# The Microsoft approach to Zero Trust networking and supporting Azure technologies

Microsoft

# What we'll cover today

→ Microsoft's enterprise environment

→ Zero Trust architecture

→ Compatibility with our existing infrastructure

→ Modern networking

# Microsoft environment today

| | |
|---|---|
| 135K | Number of employees |
| 630B | Authentication requests per month |
| 842K | Microsoft Teams meetings per month |
| 420K | Intune-managed devices hitting the network |
| 94% | On-premises workload reduction |
| 6M | Papers saved per year by using eSignatures |
| 3M | Transactions on the sales platform per day |
| 1TB | Supply chain IoT data generated daily |
| 400K | Chatbot interactions |

# Cloud networking by the numbers

**10**
ExpressRoute regions worldwide

**4**
Az LAB zone regions (2 US, 1 Asia, 1 EU)

**9**
Azure networking services deployed or testing

**24**
Azure Firewall native instances deployed

**1,200+**
ExpressRoute circuits

**150**
Lab virtual networks

**665k+**
Internal Microsoft IPs

**30**
Minutes to deploy Az FW vs weeks for HW firewall

**7,000+**
Virtual Networks

**32**
Feature requests with Azure PG

**30+**
Average customer consultations per month

**$574k**
CapEx saved using Azure Native Firewall ($36k)

# Alignment of initiatives

Deliver modern, secure connectivity to our internal applications and services

**Customer zero**

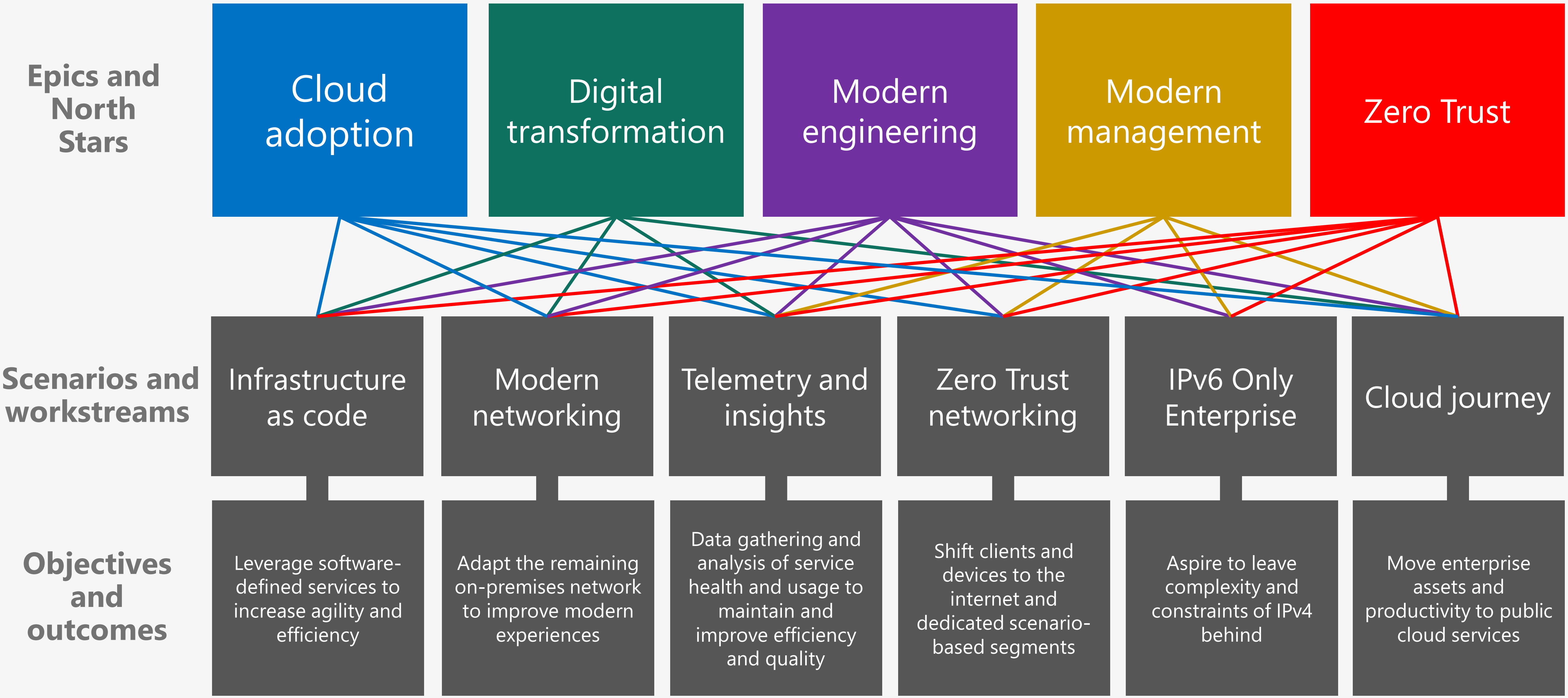
**Internet connected**

**IPv6**

**Cloud and lab optimal**

**Zero Trust networking**

# Microsoft enterprise networking 2020

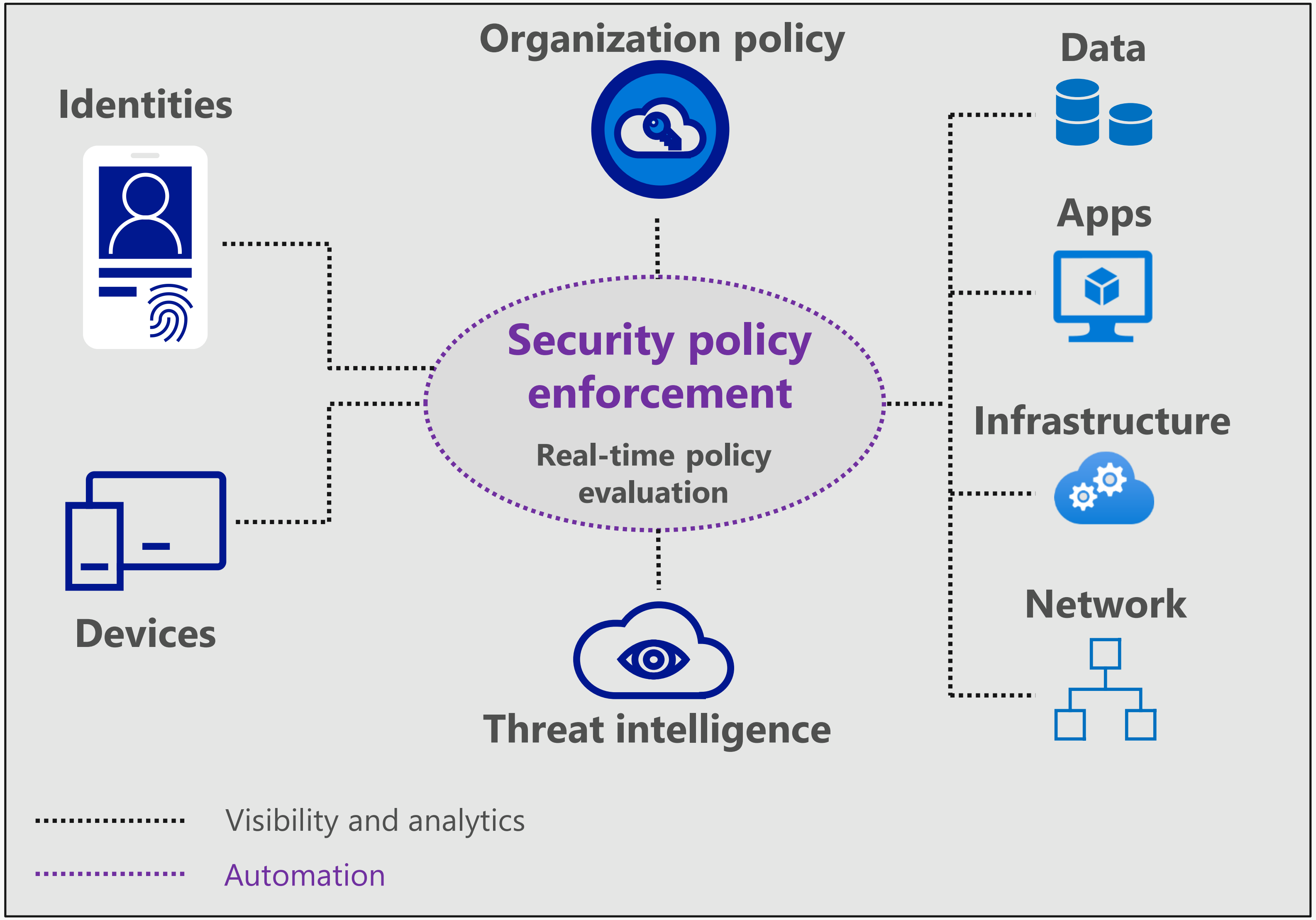


**Epics and North Stars**

- Cloud adoption
- Digital transformation
- Modern engineering
- Modern management
- Zero Trust

| **Scenarios and workstreams** | Infrastructure as code | Modern networking | Telemetry and insights | Zero Trust networking | IPv6 Only Enterprise | Cloud journey |
|---|---|---|---|---|---|---|
| **Objectives and outcomes** | Leverage software-defined services to increase agility and efficiency | Adapt the remaining on-premises network to improve modern experiences | Data gathering and analysis of service health and usage to maintain and improve efficiency and quality | Shift clients and devices to the internet and dedicated scenario-based segments | Aspire to leave complexity and constraints of IPv4 behind | Move enterprise assets and productivity to public cloud services |

# Zero Trust architecture



## Guiding principles of Zero Trust:

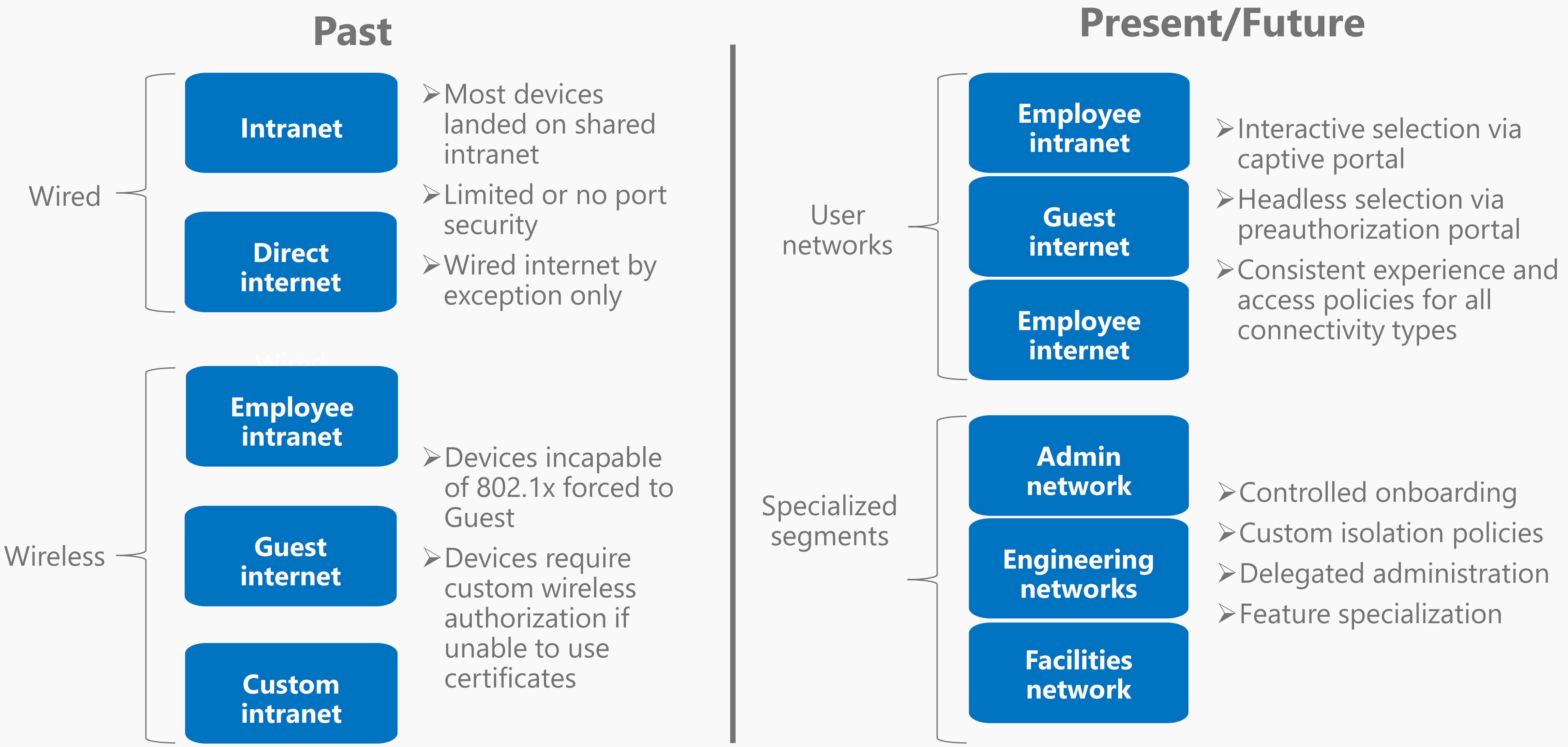
1. Verify explicitly
2. Use least-privilege access
3. Assume breach

https://www.Microsoft.com/en-us/security/

# Zero Trust networking maturity model

| Traditional | Advanced | Optimal |
|---|---|---|
| Few network-security perimeters and flat, open network | Many ingress and egress cloud microperimeters with some microsegmentation | Fully distributed ingress and egress cloud microperimeters and deeper microsegmentation |
| Minimal threat protection, static traffic filtering | Cloud native filtering and protection for known threats | ML-based threat protection and filtering with context-based signals |
| Internal traffic is not encrypted | User-to-app internal traffic is encrypted | All traffic is encrypted |

# User-connectivity specialization and standardization



## Past

Wired

- Intranet
- Direct internet

- ➢Most devices landed on shared intranet
- ➢Limited or no port security
- ➢Wired internet by exception only

Wireless

- Employee intranet
- Guest internet
- Custom intranet

- ➢Devices incapable of 802.1x forced to Guest
- ➢Devices require custom wireless authorization if unable to use certificates

## Present/Future

User networks

- Employee intranet
- Guest internet
- Employee internet

- ➢Interactive selection via captive portal
- ➢Headless selection via preauthorization portal
- ➢Consistent experience and access policies for all connectivity types

Specialized segments

- Admin network
- Engineering networks
- Facilities network

- ➢Controlled onboarding
- ➢Custom isolation policies
- ➢Delegated administration
- ➢Feature specialization

# Device assignment in Zero Trust networks

Unmanaged Internet

- Sponsored Access
- Event Access
- BYOD

**Internet only**

Managed internet

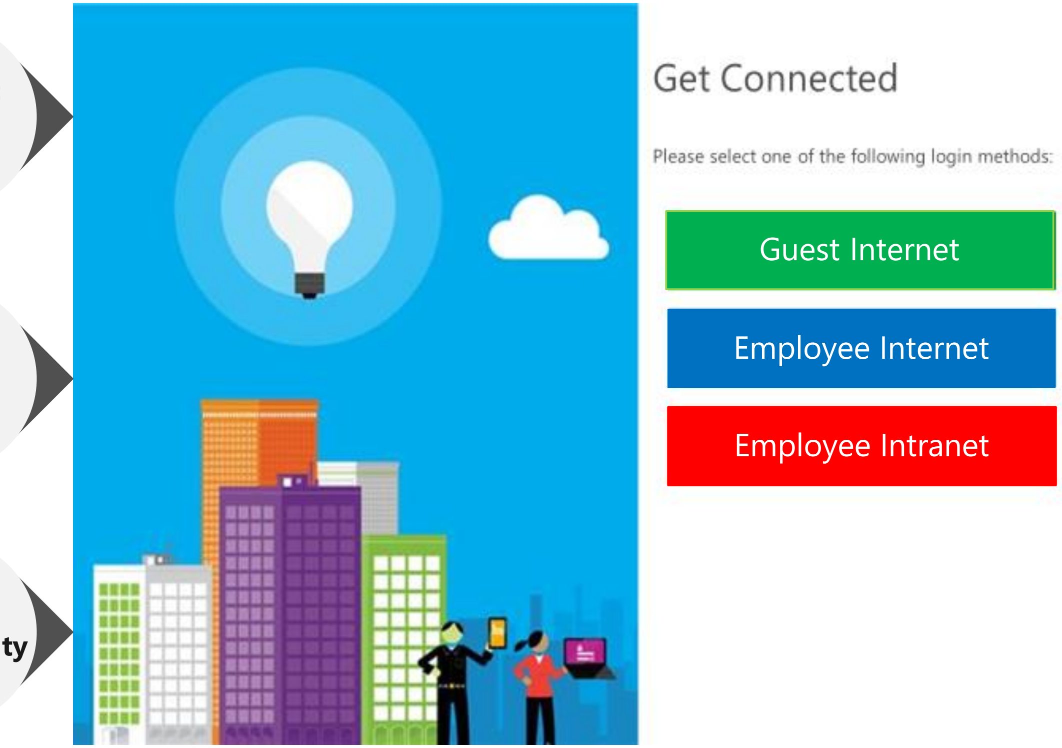
- Managed devices
- Attested devices

**Remote access**

Managed intranet

- Managed devices only
- Mandatory registration

**Direct connectivity**



Get Connected

Please select one of the following login methods:

Guests require employee sponsorship

Employees can self-sponsor

User multi-factor authentication

Device attestation and attribution

User multi-factor authentication

Device-management verification

Device-asset registration

Specialized segments

- Administration (Infra)
- Research/dev scenarios
- Facilities/building devices
- Supply chain

**Controlled access**

Preauthentication process

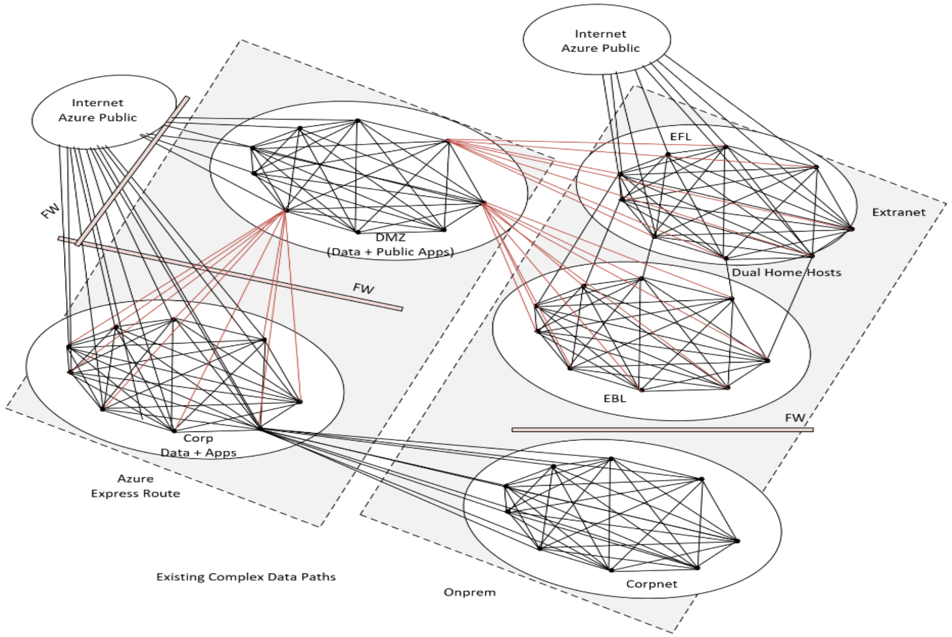
- Admin network
- Research and dev
- Facilities
- Partners

Device is preregistered for access to specialized segments

Controlled or governed access

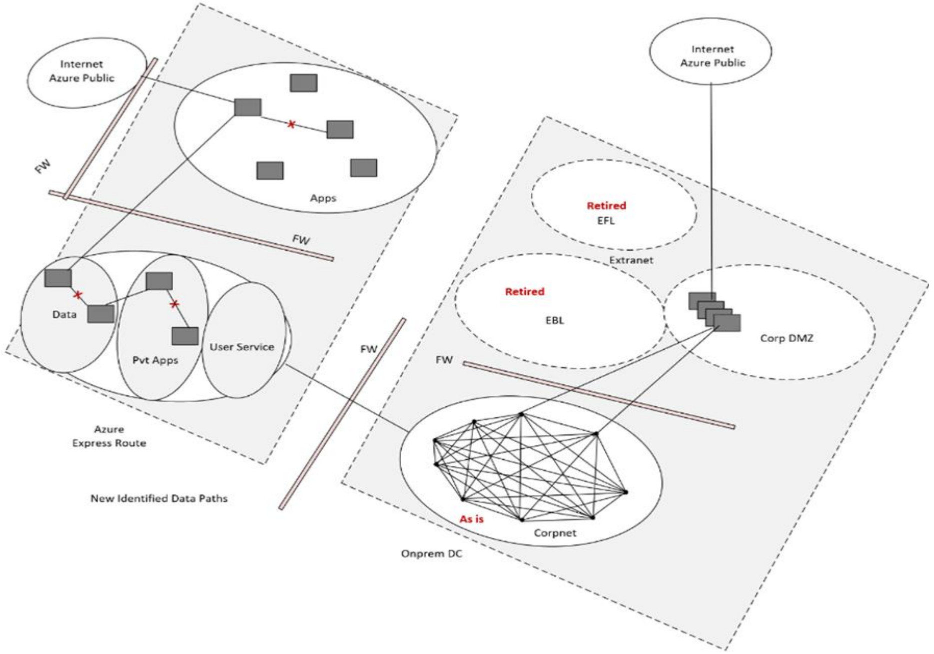
# Locking down our “open" cloud and datacenter networks

## Before



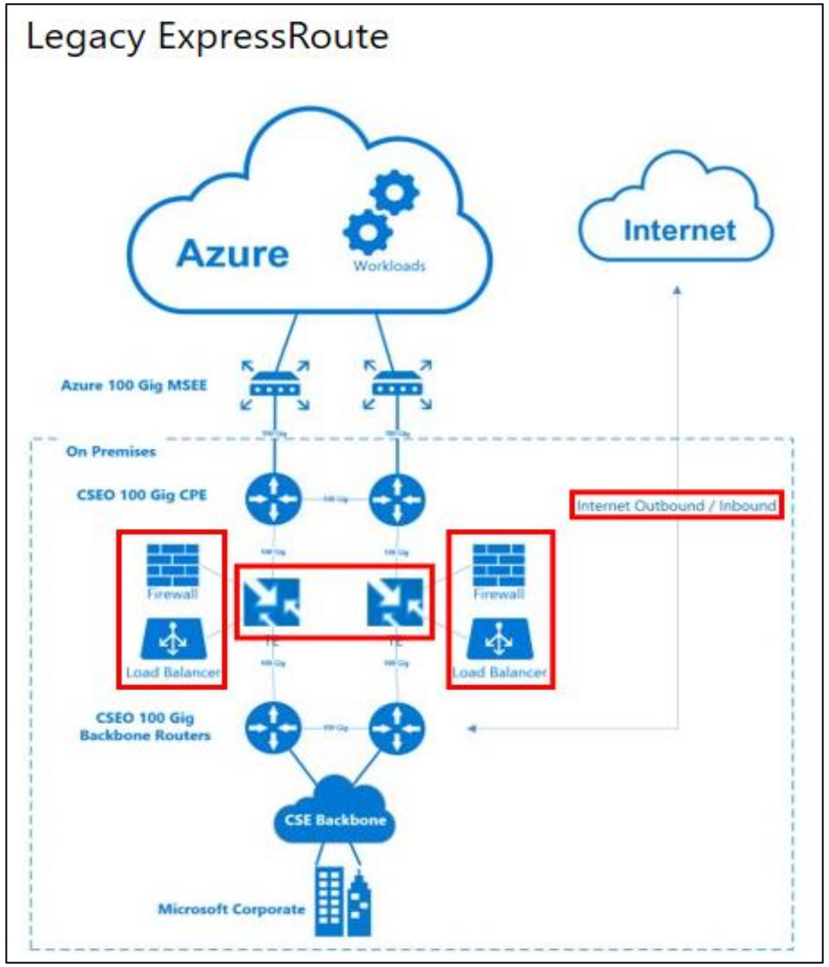
- ➢ Flat or open network enabled virus propagation
- ➢ Allowed for lateral movement from the internet
- ➢ Some networks hidden behind physical devices
- ➢ Substantial dependencies on physical devices
- ➢ **Datacenter and lab tenants provide a more permissive architecture, which must change**

## After

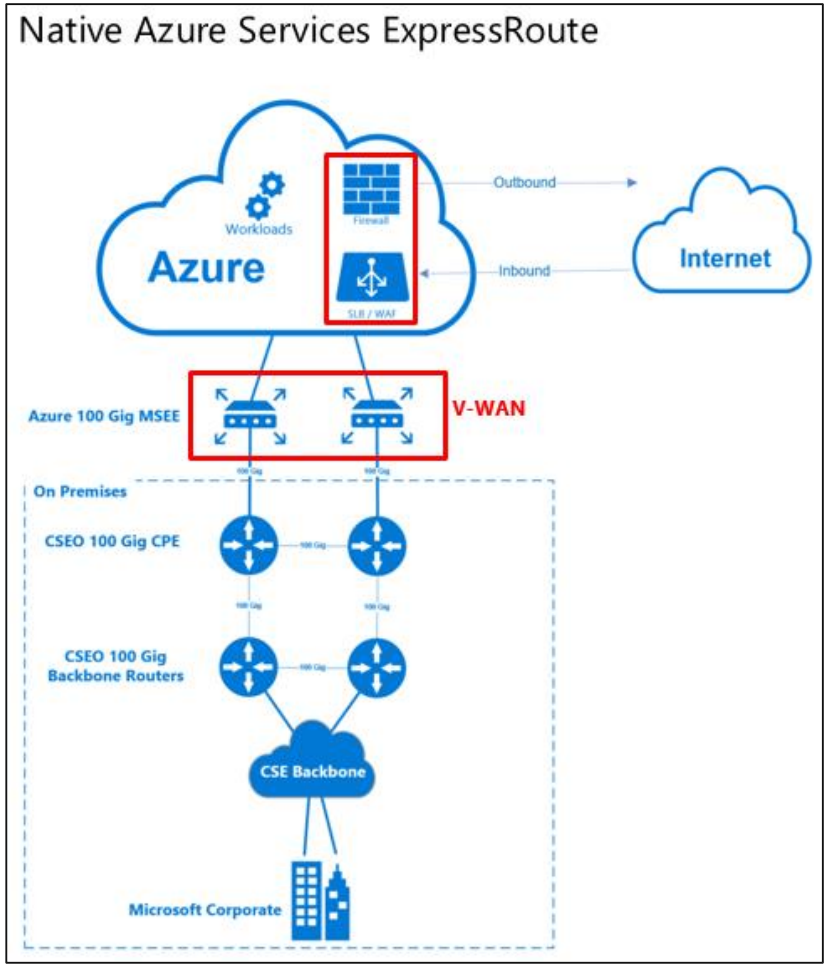


- ➢ Logical zones separate web and data tiers
- ➢ Logical zones created for environment type (DMZ, prod, LAB)
- ➢ Traffic must pass through a firewall or network security group
- ➢ Improved controls and telemetry via Azure Features
- ➢ New architecture utilizes Azure virtual appliances
- ➢ **Tenants struggling with this, as it adds better controls**

# Future scenario: *leveraging native Azure services*



Legacy ExpressRoute



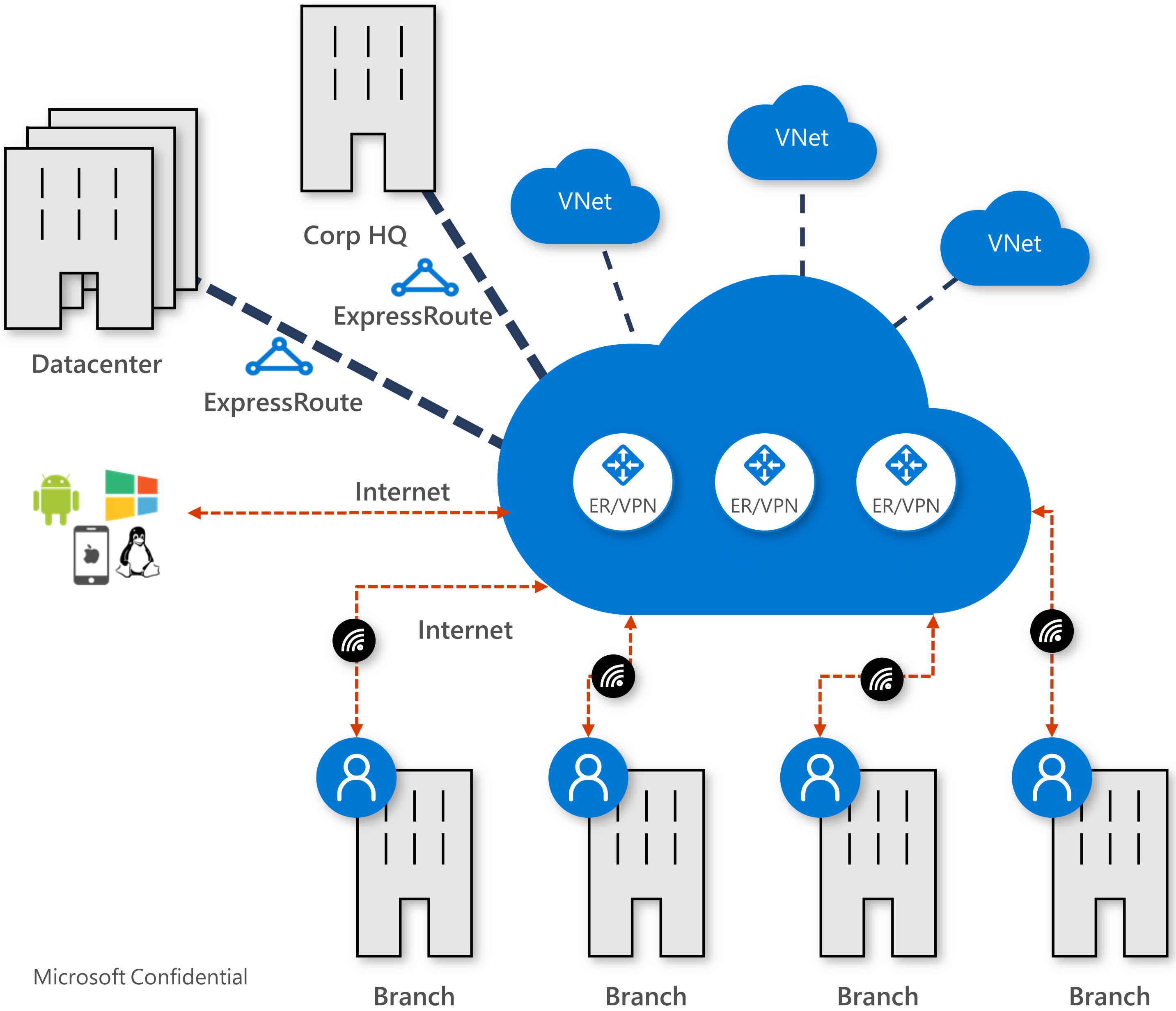
Native Azure Services ExpressRoute

Goals:
Migrate hundreds of labs to the cloud
Network segmentation (from Corpnet and each other)
Enable engineering agility and time-to-market

Solution:
Leverage cloud native
Scalable infrastructure
Central edge controls

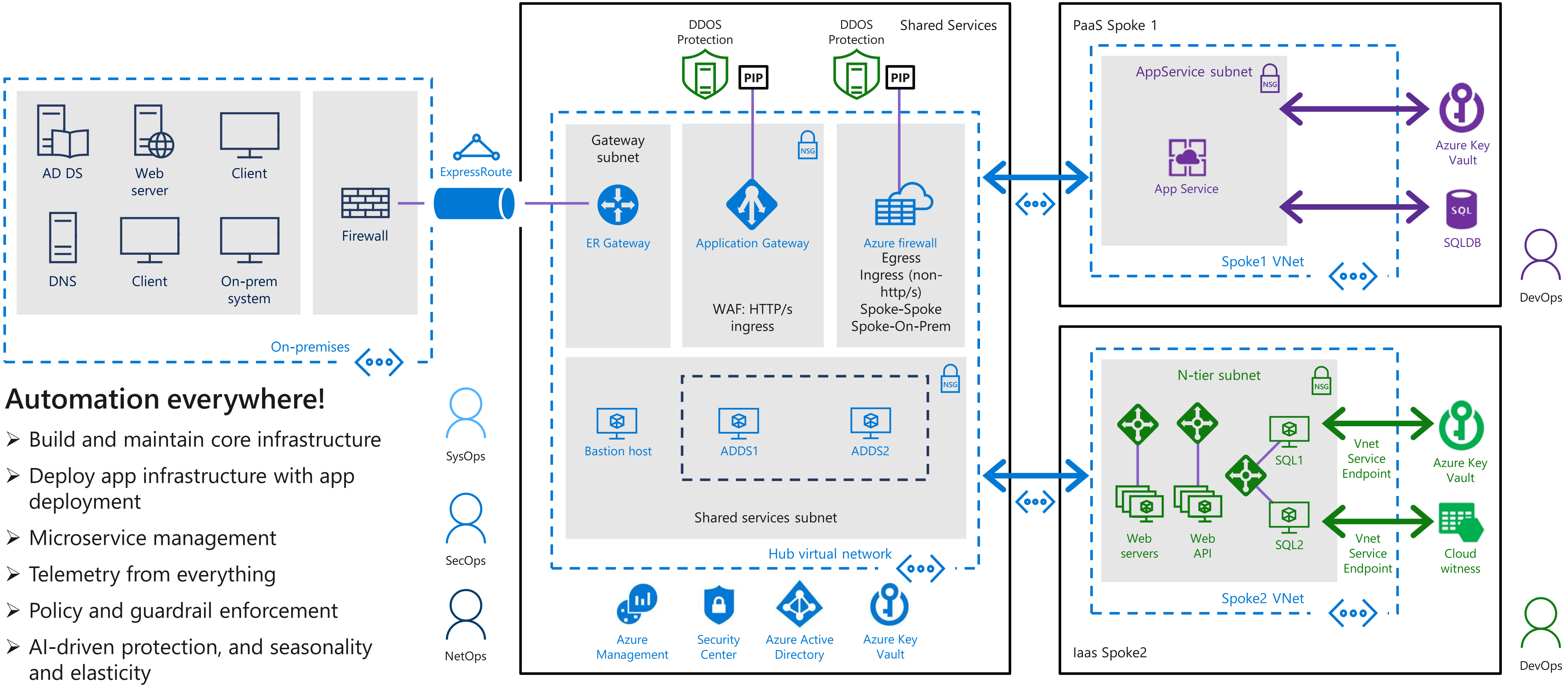
Learnings :
Scalability improved
Performance improved (lack of force tunnel)

# Future scenario: *connectivity via Azure virtual WAN*



- ➢ Large scale internet VPN for branch offices
- ➢ ExpressRoute for datacenters and HQ
- ➢ P2S VPN for mobile workers
- ➢ Local Internet breakout for O365
- ➢ Ecosystem of SDWAN and VPN partners
- ➢ 5G and Edge Computing are significant investments

# Future scenario: *Infrastructure as Code*



## Automation everywhere!

- Build and maintain core infrastructure
- Deploy app infrastructure with app deployment
- Microservice management
- Telemetry from everything
- Policy and guardrail enforcement
- AI-driven protection, and seasonality and elasticity

# Resources

Access all IT Showcase resources at Microsoft.com/ITShowcase

- Implementing a Zero Trust security model at Microsoft
- Microsoft IT Showcase

# CSEO Showcase

How Microsoft does IT

Visit the website
microsoft.com/itshowcase