INSPARK

Feedback

Building a Fortress of Your Fabric Environment:

Best Practices for Data Engineers

Innovate to Accelerate



24-01-2024 Erwin de Kreuk Data Community Austria

INSPARK

We Are InSpark

"We help organizations accelerating their digital transformation with impactful Microsoft solutions & expertise"

THANK YOU

Data Community Austria Day 2025

Awesome Partner

Microsoft

Platinum

redgate

ACP IT for innovators.

Gold

b.telligent
smart data. smart decisions.

Lucient

Bronze

Tabular Editor

paiqo
The Platform & AI Company

Power BI Camp
www.linearis.at



INSPARK


Microsoft Defender
Microsoft Purview
Microsoft Sentinel
Microsoft Priva
Microsoft Entra
Microsoft Intune
Threat Protection & Cloud Security
Data Security, Governance, Compliance & Privacy
Identity & Management

INSPARK

Erwin de Kreuk

- Principal Consultant
- Lead Data & AI InSpark

Let's connect



@erwindekreuk

linkedin.com/in/erwindekreuk

erwindekreuk.com

github.com/edkreuk

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

MVP Microsoft® Most Valuable Professional

Objectives



- Microsoft Fabric
- Challenges
- Entra ID
- Inbound / 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

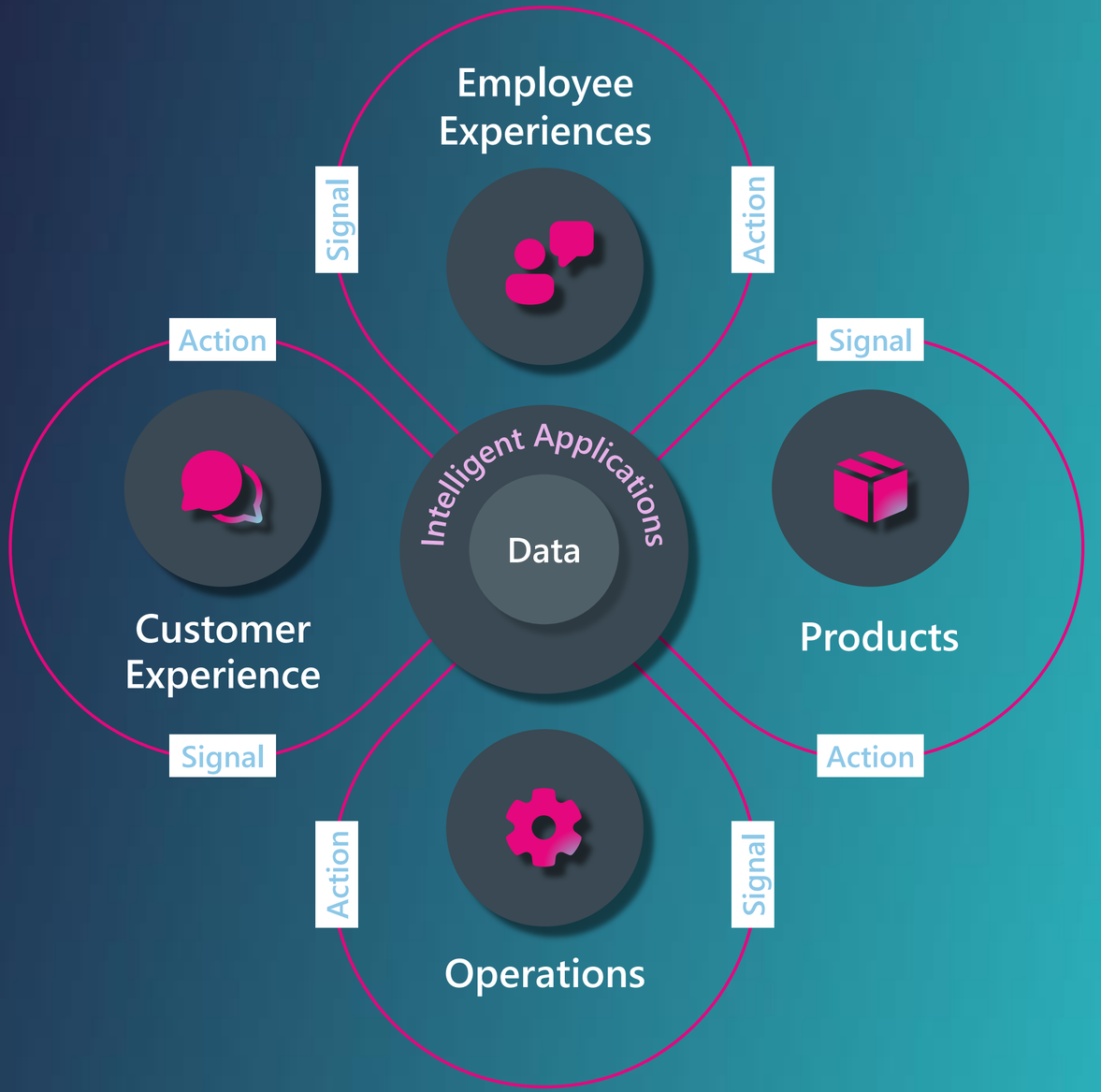


A world awash with data…

Data is the oxygen of 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

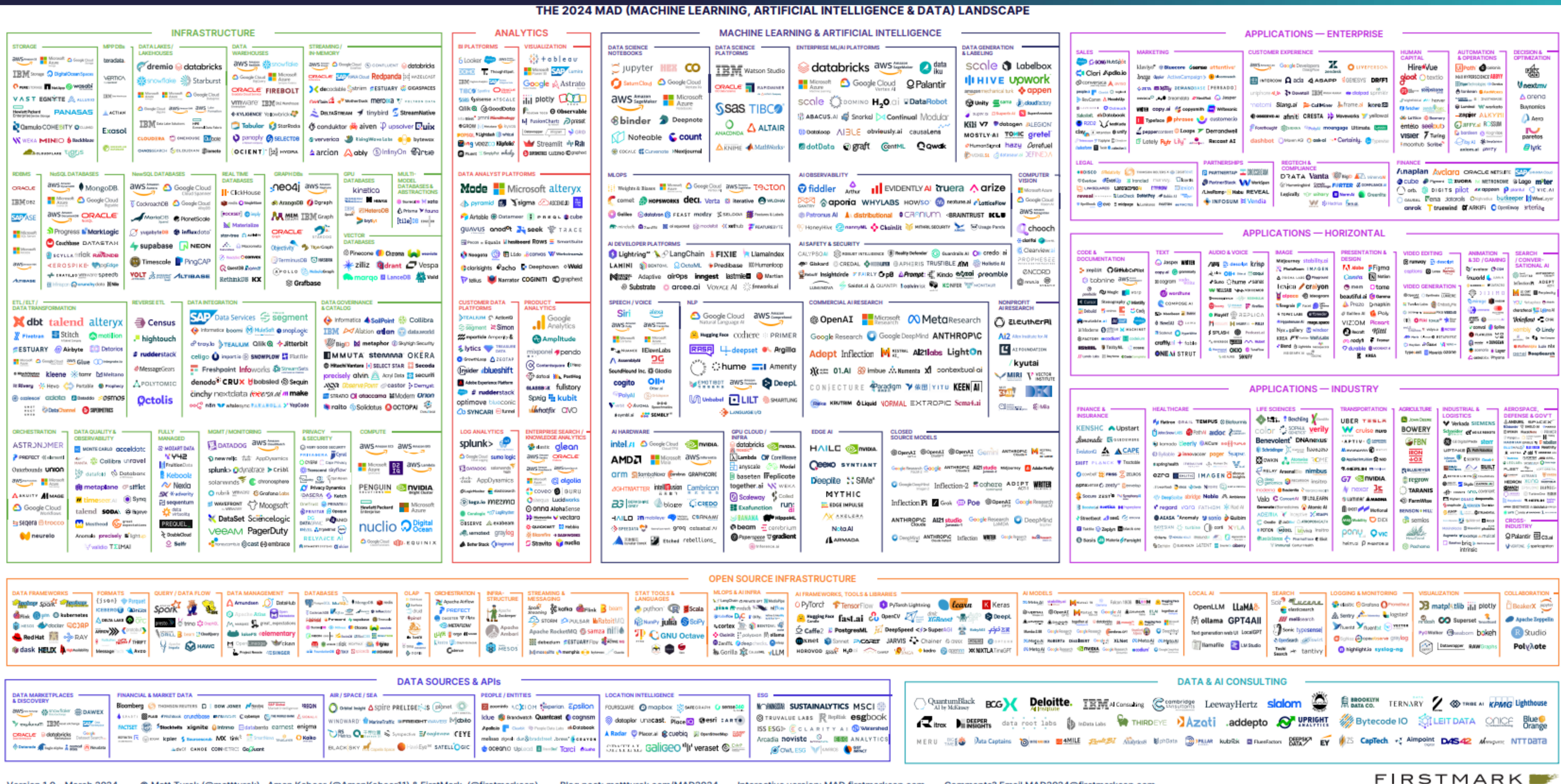


Today’s data value creation challenges

- Siloed systems and data
- Fragmented toolset, Platforms requiring advanced skills
- Costly integration and ongoing maintenance
- Proprietary Platform, Vendor Lock in
- Infrastructure not scalable as business grows
- Gaining BI adoption to streamline data sharing, collaboration
- Data and security risks, Governance & Compliance

How do you translate data into competitive advantage

The 2024 ML, AI, and Data Landscape



Unify,

I am the Chief Information Officer and don’t want to be the Chief Integration Officer. Help me govern and secure my data estate.”

Every CIO, Every Enterprise



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

Complete Analytics Platform

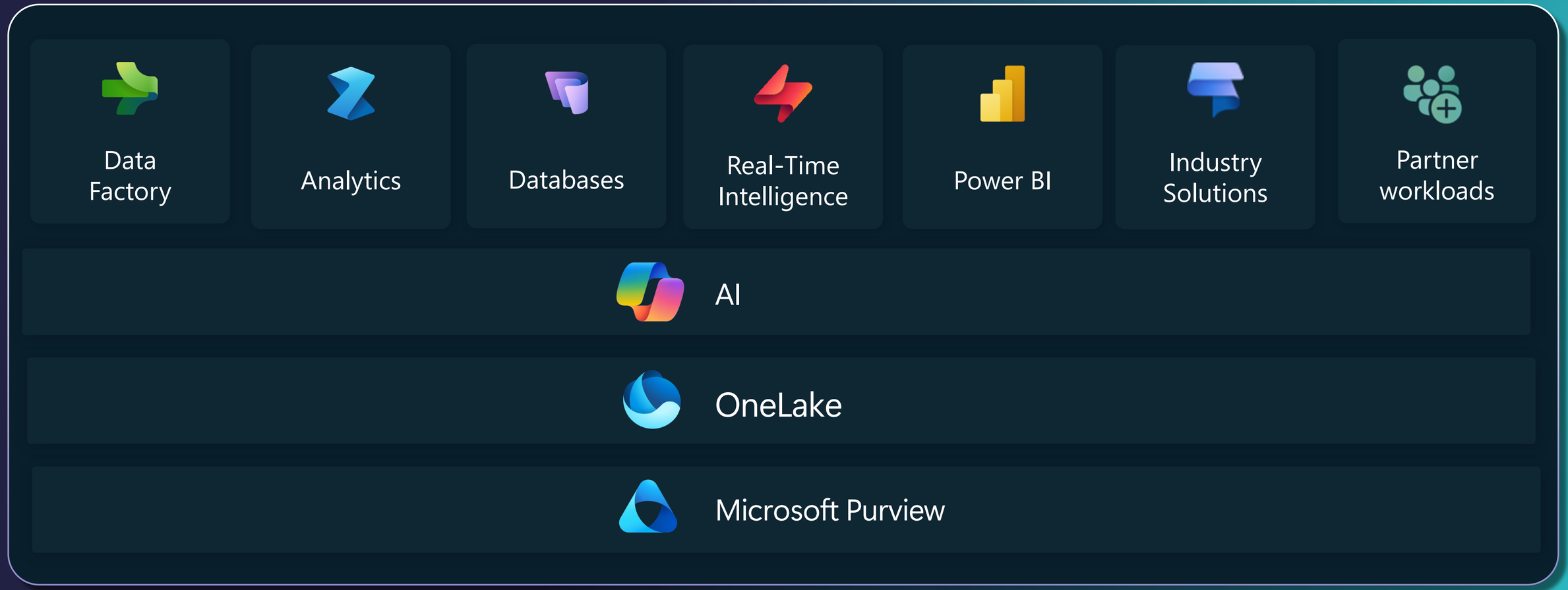
Lake Centric and Open

Empower Every Business User

AI Powered

Microsoft Fabric

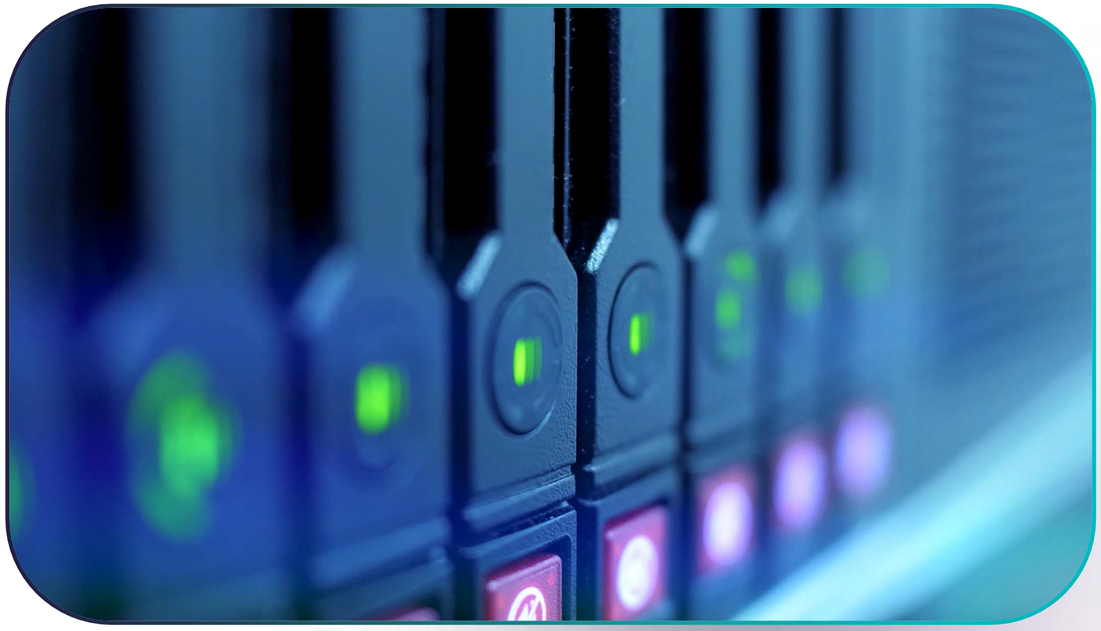
The unified data platform for AI transformation



INSPARK

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.



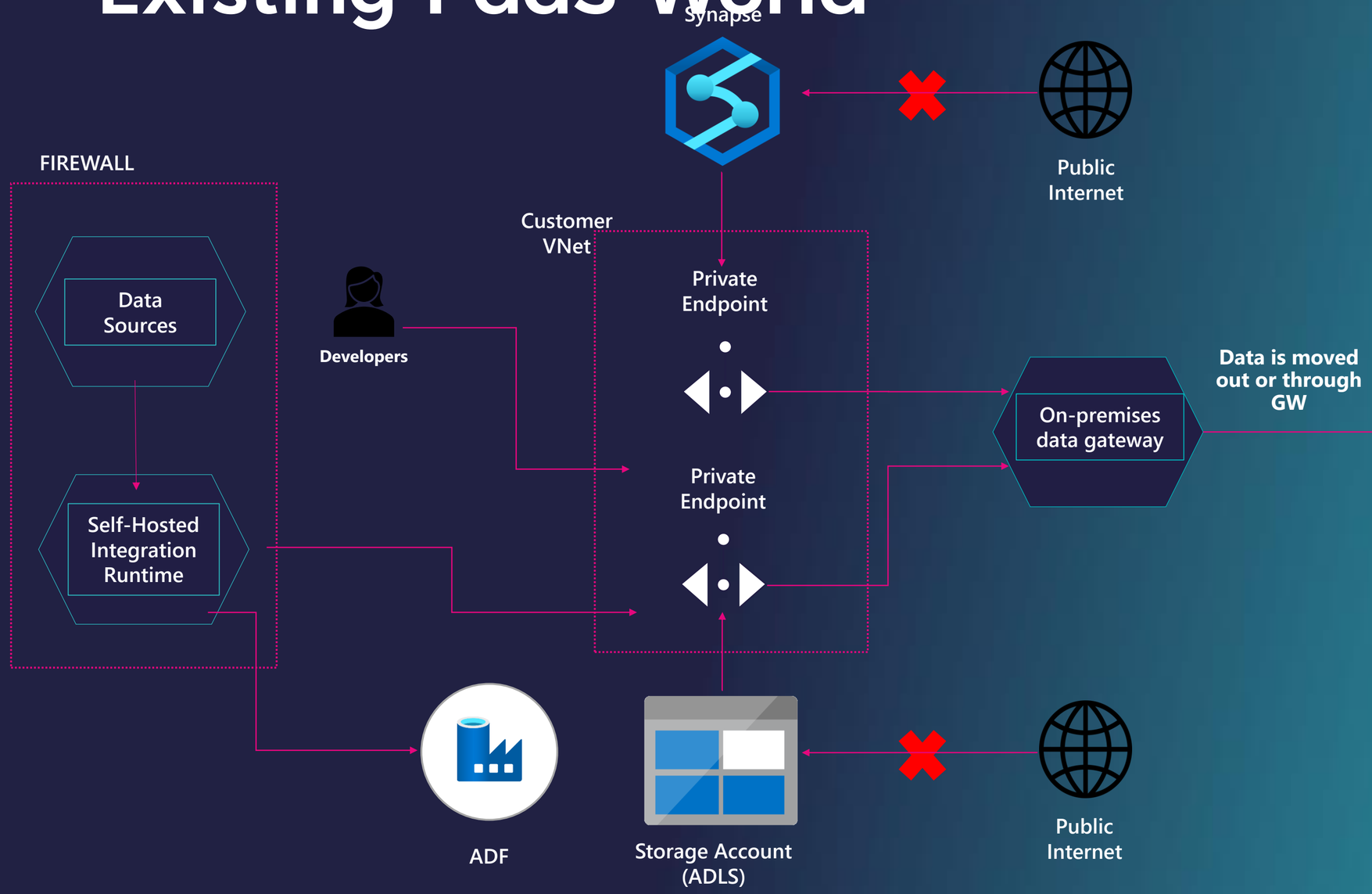
INSPARK

Common network security requirements

- Need to be able to connect to data inside a firewall\private link from Fabric (outbound).
- Inbound protection (restrict inbound by network location).
- More stringent customers (FSI\HLS):
  - Traffic needs to be private (not via public internet)
  - Endpoints should not be open to the public internet

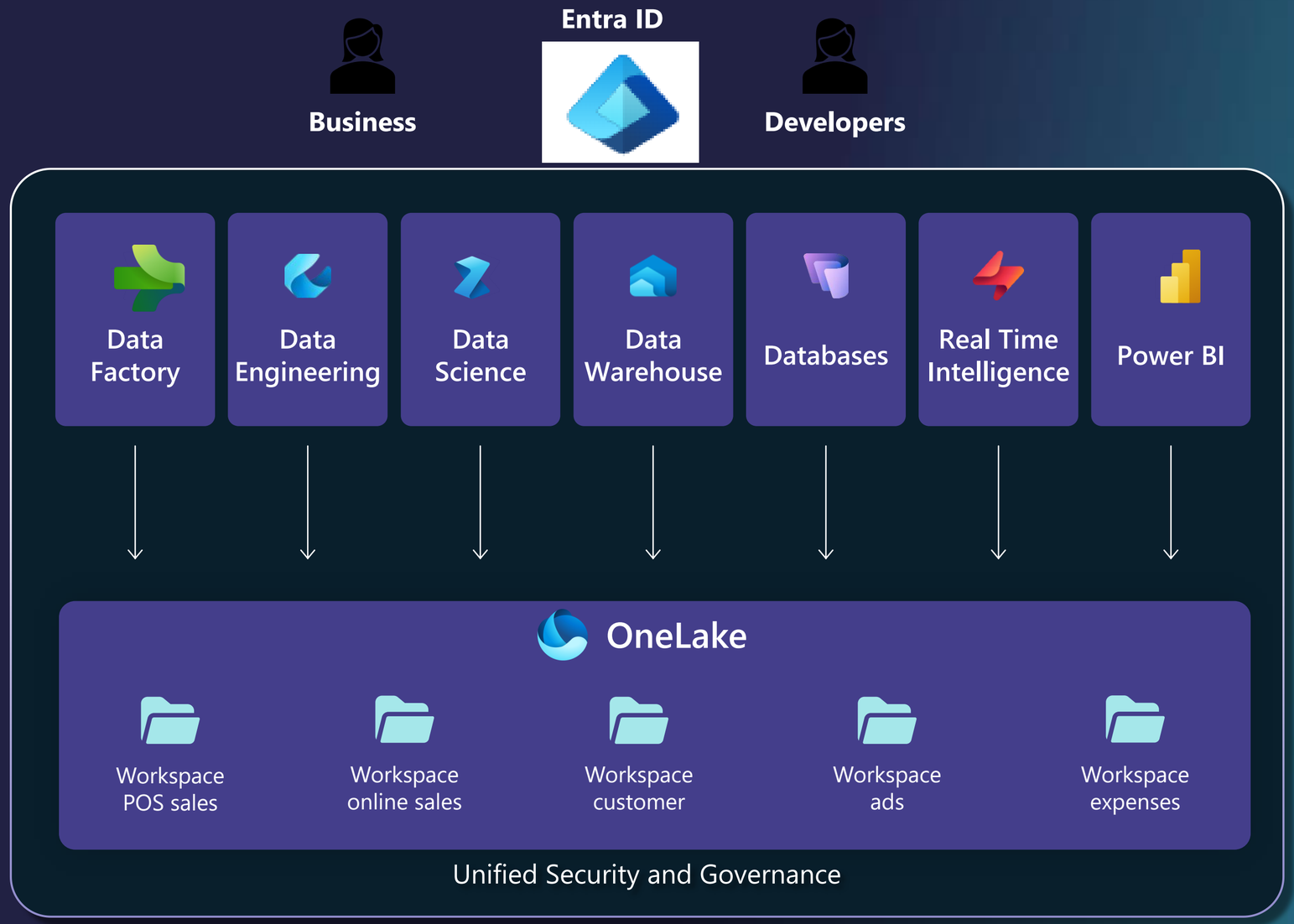


Existing PaaS World



- 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

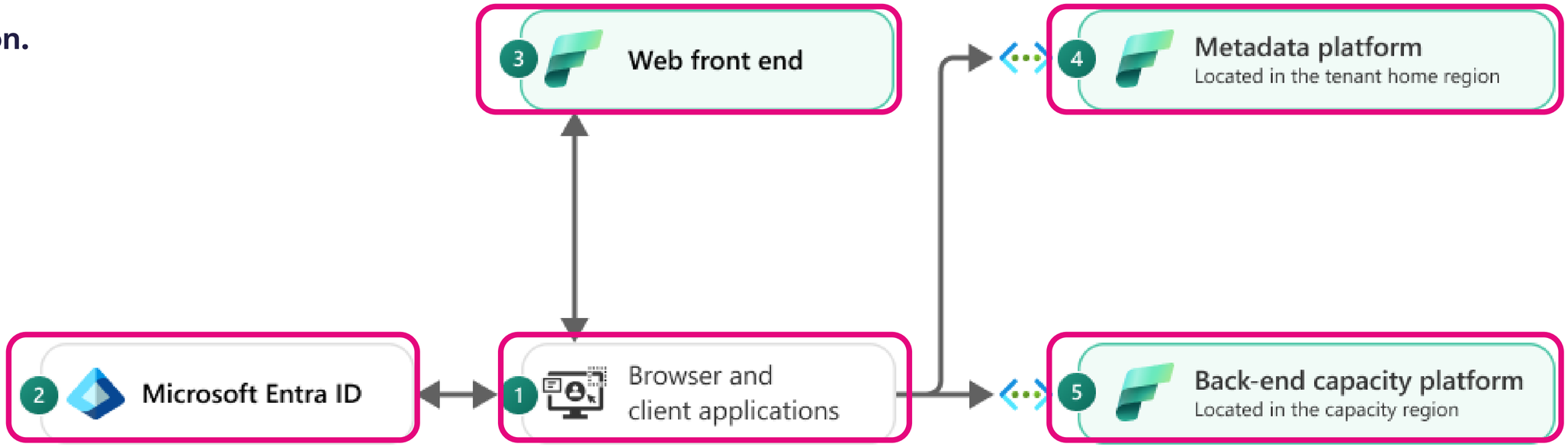
All internal communications between the experiences happens through MS backbone network

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

Microsoft Fabric Architecture

INSPARK

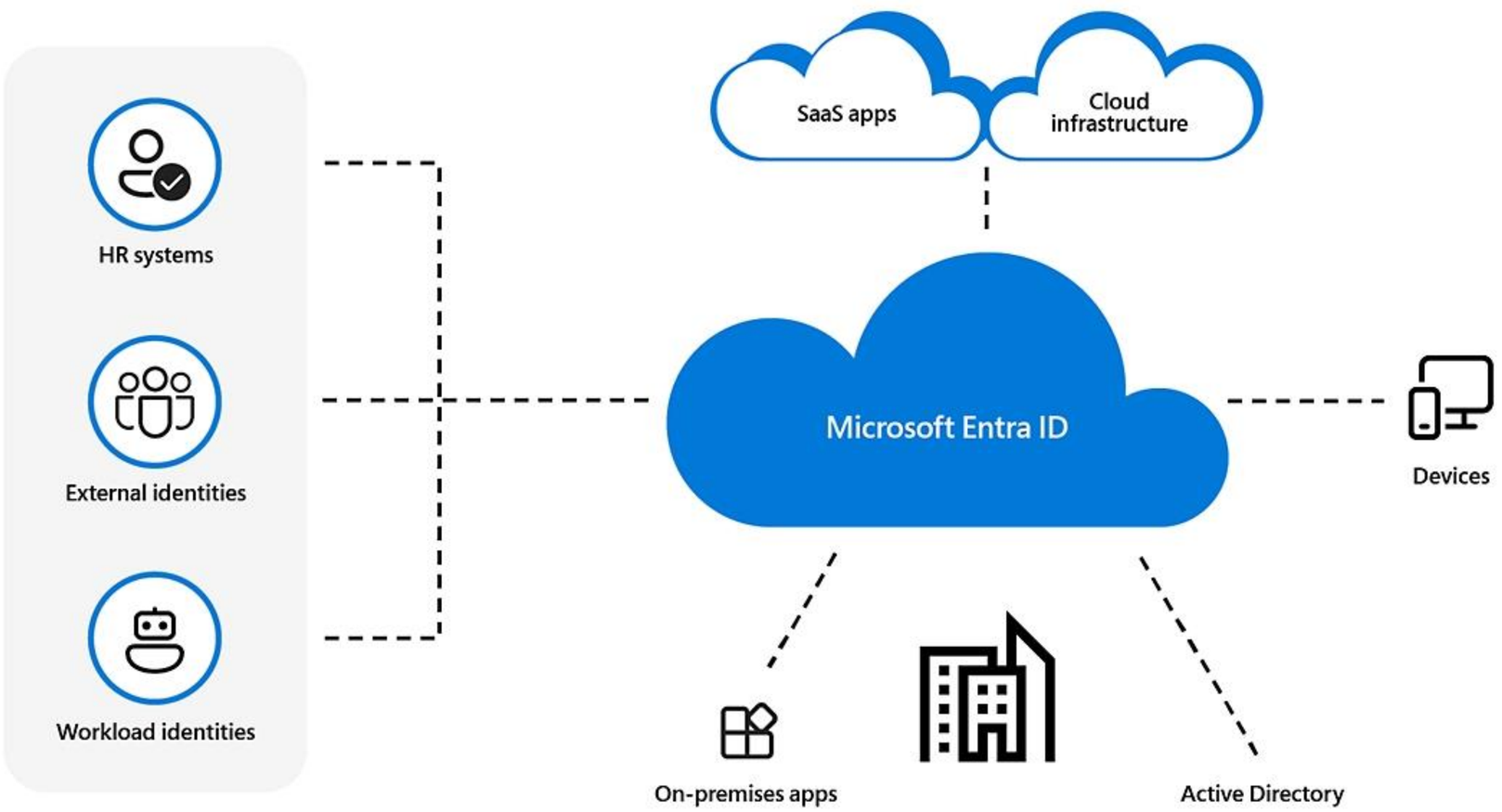
1. A user uses a browser or a client application, like Power BI Desktop, to connect to the Fabric service.
2. Authentication is handled by Microsoft Entra ID
3. The web front end receives user requests and facilitates sign-in.
4. The metadata platform stores tenant metadata, which can include customer data. Fabric services query this platform on demand in order to retrieve authorization information and to authorize and validate user requests. It's located in the tenant home region.
5. The back-end capacity platform is responsible for compute operations and for storing customer data, and it's located in the capacity region.



Entra ID

INSPARK

Microsoft Fabric Authentication



Today's identity and access challenges demand a holistic solution



Accelerated growth of identities and apps, on and off the corporate network, requiring secure, user-friendly access



Massive rise in identity cyberattacks—more than 4,000 password cyberattacks per second[1] —increasing risk of compromised accounts



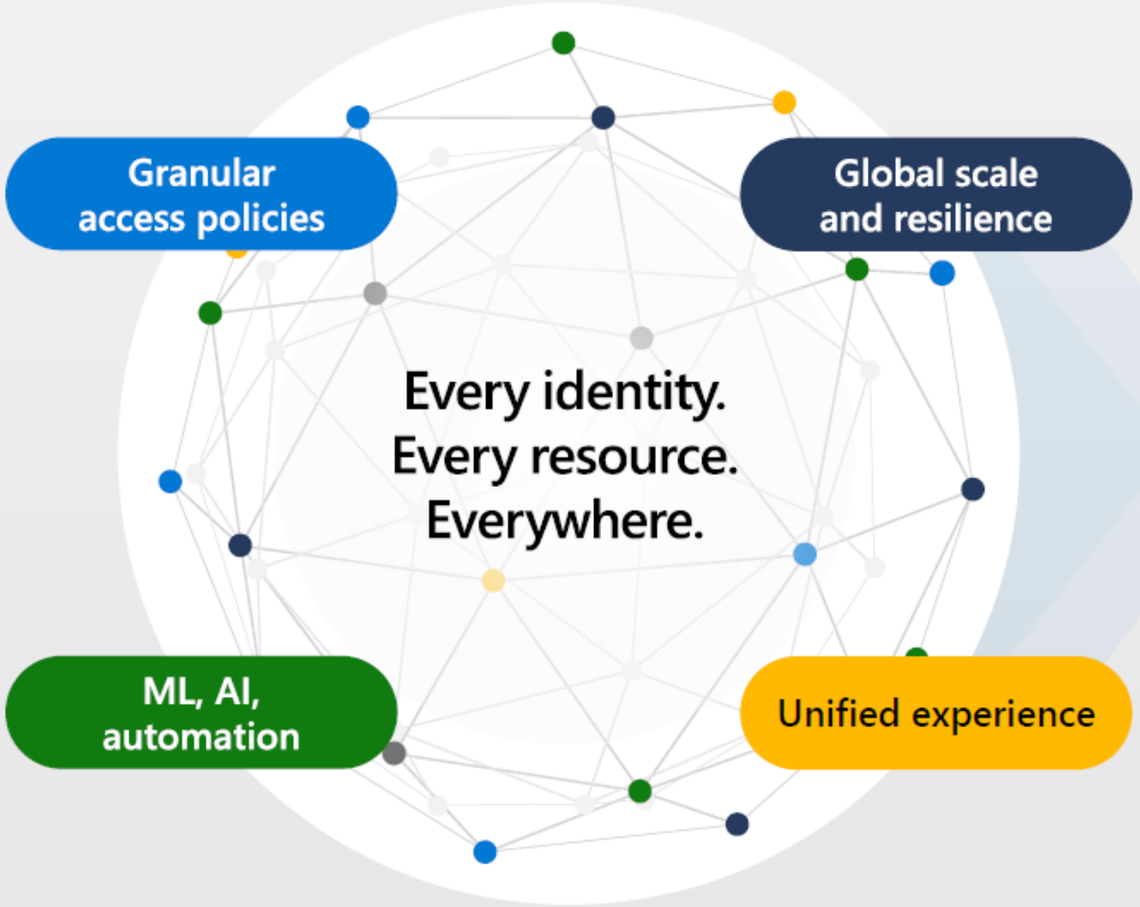
Evolving regulations and compliance requirements for protecting identities and auditing access rights

[1]Microsoft Entra expands into Security Service Edge and Microsoft Entra ID becomes Microsoft Entra ID and Microsoft Security Blog

Microsoft Entra

Secure access for a connected world

- Human identities
- Workload identities
- Customers
- Partners
- Devices



- Data
- SaaS apps
- Cloud-hosted apps and resources
- On-premises applications
- Websites

Powered by trillions of security signals

Microsoft Entra

Secure access for a connected world



Secure access to any app or resource from anywhere



Protect and verify every identity



Provide only necessary access



Simplify the user experience

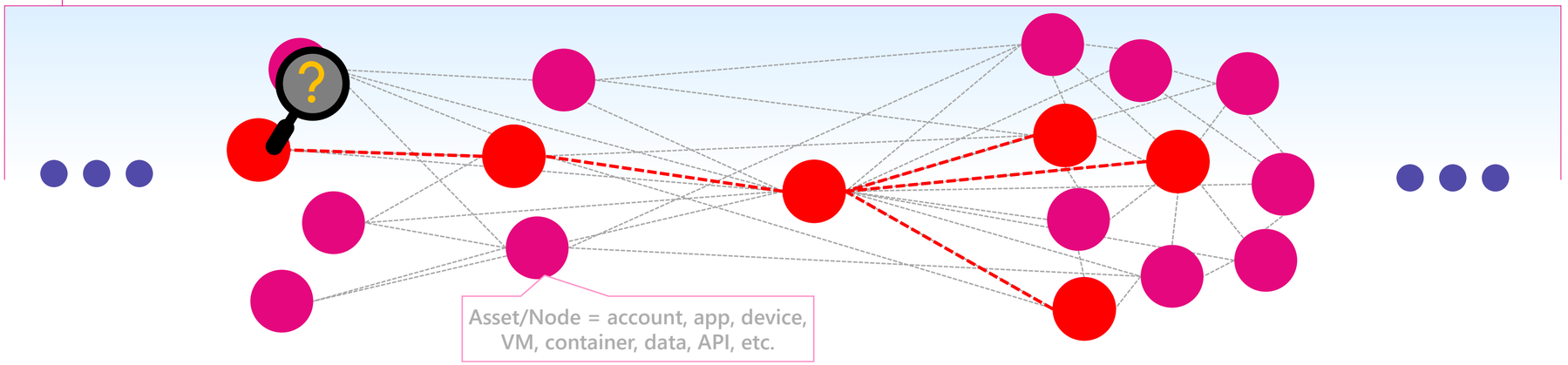
Zero Trust Principles

INSPARK

Business Enablement
Align security to the organization's mission, priorities, risks, and processes

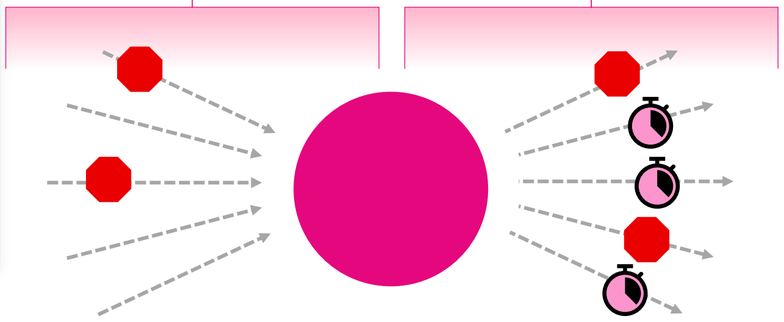
Assume Breach (Assume Compromise)
Assume attackers can and will successfully attack anything (identity, network, device, app, infrastructure, etc.) and plan accordingly

→ *Transforms from ~~"defend the network"~~ to "enable secure productivity on any network"*



Verify explicitly
Protect assets against attacker control by explicitly validating that all trust and security decisions use all relevant available information and telemetry.

→ *Reduces "attack surface" of each asset*

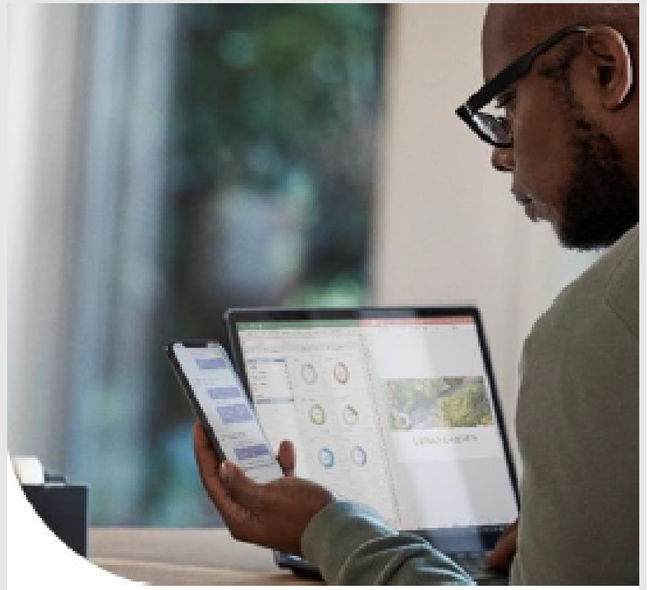


Use least privilege access
Limit access of a potentially compromised asset, typically with just-in-time and just-enough-access (JIT/JEA) and risk-based polices like adaptive access control.

→ *Reduce "blast radius" of compromises*

Multifactor authentication (MFA)

Verify user identities with strong authentication



We support a broad range of multifactor authentication options

Including passwordless technology

- Microsoft Authenticator
- Windows Hello
- FIDO2 Security key
- Biometrics
- Cert-based Auth

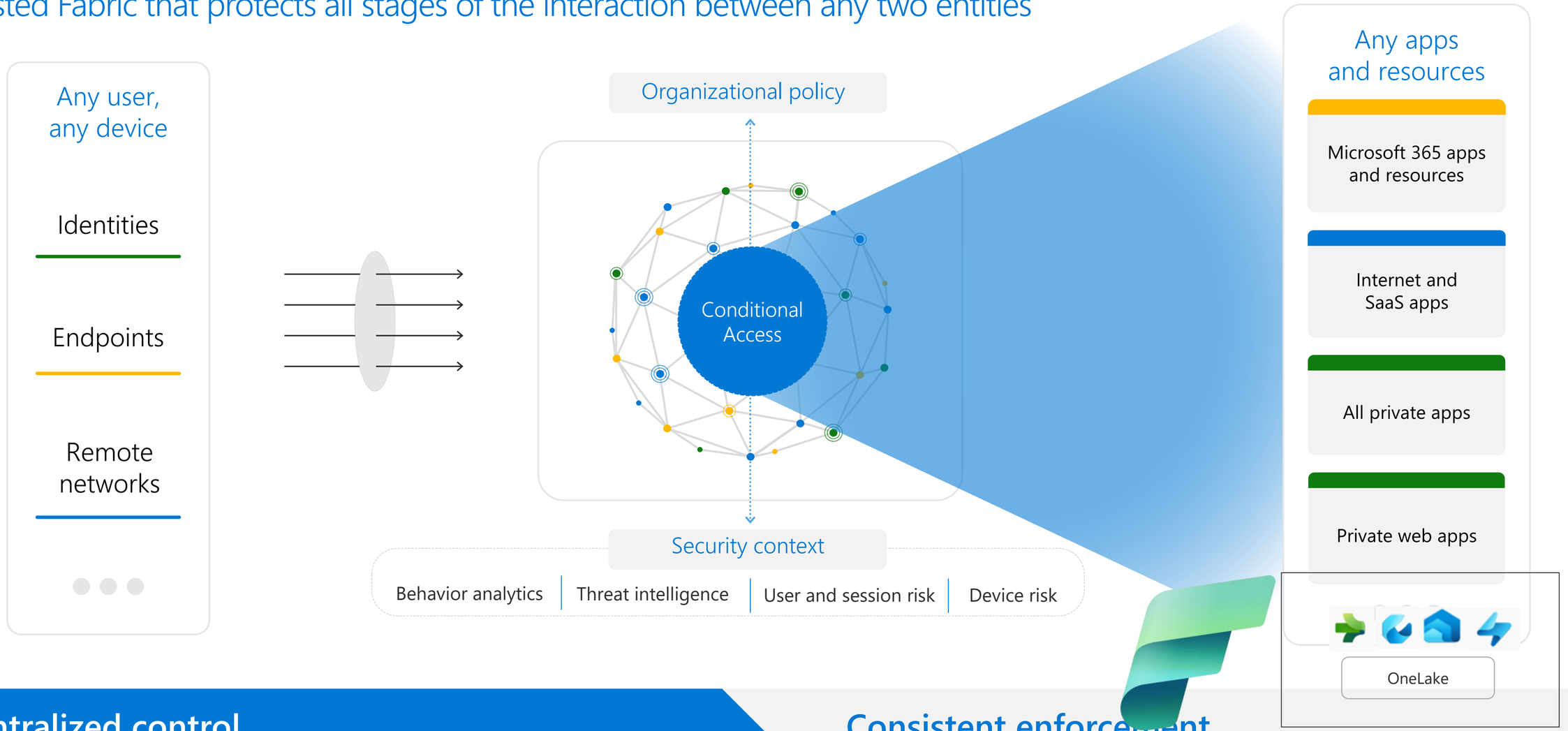
● = Including phish-resistant technology

- Push Notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, Voice

Multifactor authentication addresses 99.9% of identity cyberattacks

Conditional Access - Microsoft's Adaptive Access Vision

Trusted Fabric that protects all stages of the interaction between any two entities



Centralized control

Unified Zero Trust architecture and policy engine simplifies management of access controls and technologies (Directory, SSO, Federation, RBAC, proxy, and more)

Consistent enforcement

Centralized policy is consistently applied across all resources where the action happens (identity, data, network + infra and apps across cloud, on-premises, IoT, OT, and more)

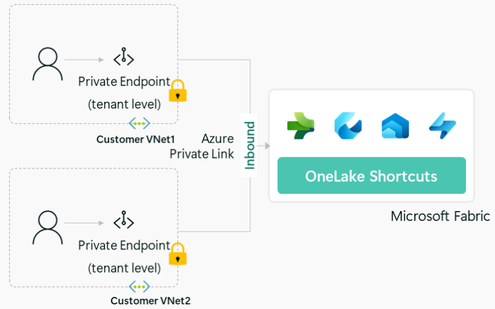


Demo

Microsoft Fabric

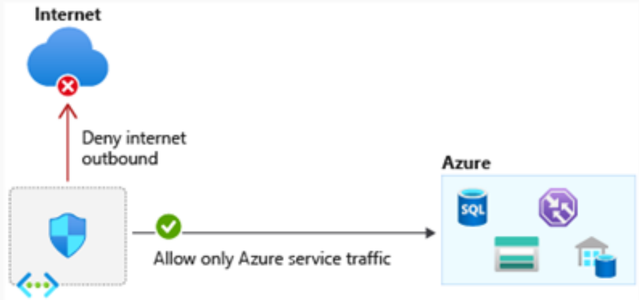
Secure inbound and outbound network connections

Secure and protect data across your organization



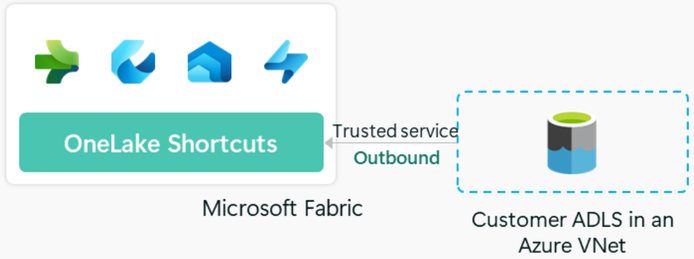
Fabric inbound security

Seamlessly secure inbound data access scenarios with Fabric's holistic identity and network security



Service tags

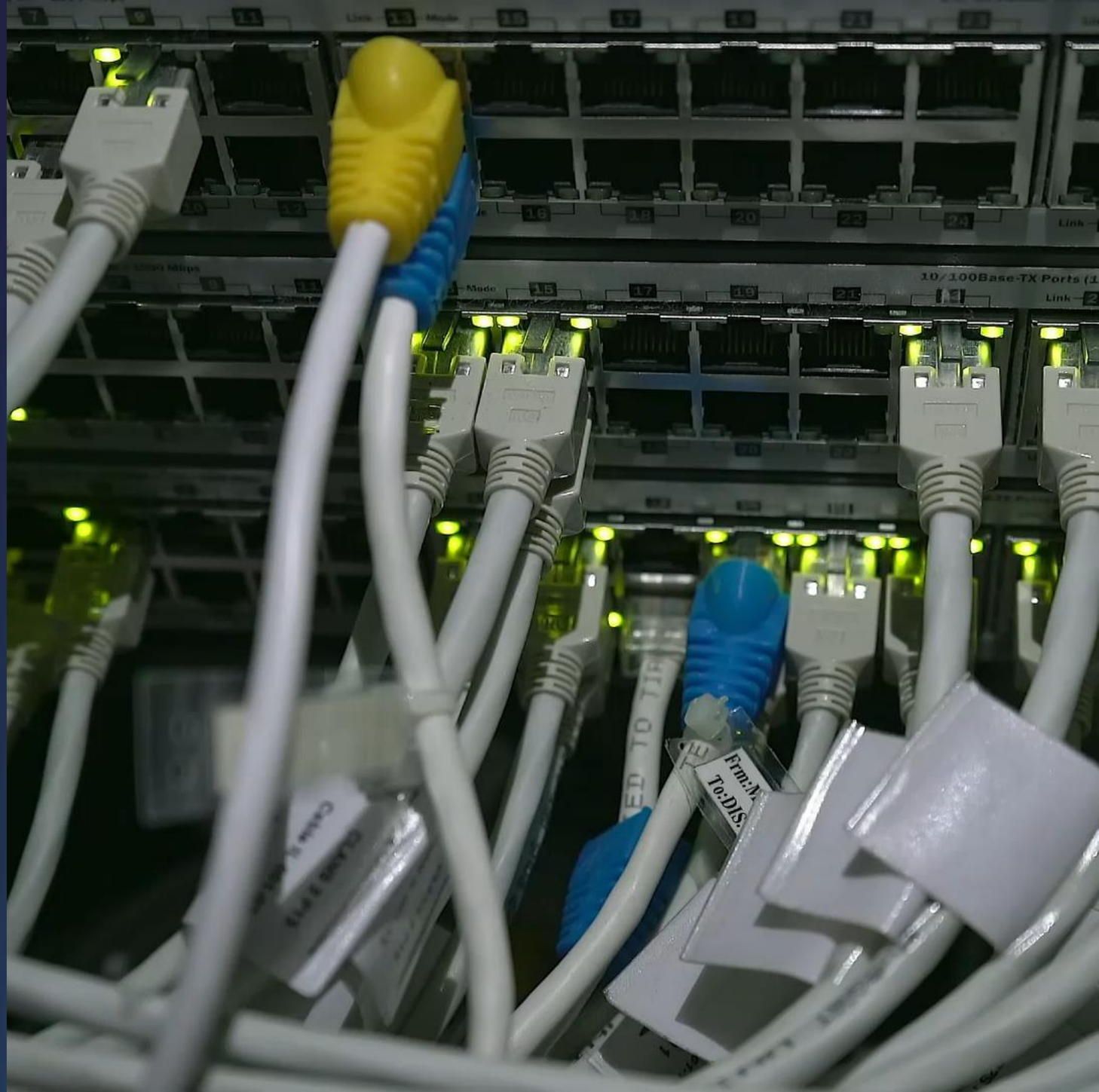
Minimize the complexity of updating network security rules using Azure service tags to group and manage IP addresses for a service



Fabric outbound security

Securely connect to your protected data sources and/or ingest data into OneLake

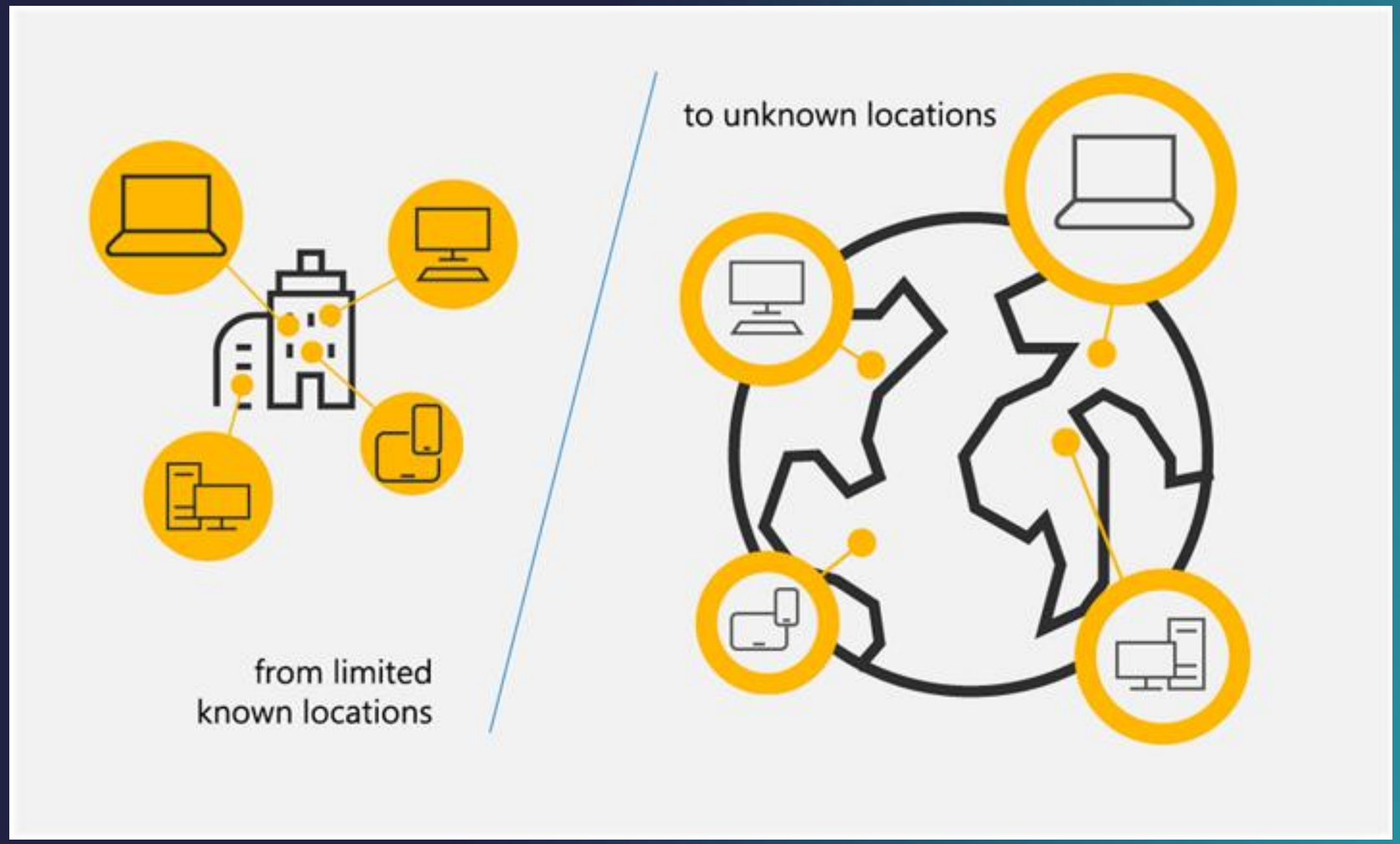
Securing inbound connections



Inbound protection options

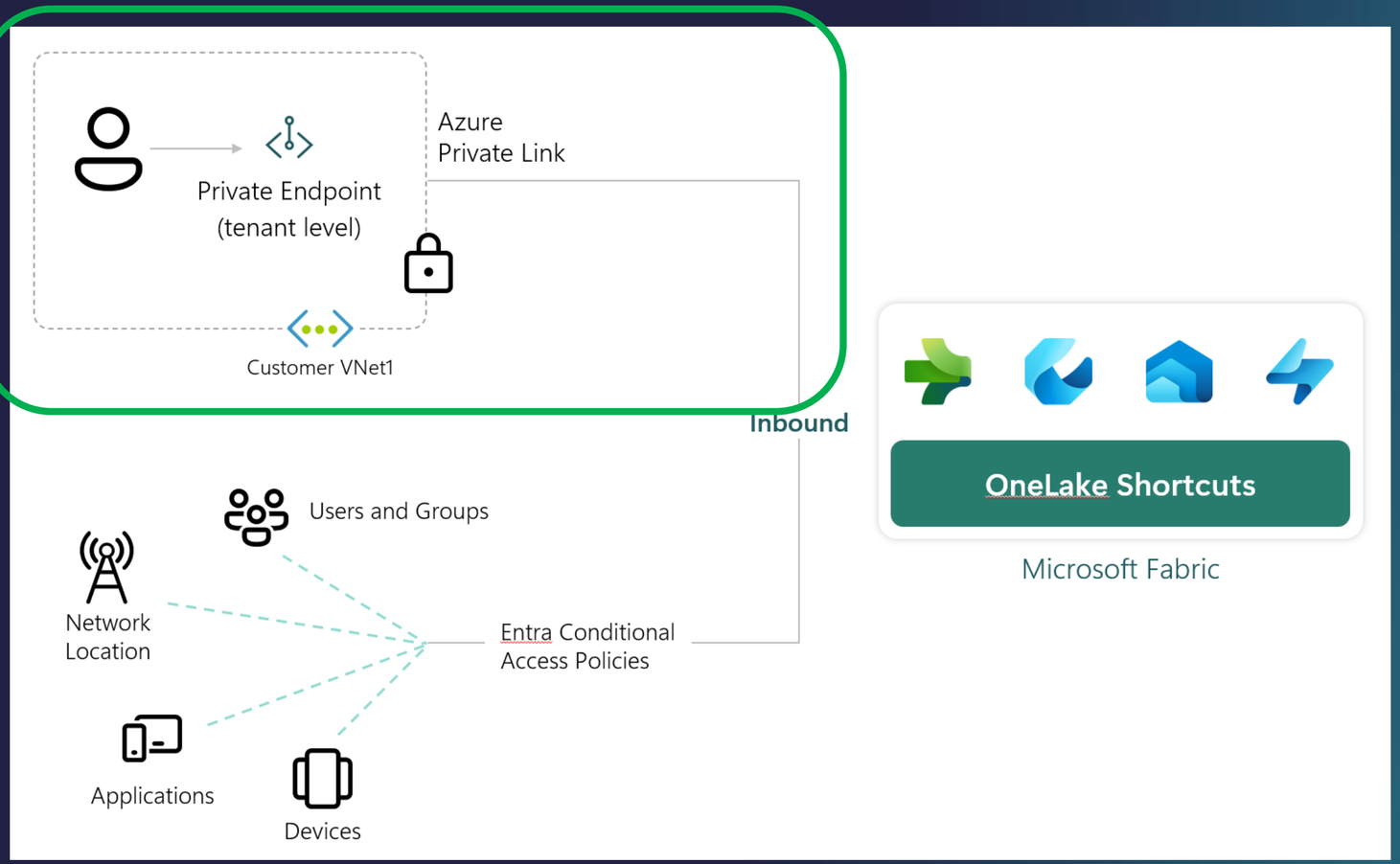
Perimeter Network Security

Zero Trust Approach



Perimeter Network Security for your tenant

Private Link for Fabric

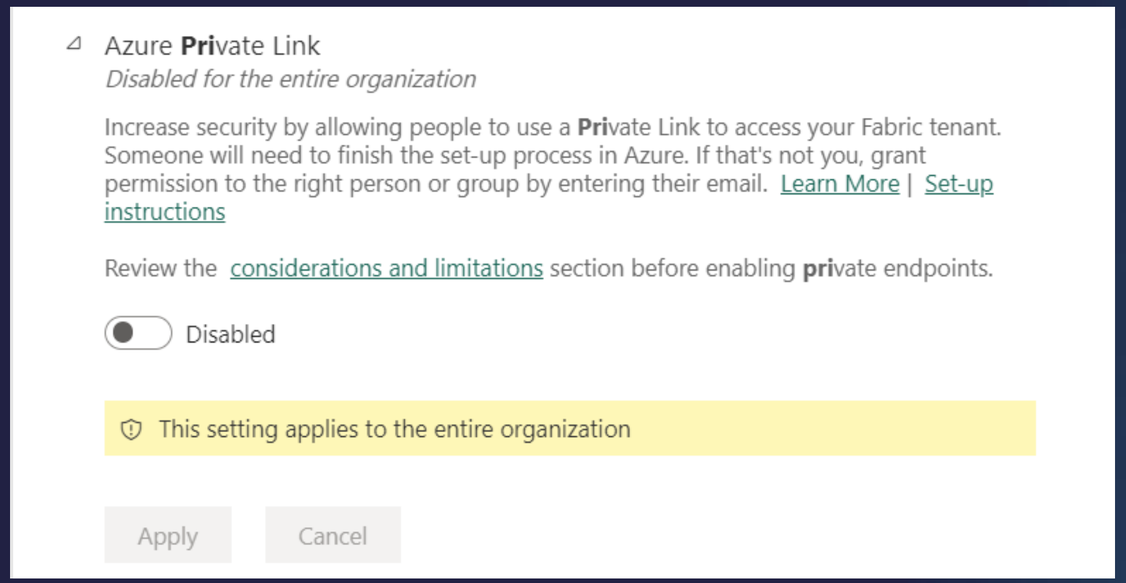


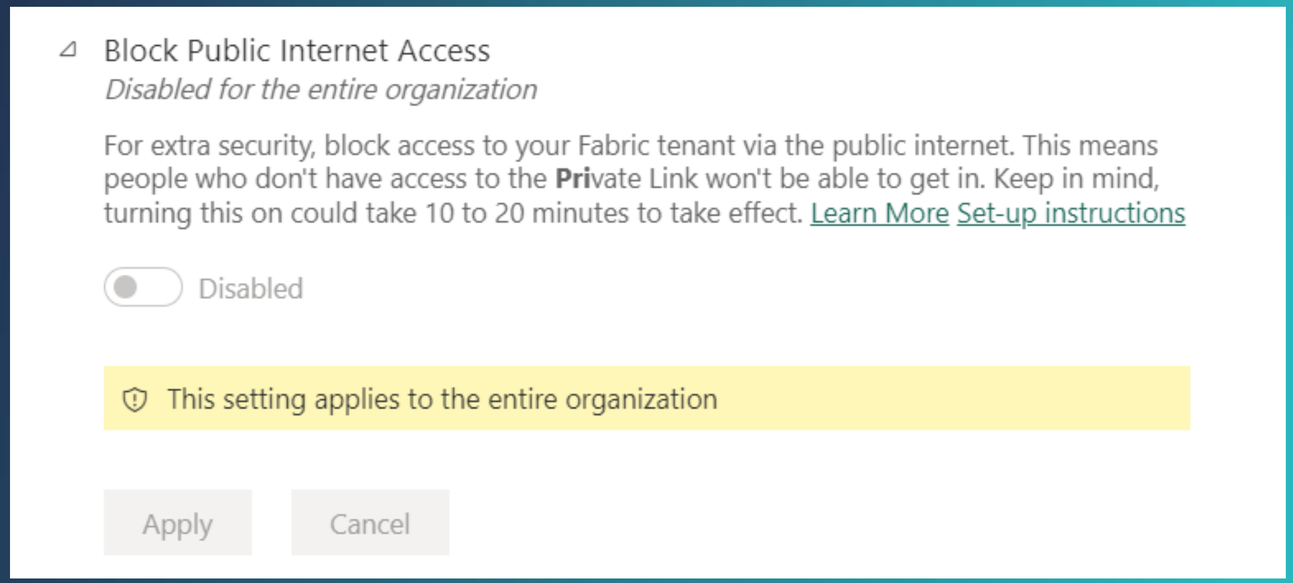
What it means:

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)
6. Only available on tenant level

Perimeter Network Security for your tenant

Private Link for Fabric (Admin Portal)



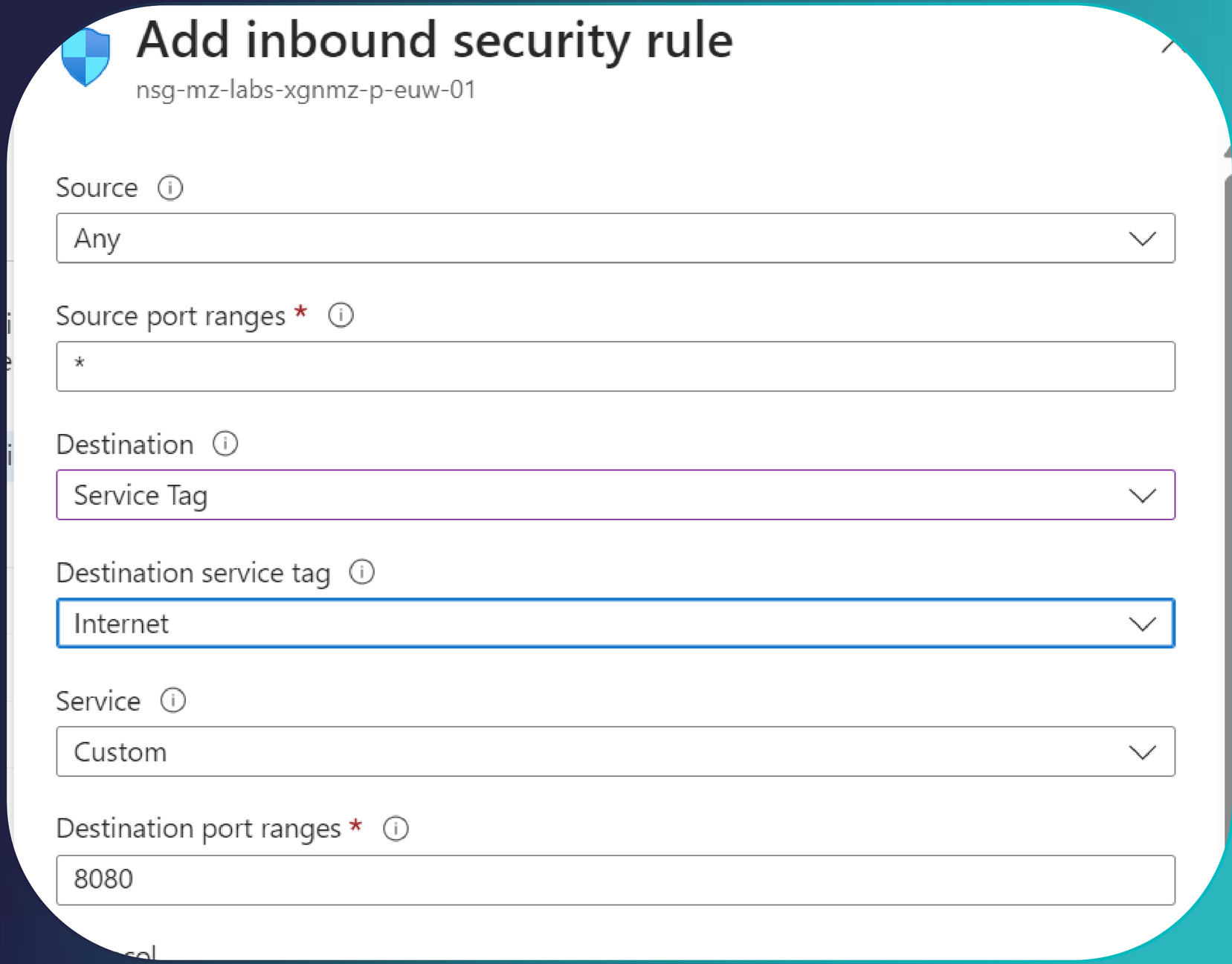


INSPARK

Limitations

- Fabric supports up to 450 capacities in a tenant where Private Link is enabled.
- When capacity is newly created, it won't support private link until its endpoint is reflected in the private DNS zone. This can take up to 24 hours. Trial capacity is not supported
- Tenant migration is blocked when Private Link is turned on in the Fabric admin portal.
- Customers can't connect to Fabric resources in multiple tenants from a single virtual network, but rather only the last tenant to set up Private Link.
- Each private endpoint can be connected to one tenant only. You can't set up a private link to be used by more than one tenant.
- On-premises data gateways aren't supported and fail to register when Private Link is enabled. To run the gateway configurator successfully, Private Link must be disabled. Learn more about this scenario. VNet data gateways will work.

Service Tags



Service tags

- **You can use Azure service tags to enable connections to and from Microsoft Fabric.**
- **A service tag is a defined group of IP addresses that is automatically managed, as a group, to minimize the complexity of updates or changes to network security rules**
- **You can use the service tags to define network access controls:**
  - Network security groups.
  - Azure Firewall.
  - User-defined routes..

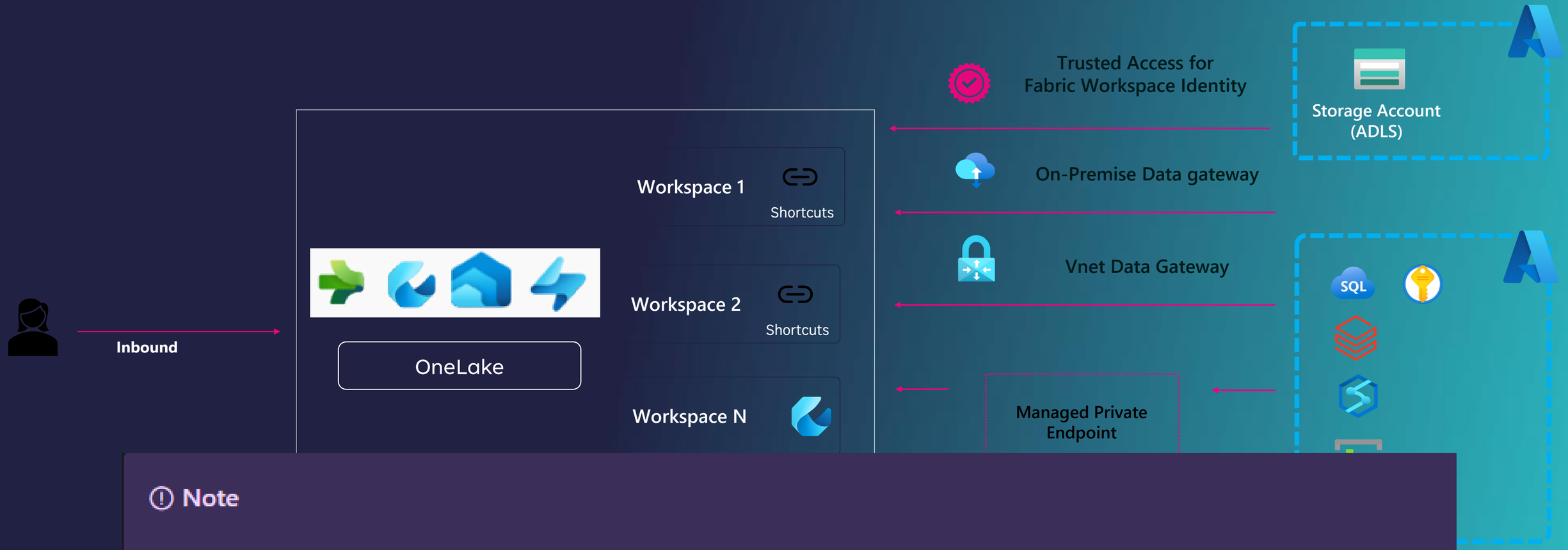
Tag	Purpose	Can use inbound or outbound?	Can be regional?	Can use with Azure Firewall?
DataFactory	Azure Data Factory	Both	No	Yes
DataFactoryManagement	On premises data pipeline activity	Outbound	No	Yes
EventHub	Azure Event Hubs	Outbound	Yes	Yes
Power BI	Power BI and Microsoft Fabric	Both	No	Yes
PowerQueryOnline	Power Query Online	Both	No	Yes
KustoAnalytics	Real-Time Intelligence	Both	No	No
SQL	Fabric SQL database	Both	Yes	Yes

Getting secured data into Fabric



How to connect/load data in the VNET from Fabric

Getting data into Fabric



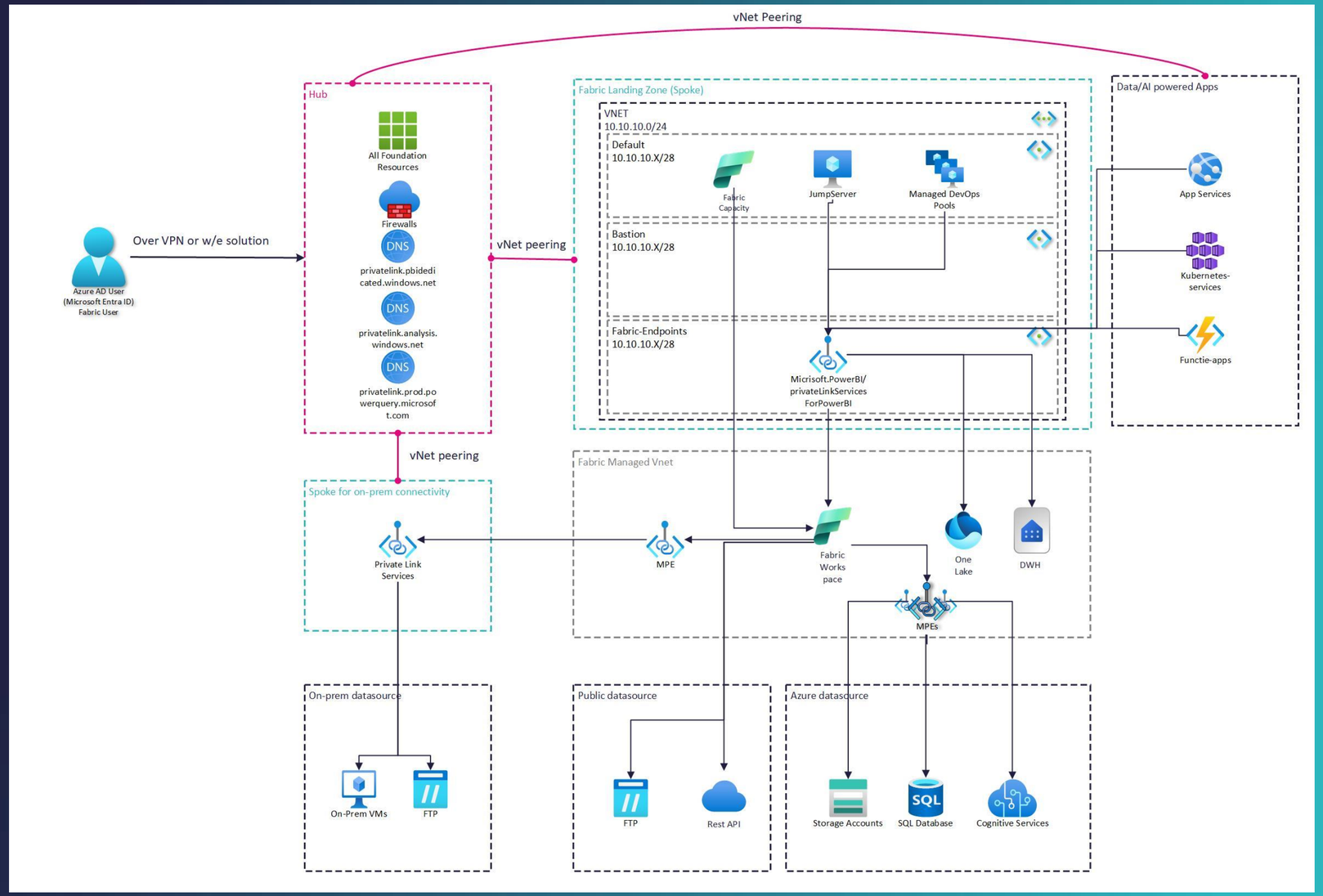
Note

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 | Mic

How to connect/load data in the VNET from Fabric

Getting data into Fabric





Demo

INSPARK



Microsoft Fabric

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



Microsoft Purview

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

Data ownership	Unmatched security & compliance	Unified governance

INSPARK

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

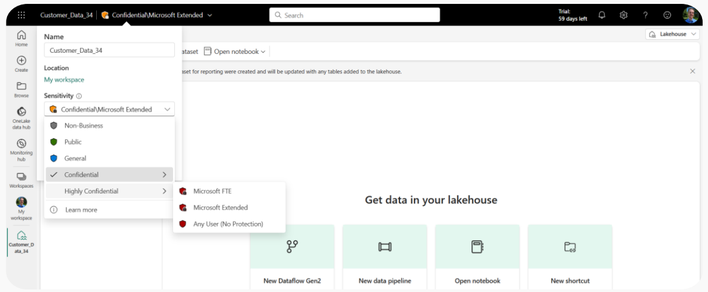
Across IaaS, and SaaS

Microsoft Purview

Purview security and compliance features to protect your data in Fabric

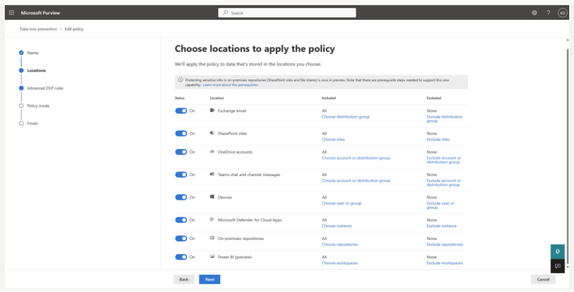
*Additional Microsoft Purview purchase required

Secure and protect data across your organization



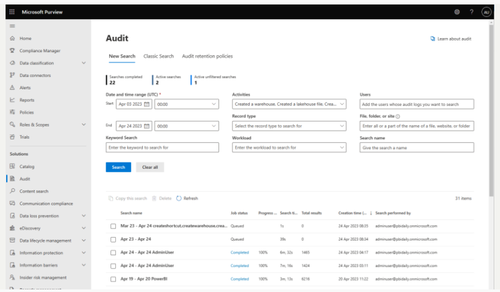
Information Protection labels

Classify sensitive Fabric data using the same sensitivity labels that are used in Microsoft 365—enforced even when the data is exported



Data Loss Prevention policies

Automatically detect the upload of sensitive data such as PII and trigger automatic risk remediation actions such as alerts



Audit

Log user activities from Microsoft Fabric to support security, forensic, and internal investigations

Compliance with Microsoft Fabric

Microsoft Fabric is a core Microsoft online service and supports a wide range of compliance standards including:

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





Erwin de Kreuk

Feedback

Thank You



@erwindekreuk

linkedin.com/in/erwindekreuk

erwindekreuk.com

github.com/edkreuk

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

Let's connect

MVP Microsoft® Most Valuable Professional



INSPARK