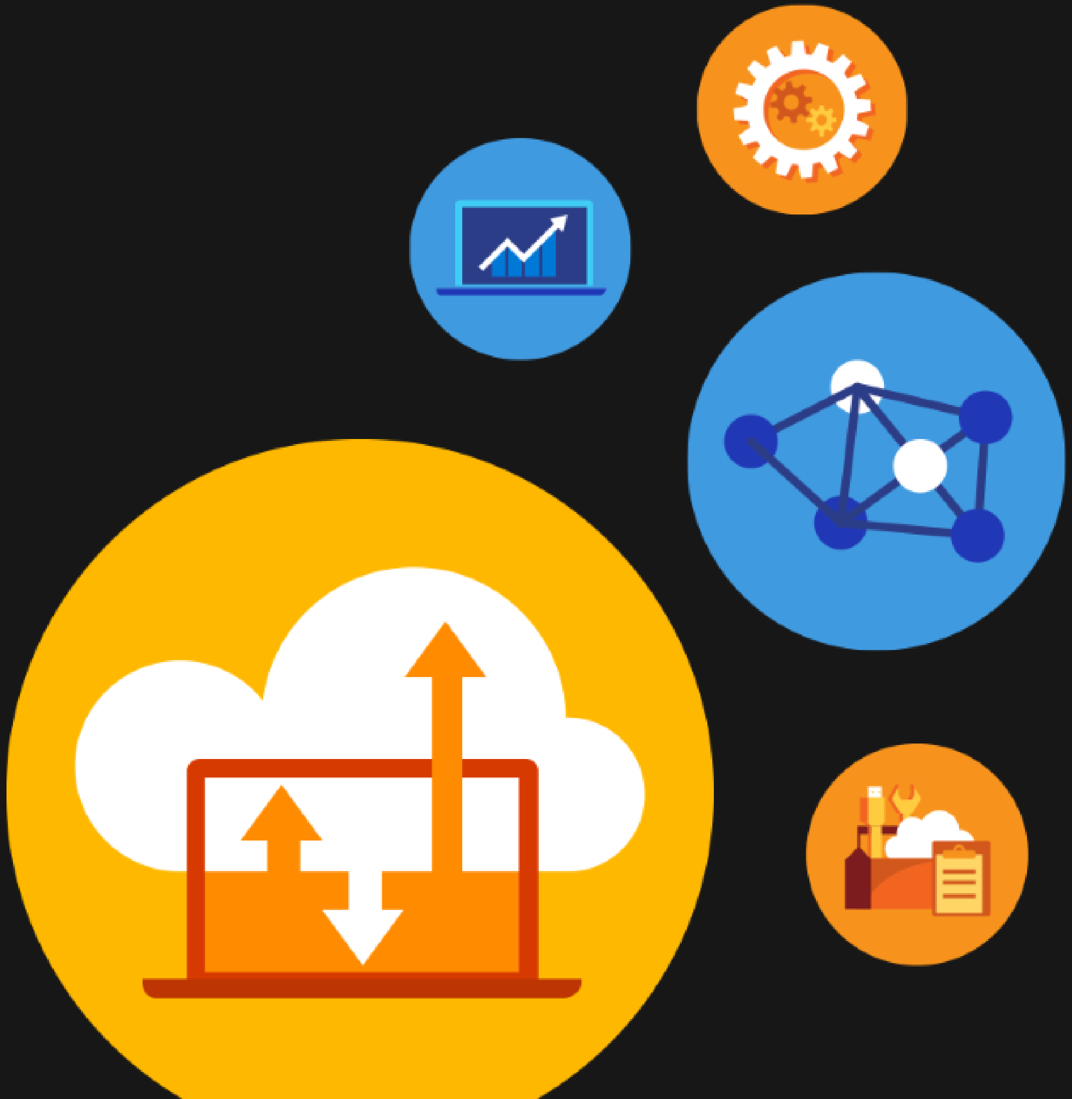
The Cloud is Changing the Paradigm for Safeguarding Information Systems & Applications

Scott Oxley
Security Architect
Azure Government
Scott.oxley@microsoft.com

Ryan Socal
Senior Program Manager
Azure Government
ryansoc@microsoft.com



Microsoft

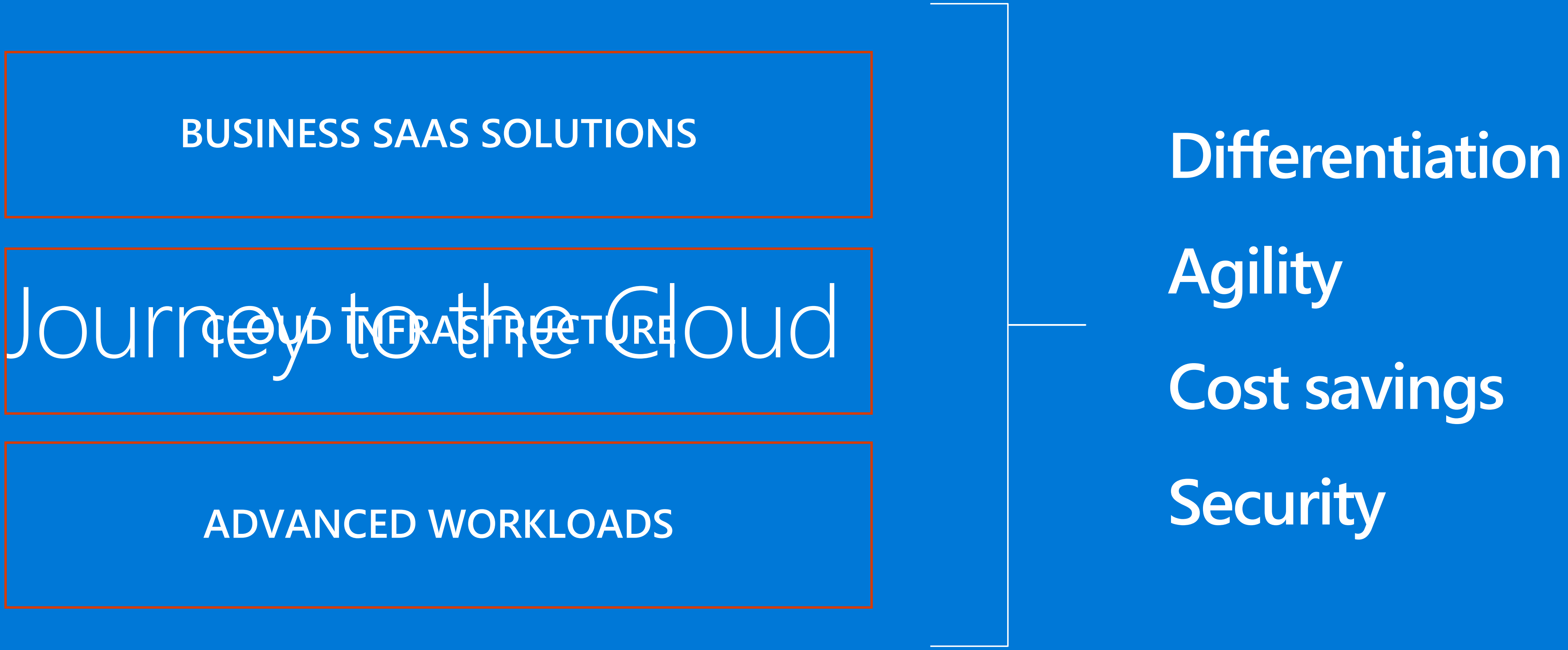
Microsoft

Agenda

1. What is the Cloud
2. What is Azure Government
3. A Network of Secured Systems
4. Software Defined Networking & Security
5. Resources & Questions

What is the Cloud?

Journey to the Cloud



BUSINESS SAAS SOLUTIONS

CLOUD INFRASTRUCTURE

ADVANCED WORKLOADS

Differentiation

Agility

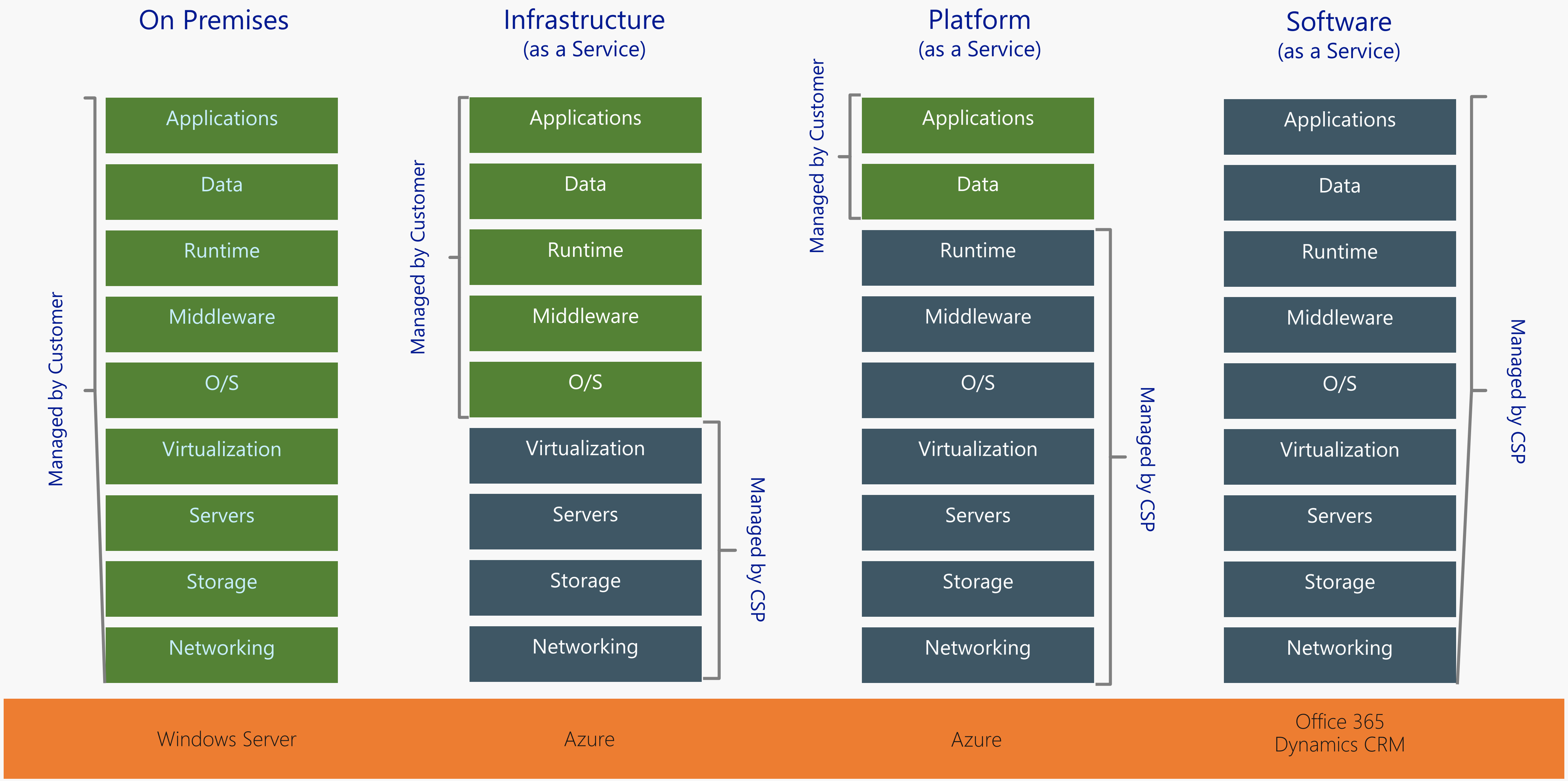
Cost savings

Security

5-4-3 : Cloud!

- 5 Characteristics:
  - On-Demand
  - Device Independent
  - Multi-Tenant
  - Rapidly Elastic
  - Measured Service
- 4 Deployment Types:
  - Private
  - Public
  - Community
  - Hybrid
- 3 Service Models:
  - IaaS
  - PaaS
  - SaaS

What a Cloud Looks Like:



On Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking
Windows Server	Azure	Azure	Office 365 Dynamics CRM

What is Azure Government?

Azure Government

- Secure/compliant cloud for US government only
- Operated by screened US persons
- Agencies can take advantage of instant scalability

Microsoft Azure

We are investing big in Government!

100

New releases in the last 3 months in Azure Gov

21 Virtual Machine Images including SUSE, SQL Server, Ubuntu, Visual Studio, and Dynamics

7 FedRAMP certified services – ARM, Media Services, Automation, Batch, Scheduler, Log Analytics, Redis Cache

Azure Blueprint for FedRAMP High Baseline

Azure Resource Manager – Event Hubs

Azure Resource Manager – Service Bus

Portal Extension – Log Analytics

Portal Extension – Service Bus

Portal Extension – Event Hubs

VM Extension – VM Snapshot

VM Extension – VM Snapshot Linux

Presence & Connectivity

Defense

Microsoft Government Cloud

The most comprehensive cloud for DoD missions

Office 365

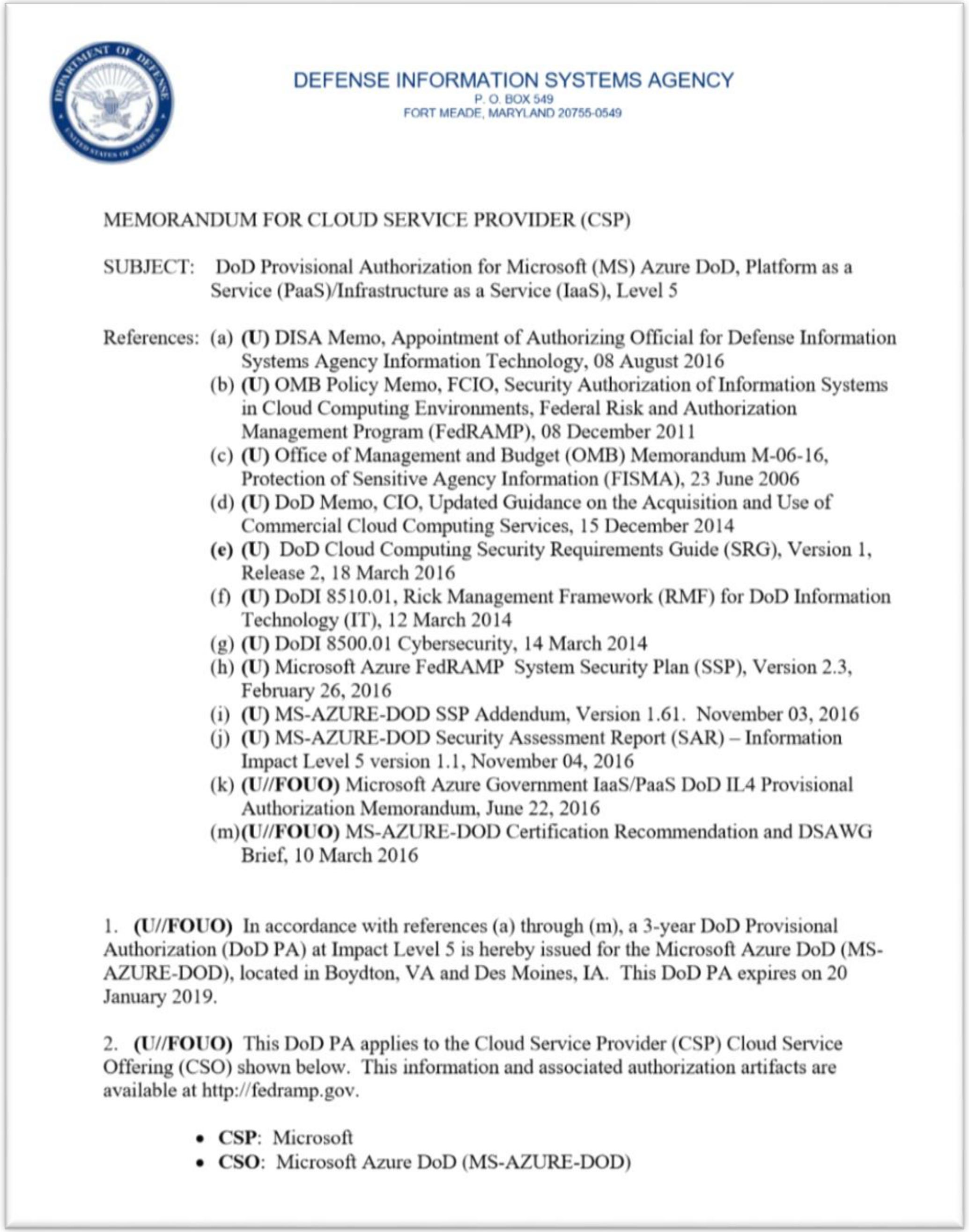
Microsoft Azure Government

Complete Cloud Solution for DoD with L5 with O365 and Azure Government

DoD Region live supporting L5 mission workloads

Azure DoD L5

- Achieved Jan 6 2017 highlighting our commitment to the deepest levels of compliance for our customers
- Implementation for the Department of Defense involves a dedicated Azure region infrastructure
- Availability today
    - Connectivity to DoD network through express route
    - Support for traffic inspection using DoD infrastructure
    - Ability to connect without internet / during cyber event



DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

MEMORANDUM FOR CLOUD SERVICE PROVIDER (CSP)

SUBJECT: DoD Provisional Authorization for Microsoft (MS) Azure DoD, Platform as a Service (PaaS)/Infrastructure as a Service (IaaS), Level 5

References: (a) **(U)** DISA Memo, Appointment of Authorizing Official for Defense Information Systems Agency Information Technology, 08 August 2016
(b) **(U)** OMB Policy Memo, FCIO, Security Authorization of Information Systems in Cloud Computing Environments, Federal Risk and Authorization Management Program (FedRAMP), 08 December 2011
(c) **(U)** Office of Management and Budget (OMB) Memorandum M-06-16, Protection of Sensitive Agency Information (FISMA), 23 June 2006
(d) **(U)** DoD Memo, CIO, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, 15 December 2014
(e) **(U)** DoD Cloud Computing Security Requirements Guide (SRG), Version 1, Release 2, 18 March 2016
(f) **(U)** DoDI 8510.01, Rick Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014
(g) **(U)** DoDI 8500.01 Cybersecurity, 14 March 2014
(h) **(U)** Microsoft Azure FedRAMP System Security Plan (SSP), Version 2.3, February 26, 2016
(i) **(U)** MS-AZURE-DOD SSP Addendum, Version 1.61. November 03, 2016
(j) **(U)** MS-AZURE-DOD Security Assessment Report (SAR) – Information Impact Level 5 version 1.1, November 04, 2016
(k) **(U//FOUO)** Microsoft Azure Government IaaS/PaaS DoD IL4 Provisional Authorization Memorandum, June 22, 2016
(m)**(U//FOUO)** MS-AZURE-DOD Certification Recommendation and DSAWG Brief, 10 March 2016

1. **(U//FOUO)** In accordance with references (a) through (m), a 3-year DoD Provisional Authorization (DoD PA) at Impact Level 5 is hereby issued for the Microsoft Azure DoD (MS-AZURE-DOD), located in Boydton, VA and Des Moines, IA. This DoD PA expires on 20 January 2019.

2. **(U//FOUO)** This DoD PA applies to the Cloud Service Provider (CSP) Cloud Service Offering (CSO) shown below. This information and associated authorization artifacts are available at http://fedramp.gov.

- **CSP**: Microsoft
- **CSO**: Microsoft Azure DoD (MS-AZURE-DOD)

Security & Compliance

The Trusted Cloud

Azure has the deepest and most comprehensive compliance coverage in the industry

GLOBAL

- ISO 27001
- ISO 27018
- ISO 27017
- ISO 22301
- ISO 9001
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CSA STAR Self-Assessment
- CSA STAR Certification
- CSA STAR Attestation

US GOV

- Moderate JAB P-ATO
- High JAB P-ATO
- DoD DISA SRG Level 2
- DoD DISA SRG Level 4
- DoD DISA SRG Level 5
- SP 800-171
- FIPS 140-2
- Section 508 VPAT
- ITAR
- CJIS
- IRS 1075

INDUSTRY

- PCI DSS Level 1
- CDSA
- MPAA
- FACT UK
- Shared Assessments
- FISC Japan
- HIPAA / HITECH Act
- HITRUST
- GxP 21 CFR Part 11
- MARS-E
- IG Toolkit UK
- FERPA
- GLBA
- FFIEC

REGIONAL

- Argentina PDPA
- EU Model Clauses
- UK G-Cloud
- China DJCP
- China GB 18030
- China TRUCS
- Singapore MTCS
- Australia IRAP/CCSL
- New Zealand GCIO
- Japan My Number Act
- ENISA IAF
- Japan CS Mark Gold
- Spain ENS
- Spain DPA
- India MeitY
- Canada Privacy Laws
- Privacy Shield
- Germany IT Grundschutz workbook

Department of Justice ★ Federal Bureau of Investigation
★ Criminal Justice Information Services Division ★
To Connect
To Identify
To Know
Serving Our Citizens
CJIS

CJIS: 24 states

covering more than 2/3 of the population

FedRAMP

32 Azure Government services authorized

FedRAMP High
June 2016

Supports
FISMA High

TIC 2.0
Compliant

32 services covered

Making compliance easier for you.

Azure Blueprint

Fast track to certification and compliance of applications built on Azure

- Architecture
- Deployment
- Certification
- Expertise
- Partnership

5-step process that streamlines paperwork through templates and tools, and allows your security professionals to focus on security—not paperwork

Azure US Federal Civilian Blueprint

For applications and infrastructure requiring FedRAMP Moderate or High

Architecture

Resources that outline baseline system configurations and control mappings to streamline secure design

Certification

Artifacts that streamline paperwork through templates and tools, reducing control responsibility for customers by nearly 30% for IaaS and 40% for PaaS.

Deployment

ARM template with baselined three tier application that can be customized to suit your needs

Expertise

Customer access to Azure SMEs and partners to handle your toughest questions or consulting needs.

Azure Blueprint

Solutions to address vertical industries

- US Federal Civilian
  Covering FedRAMP & FedRAMP High
- US Defense
  Covering DISA L4 and DISA L5
- Defense Industrial Base
  Covering 800-171, ITAR and DFARs
- US State & Local Gov.
  Covering CJIS & IRS 1075
- Online Commerce
  Covering PCI
- Energy & Critical Infra.
  Coming soon
- Financial Services
  Covering FFIEC, GLBA, SOC
- Media & Entertainment
  Coming soon
- UK Public Sector
  Covering UK Gov-Cloud
- Healthcare
  Covering HIPAA, HITECH, HITRUST, MARS-e

Defense Federal Acquisition Regulation Supplement (DFARS)

Defense Federal Acquisition Regulation Supplement Support with Azure Government

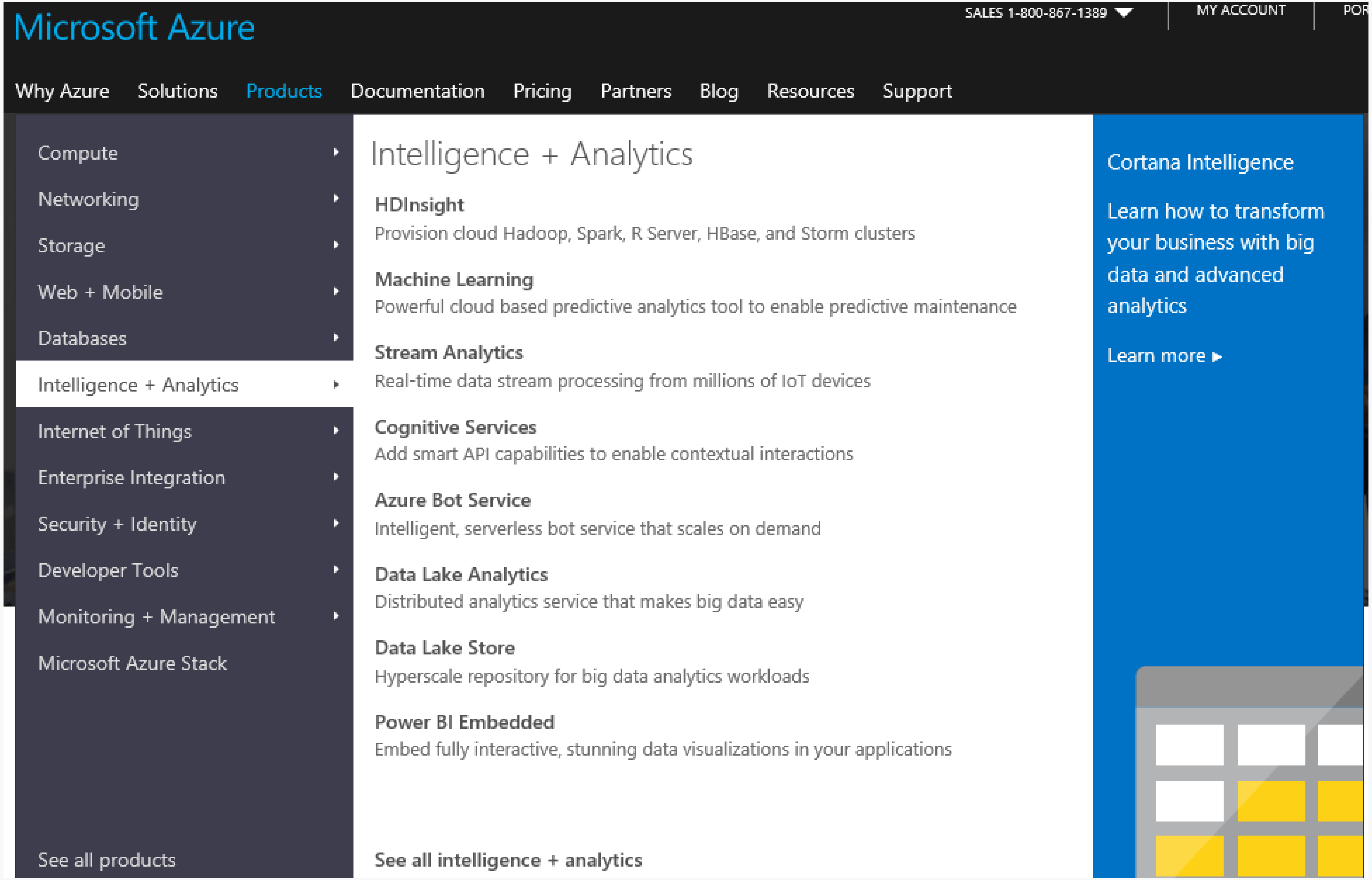
- Azure Government accepts DFARS Contractual Flow-Downs
- Exceeds DFARS Security Requirements
  - FedRAMP High
  - DISA L4 & L5
- Independently Validated by 3PAO
  - DFARS 252.204-7012
  - NIST 800-171

DFARS 252.204-7012	Azure Government
Adequate Security	✓
Cyber Incident Reporting	✓
Malicious Software	✓
Media Preservation and Protection	✓
Forensic Analysis	✓
Cyber Incident Damage Assessment	✓

Cloud Multi-Tenancy: Network of Secured Systems

Microsoft

Azure Products view from Azure.com



Microsoft Azure

SALES 1-800-867-1389 ▼ | MY ACCOUNT | POR

Why Azure · Solutions · Products · Documentation · Pricing · Partners · Blog · Resources · Support

- Compute ▸
- Networking ▸
- Storage ▸
- Web + Mobile ▸
- Databases ▸
- Intelligence + Analytics ▸
- Internet of Things ▸
- Enterprise Integration ▸
- Security + Identity ▸
- Developer Tools ▸
- Monitoring + Management ▸
- Microsoft Azure Stack

See all products

Intelligence + Analytics

HDInsight
Provision cloud Hadoop, Spark, R Server, HBase, and Storm clusters

Machine Learning
Powerful cloud based predictive analytics tool to enable predictive maintenance

Stream Analytics
Real-time data stream processing from millions of IoT devices

Cognitive Services
Add smart API capabilities to enable contextual interactions

Azure Bot Service
Intelligent, serverless bot service that scales on demand

Data Lake Analytics
Distributed analytics service that makes big data easy

Data Lake Store
Hyperscale repository for big data analytics workloads

Power BI Embedded
Embed fully interactive, stunning data visualizations in your applications

See all intelligence + analytics

Cortana Intelligence

Learn how to transform your business with big data and advanced analytics

Learn more ▸

Security & Management

- Security Center
- Portal
- Azure Active Directory
- Azure AD B2C
- Multi-Factor Authentication
- Automation
- Scheduler
- Key Vault
- Store/ Marketplace
- VM Image Gallery & VM Depot

Platform Services

Media & CDN

- Media Services
- Media Analytics
- Content Delivery Network

Integration

- API Management
- BizTalk Services
- Logic Apps
- Service Bus

Compute Services

- Container Service
- VM Scale Sets
- Batch
- RemoteApp
- Dev/Test Lab

Application Platform

- Web Apps
- Mobile Apps
- API Apps
- Cloud Services
- Service Fabric
- Notification Hubs
- Functions

Developer Services

- Visual Studio
- Mobile Engagement
- VS Team Services
- Xamarin
- Application Insights
- HockeyApp

Data

- SQL Database
- SQL Data Warehouse
- DocumentDB
- SQL Server Stretch Database
- Redis Cache
- Storage Tables
- Azure Search

Intelligence

- Cognitive Services
- Bot Framework
- Cortana

Analytics & IoT

- HDInsight
- Machine Learning
- Stream Analytics
- Data Catalog
- Data Lake Analytics Service
- Data Lake Store
- IoT Hub
- Event Hubs
- Data Factory
- Power BI Embedded

Hybrid Cloud

- Azure AD Health Monitoring
- AD Privileged Identity Management
- Domain Services
- Backup
- Operational Analytics
- Import/Export
- Azure Site Recovery
- StorSimple

Infrastructure Services

Compute

- Virtual Machines
- Containers

Storage

- Blob
- Queues
- Files
- Disks

Networking

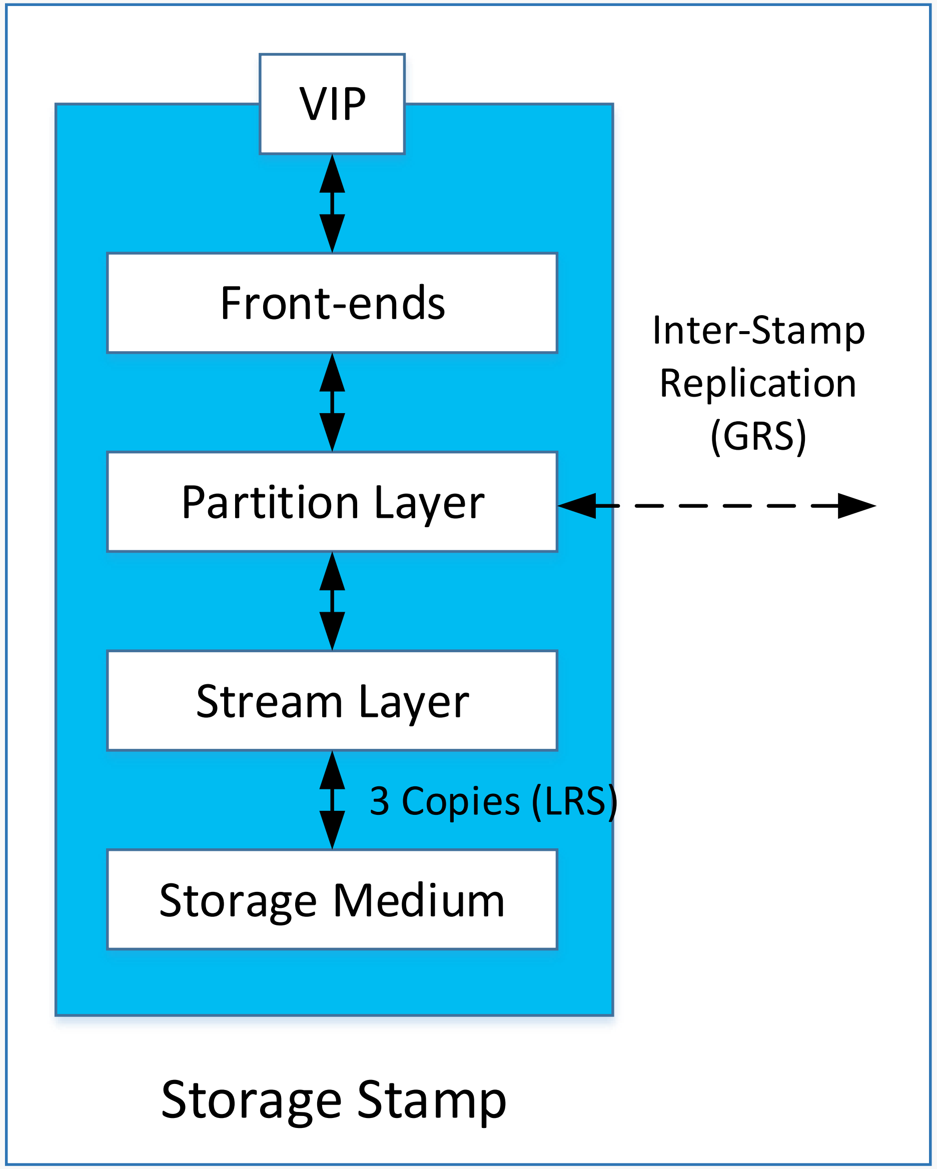
- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- App Gateway

38 Azure regions, more than any cloud provider

PaaS (Storage) Overview

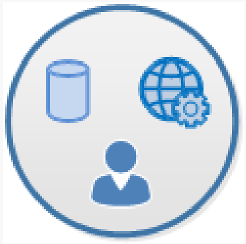
- Storage stamp is a cluster of 10-20 racks of storage nodes (10s of PB)
- **Front-end:** authenticates and authorizes access to storage accounts on stamp; caches and streams objects from Stream layer
- **Partition layer:** load balancing by spreading partition names across partition servers; stores object data; replicates data to other stamps
- **Stream layer**: stores bits on disk; replicates data across many servers for durability; does not understand object constructs

- *http://sigops.org/sosp/sosp11/current/2011-Cascais/printable/11-calder.pdf*

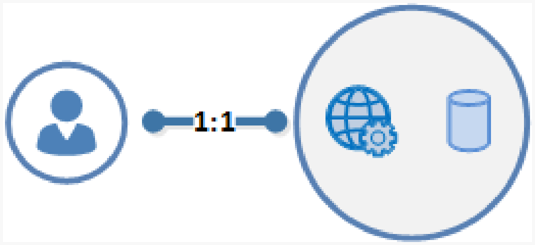


Multi-Tenancy and the Road Ahead

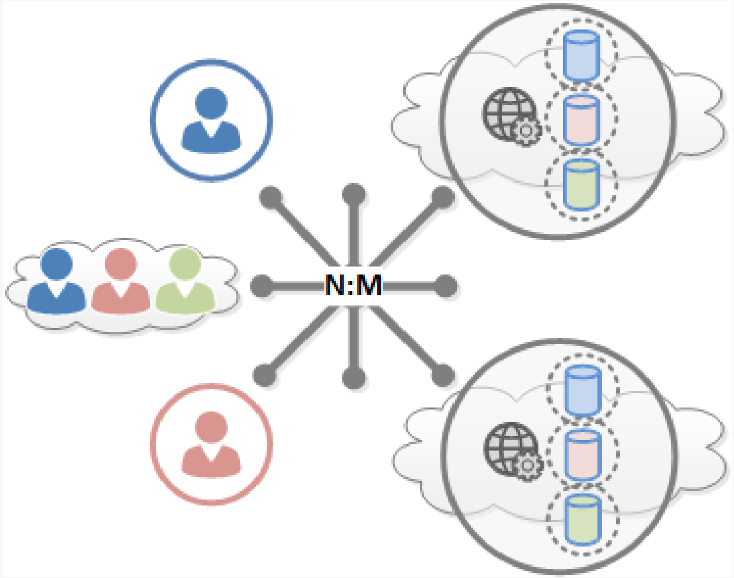
- Assumptions still based on enterprise or on premise agency specific networks
  - Content delivery is no longer 1:1, it is now many:many
  - Network & interconnects are MT
  - Physical & logical isolation; multi-dimensional network



Traditional
on-premise



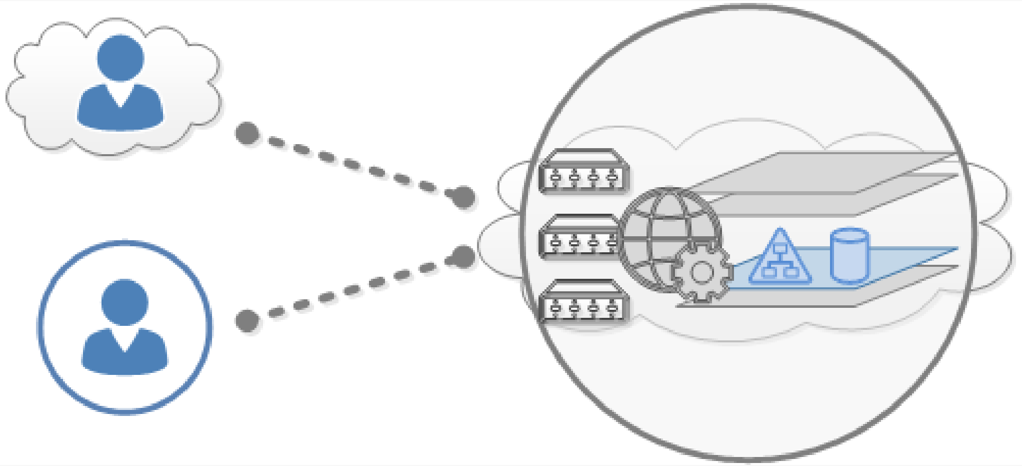
Managed Service



Cloud Services

Multi-Tenancy and the Road Ahead

- Network is not considered the system boundary on its own
  - ➢ Providers’ network is no longer a given customer boundary
  - ➢ Different network layers
  - ➢ Identification of customer data in MT is at the application layer
    - ✓ Not optimal to perform functions at the network layer

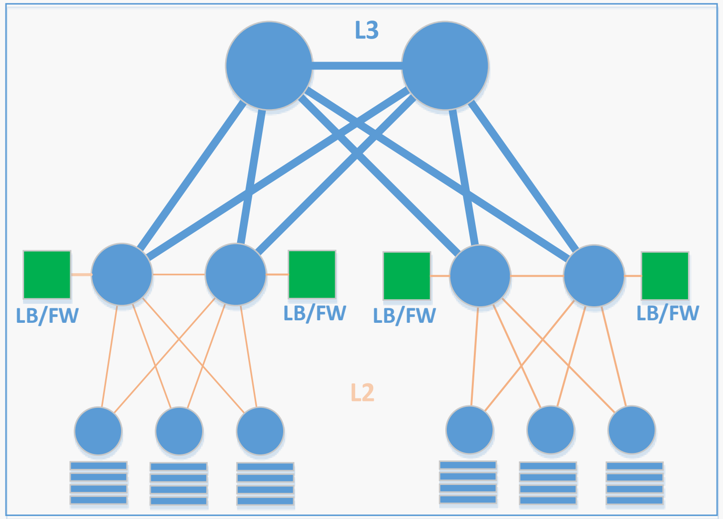


Classic vs. Hyper-scale networks

Large L2 Domains

HW-based service modules

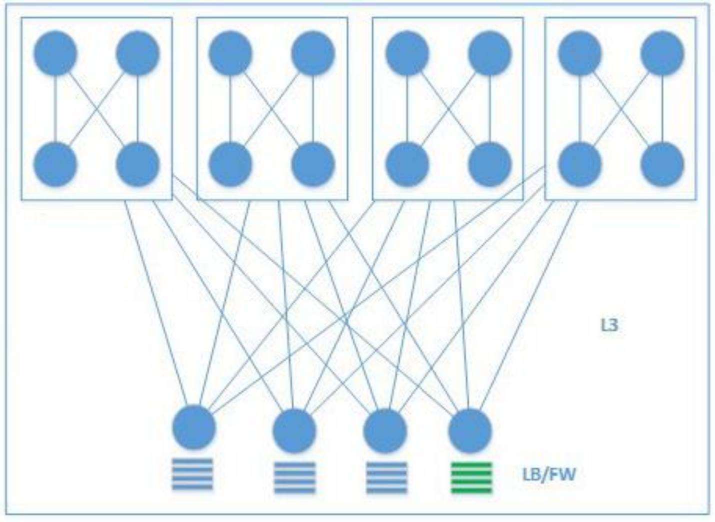
Simple Tree Design



L3 at all layers

Services in software

Clos-based design

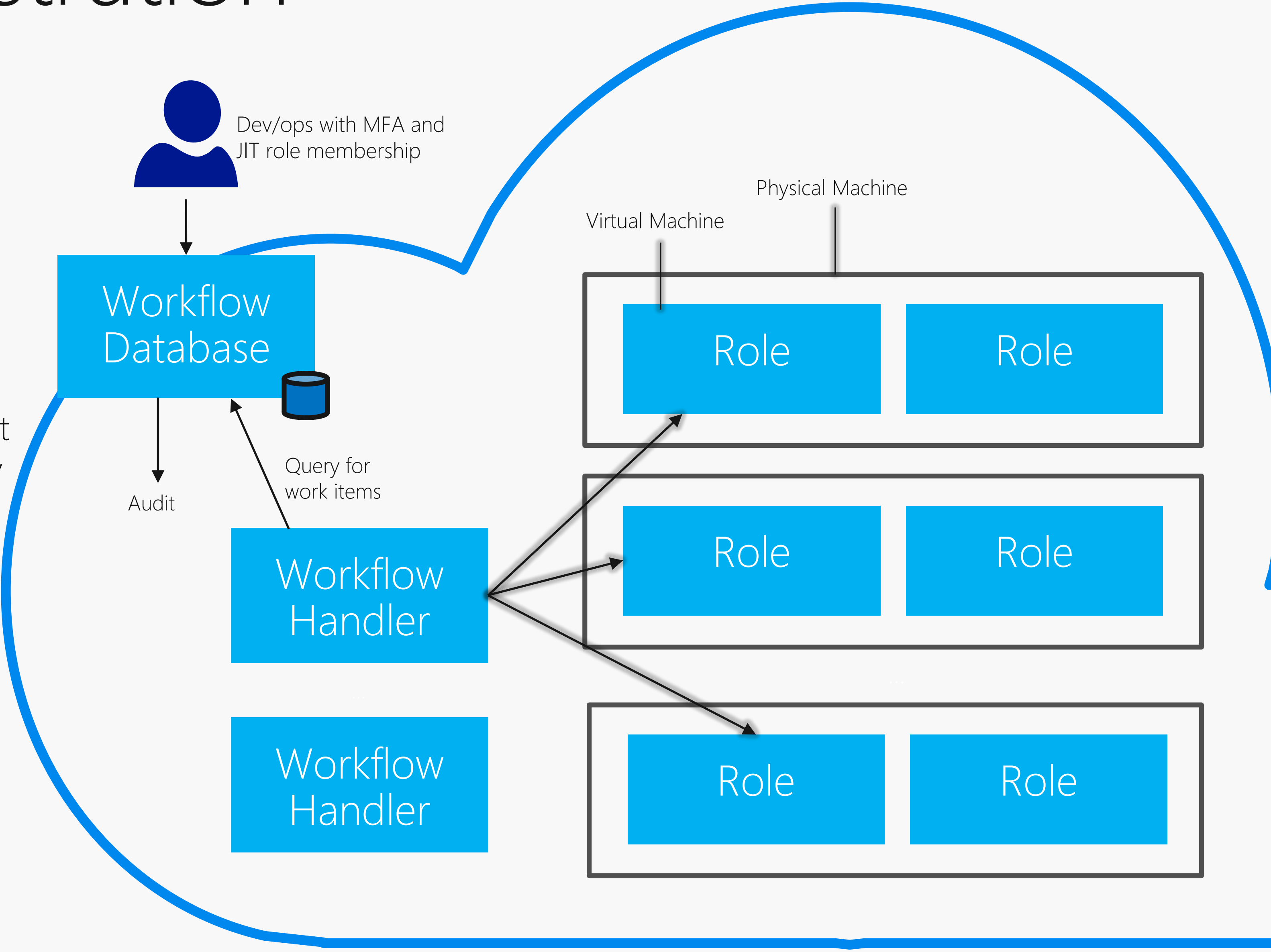


Low due to diversity and manual provisioning process	**Agility**	↑	Automated network provisioning, integrated process
Low due to complex hardware and lack of automated operations	**Efficiency**	↑	Simplify requirements, optimize design, and unify infrastructure
Low due to high complexity and human error	**Availability**	↑	Resilient design, automated monitoring and remediation, minimum human involvement

Secure Administration

Distributed deployment workflow execution engine.

- Workflows are pre-defined common service management tasks as compiled binaries (e.g. restart a machine, offline a replica, upgrade a role).
- Workflows are classified based on the actions they take (e.g. privileged, non-privileged).
- User (dev/ops) submitting workflow execution must belong to the appropriate security groups. Security group membership is just-in-time. Access to sensitive workflows requires manual approval following a “two-key” authorization model.
- After MFA (with smartcard) and just-in-time role elevation (with approval) dev/ops submit a workflow to the DMS workflow database.
- The workflow submission is audited.
- Soon after, a DMS workflow handler will query the database for new work items, and execute them against the roles in question.



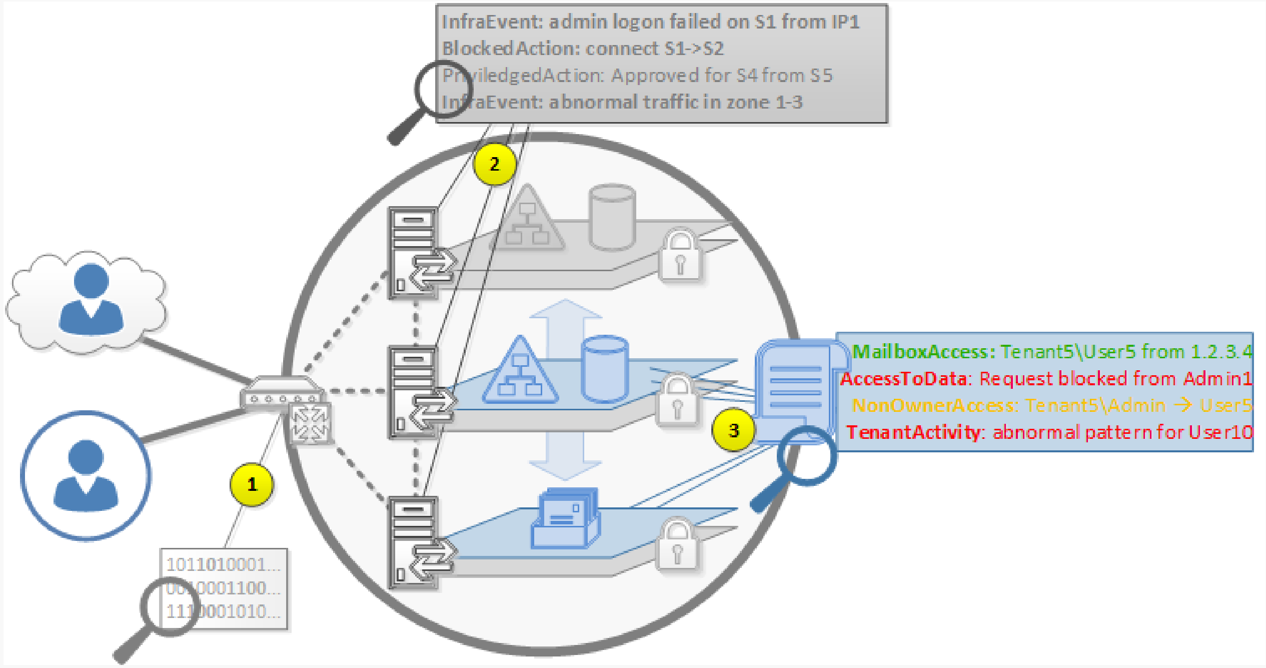
Network Visibility: Monitoring, Logging & Telemetry

- Customers expect…
  - Transparency & control
  - Identity management, MFA, claims-based validation
  - Telemetry
  - High fidelity & real-time anomaly detection
  - End-to-end visibility

… this is delivered by the CSP & inherent at the app layer, which provides richer contextual data

- Traditional perimeter monitoring has limited value because of its incomplete contextual awareness about all data & systems access patterns

  - Embedded security throughout life cycle of threat core to cloud



```
InfraEvent: admin logon failed on S1 from IP1
BlockedAction: connect S1->S2
PriviledgedAction: Approved for S4 from S5
InfraEvent: abnormal traffic in zone 1-3
```

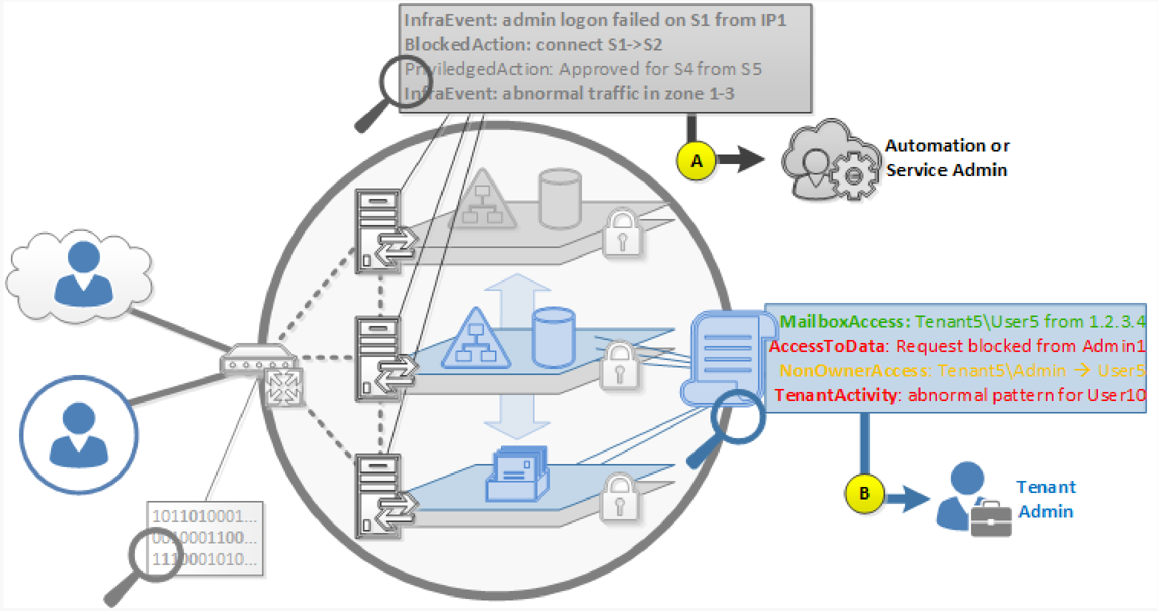
```
MailboxAccess: Tenant5\User5 from 1.2.3.4
AccessToData: Request blocked from Admin1
NonOwnerAccess: Tenant5\Admin → User5
TenantActivity: abnormal pattern for User10
```

```
1011010001…
0010001100…
1110001010…
```

Security State Visibility:
Telemetry, Logging, Correlation & Monitoring

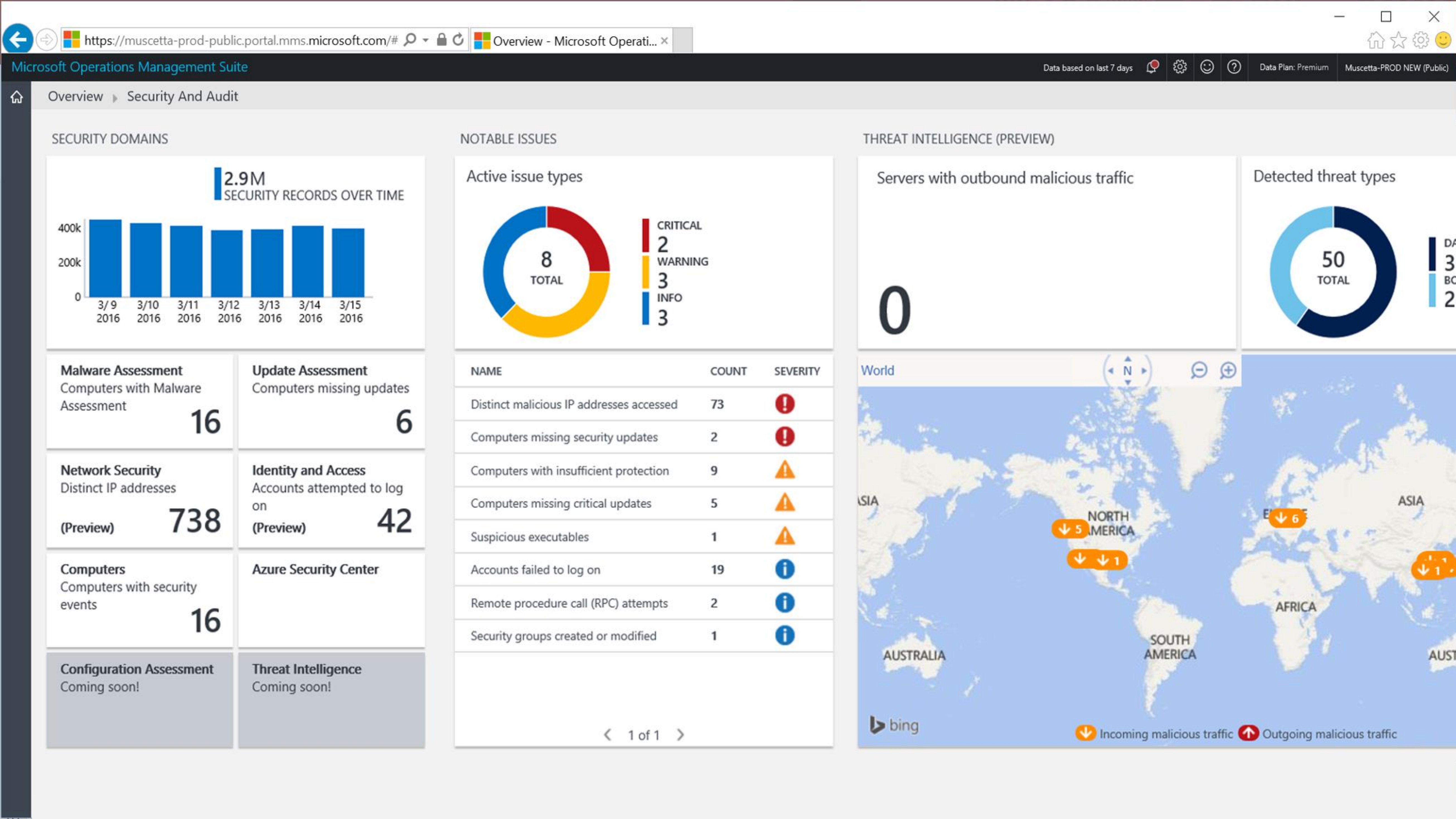
- Shift to cloud scale Logging & monitoring enhances control & capabilities
  - ➢ CSP provides logging capabilities based on industry best practices
    - ✓ CSP use on *service* logs
    - ✓ Customer control & retrieval of *tenant* logs
    - ✓ Cloud scale common logging & monitoring is MT friendly
  - ➢ Customers acting on output of log data

- Shared Services Model across USG
  - ➢ Perimeter security vs. embedded security
  - ➢ Broader sharing of common services



```
InfraEvent: admin logon failed on S1 from IP1
BlockedAction: connect S1->S2
PriviledgedAction: Approved for S4 from S5
InfraEvent: abnormal traffic in zone 1-3
```

```
MailboxAccess: Tenant5\User5 from 1.2.3.4
AccessToData: Request blocked from Admin1
NonOwnerAccess: Tenant5\Admin → User5
TenantActivity: abnormal pattern for User10
```


https://muscetta-prod-public.portal.mms.microsoft.com/#
Overview - Microsoft Operati...
Microsoft Operations Management Suite
Data based on last 7 days
Data Plan: Premium
Muscetta-PROD NEW (Public)
Overview
Security And Audit

SECURITY DOMAINS

2.9M
SECURITY RECORDS OVER TIME

400k
200k
0
3/9 2016
3/10 2016
3/11 2016
3/12 2016
3/13 2016
3/14 2016
3/15 2016

Malware Assessment
Computers with Malware Assessment
16

Update Assessment
Computers missing updates
6

Network Security
Distinct IP addresses
(Preview)
738

Identity and Access
Accounts attempted to log on
(Preview)
42

Computers
Computers with security events
16

Azure Security Center

Configuration Assessment
Coming soon!

Threat Intelligence
Coming soon!

NOTABLE ISSUES

Active issue types

NAME	COUNT	SEVERITY
Distinct malicious IP addresses accessed	73	!
Computers missing security updates	2	!
Computers with insufficient protection	9	⚠
Computers missing critical updates	5	⚠
Suspicious executables	1	⚠
Accounts failed to log on	19	ℹ
Remote procedure call (RPC) attempts	2	ℹ
Security groups created or modified	1	ℹ

‹ 1 of 1 ›

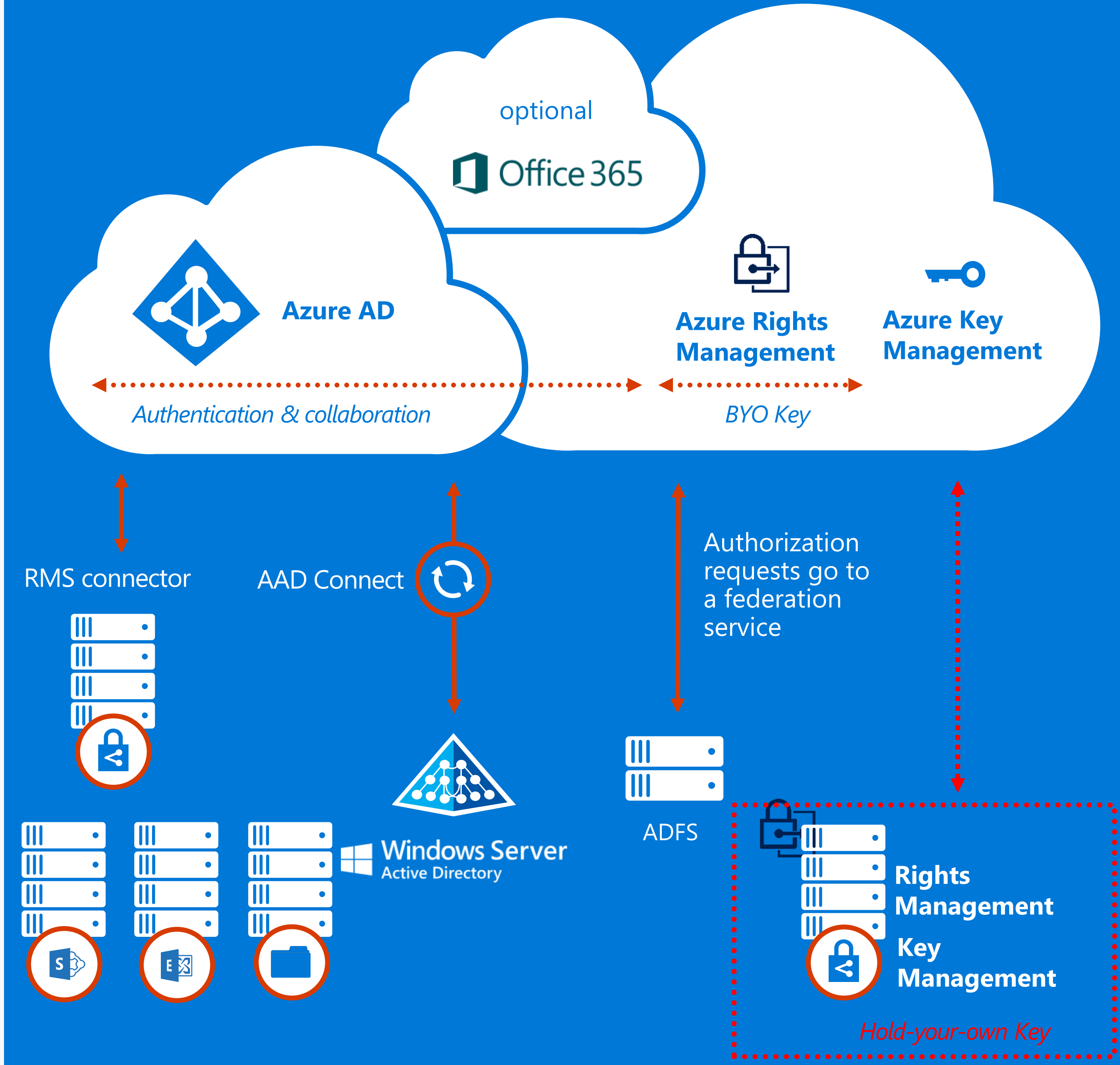
THREAT INTELLIGENCE (PREVIEW)

Servers with outbound malicious traffic
0

Detected threat types

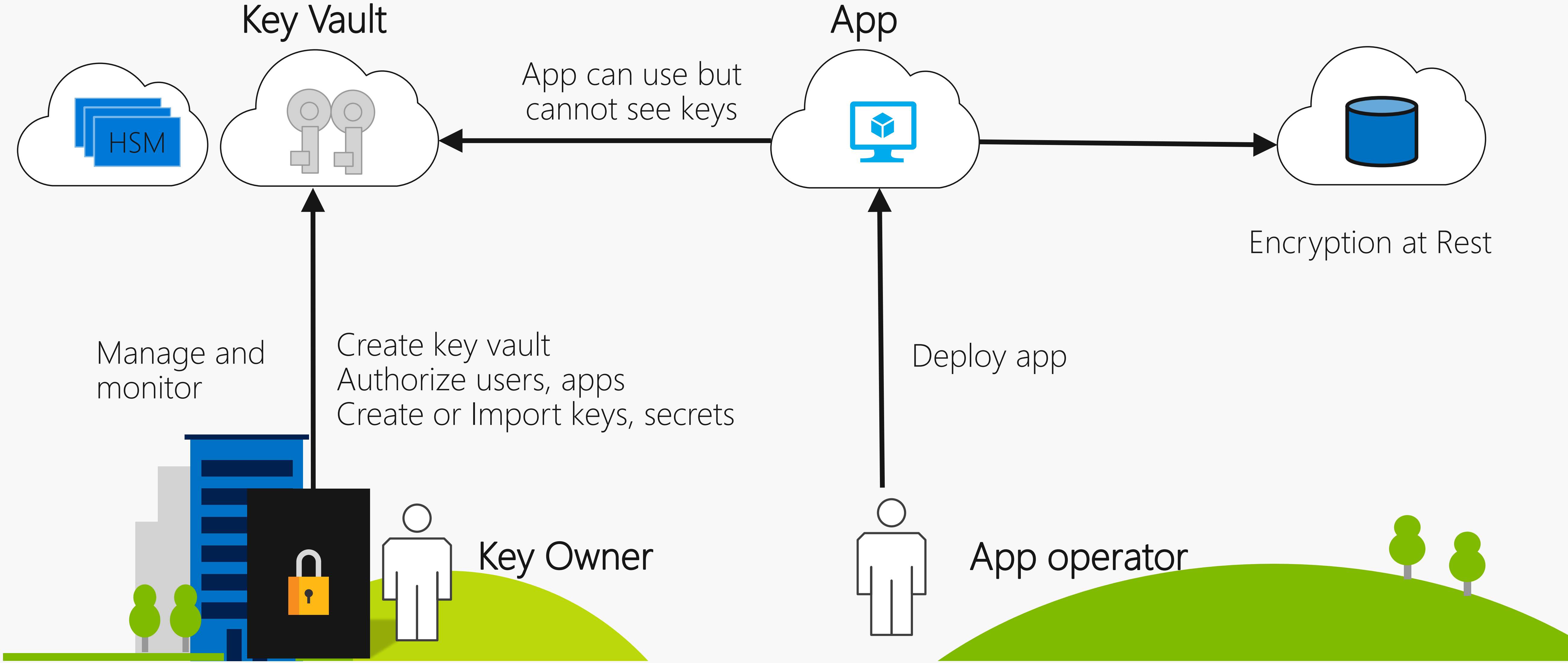
Data Loss Prevention

- Data protection for organizations at different stages of cloud adoption
- Ensures security because sensitive data is never sent to the RMS server
- Integration with on-premises assets with minimal effort
- **Hold your key on premises**



Classified as Microsoft General

Secrets Management



Key Vault

App

App can use but cannot see keys

Encryption at Rest

Manage and monitor

Create key vault
Authorize users, apps
Create or Import keys, secrets

Deploy app

Key Owner

App operator

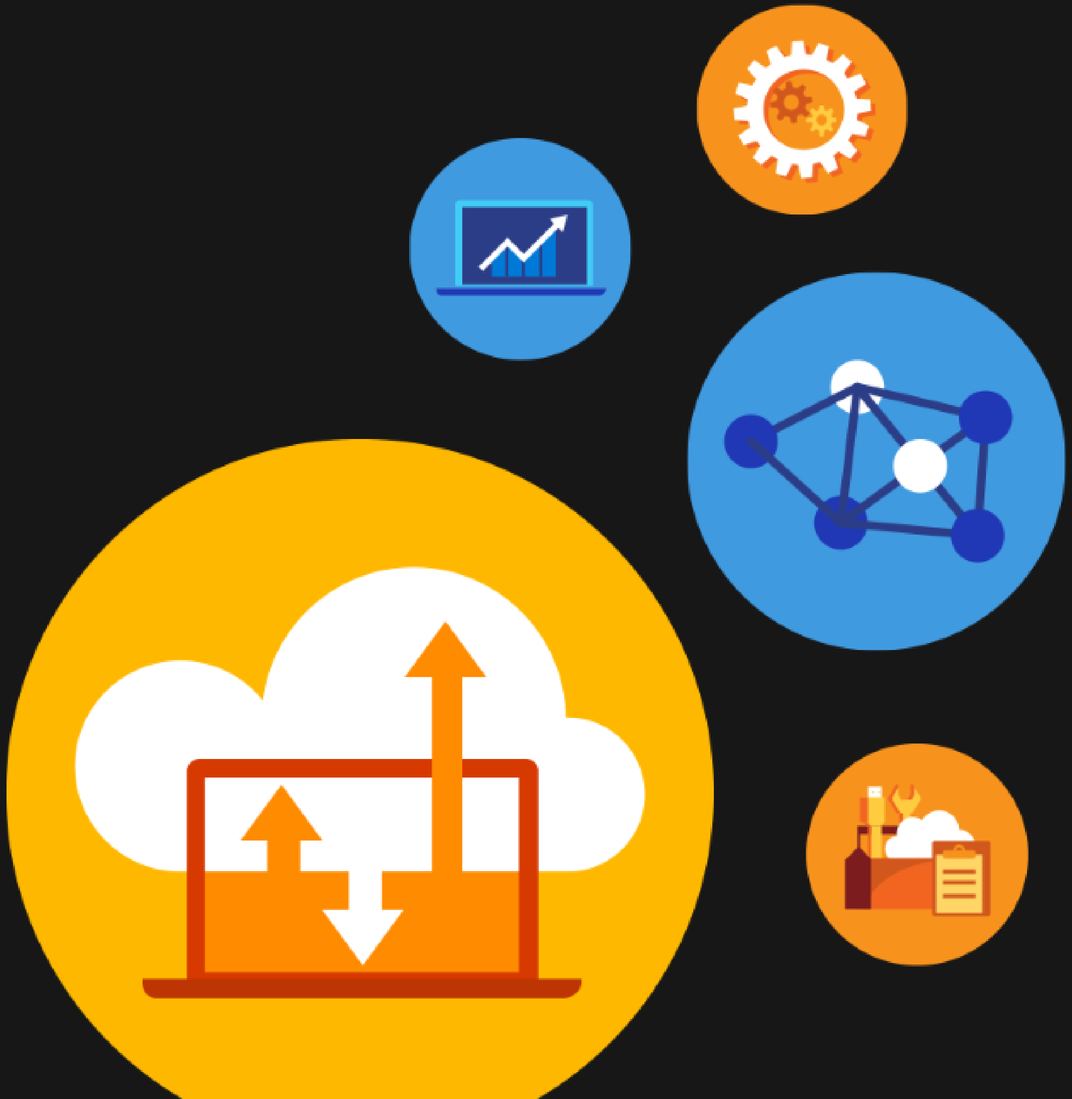
Powering the Cloud: Software Provisioned Services

- What is it?
  - ➢ Software capabilities at hyperscale
  - ➢ Services your applications depend on
    - ✓ Virtual Networks for IaaS & PaaS
    - ✓ Software Defined Networking
    - ✓ Software Load Balancing
    - ✓ Virtual Appliances
    - ✓ Cloud Services Endpoints

- For customer, greatest relevant value at virtual network layer not at physical network layer of CSO (Cloud Service Offering)

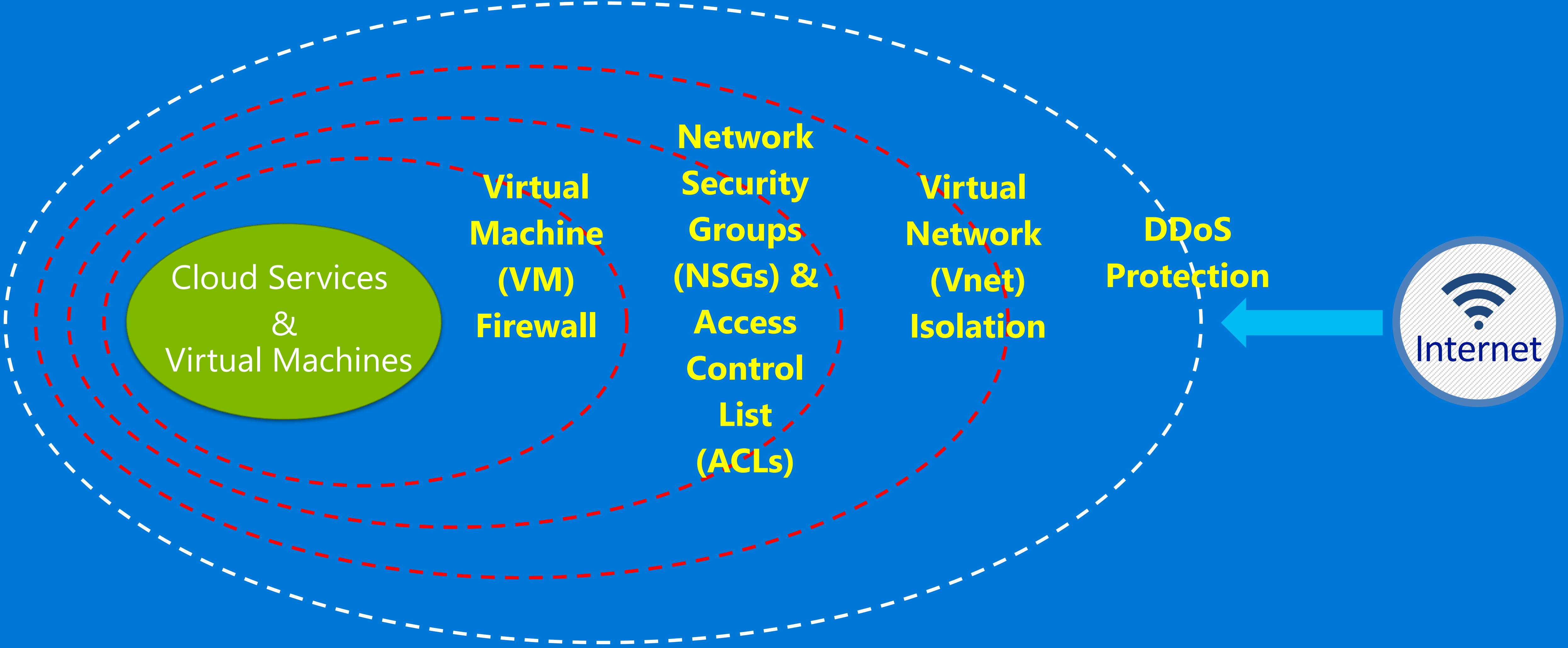
- Rate of innovation means all future investments at the software layer; which can now out pace and out scale traditional hardware

Azure Software Defined Networking & Security



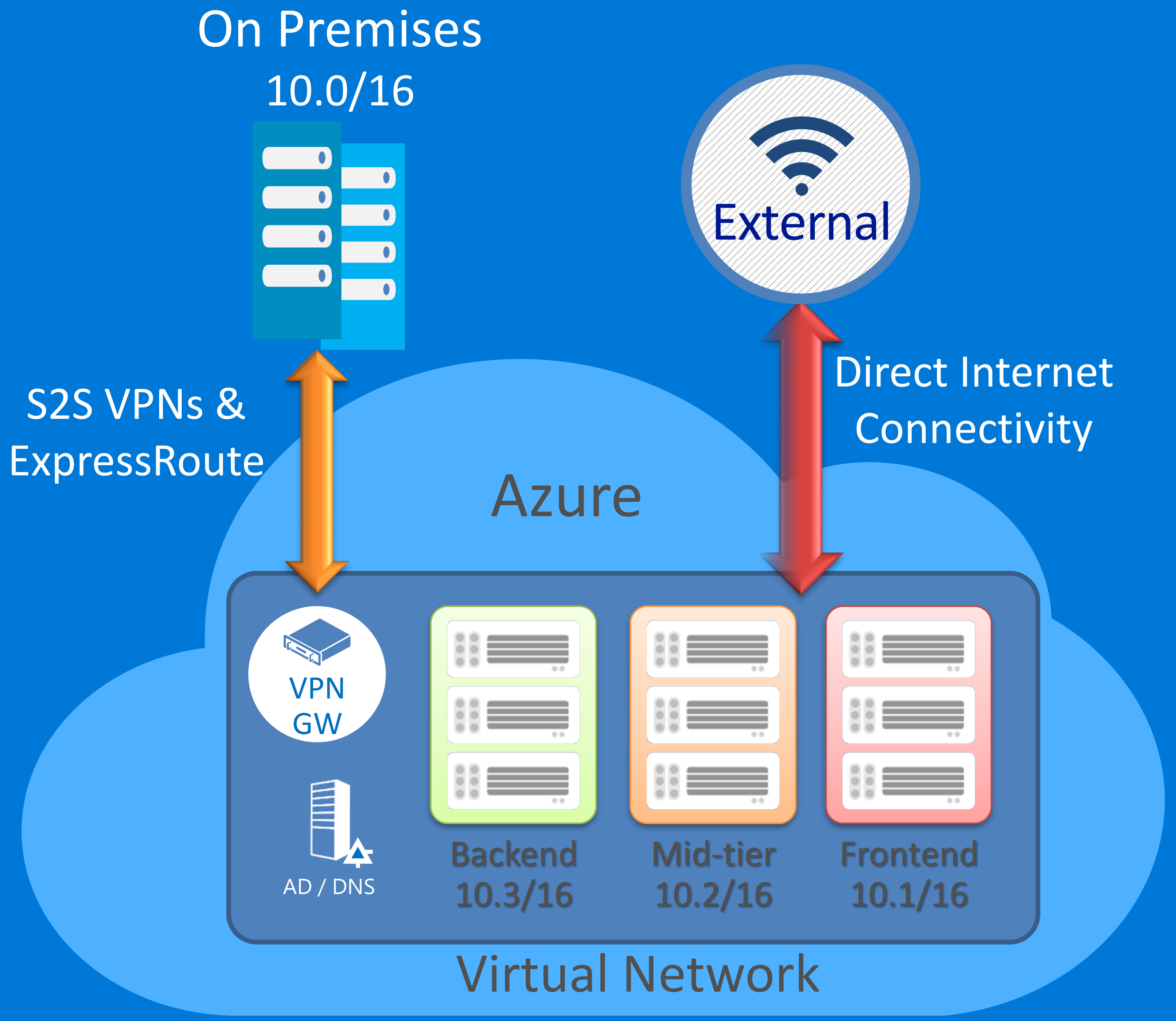
Microsoft

Layered Security, Protection, and Isolation


Cloud Services
&
Virtual Machines
Virtual Machine (VM) Firewall
Network Security Groups (NSGs) & Access Control List (ACLs)
Virtual Network (Vnet) Isolation
DDoS Protection
Internet

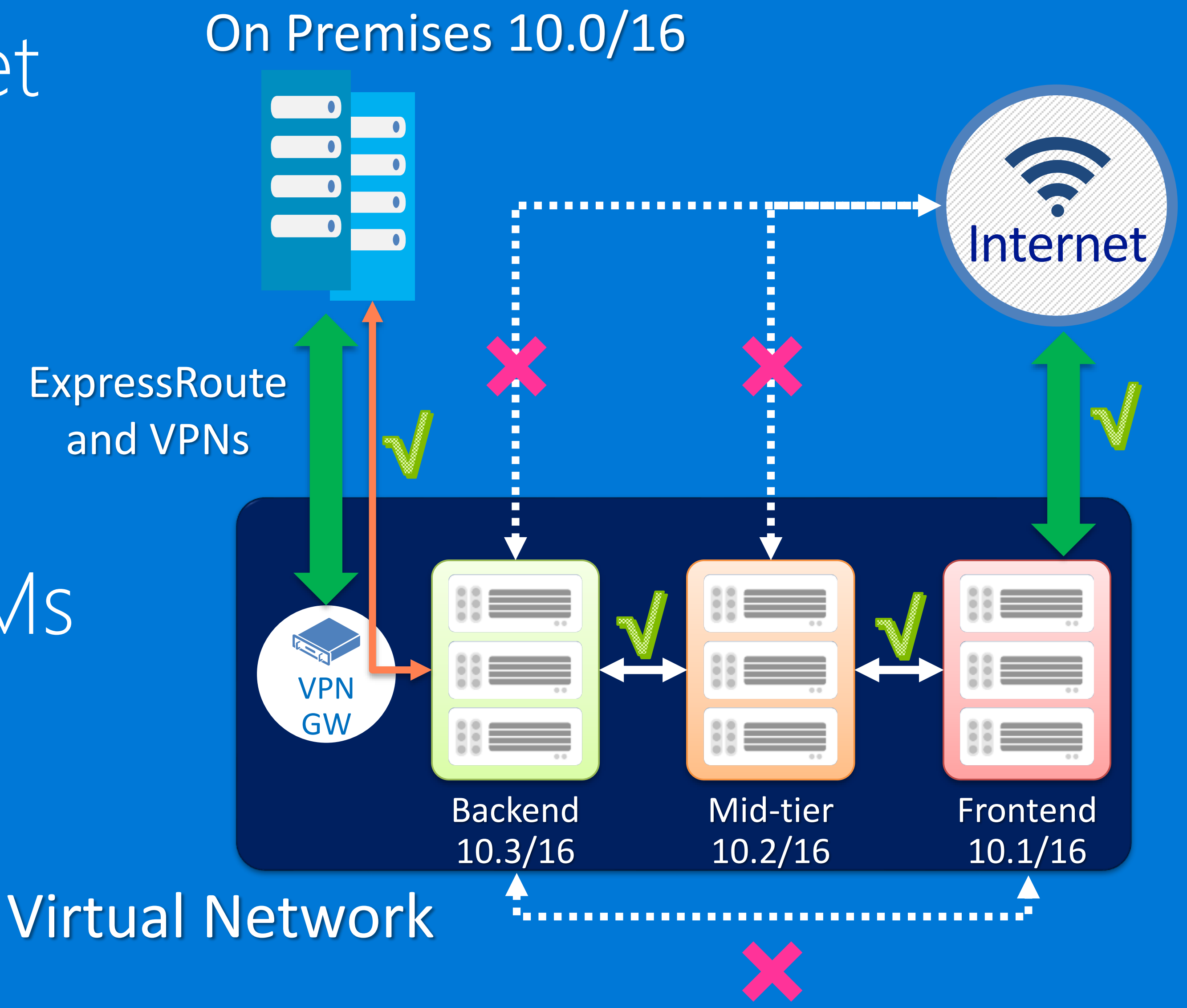
Azure Virtual Network

- Logical isolation with control over network
- Create subnets with your private or public* IP address spaces
- Stable and persistent private IP addresses
- Bring your own DNS or use Azure-provided DNS
- Secure VMs with Network Security Groups



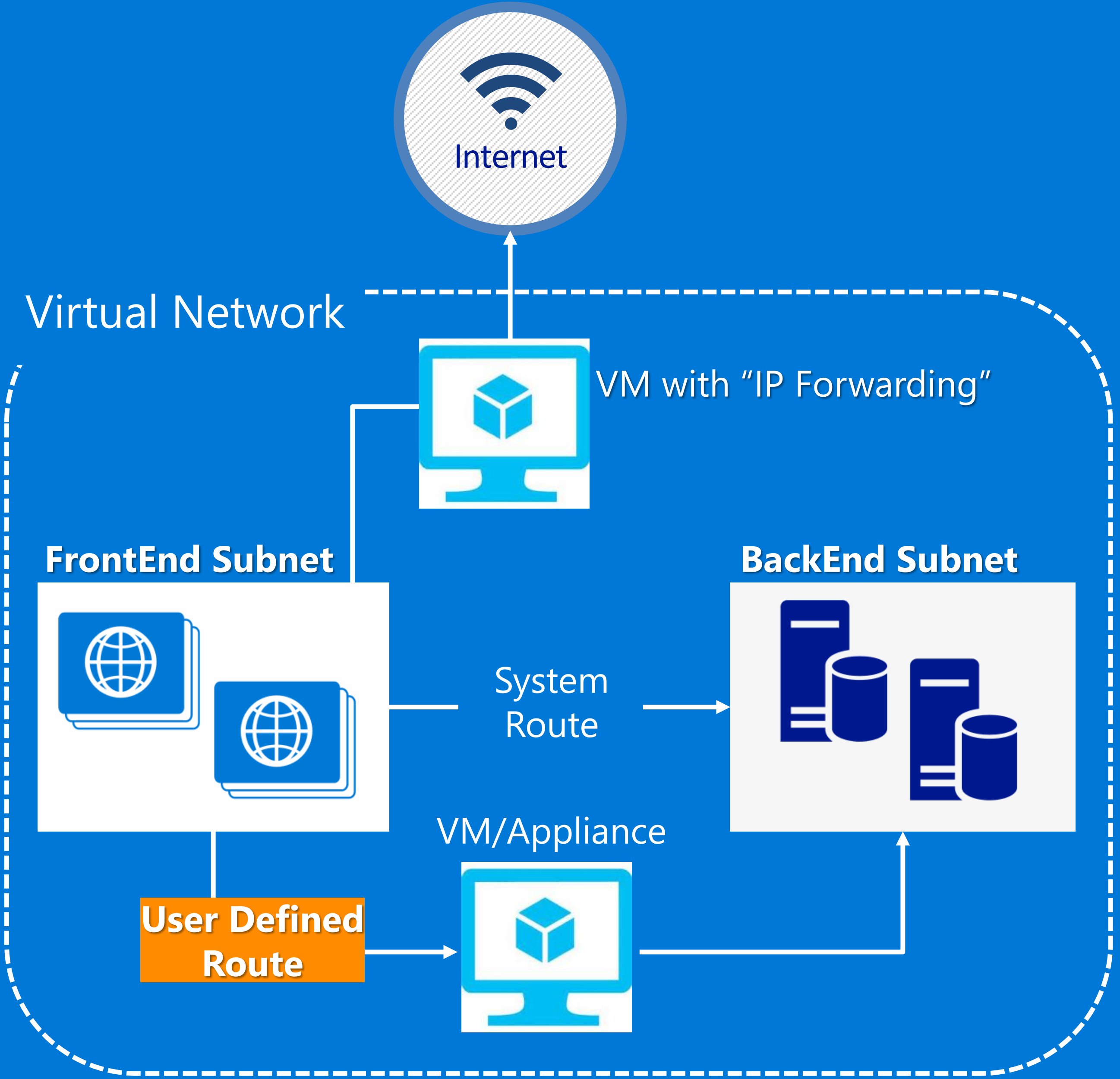
Network Security Groups

- Segment network to meet security needs
- Can protect Internet and internal traffic
- Enables DMZ subnets
- Associated to subnets/VMs and now NICs
- ACLs can be updated independent of VMs

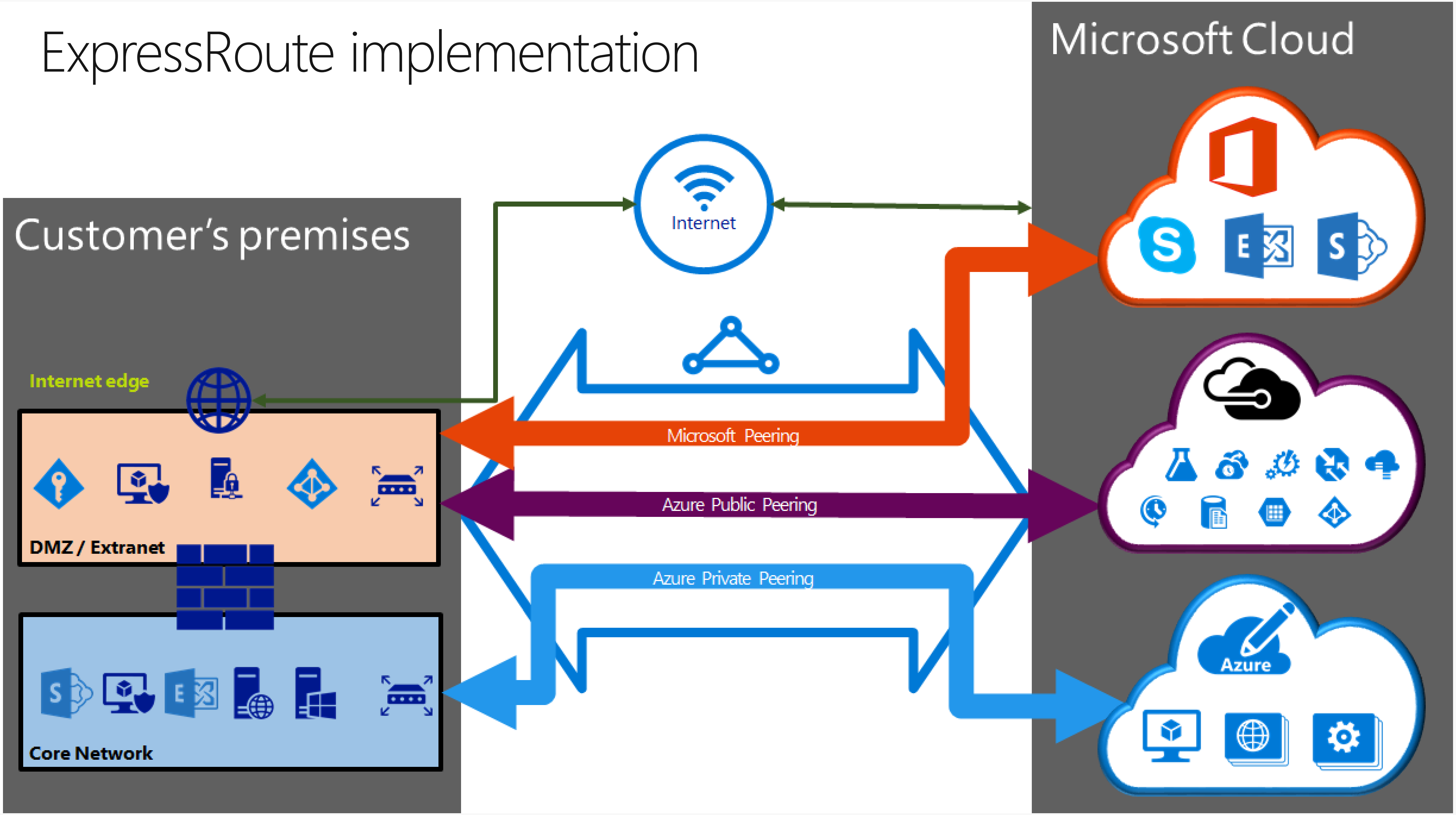


User Defined Routes

- Control traffic flow in your network with custom routes
- Attach route tables to subnets
- Specify next hop for any address prefix
- Set default route to force tunnel all traffic to on-premises or appliance



ExpressRoute implementation



Azure Government

Resources

Azure Government Site
azure.com/gov

Azure Government Blog
aka.ms/govblog

Azure Government Free Trial
aka.ms/azuregovtrial Azure Government

Azure Government Documentation
https://aka.ms/azuregovdocs

Azure Government DC User Community
meetup.com/DCAzureGov

Questions?