Azure Security

Karl Ots, Zure Ltd

12.12.2019

Microsoft® MVP Most Valuable Professional

CISSP®

Microsoft CERTIFIED Trainer

Karl Ots

Chief Consulting Officer

karl.ots@zure.com

- Cloud & cybersecurity expert from Finland
- Community leader, speaker, author & patented inventor
- Working on Azure since 2011
- Helped to secure 100+ Azure applications, from startups to Fortune 500 enterprises
- zure.ly/karl

Agenda

- Introduction to cloud security
- Azure security controls
- Where to learn more

Security

Evolution of attacks

In the beginning

Isolated cases of nation-state espionage and young hackers exploring networks

Computing becomes pervasive

Computers used as tools to facilitate traditional offenses; hacking cases increase with motives becoming more diverse (e.g., fraud, hactivisim)

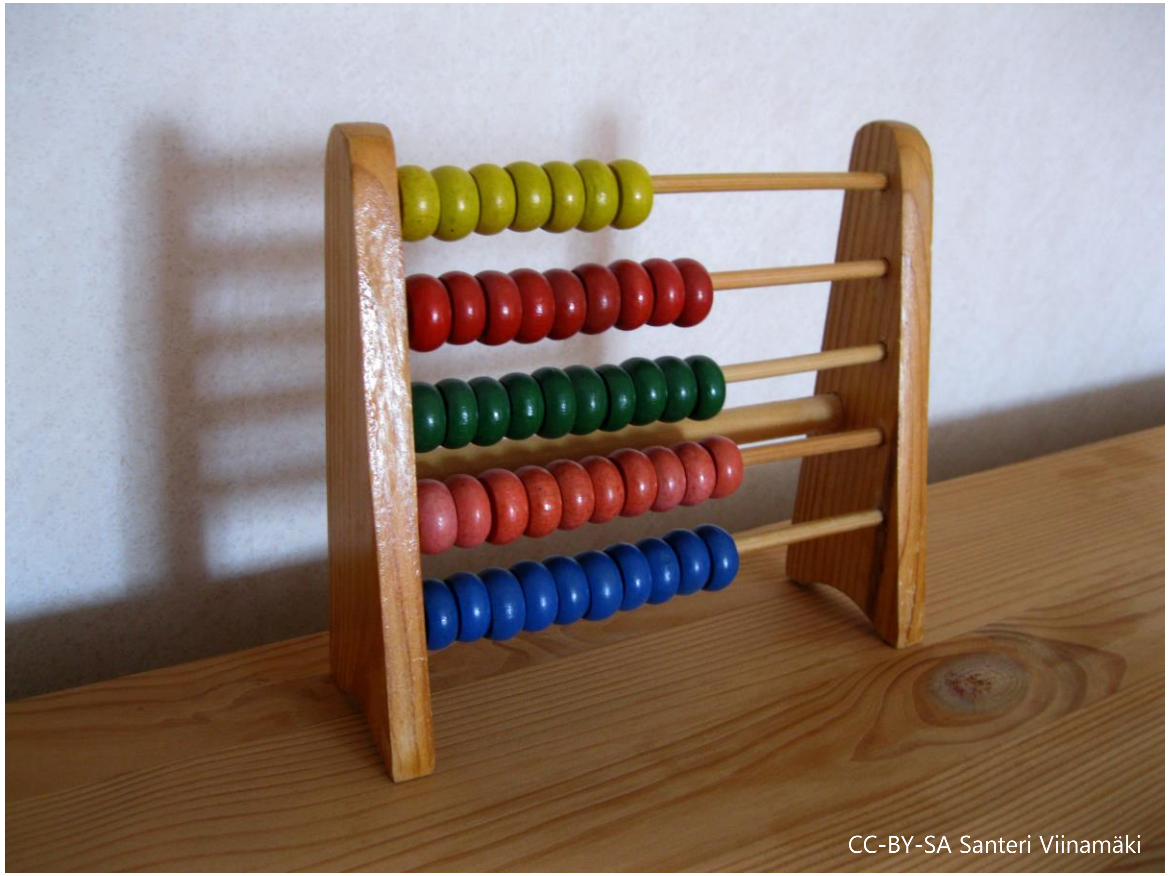
Today

Massive data thefts across verticals; rampant economic and military espionage; advanced persistent threats, destructive attacks

Global threats

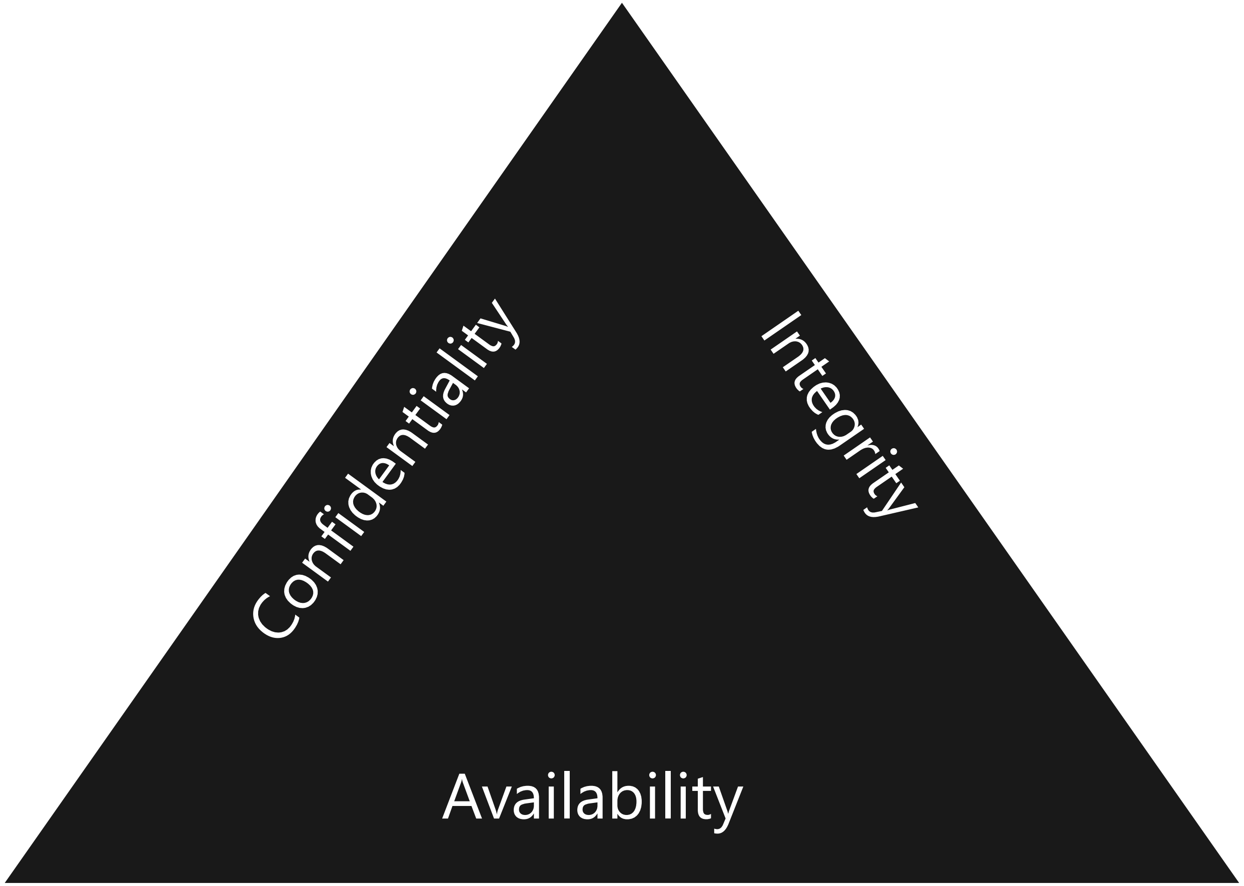
- **90% of all cyberattacks, of both incidents and breaches, are delivered via Phishing emails**. Targeted phishing campaigns continue to be the tip of the spear for espionage-related breaches. (Verizon’s 2017 Data Breach Investigations Report)
- **90% of all security incidents within Information are Denial of Service, Web Application Attacks and Crimeware** (Verizon’s 2017 Data Breach Investigations Report)
- **$1.8 million was the average cost of a spear-phishing attack** for U.S. businesses in 2016 (Cloudmark report / $1.6 million cost average across all companies globally. 1 in 6 companies (300 IT decision makers surveyed) reported a decrease in stock price as a result in a spear phishing attack.)

Absolutely secure computer



CC-BY-SA Santeri Viinamäki

The CIA security triad

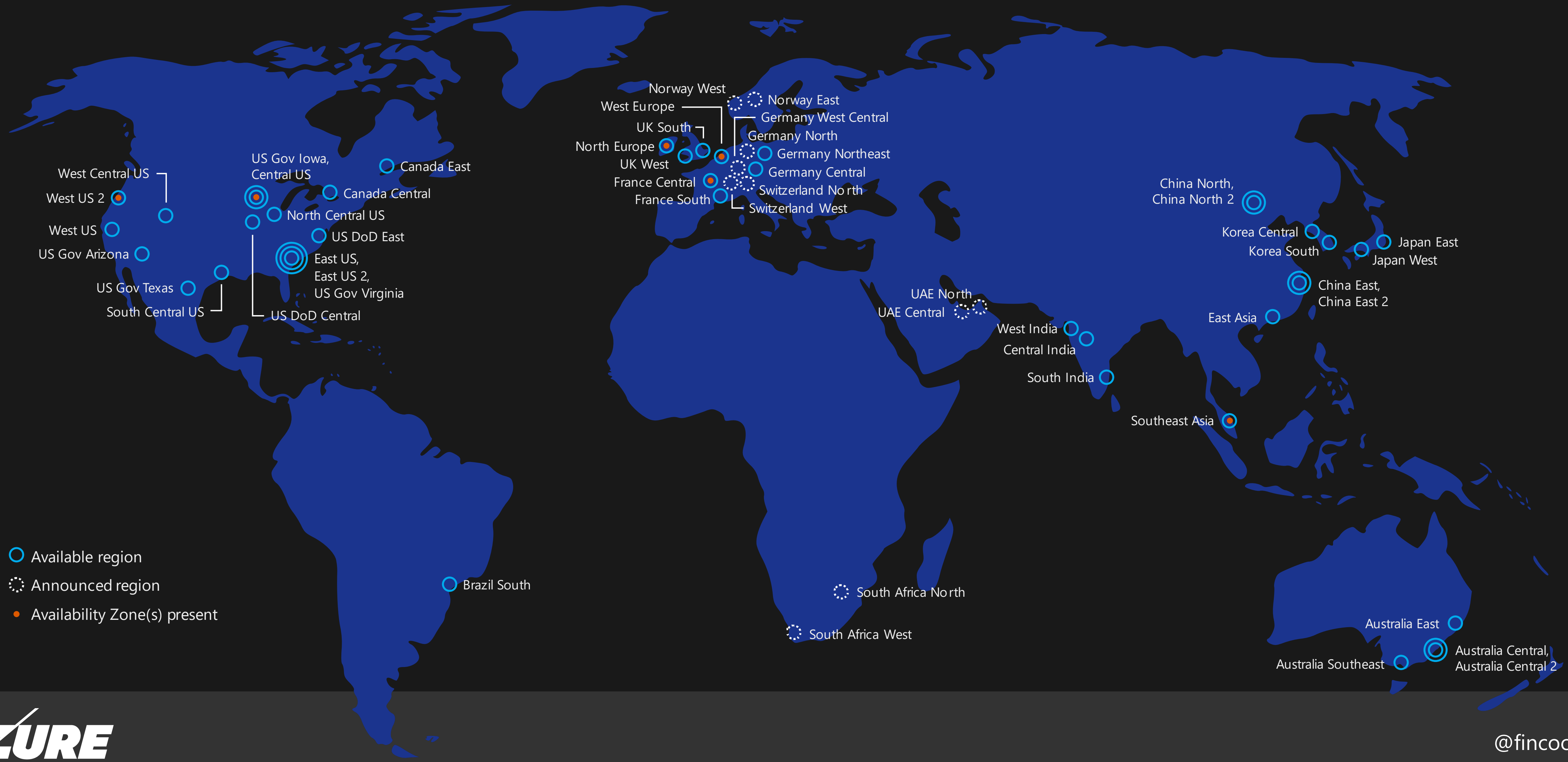


Classic security controls

- Authentication and authorization
- Encryption
- Monitoring
- Backup, Resiliency and Disaster Recovery
- Host hardening (pre-PaaS)

Azure security controls

Azure datacenter regions



○ Available region

◌ Announced region

● Availability Zone(s) present

Security controls for Azure applications

- Subscriptions and Resource Groups
- AAD and RBAC
- ARM Templates, Policies and Locks
- Logging, Alerting & Auditing
- Data Encryption
- Backups & Disaster Recovery
- Privacy & Compliance
- Network security

Cloud security responsibilities

🟦 Customer management of risk

Data Classification and data accountability

◪ Shared management of risk

Identity & access management | End Point Devices

⬛ Provider management of risk

Physical | Networking

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability	🟦	🟦	🟦	🟦
Client & end-point protection	🟦	🟦	🟦	◪
Identity & access management	🟦	🟦	◪	◪
Application level controls	🟦	🟦	◪	⬛
Network controls	🟦	◪	⬛	⬛
Host Infrastructure	🟦	◪	⬛	⬛
Physical Security	🟦	⬛	⬛	⬛

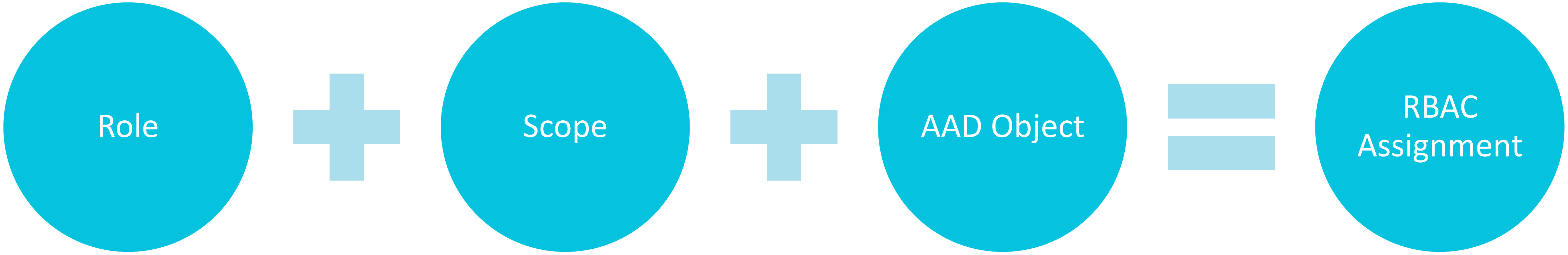
🟦 Cloud Customer ⬛ Cloud Provider

Azure Resource Manager terminology

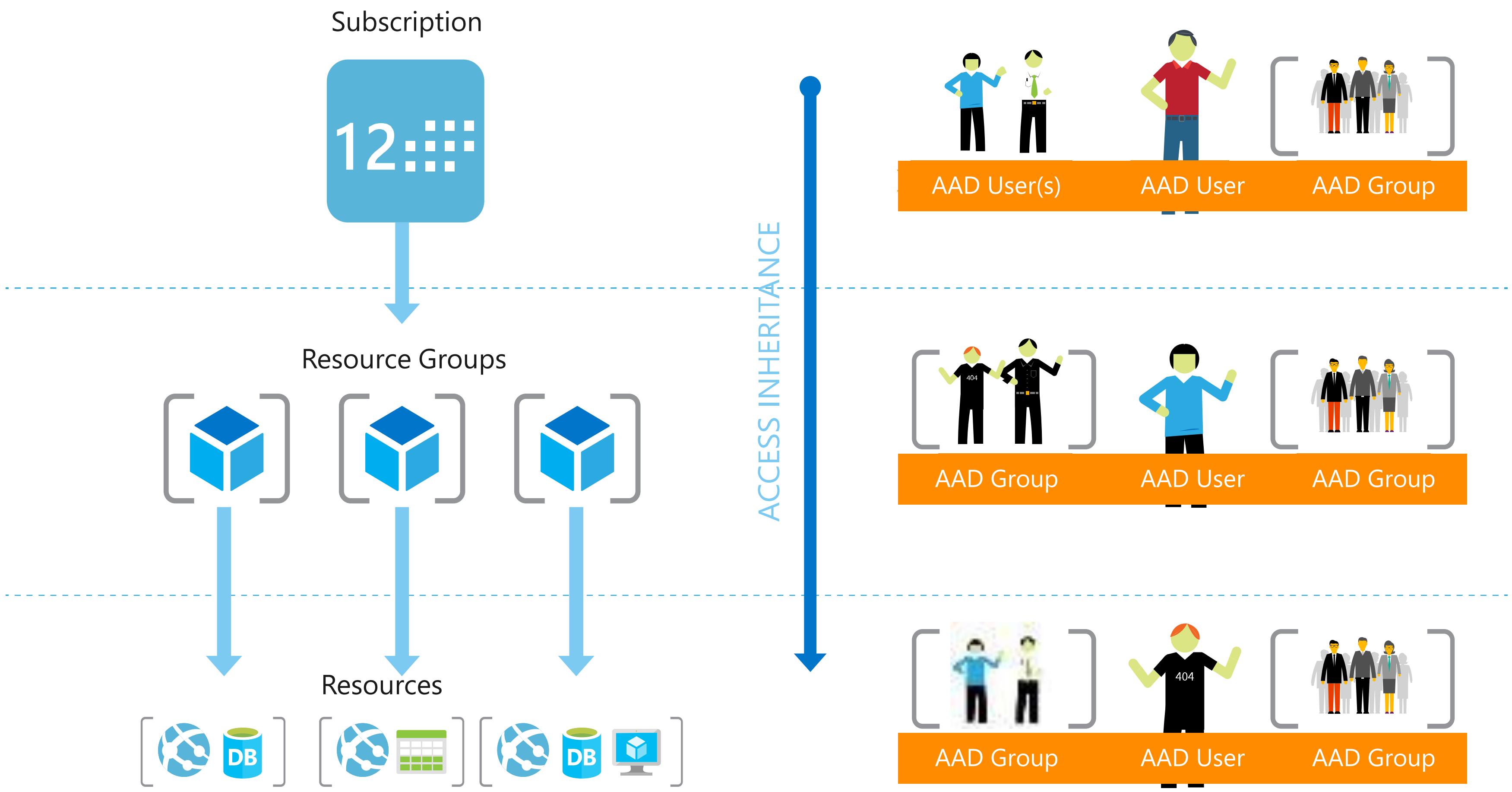
- Tenant
    - Azure AD Directory
- Subscription
    - Logical, hierarchical and fiscal container for resource groups
- Resource Group
    - A container that holds related resources for an Azure solution.
- Resource Provider
    - A service that supplies the resources you can deploy and manage through Resource Manager.
- Resource
    - A manageable item that is available through Azure.

Multiple subscriptions can trust the same AAD directory, but each subscription can only trust a single directory.

Role Based Access Control



Role-Based Access Control



Owner

Can perform all management operations for a resource and its child resources including access management and granting access to others.

Contributor

Can perform all management operations for a resource including create and delete resources. A contributor *cannot grant access* to other.

Reader

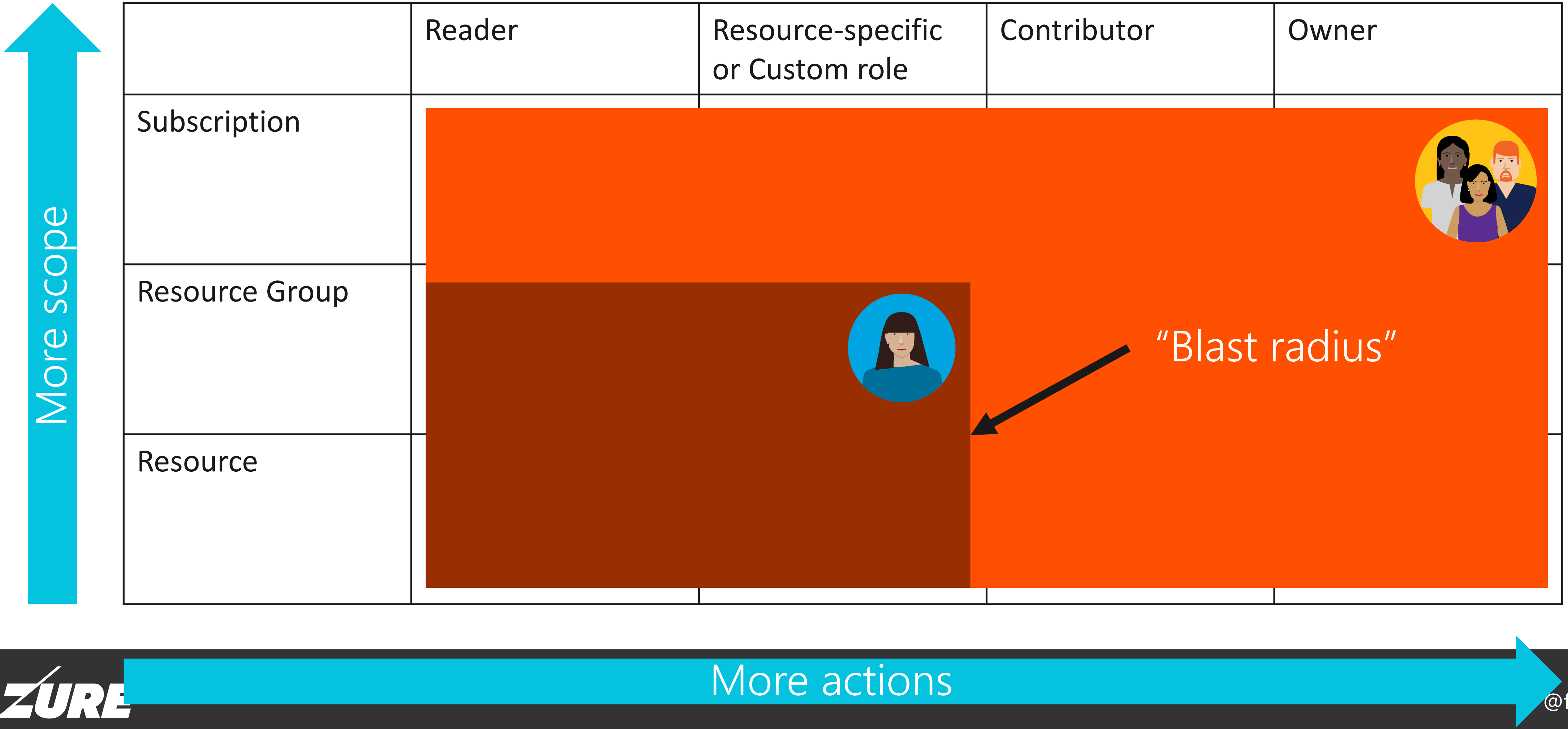
Has *read-only access* to a resource and its child resources. A reader cannot read secrets.

RBAC Roles

- A collection of actions
  - Microsoft.Compute/virtualMachines/*
  - Microsoft.Compute/virtualMachines/start/action
  - Microsoft.Network/virtualNetworks/read
- +70 built-in roles for Azure RBAC
  - e.g. Virtual Machine Contributor, Backup Contributor, Security Reader, etc.

Fundamental Roles	Owner	Contributor	Reader	User Access Administrator
What can you do?	• Full access to all resources • Delegate access to others • Applies to all resource types.	• Create and manage all of types of Azure resources • Cannot grant access to others • Applies to all resource types.	• View Azure resources • Applies to all resource types.	• Manage user access to Azure resources

What’s your blast radius?



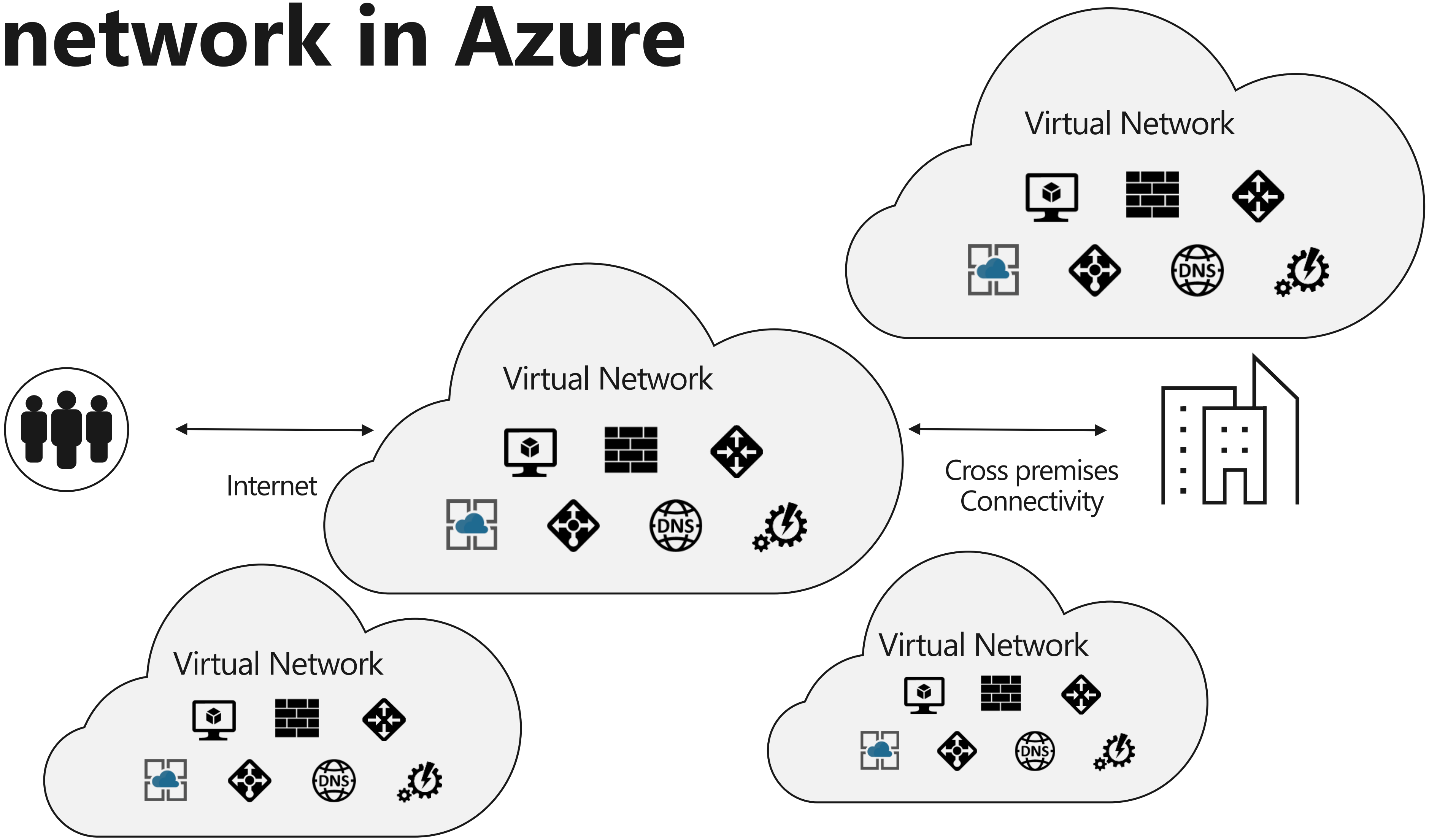
	Reader	Resource-specific or Custom role	Contributor	Owner
Subscription				
Resource Group				
Resource				

Manage to Least Privilege

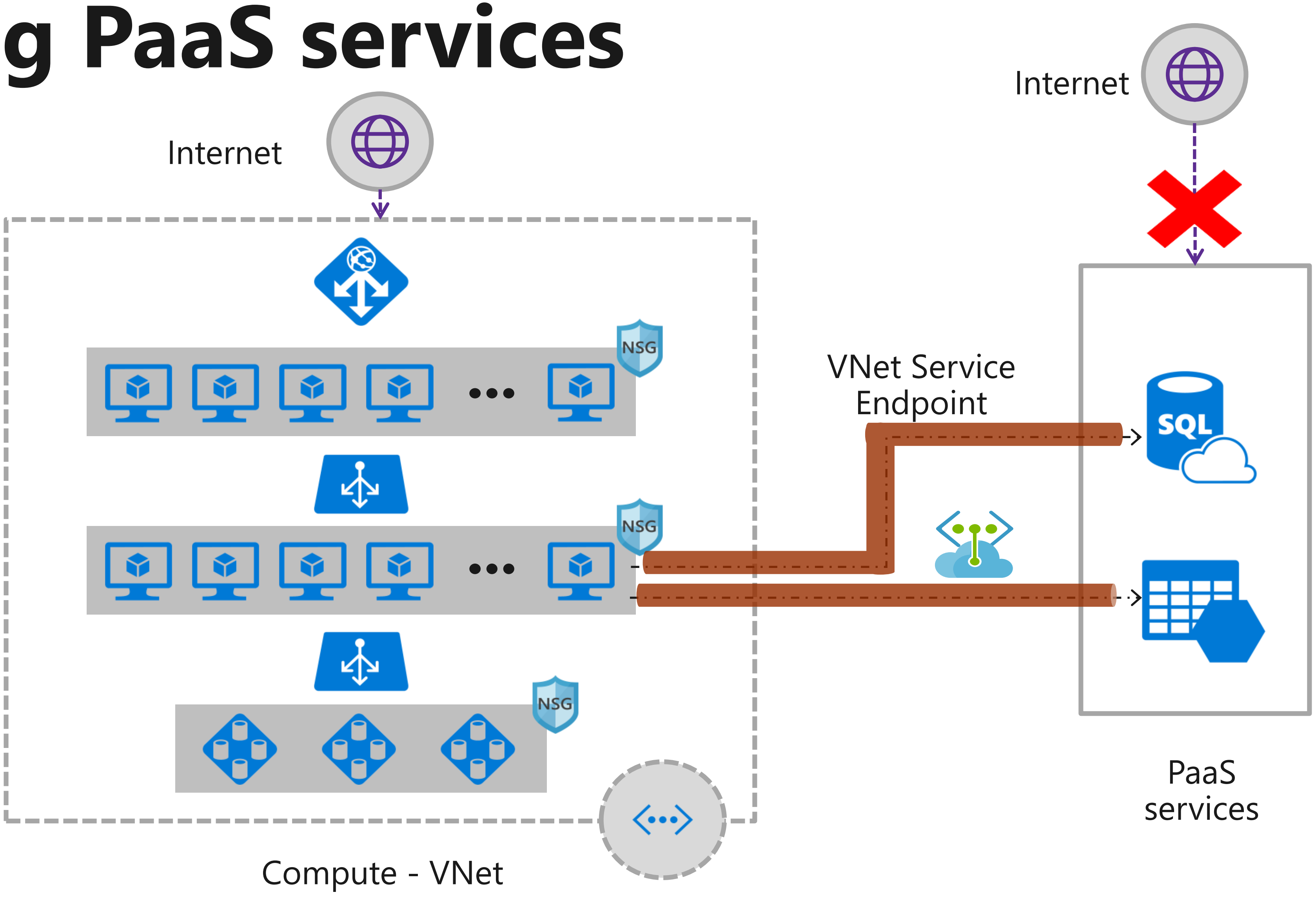
	Reader	Resource-specific or Custom role	Contributor	Owner
Subscription	Observers	People doing real work		Use “break glass” account
Resource Group				
Resource	Single-purpose robots or targeted debug			

“Use minimum role assignments to get normal work done.”

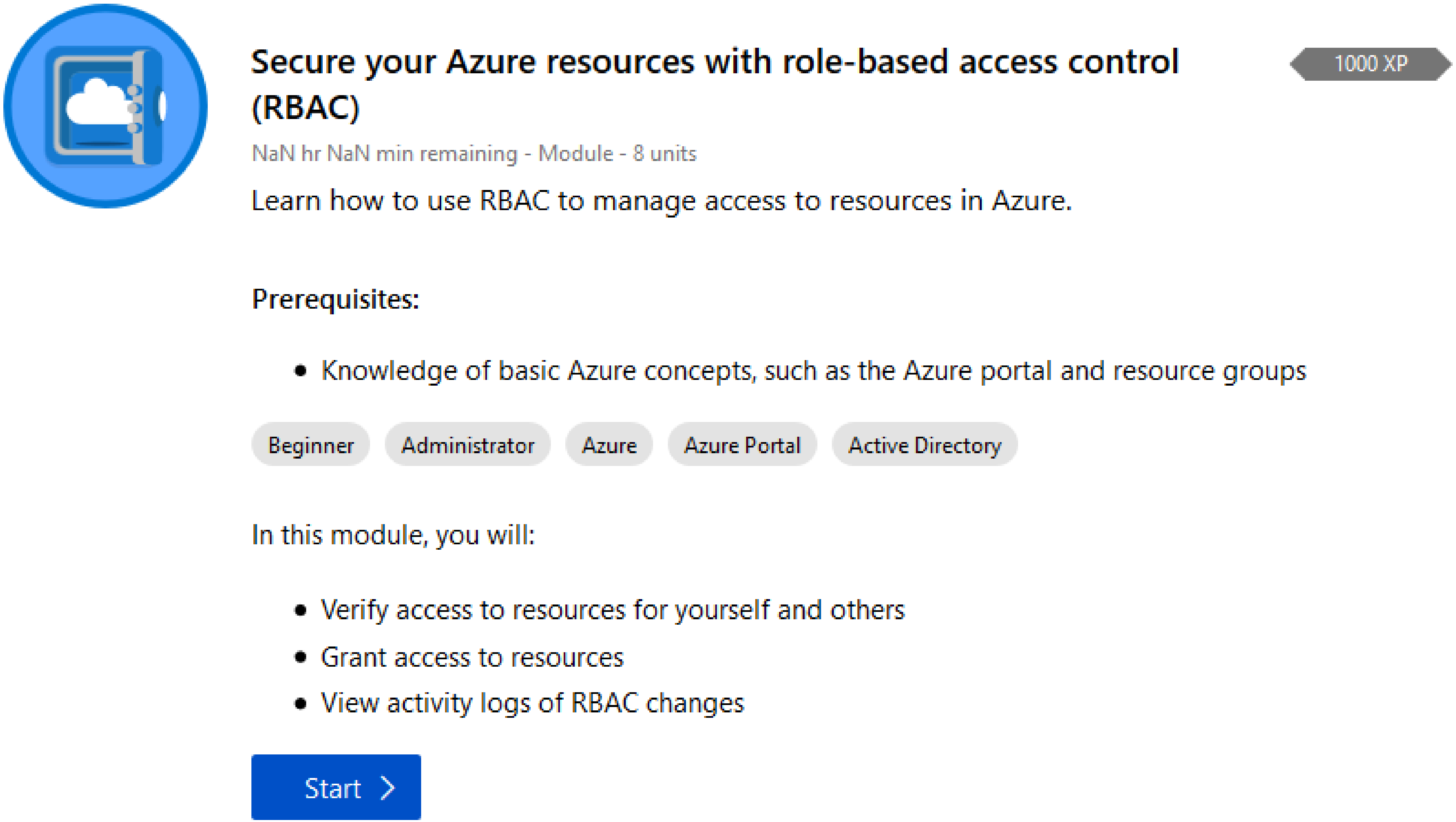
Your network in Azure



Securing PaaS services



Wrap up



Secure your Azure resources with role-based access control (RBAC)

NaN hr NaN min remaining - Module - 8 units

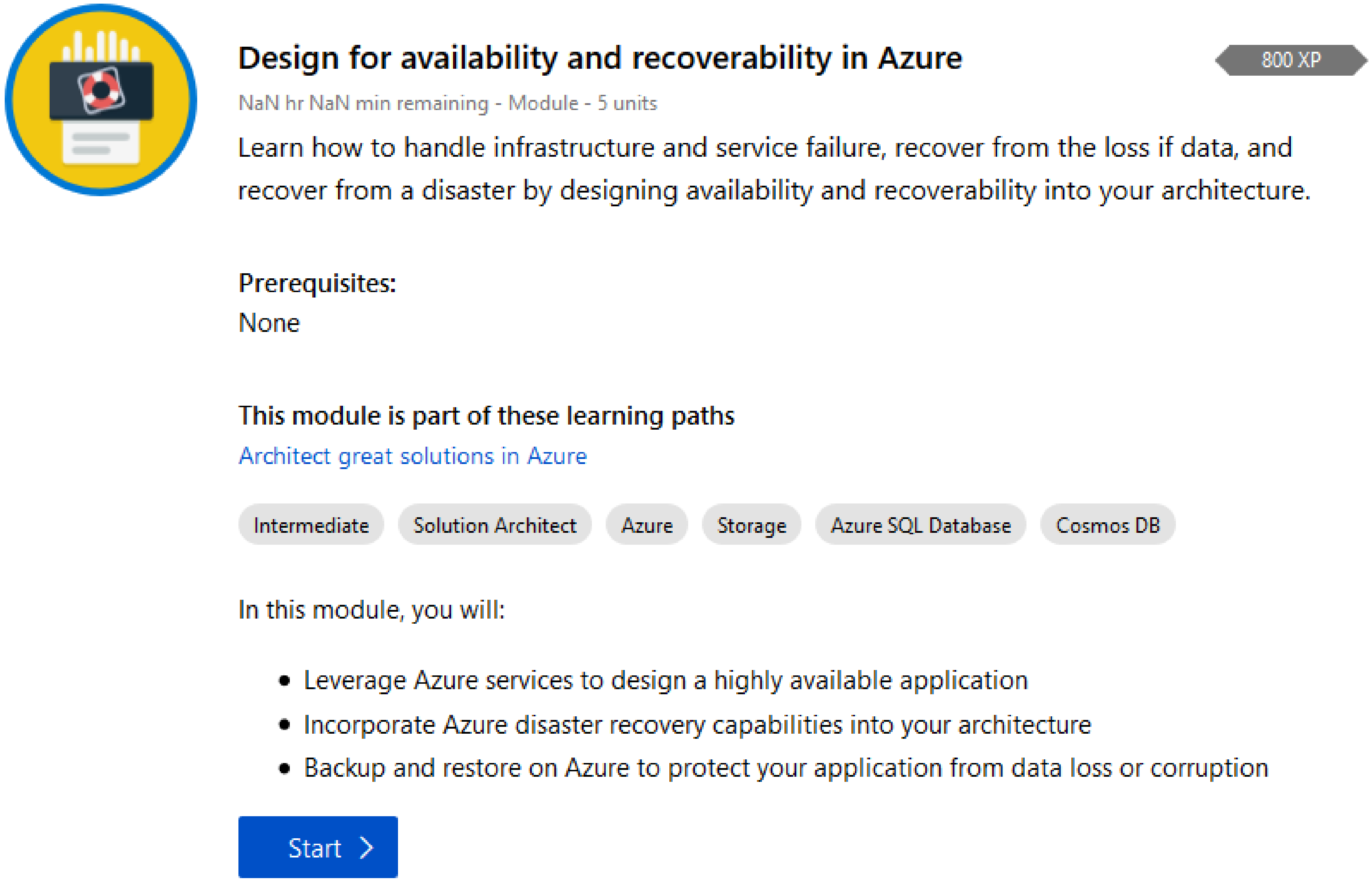
Learn how to use RBAC to manage access to resources in Azure.

Prerequisites:

- Knowledge of basic Azure concepts, such as the Azure portal and resource groups

In this module, you will:

- Verify access to resources for yourself and others
- Grant access to resources
- View activity logs of RBAC changes



Design for availability and recoverability in Azure

800 XP

NaN hr NaN min remaining - Module - 5 units

Learn how to handle infrastructure and service failure, recover from the loss if data, and recover from a disaster by designing availability and recoverability into your architecture.

Prerequisites:

None

This module is part of these learning paths

Architect great solutions in Azure

Intermediate · Solution Architect · Azure · Storage · Azure SQL Database · Cosmos DB

In this module, you will:

- Leverage Azure services to design a highly available application
- Incorporate Azure disaster recovery capabilities into your architecture
- Backup and restore on Azure to protect your application from data loss or corruption

Materials

- Secure DevOps Kit for Azure:
  - azsk.azurewebsites.net
  - Microsoft Ignite 2018 session THR2104 Assess your Microsoft Azure security like a pro
- STRIDE Threat Modeling Lessons from Star Wars:
  - youtube.com/watch?v=Y3VQpg04vXo
- Azure Security and Compliance Blueprint (not Azure Blueprint):
  - docs.microsoft.com/en-us/azure/security/blueprints/gdpr-paaswa-overview
- Azure Virtual Datacenter:
  - docs.microsoft.com/en-us/azure/architecture/vdc/

Resources

- Azure Virtual Datacenter guide:
  - aka.ms/VDC
- Azure Security data export to SIEM
  - https://docs.microsoft.com/en-us/azure/security-center/security-center-export-data-to-siem
- Provision alerts from Secure DevOps kit for Azure (AzSK):
  - https://github.com/azsk/DevOpsKit-docs/blob/master/01-Subscription-Security/Readme.md#azsk-subscription-activity-alerts-1
- Azure Trust Center:
  - https://www.microsoft.com/en-us/trustcenter/cloudservices/azure
- Assess your Microsoft Azure security like a pro - THR2104
  - https://www.youtube.com/watch?v=KHEPdbwAnys

ZURE