



# Azure Infrastructure Security

## ultimate security in the cloud era

Tom Janetscheck

Principal Consultant | Devoteam Alegri



@azureandbeyond

Platinum Sponsor 2019



Microsoft



# About me

# Tom Janetscheck



# Principal Consultant @ Devoteam Alegri

Focused on Enterprise Security, Azure Governance & Infrastructure

Microsoft Azure MVP & P-CSA

Twitter: @azureandbeyonc

Blog: <http://azureandbeyond.com>



# Cloud momentum continues to accelerate



“The question is no longer:  
‘How do I move to the cloud?’  
Instead, it’s ‘Now that I’m in the  
cloud, how do I make sure I’ve  
**optimized my investment and**  
**risk exposure?’”<sup>1</sup>**

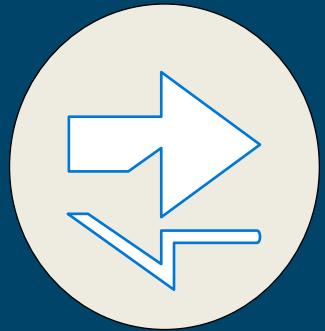
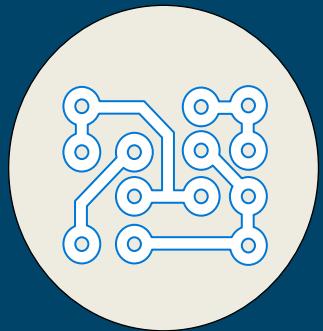


“By 2020 clouds will stop being  
referred to as ‘public’ and  
‘private’. It will simply be **the way**  
**business is done** and IT is  
provisioned.”<sup>2</sup>

<sup>1</sup>KPMG: [2014 Cloud Survey Report, Elevating business in the cloud, December 10, 2014](#)

<sup>2</sup>IDC: [IDC Market Spotlight, Cloud Definitions and Opportunity, April 2015](#)

# But cloud security concerns persist



Management is  
increasingly distributed

Cloud environments  
are more dynamic

Attackers continue to  
innovate

# Cloud Security is a Shared Responsibility

## MICROSOFT COMMITMENT

Securing and managing the cloud foundation



Physical assets



Datacenter operations



Cloud infrastructure

## JOINT RESPONSIBILITY

Securing and managing your cloud resources



Virtual machines



Applications & workloads



Data

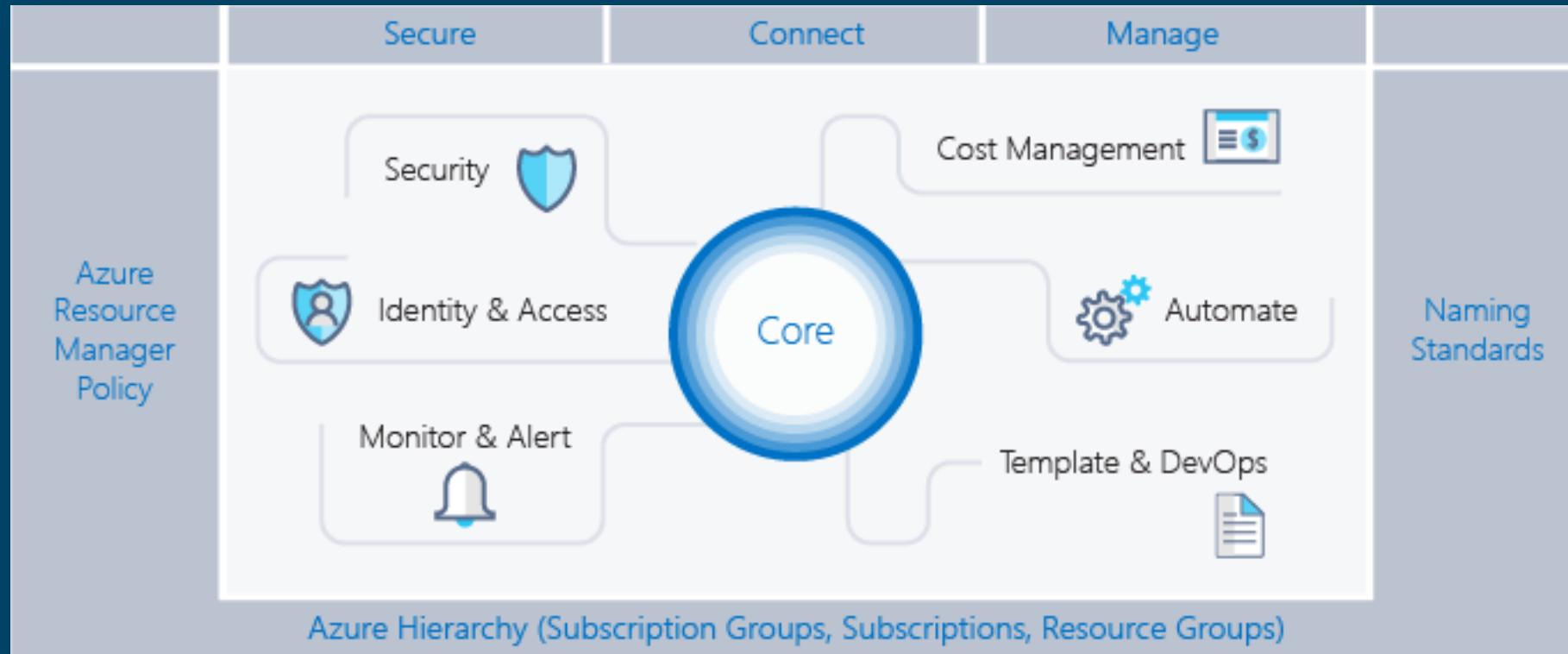
# Azure Governance

# Governance – a definition

Establishment of **policies**, and continuous **monitoring** of their proper **implementation**, by the members of the governing body of an organization [...]<sup>1</sup>

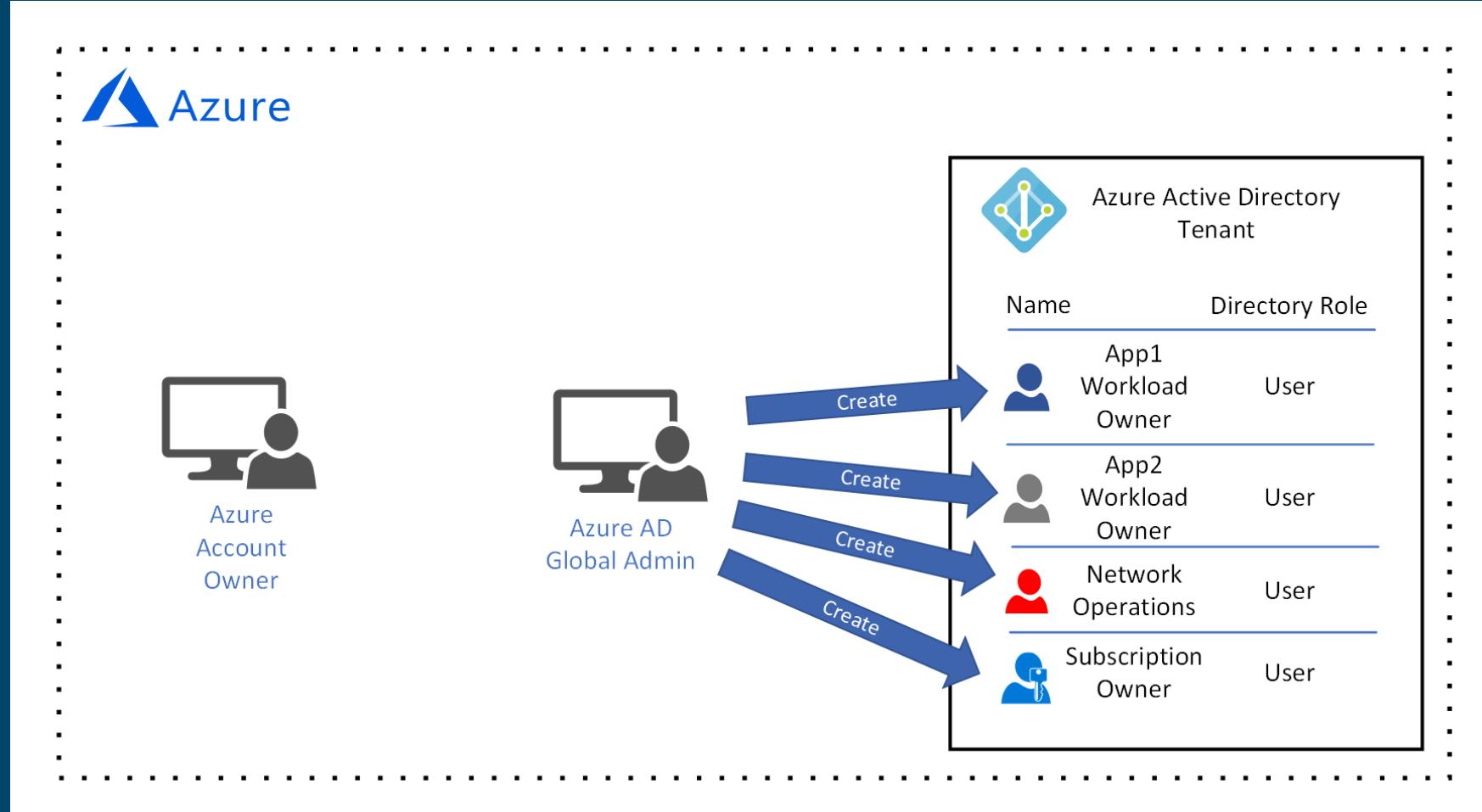
<sup>1</sup>Source: [BusinessDictionary](#)

# Azure Governance Scaffold



Source: <https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/appendix/azure-scaffold>

# Azure Account Owner vs. Azure AD Global Admin





# 5 tips and best practices



Common sense...

...is not so common

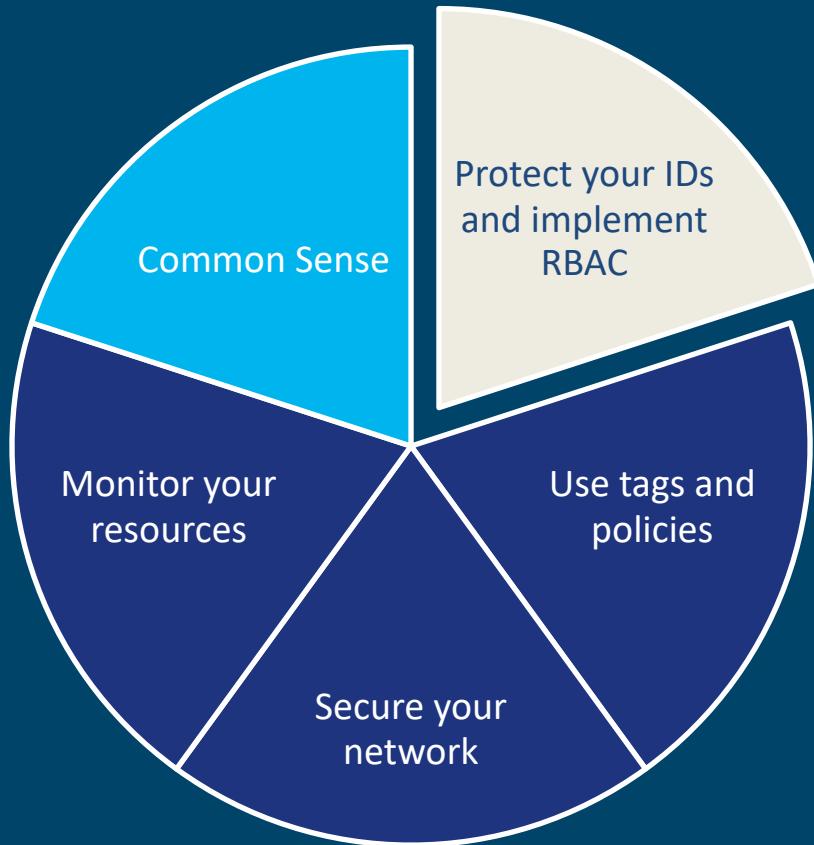
*Voltaire*



# 5 tips and best practices



# 5 tips and best practices





# Identity protection is essential

Use passphrases  
rather than (complex)  
passwords

## Implement multi-factor authentication

Adhere to the principle of least privilege

Establish privileged  
identity/access  
management  
(PIM/PAM)

# Enable conditional access policies



# Identity protection is essential

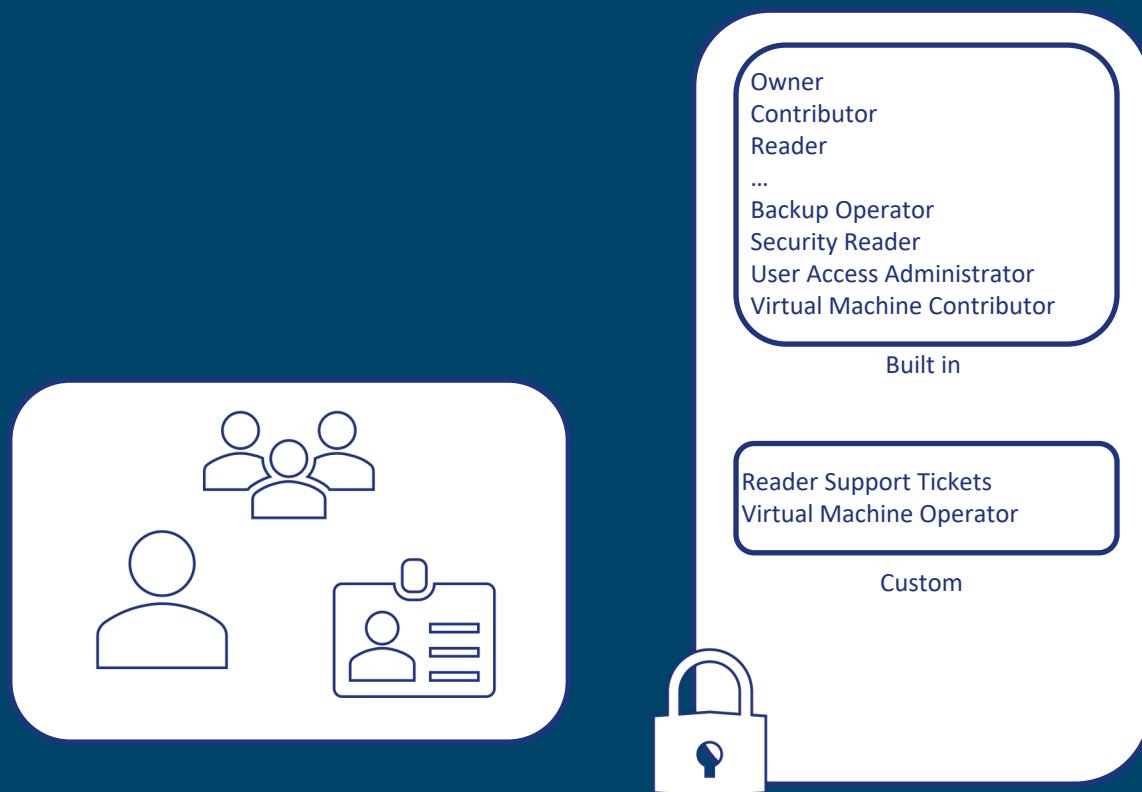
# Role-based access control

1. Security principal = user, group, service principal



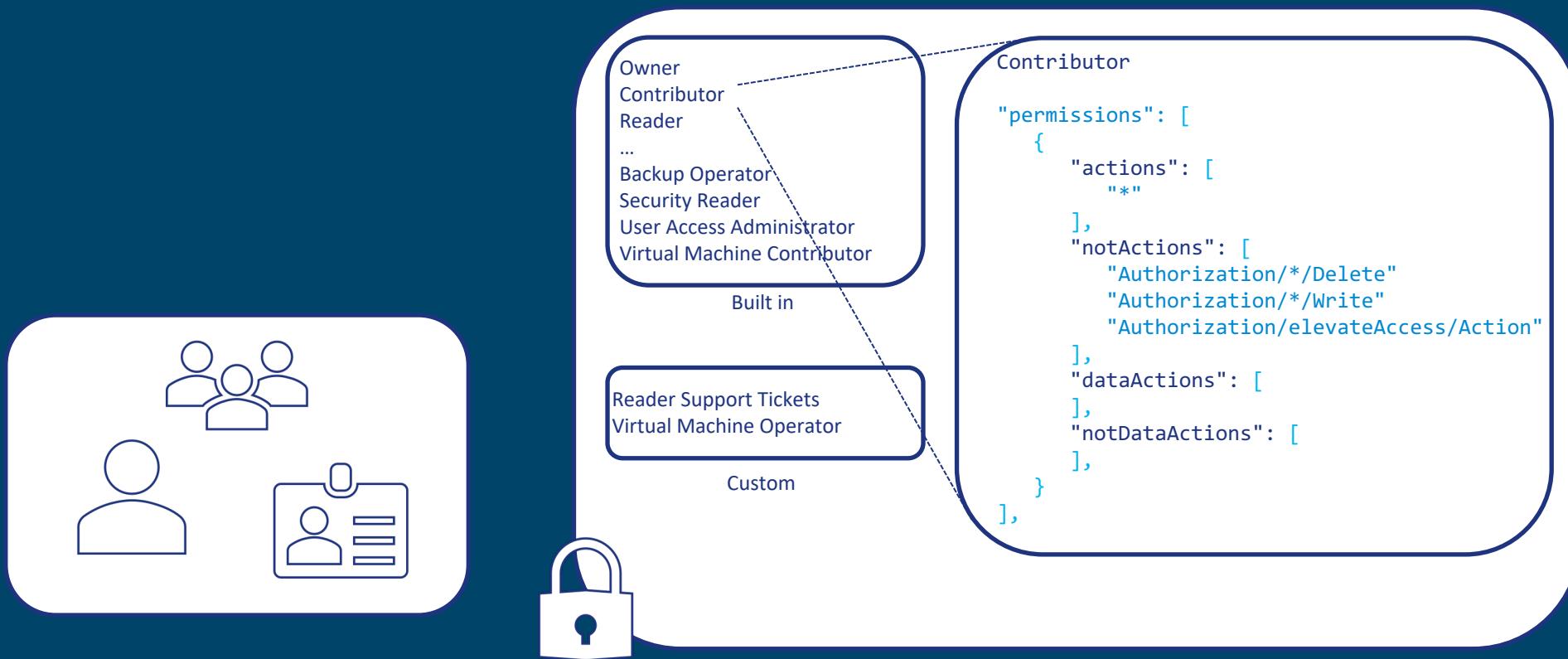
# Role-based access control

1. Security principal = user, group, service principal
2. Role definition = set of management rights



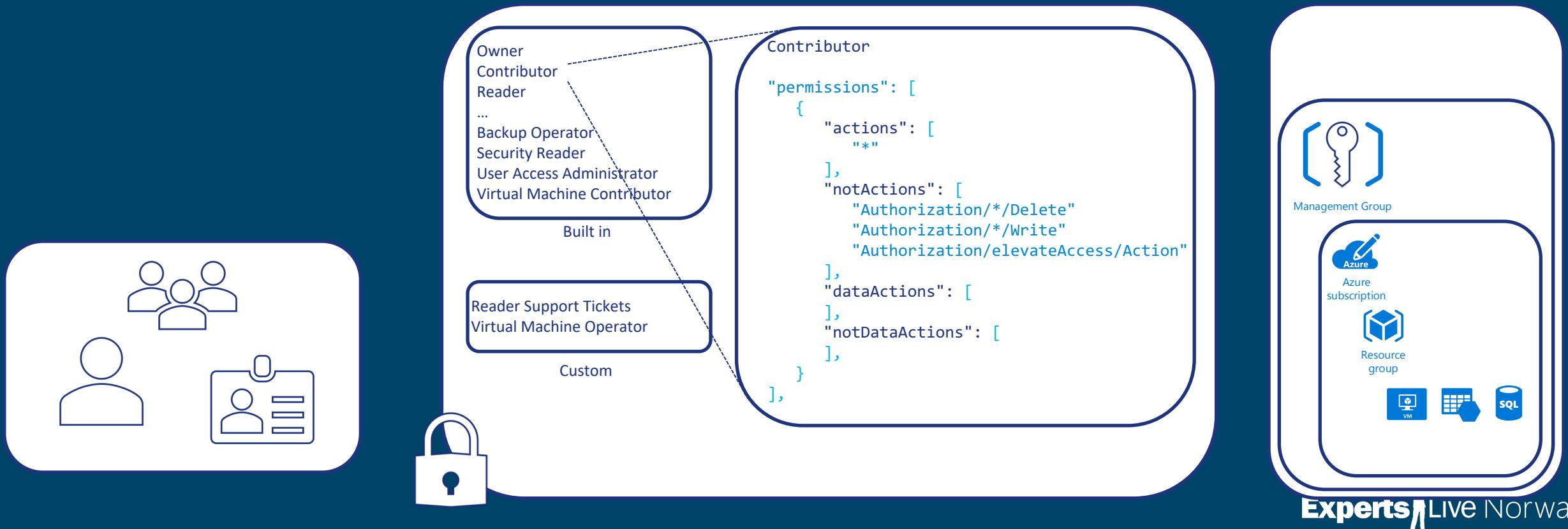
# Role-based access control

1. Security principal = user, group, service principal
2. Role definition = set of management rights

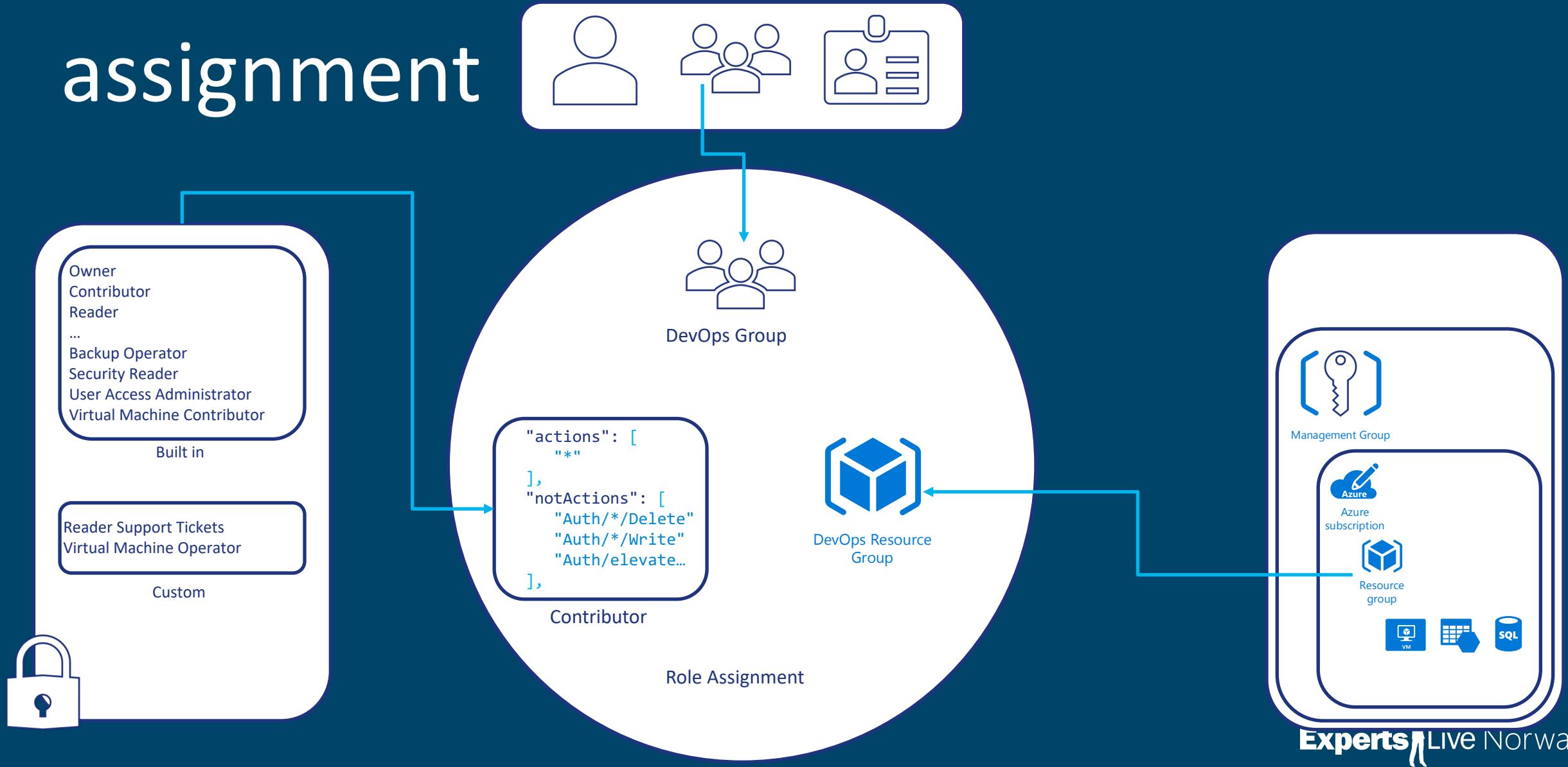


# Role-based access control

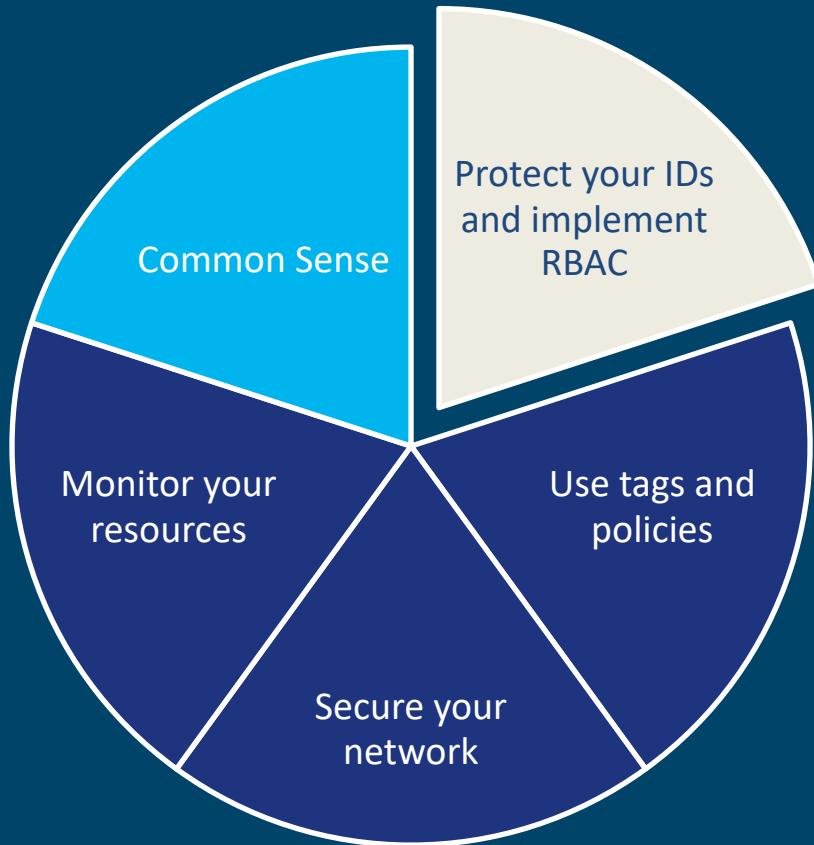
1. Security principal = user, group, service principal
2. Role definition = set of management rights
3. Scope = MG, subscription, RG, resource



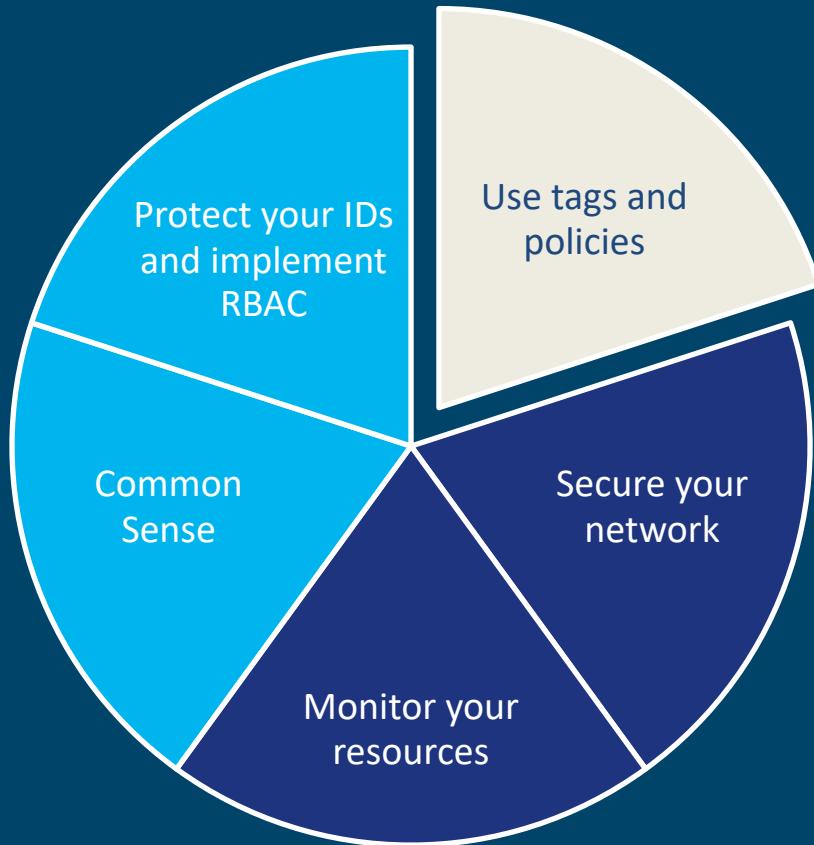
# Role-based access control – Role assignment



# 5 tips and best practices

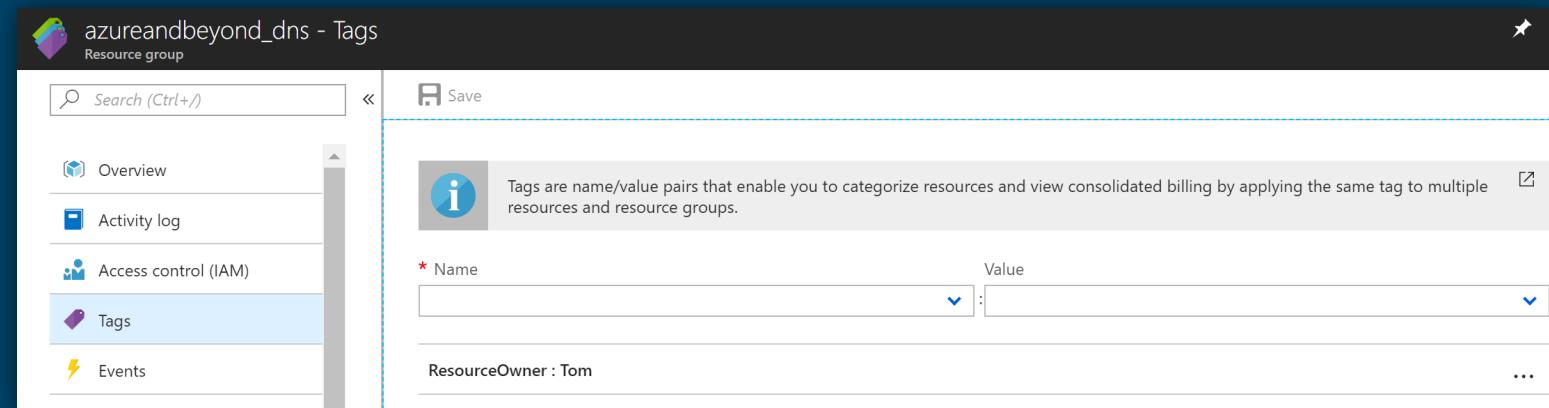


# 5 tips and best practices



# Resource Tags

- Name:Value, e.g. CostCenter:ProdIT, ResourceOwner:Tom
- Help to define responsibility and view consolidated billing
- Always tag RGs
  - Owner
  - Dept
  - CostCenter
  - [...]
- Tag resources as needed
- Define tags in advance



```
PS C:\> Get-AzureRmResource -TagName ResourceOwner -TagValue Tom | ft
```

Name	ResourceGroupName	ResourceType	Location
---	---	---	-----
azureandbeyond.eu	azureandbeyond_dns	Microsoft.Network/dnszones	global
lifecycletest	blobstorage-lifecyclemgmt	Microsoft.Storage/storageAccounts	westcentralus

# Resource Policies

- Rule enforcements on MG, subscription or RG level
- Initiative definitions vs. Policy definitions
- Effect types:
  - Append
  - Deny
  - Audit

MicrosoftIgnite2018  
Initiative Definition

Assign Edit initiative

Name  
MicrosoftIgnite2018

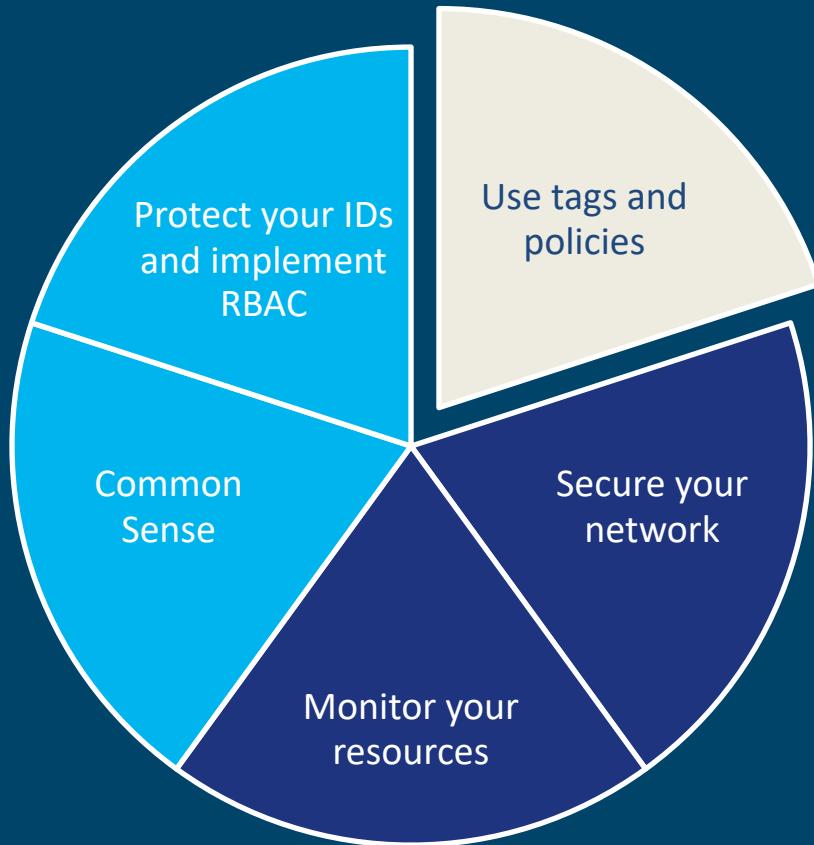
Description  
Initiative definition with two policies to demonstrate at Microsoft Ignite 2018

Category  
General

Filter by policy name or definition id... All effects

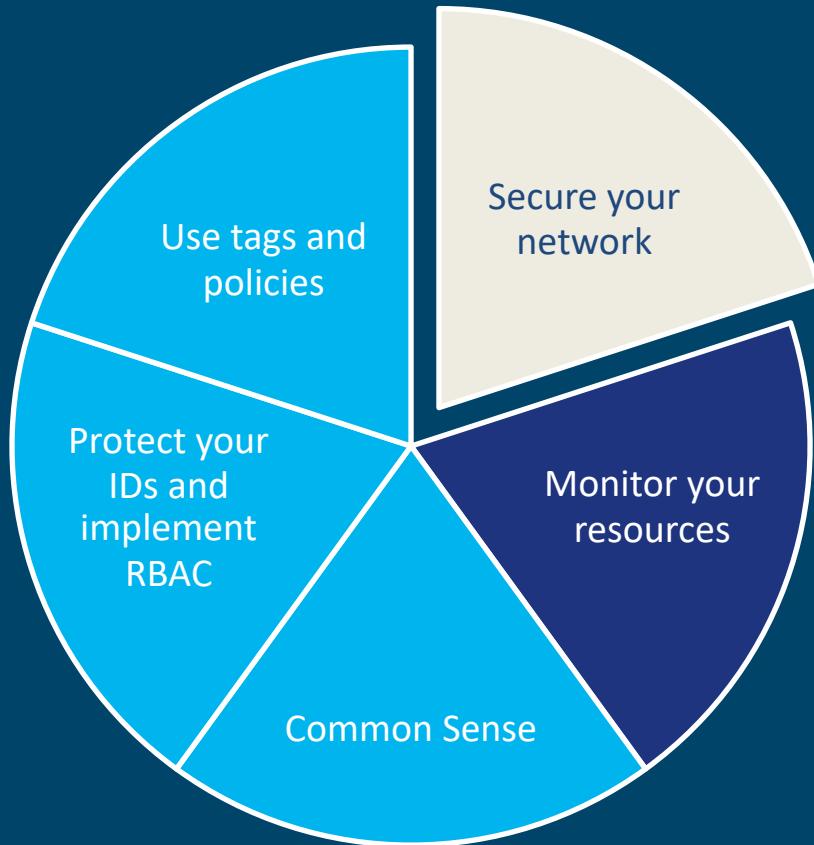
POLICY	EFFECT TYPE
Apply tag and its default value	Append
Allowed locations	Deny
Audit usage of custom RBAC rules	Audit

# 5 tips and best practices

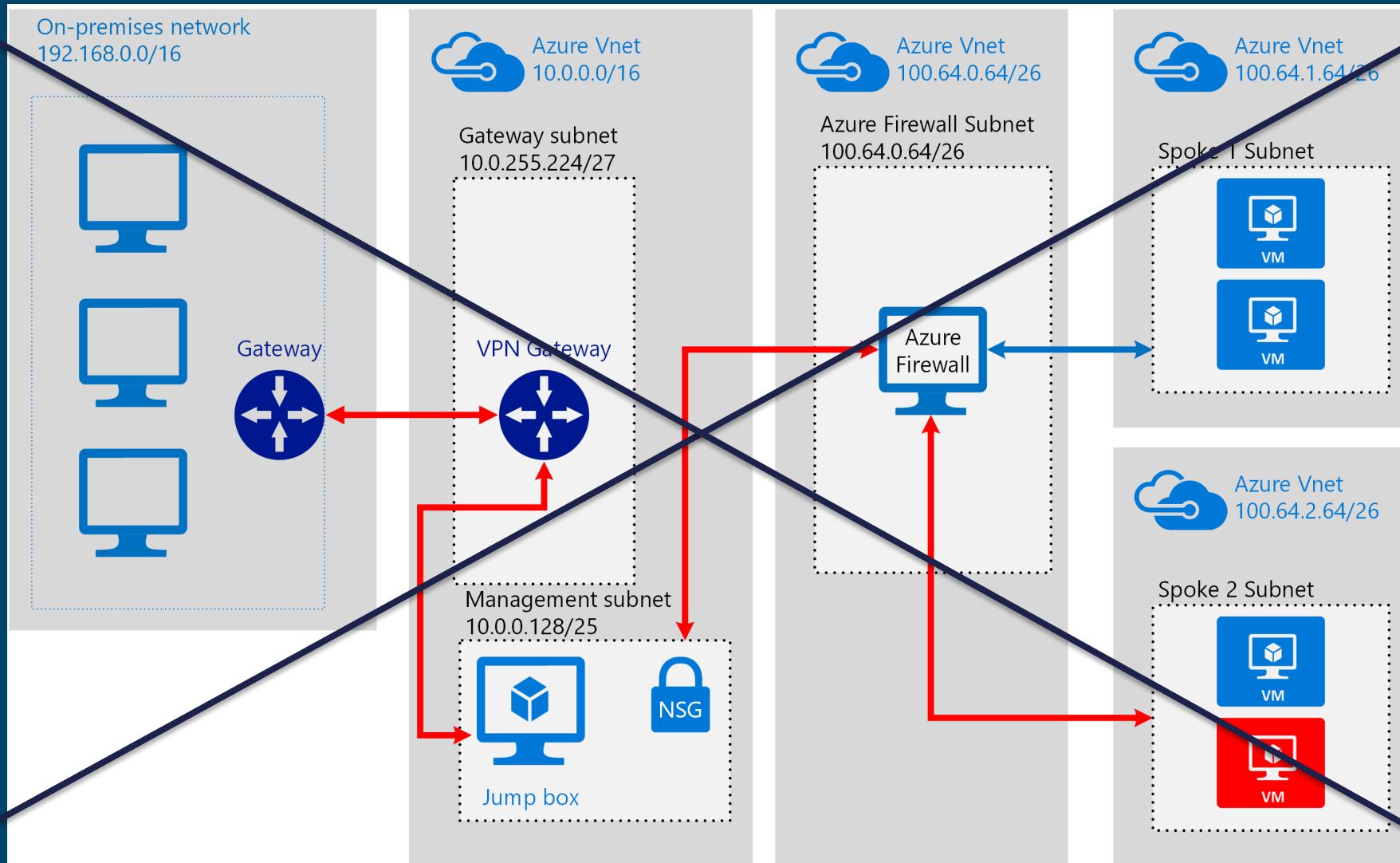




# 5 tips and best practices

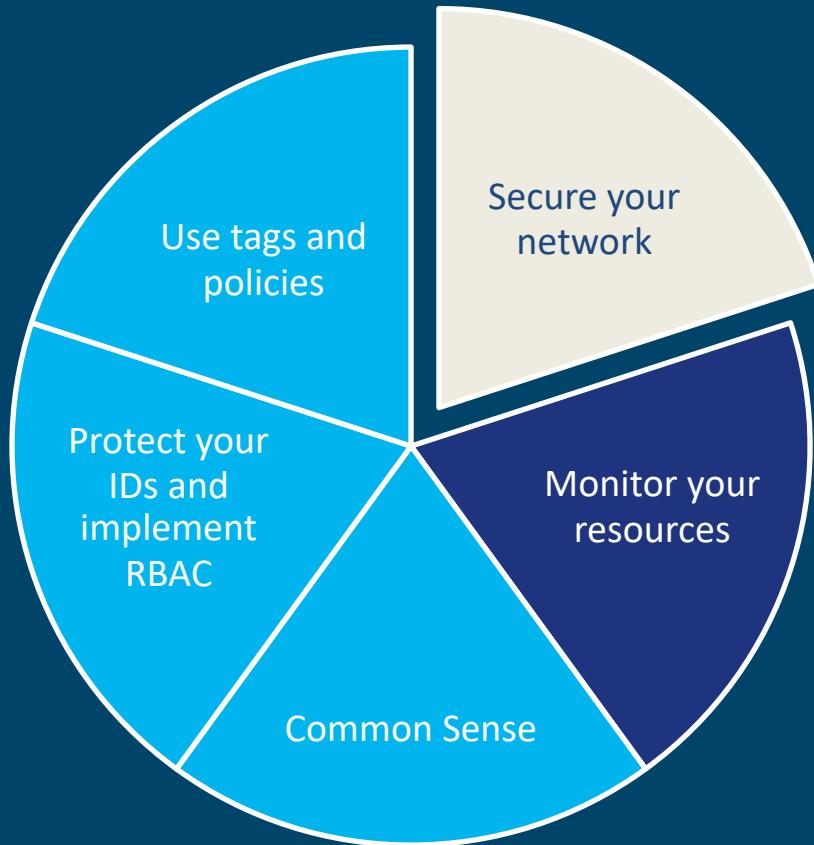


# Hybrid network risks

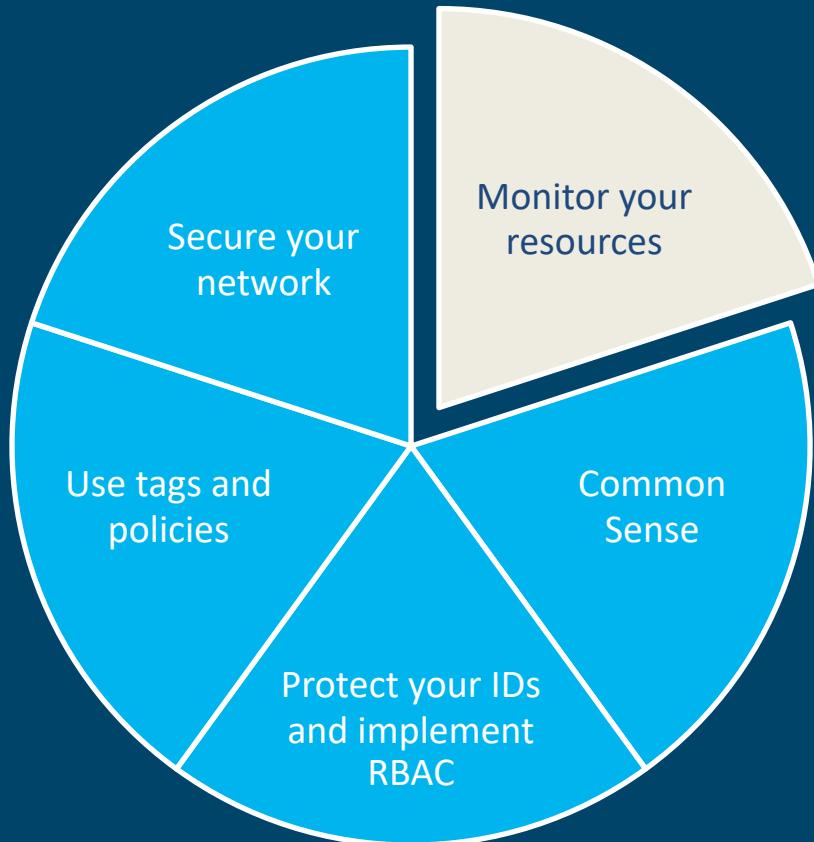




# 5 tips and best practices



# 5 tips and best practices



# Azure Security Center

Home > Security Center - Overview

## Security Center - Overview

Showing 4 subscriptions

Subscriptions What's new

### Policy & compliance

Secure score: 479 OF 740 (Secure score impact changed. Learn more)

Regulatory compliance:

- SOC TSP: 1 of 13 passed controls
- ISO 27001: 3 of 21 passed controls
- PCI DSS 3.2: 5 of 33 passed controls

Subscription coverage: 42 Covered resources (4 TOTAL, 1 Fully covered, 3 Partially covered, 0 Not covered)

### Resource security hygiene

Recommendations: 16 TOTAL (High Severity: 10, Medium Severity: 1, Low Severity: 5), 37 Unhealthy resources

Resource health monitoring:

- Compute & apps: 13
- Data & storage: 13
- Networking: 7
- Identity & access: 9

### Threat protection

Security alerts by severity:

- High Severity: 21
- Medium Severity: 20
- Low Severity: 26

Attacked resources: 10

Security alerts over time:

Most prevalent alerts:

- [Preview] Traffic from unrecommended sources: 3 Resources
- Security incident detected: 2 Resources
- Suspicious authentication activity: 2 Resources

Manage and govern your security posture

Define and assign Azure Security Center policies in order to review and track compliance to security standards.

Learn more >

Top recommendations by secure score impact:

- Enable MFA for accounts with owner permissions: +50
- Enable Network Security Groups on subnets: +30
- Install a vulnerability assessment solution on your resources: +30

Most prevalent alerts:

- [Preview] Traffic from unrecommended sources: 3 Resources
- Security incident detected: 2 Resources
- Suspicious authentication activity: 2 Resources



# Azure Security

# Cloud security starts with...

„...challenges?“

„Are you ever

...“?

“...security by de-

“It's not a security breach if it wasn't  
secure before!“

“Who actually  
owns security?“

„How do I figure  
out what I don't  
know?“

„Not knowing where  
to start is my top  
AzSec challenge“

## ... infrastructure as code!

```
1 #!/bin/bash
2
3 # Change these variables according to your needs
4 RESOURCE_GROUP_NAME=terraformstate
5 STORAGE_ACCOUNT_NAME=tfstate$RANDOM
6 CONTAINER_NAME=tfstate
7 VAULT_NAME=yourKeyVault$RANDOM
8 SECRET_NAME=yourSecret
9
10 # Create Resource Group, Storage Account and Container for Terraform backend (see https://www.terraform.io/docs/backends/types/azurerm.html)
11
12 # Create resource group
13 az group create --name $RESOURCE_GROUP_NAME --location westeurope
14
15 # Create storage account
16 az storage account create --resource-group $RESOURCE_GROUP_NAME --name $STORAGE_ACCOUNT_NAME
17
18 # Get storage account key
19 ACCOUNT_KEY=$(az storage account keys list --resource-group $RESOURCE_GROUP_NAME --account-name $STORAGE_ACCOUNT_NAME --query key1 -o tsv)
20
```

\$outputs = (new-azurermresourcegroupdeployment

- Name AzSecLab-Core
- ResourceGroupName \$resourceGroupName
- TemplateUri https://azureseclab.blob.core.windows.net/
- VaultName \$vaultName
- SecretName \$secret.Name
- VaultResourceGroup \$resourceGroupName

).Outputs

```
# Azure Key Vault data source
data "azurerm_key_vault_secrets" "labuser" {
  name      = "labuser"
  vault_uri = "https://yourKeyVaultName.vault.azure.net/secrets/labuser"
}

# get my external IP address
data "http" "myExtIp" {
  url = "http://ident.me/ip"
}
```

creates references to an Azure Key Vault secrets and an external IP address from the website.

## Data sources

With data sources in Terraform we can reference external objects that are needed during deployments. The passage

```
# Azure Key Vault data source to access local admin password
data "azurerm_key_vault_secret" "mySecret" {
    name      = "labuser"
    vault_uri = "https://yourKeyVault.vault.azure.net/"
}

# get my external IP address to enter into NSG rule
data "http" "myExtIp" {
    url = "http://ident.me/"
}

"resources": [
    {
        "type": "Microsoft.Network/networkSecurityGroups",
        "name": "nsg-allow-ssh",
        "location": "West US",
        "tags": {
            "Name": "nsg-allow-ssh"
        },
        "properties": {
            "securityRules": [
                {
                    "name": "AllowSSH",
                    "priority": 100,
                    "sourceAddressPrefix": "*",
                    "destinationAddressPrefix": "*",
                    "sourcePortRange": "*",
                    "destinationPortRange": "22",
                    "access": "Allow",
                    "protocol": "TCP",
                    "direction": "Inbound"
                }
            ]
        }
    }
]
```

creates references to an Azure Key external IP address from the website

```
"resources": [
    {
        "apiVersion": "2017-05-10",
        "name": "linkedTemplate",
        "type": "Microsoft.Resources/deployments",
        "properties": {
            "mode": "Incremental",
            <nested-template-or-external-template>
        }
    }
]
```

<https://github.com/azureandbeyond/AzureSecurity>

# Azure Security Services and Capabilities

## Network Security

- Virtual Network Service Endpoints
- DDoS Protection
- Network Security Groups
- NSG Service Tags
- NSG Application Security Groups
- NSG Augmented Rules
- Global Virtual Network Peering
- Azure DNS Private Zones
- Site-to-Site VPN
- Point-to-Site VPN
- ExpressRoute
- Azure Virtual Networks
- Virtual Network Appliances
- Azure Load Balancer
- Azure Load Balancer HA Ports
- Azure Application Gateway
- Azure Firewall
- Azure Web Application Firewall
- Service Endpoints

## Monitoring and Logging

- Azure Log Analytics
- Azure Monitor
- Network Watcher
- VS AppCenter Mobile Analytics

## Compliance Program

- Microsoft Trust Center
- Service Trust Platform
- Compliance Manager
- Azure IP Advantage (legal)

## Identity and Access Management

- Azure Active Directory
- Azure Active Directory B2C
- Azure Active Directory Domain Services
- Azure Active Directory MFA
- Conditional Access
- Azure Active Directory Identity Protection
- Azure Active Directory Privileged Identity Management
- Azure Active Directory App Proxy
- Azure Active Directory Connect
- Azure RBAC
- Azure Active Directory Access Reviews
- Azure Active Directory Managed Service Identity

## Security Docs Site

- Azure Security Information Site on Azure.com

## DDoS Mitigation

- Azure DDoS Protection
- Azure Traffic Manager
- Autoscaling
- Azure CDN
- Azure Load Balancers
- Fabric level edge protection

## Infrastructure Security

- Comes with Azure Data Centers
- Azure Advanced Threat Protection
- Confidential Computing

## Pen Testing

- Per AUP
- Per TOS
- No contact required

## Data Loss Prevention

- Cloud App Discovery
- Azure Information Protection

## Encryption

- Azure Key Vault
- Azure client-side encryption library
- Azure Storage Service Encryption
- Azure Disk Encryption
- SQL Transparent Data Encryption
- SQL Always Encrypted
- SQL Cell/Column Level Encryption
- Azure CosmosDB encrypt by default
- Azure Data Lake encrypt by default
- VPN protocol encryption (ssl/ipsec)
- SMB 3.0 wire encryption

## Configuration and Management

- Azure Security Center
- Azure Sentinel
- Azure Resource Manager
- Azure Resource Graph
- ARM Management Groups
- Azure Policy
- Azure Blueprints
- Azure Automation
- Azure Advisor
- Azure API Gateway

# Microsoft Azure Security Center

Unify security management and enable advanced threat protection for hybrid cloud workloads



## Unified visibility and control

Dynamically discover and manage the security of your hybrid cloud workloads in a single cloud-based console



## Adaptive threat prevention

Enable actionable, adaptive protections that identify and mitigate risk to reduce exposure to attacks



## Intelligent detection and response

Use advanced analytics and Microsoft Intelligent Security Graph to rapidly detect and respond to evolving cyber threats

# Azure Security Center Pipeline

Data sources:



Computers



Azure Services



Security Data  
& Alerts



REST APIs

## DETECT



Built-in Analytics &  
Machine Learning



Custom Alert Rules



Enrichment



Threat Intelligence



Prioritization



Fusion

## RESPOND



Search



Alert Exploration

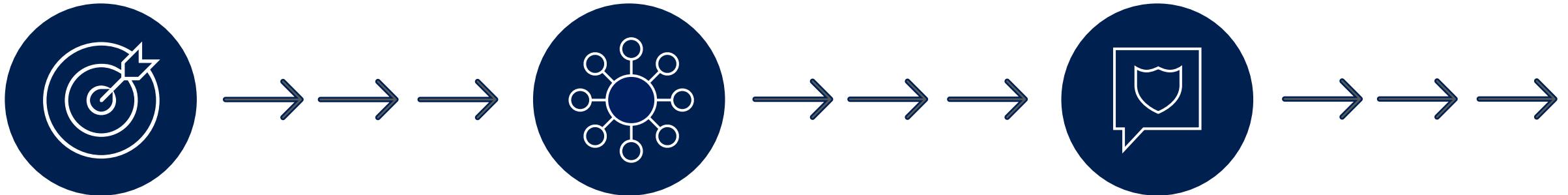


Investigation



Automation &  
Orchestration

# Detect threats across the kill chain



## TARGET AND ATTACK

Inbound brute force RDP, SSH, SQL attacks and more

Application and DDoS attacks (WAF partners)

Intrusion detection (NG Firewall partners)

## INSTALL AND EXPLOIT

In-memory malware and exploit attempts

Suspicious process execution

Lateral movement

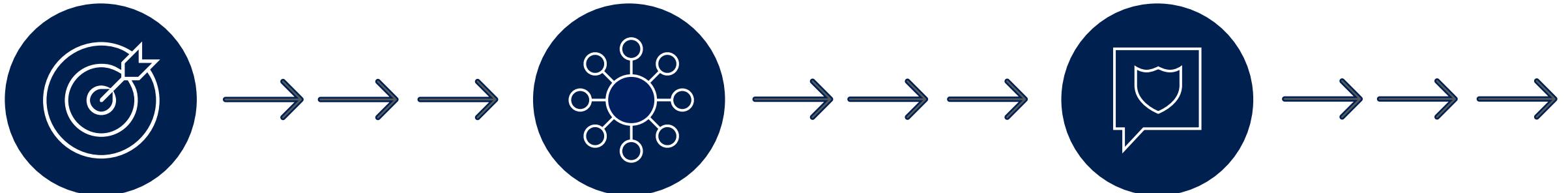
Internal reconnaissance

## POST BREACH

Communication to a known malicious IP (data exfiltration or command and control)

Using compromised resources to mount additional attacks (outbound port scanning, brute force RDP/SSH attacks, DDoS, and spam)

# Detect threats across the kill chain



## TARGET AND ATTACK

Inbound brute force RDP, SSH, SQL attacks and more

Application and DDoS attacks (WAF partners)

Intrusion detection (NG Firewall partners)

## INSTALL AND EXPLOIT

In-memory malware and exploit attempts

Suspicious process execution

Lateral movement

Internal reconnaissance

## POST BREACH

Communication to a known malicious IP (data exfiltration or command and control)

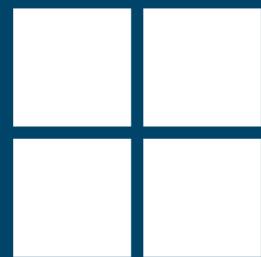
Using compromised resources to mount additional attacks (outbound port scanning, brute force RDP/SSH attacks, DDoS, and spam)

# DEMO



# Thank You!

Platinum



Microsoft

Gold

audiocodes

Silver



au2mator

pexip

Jabra

logitech