



#AzureEvent
#BuildWithAzure

Azure Workshop GDPR, Security and Privacy features for cloud applications

Ben Roscorla, Mike Ormond, Robin Lester

vipazure@microsoft.com

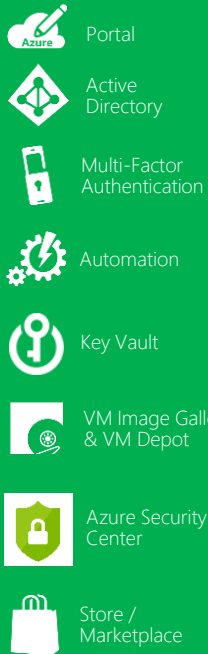


Securing your investment

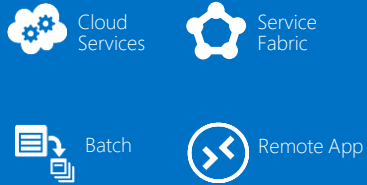


Azure Platform Services

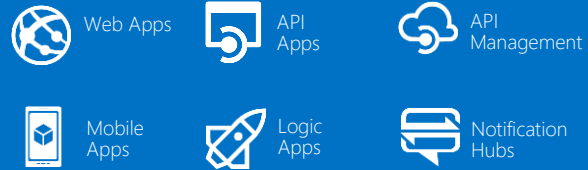
Security & Management



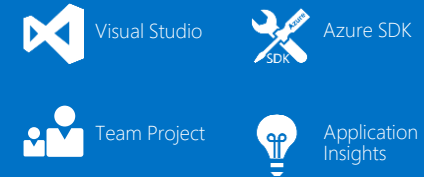
Compute



Web and Mobile



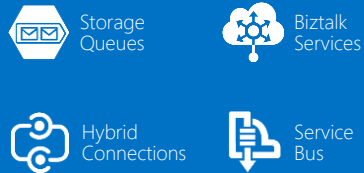
Developer Services



Hybrid Operations



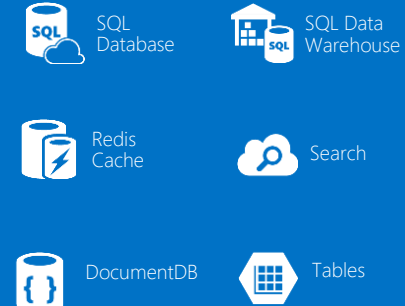
Integration



Analytics & IoT



Data



Media & CDN



Azure Infrastructure Services

Compute



Storage



Networking



Security Imperative

Securing Investment

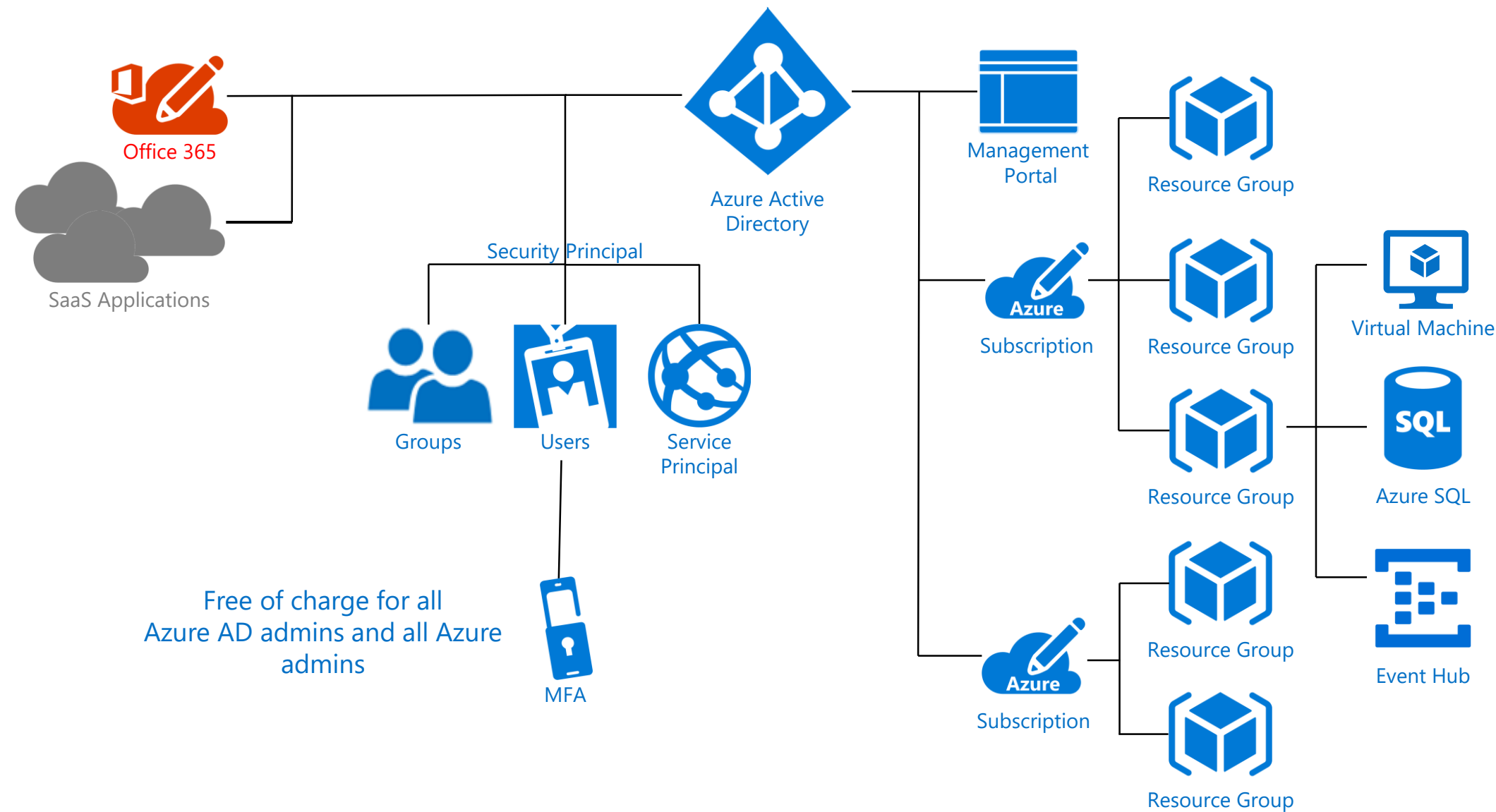
Securing Infrastructure

Securing Data

Securing Applications

Monitoring & Ops

Azure Active Directory and Azure



Identity Management

Centralize your identity management

Manage from a single location (Hybrid/Federation), Manage Privileged Accounts, Automatic Revoke

Enable Single Sign-On (SSO)

Multiple Devices, Locations, Azure AD Connect

Deploy password management

Azure AD Password Reset, SSPR Reporting

Enforce multi-factor authentication (MFA) for users

Cloud/On-Premise, Conditional Access

Use role based access control (RBAC)

Separation of Duties, Least Privilege

Control locations where resources are created using resource manager

Policies

Guide developers to leverage identity capabilities for SaaS apps

SDL, OAuth idp

Actively monitor for suspicious activities

Azure AD Identity Protection – anomaly reports



<https://docs.microsoft.com/en-us/azure/security/azure-security-identity-management-best-practices>

Security Imperative

Securing Investment

Securing Infrastructure

Securing Data

Securing Applications

Monitoring & Ops

Top level Azure Roles


Account administrator

- Can manage billing information
- One per subscription
- Can create subscriptions
- Can designate Service administrator
- Change using the Transfer function

Service administrator

- Full control over all resources in a subscription
- Can designate Co-Admins (legacy – do not use)

<https://docs.microsoft.com/en-us/azure/billing/billing-add-change-azure-subscription-administrator>

EDIT YOUR SUBSCRIPTION

Make it yours

Personalize your subscriptions to keep them organized. [Privacy & Cookies](#)

GIVE YOUR SUBSCRIPTION A FRIENDLY NAME

SERVICE ADMINISTRATOR

<https://account.azure.com> →
Subscription → Edit Subscription

Consider use of “Break Glass” Accounts

- Do not use account for daily work
- Write down strong random password and lock it away
- Do not share password
- Change password every time you use it and on scheduled basis
- Enable per-user MFA



Demo

Azure AD and the Portal



Resource Groups



Supports

Set Permissions

Monitor and alerting rules –
Activity Logs

Billing – Rolled up on RG
Deployment container

Consistent Management Layer



<https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-resource-provider-operations>

Security Imperative

Securing Investment

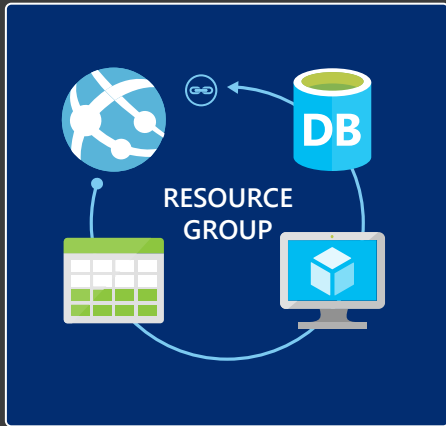
Securing Infrastructure

Securing Data

Securing Applications

Monitoring & Ops

Azure Resource Manager



Describe

Deploy

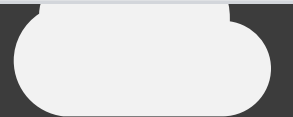
Control

JSON

```
{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0",
  "parameters": {
    "parameter1": {
      "type": "String",
      "defaultValue": "defaultValue"
    }
  },
  "variables": {
    "variable1": "variable1"
  },
  "resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "name": "storageAccount",
      "apiVersion": "2016-01-01",
      "location": "[resourceGroup().location]",
      "properties": {
        "sku": {
          "name": "Standard_LRS"
        },
        "kind": "Storage"
      }
    }
  ],
  "outputs": {
    "output1": {
      "type": "String",
      "value": "[variable1]"
    }
  }
}
```



MICROSOFT AZURE STACK



MICROSOFT AZURE

App



Database

010101
101010
010101

Compute



Network



Storage



<https://docs.microsoft.com/en-gb/azure/azure-resource-manager/resource-group-overview>

Security Imperative

Securing Investment

Securing Infrastructure

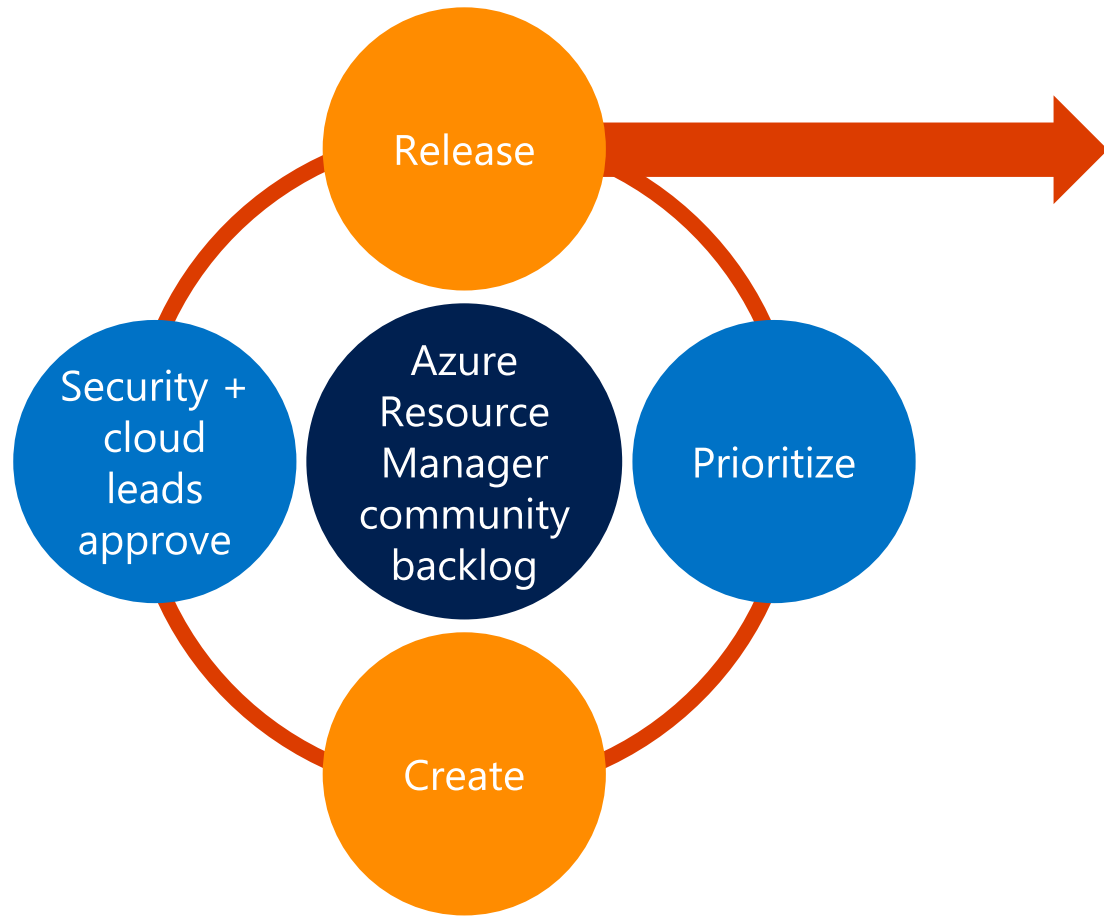
Securing Data

Securing Applications

Monitoring & Ops

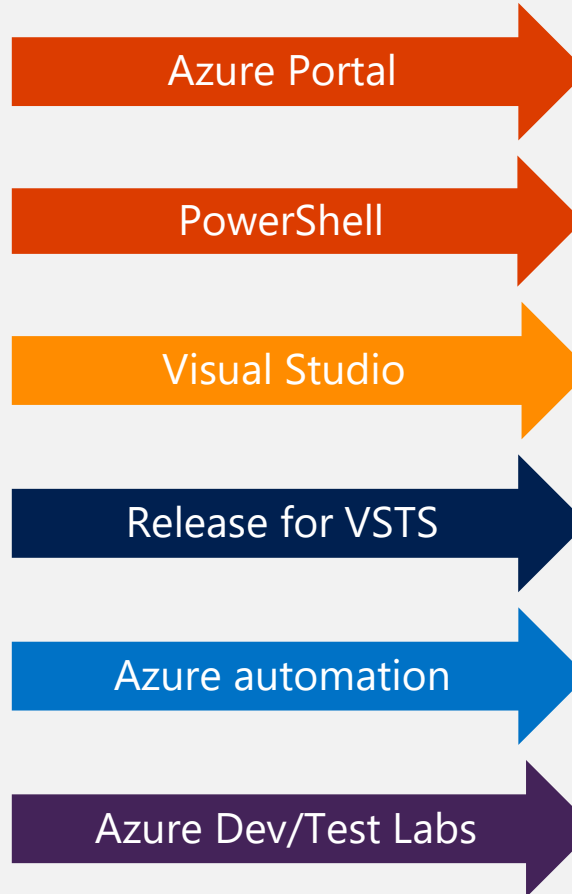
Templates

Centrally managed, community participation



Consumer-driven activity

Many options to deploy:



Security Imperative

Securing Investment

Securing Infrastructure

Securing Data

Securing Applications

Monitoring & Ops

Demo

Resource Groups & Templates



Role Based Access Control

Used only for Azure administration

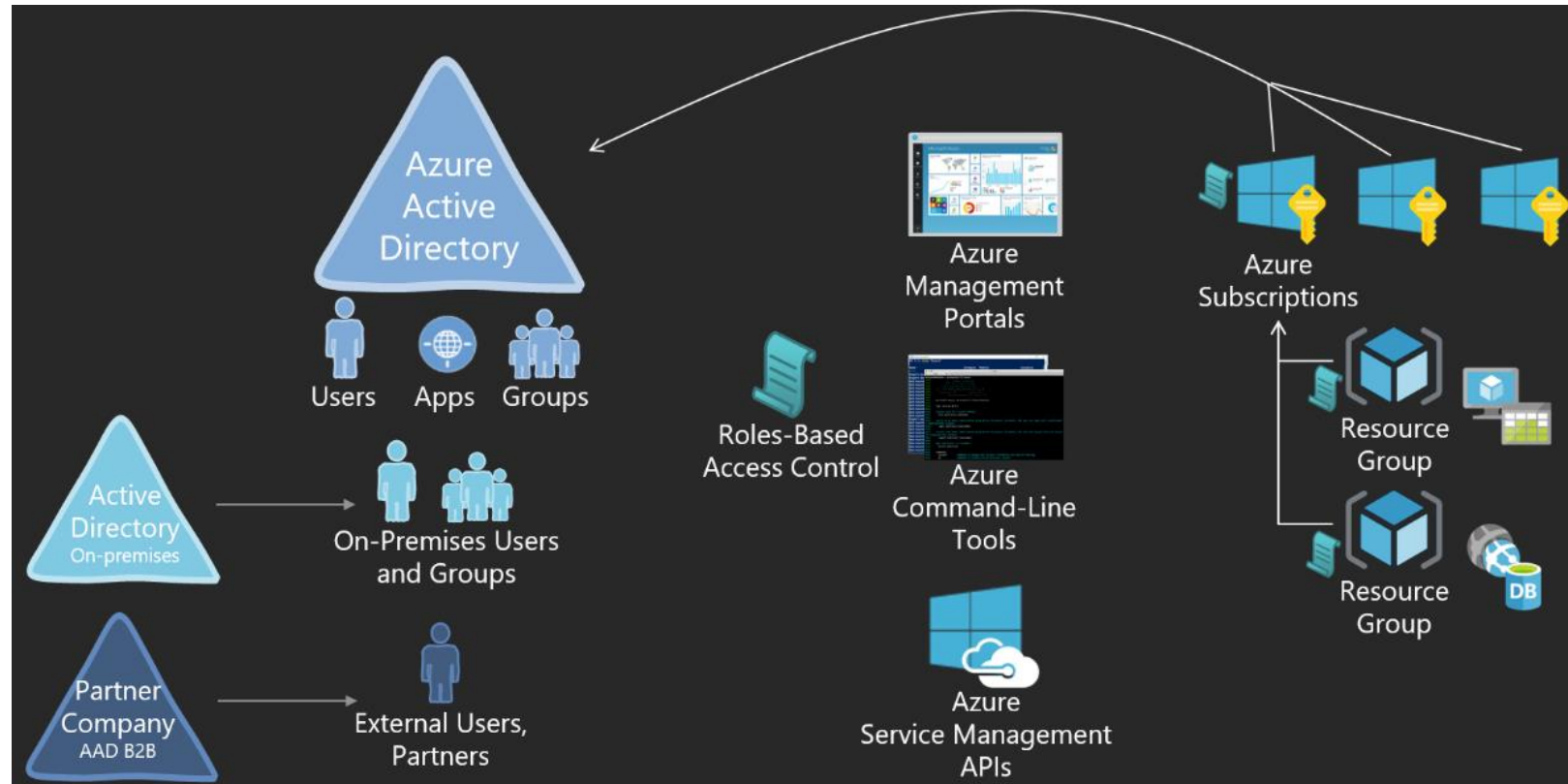
Manage resource in Azure—
i.e. Virtual Machines, storage, networks, etc.

Remember that Azure AD is
not an Azure resource

Roles composed of
Actions

Not Actions (excluded
operations)

Scopes



Built in Roles

Basic Account Types

- **Owner** has full access to all resources including the right to delegate access to others.
- **Contributor** can create and manage all types of Azure resources but can't grant access to others.
- **Reader** can view existing Azure resources.

- + **Others and Custom created**

Role assignment changes are captured in events where the ResourceProviderName is Microsoft.Authorization.

Built in: <https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-built-in-roles>

Custom RBAC Roles: <https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-custom-roles>

A Role is a collection of Actions - Owner

```
(Get-AzureRmProviderOperation Microsoft.Compute/*).Operation  
Microsoft.Compute/virtualMachineScaleSets/read  
Microsoft.Compute/virtualMachineScaleSets/write
```

```
Get-AzureRmRoleDefinition -Name Owner
```

```
Name           : Owner  
Id              : 8e3af657-a8ff-443c-a75c-2fe8c4bcb635  
IsCustom        : False  
Description     : Lets you manage everything, including  
                  access to resources.
```

```
Actions         : {*}  
NotActions      : {}  
AssignableScopes : {/}
```


Contributor and Owner

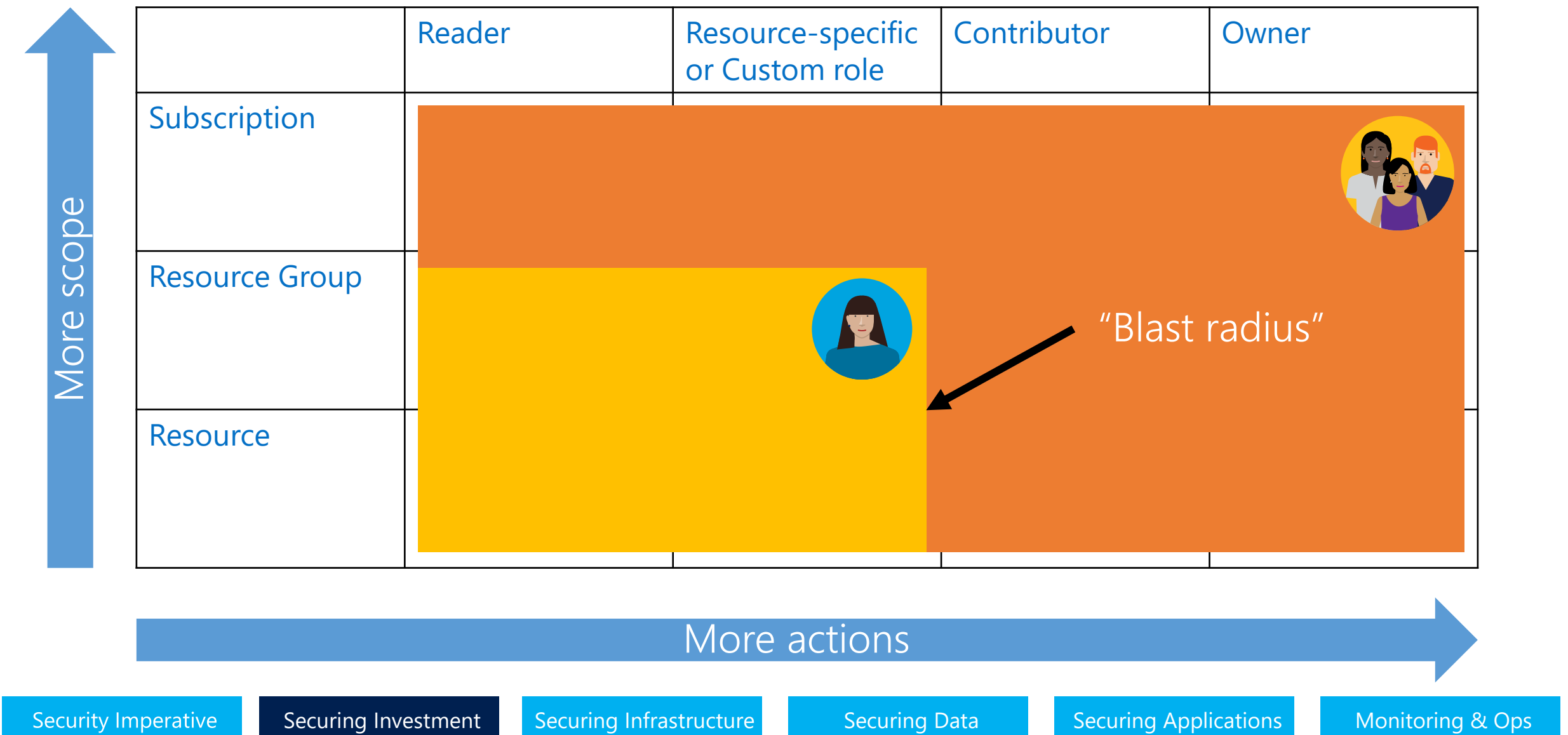
Name : Contributor
Id : b24988ac-6180-42a0-ab88-20f7382dd24c
IsCustom : False
Description : Lets you manage everything except access to resources.
Actions : {*}
NotActions : {Microsoft.Authorization/*/Delete,
Microsoft.Authorization/*/Write,
Microsoft.Authorization/elevateAccess/Action}
AssignableScopes : {/}

Name : Reader
Id : acdd72a7-3385-48ef-bd42-f606fba81ae7
IsCustom : False
Description : Lets you view everything, but not make any changes.
Actions : {*/read}
NotActions : {}
AssignableScopes : {/}

Virtual Machine Contributor

Name : Virtual Machine Contributor
Id : 9980e02c-c2be-4d73-94e8-173b1dc7cf3c
IsCustom : False
Description : Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
Actions : {Microsoft.Authorization/*/read,
Microsoft.Compute/availabilitySets/*,
Microsoft.Compute/locations/*,
Microsoft.Compute/virtualMachines/*...}
NotActions : {}
AssignableScopes : {/}

Manage to least Privilege

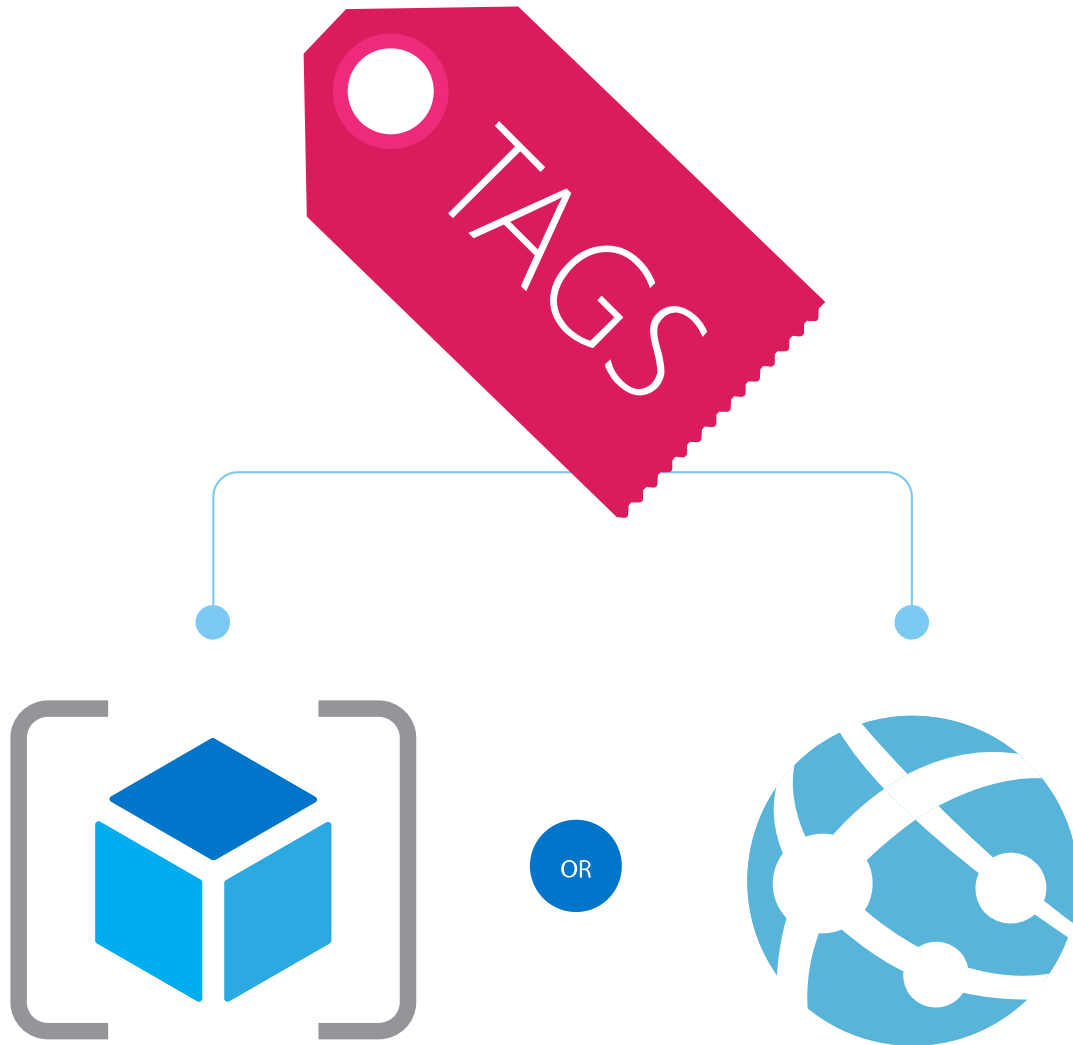


Demo

Role Assignment



Tags



Resource Tags

Name-value pairs assigned to resources or resource groups

Subscription-wide taxonomy

Each resource can have up to 15 tags

Best Practices on using Resource Tags: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags>

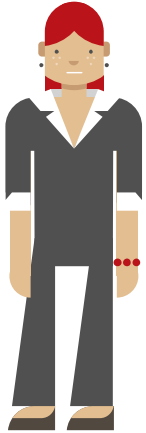
Policies

...enables you to address many concerns.

Requires

Microsoft.Authorization/policydefinitions/write or
Microsoft.Authorization/policyassignment/write

Finance/Business



- How can I be notified when costly resources are created?
- How can I ensure that new resources are identified with common information like "Cost Center"

```
{  
  "if" : {  
    "<condition>" | "<logical  
operator>  
  },  
  "then" : {  
    "effect" : "deny | audit | append"  
  }  
}
```

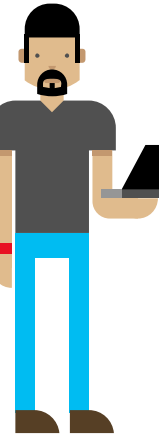


Security/Risk Mgmt.

- How do I ensure we don't violate data sovereignty rules?
- How can I find out when resources are created so I can verify they follow our Security Policies

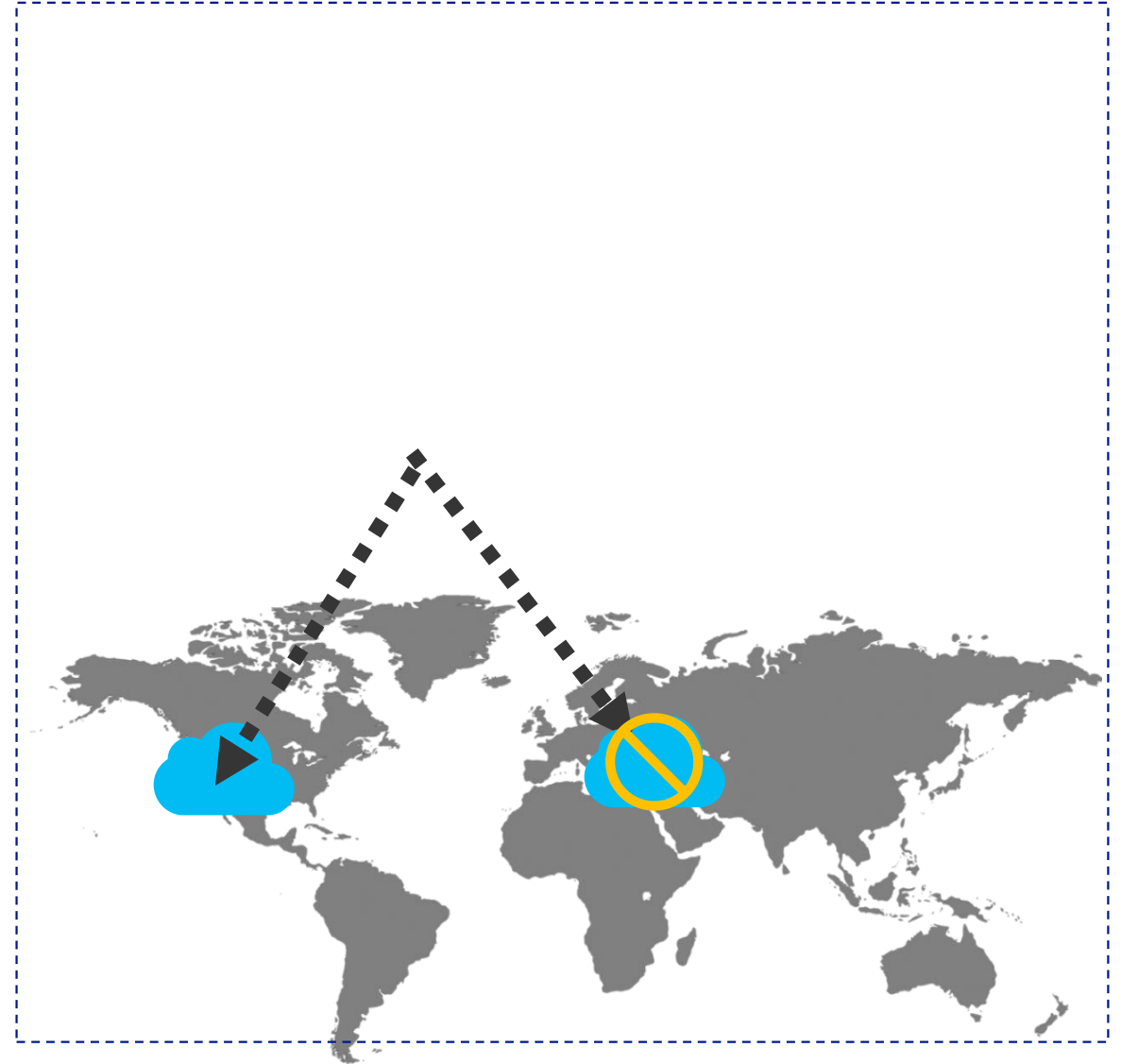
Technology Pro

- How can ensure my subscriptions have only allowed resources?
- Can I make sure developers follow our established naming conventions?

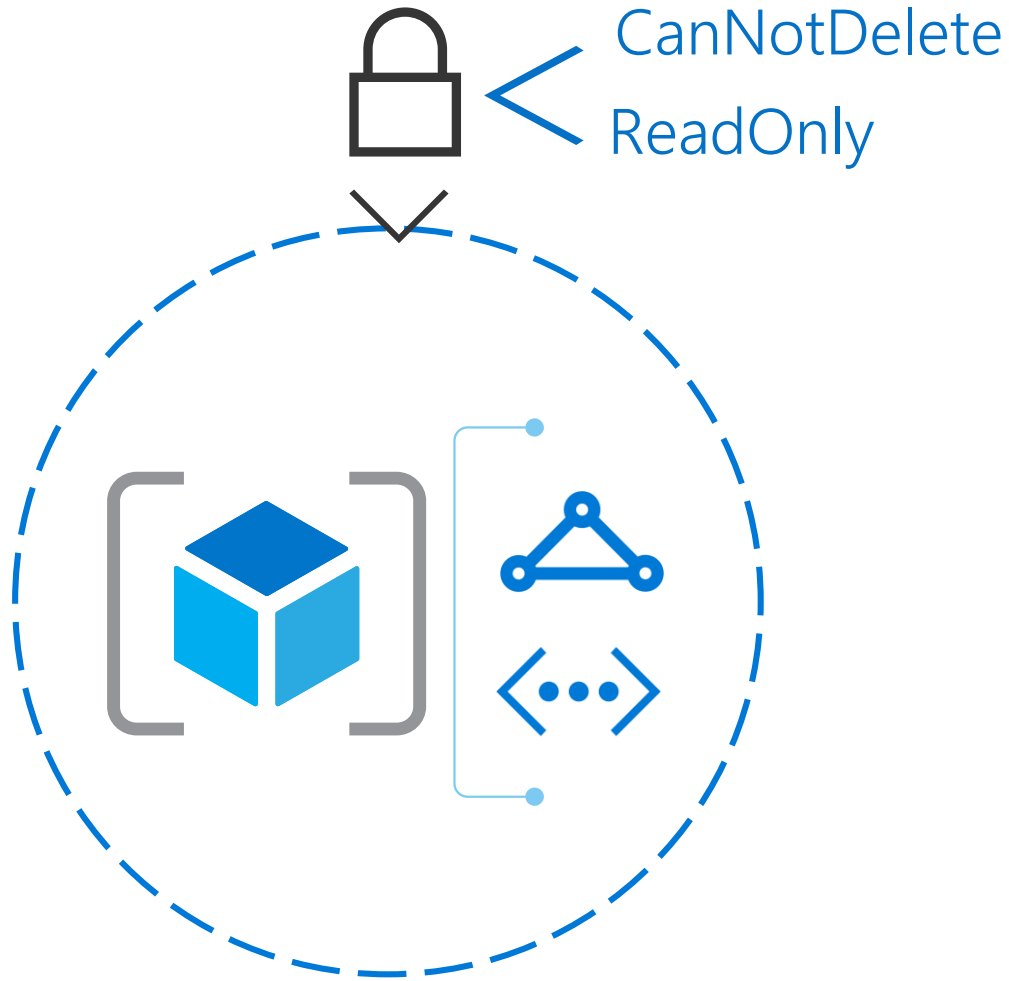


Link to Azure Resource Manager Policy Introduction: <https://azure.microsoft.com/en-us/documentation/articles/resource-manager-policy/> and <https://docs.microsoft.com/en-us/azure/azure-policy/create-manage-policy>

Policies



Resource Locks



Requires

Microsoft.Authorization/* or Microsoft.Authorization/locks*
By Default Owner & User Access Administrator

Security/Risk Mgmt.

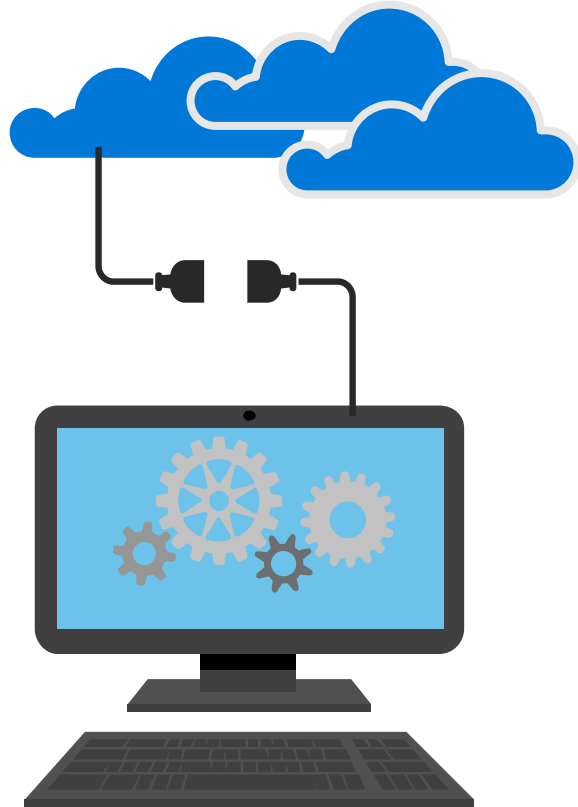
- Prevents the deletion of Security related functions such as NVA and NSG

Technology Pro

- Ensures stability of subscriptions by locking key resources from deletion or modification.

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>

Automation



Technology Pro

- Allow Technology Pros to create libraries of re-usable code to manage their environments

Security/Risk Mgmt.

- Provide consistent deployment of needed tools and resources for security management (agents, etc)

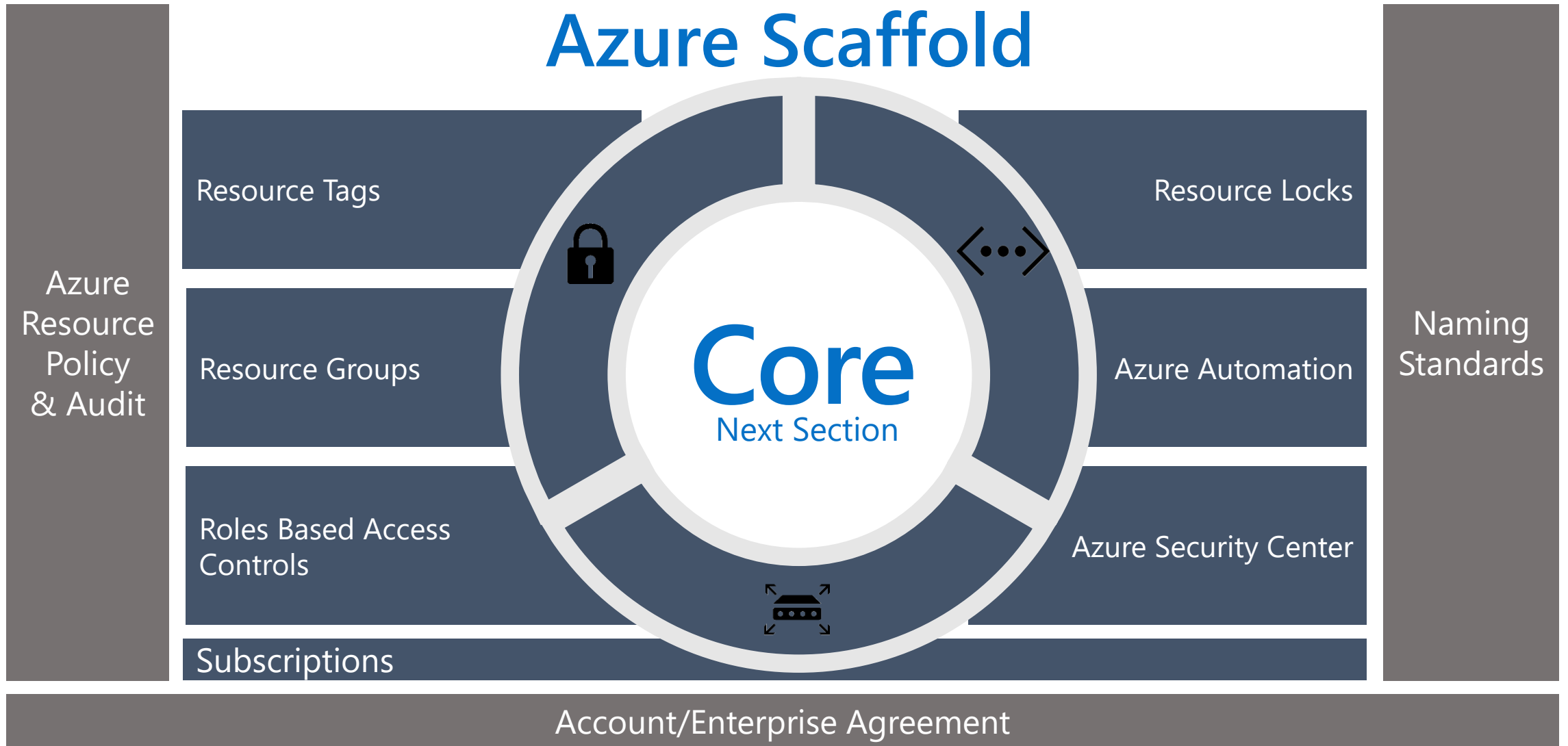
Demo

Tags, Policies and Resource Locks



Enterprise Scaffold

Azure Scaffold



<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-subscription-governance>

Security Imperative

Securing Investment

Securing Infrastructure

Securing Data

Securing Applications

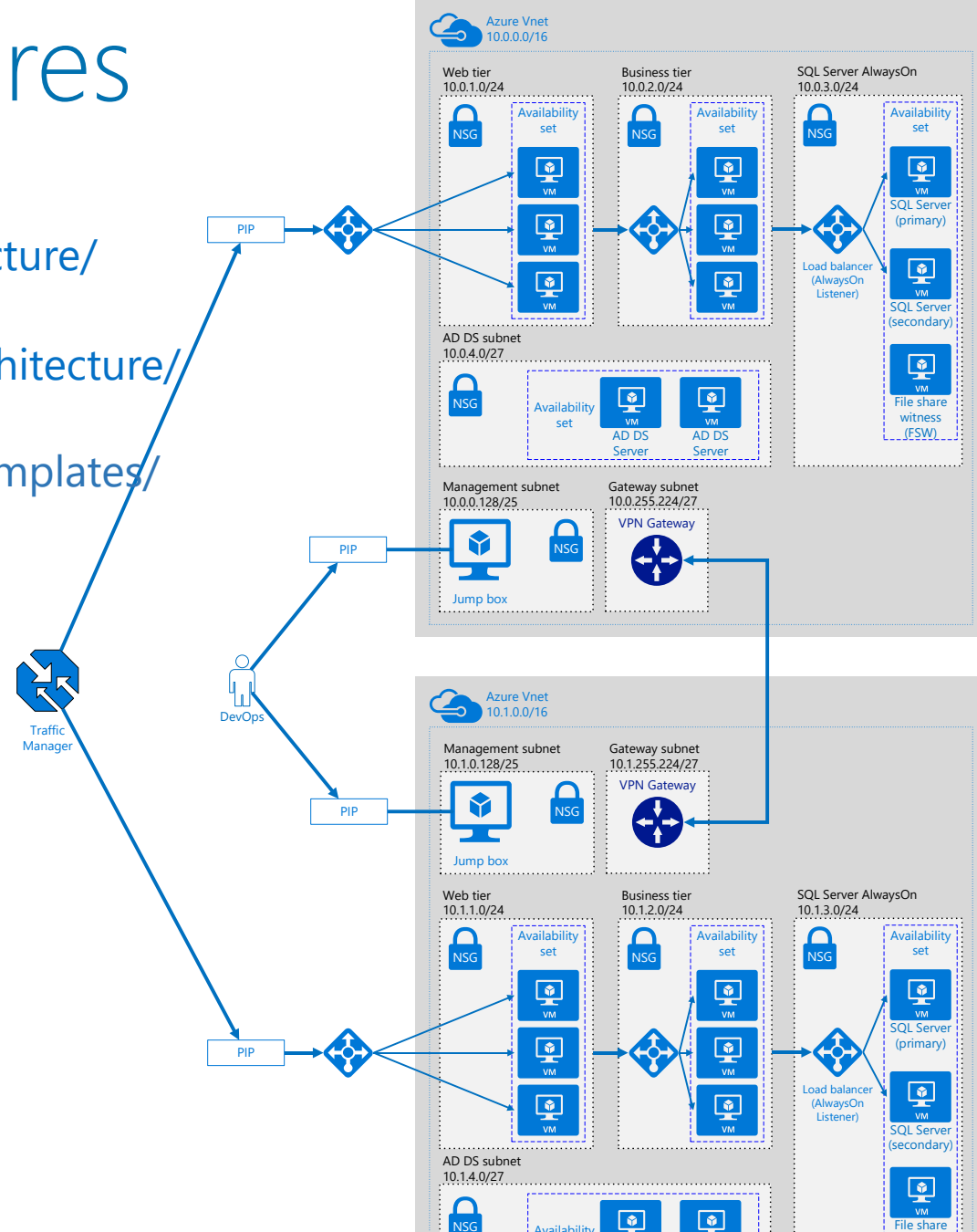
Monitoring & Ops

Reference Architectures

<https://docs.microsoft.com/en-us/azure/architecture/>

<https://azure.microsoft.com/en-us/solutions/architecture/>

<https://azure.microsoft.com/en-gb/resources/templates/>



Security Imperative

Securing Investment

Securing Infrastructure

Securing Data

Securing Applications

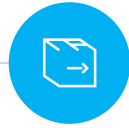
Monitoring & Ops

Azure Blueprint

Fast track to certification and compliance of applications built on Azure



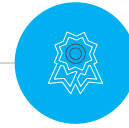
Architecture



Deployment



Verification



Expertise



Partnership

5-step model that streamlines cloud adoption. Through the use of simple to use templates and tools, and allows your developers to focus on solutions.

<https://servicetrust.microsoft.com/Documents/TrustDocuments>

Security Imperative

Securing Investment

Securing Infrastructure

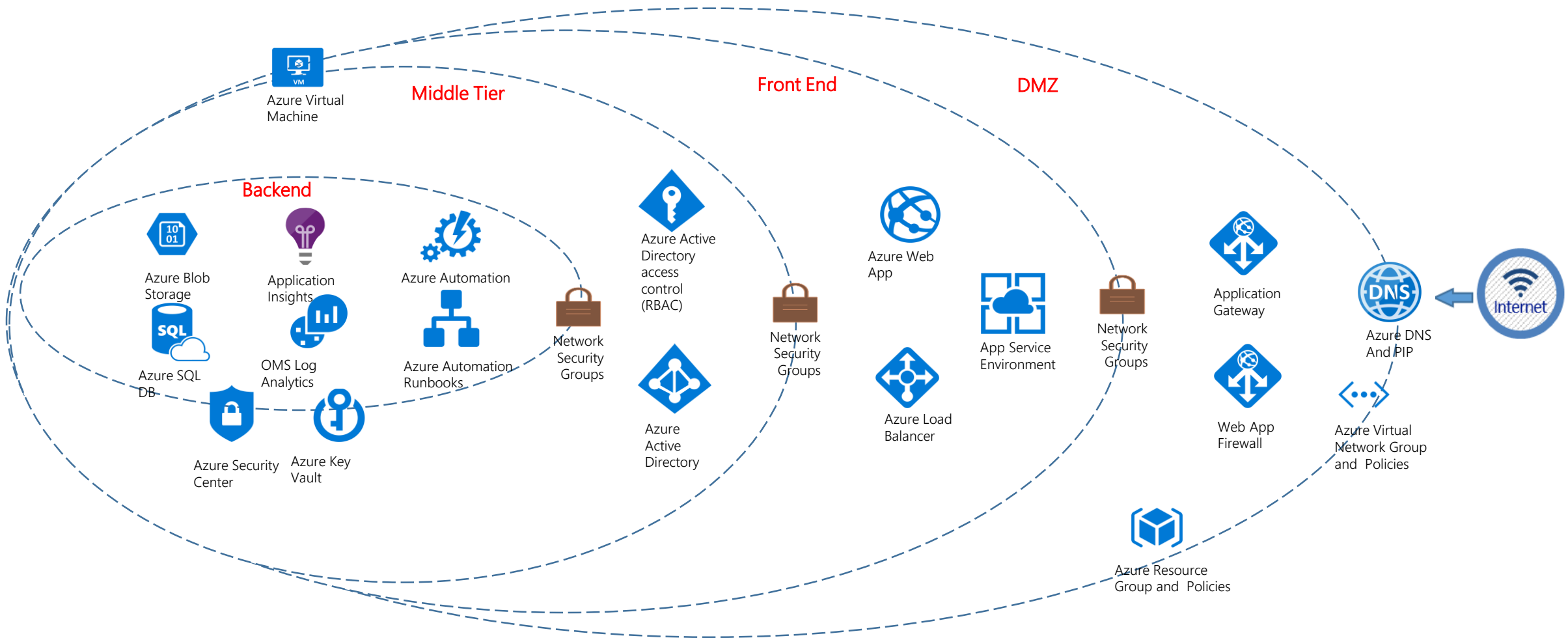
Securing Data

Securing Applications

Monitoring & Ops

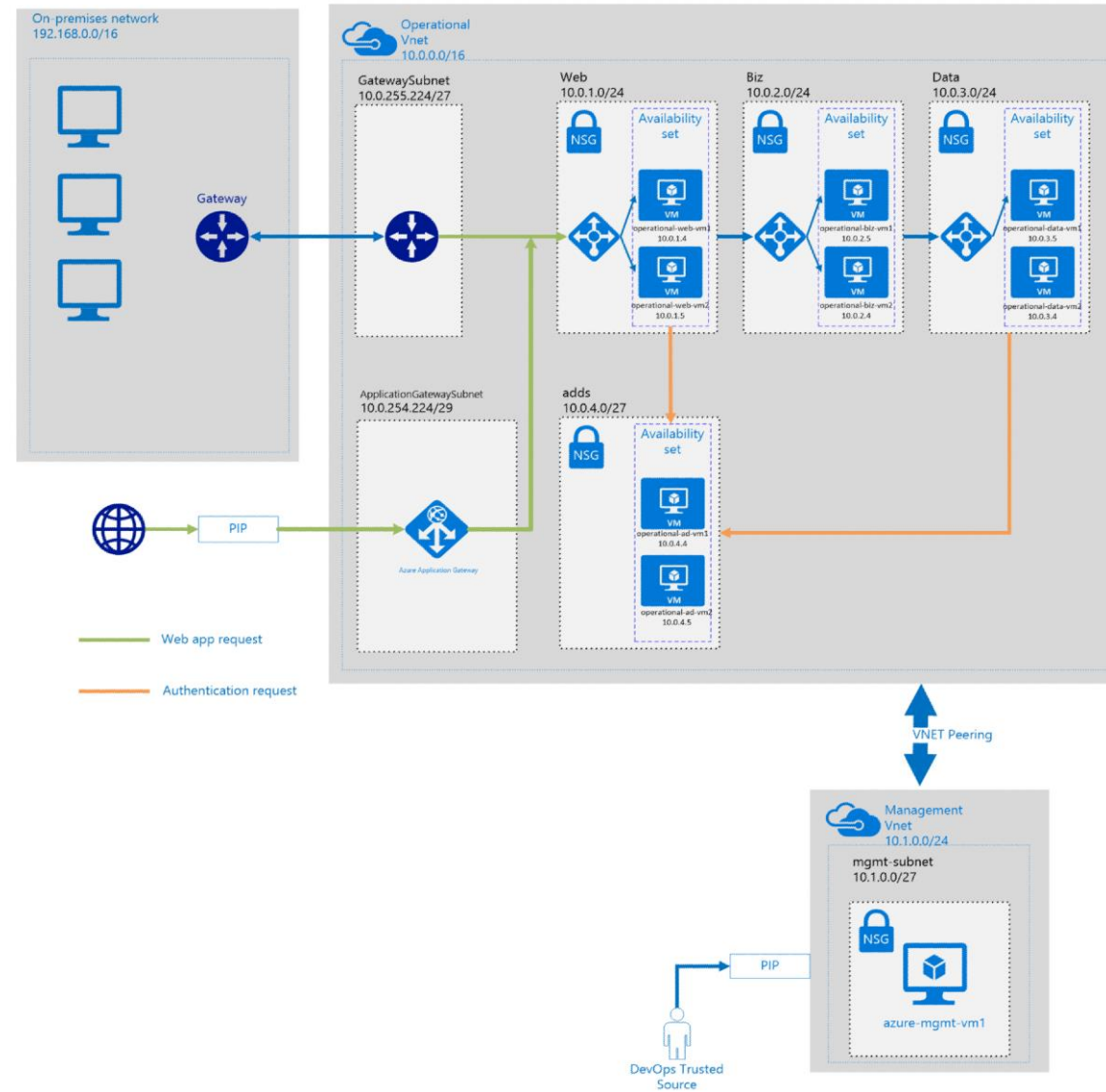
PCI-DSS Blueprint

4 tier (3 tier + DMZ) design overview



[<http://aka.ms/pciblueprint>]

G-Cloud Blueprint



<https://github.com/mspnp/reference-architectures/tree/master/compliance/uk-official/three-tier-web-with-adds>

Security Imperative

Securing Investment

Securing Infrastructure

Securing Data

Securing Applications

Monitoring & Ops