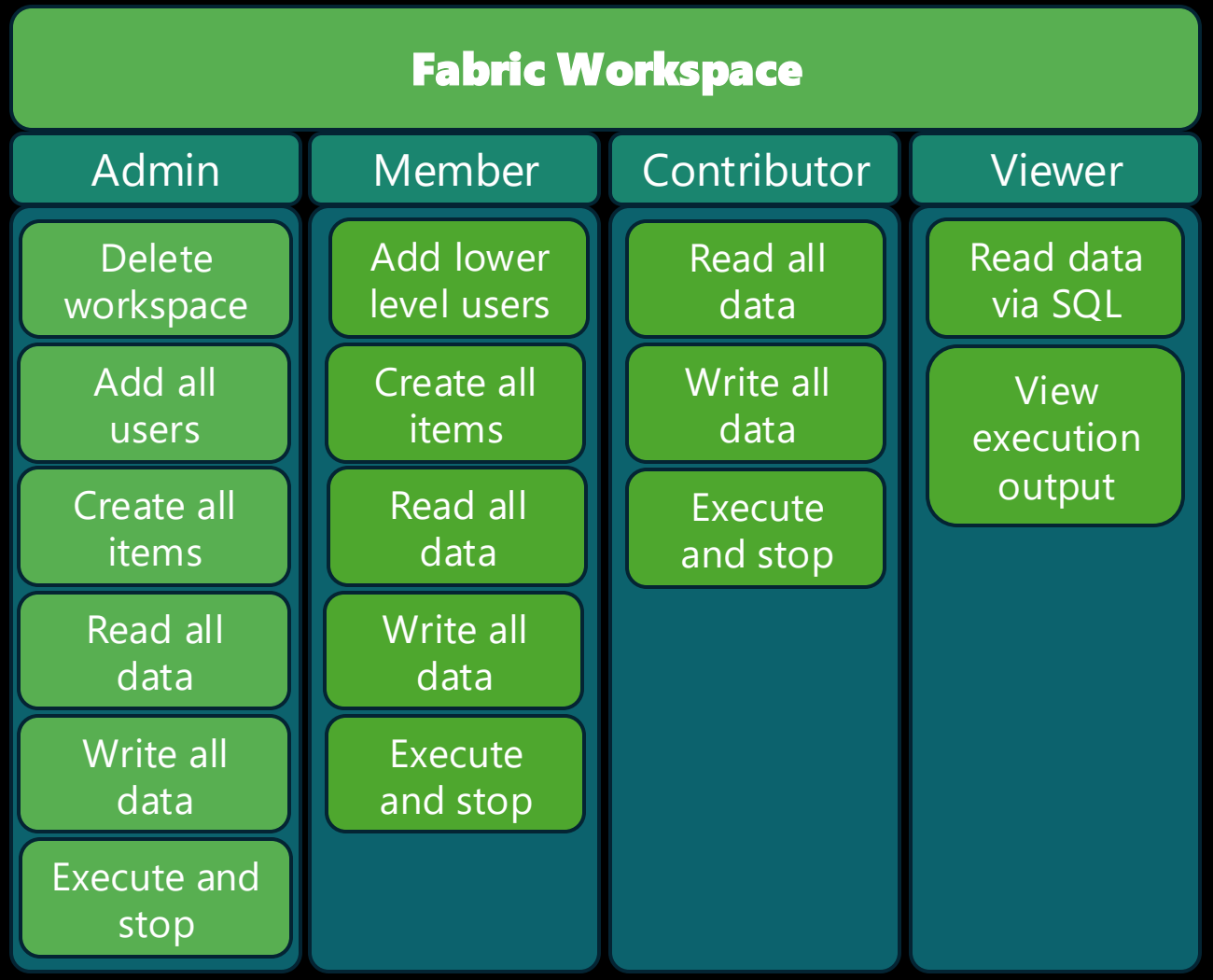
Outbound

- Trusted Workspace Access
- Managed VNETs
- Managed Private Endpoints
  - Only for Eventstreams
  - Only to Event Hubs and IoT Hubs



Permission Model

- It all starts with the Workspace



Permission Model

- Additional roles
  - Unrestricted viewer
  - Ingestor
  - Monitor

- Workspace Identity



Compute Engine (RTI)

- KQL
  - User and application authentication
  - RBAC authorization
  - Object permissions
  - Restricted View
  - Row level security




Demo





Thank you!



Session Feedback

Rune Ovlien Rakeie

Principal Cloud Architect
Tietoevry

in • /runeovlienrakeie

• @datarune.online

Johan Ludvig Brattås

Director
Deloitte

in • /johanludvig

• @sqlclause.online