cloudneeti

Stay secure. Stay compliant.

Azure Security

Top 10 ways to protect your cloud assets

Learning is better with Pizza

Gururaj Pandurangi, CEO, Cloudneeti

Microsoft CERTIFIED Solutions Developer

Azure Solutions Architect

amazon web services | Certified

An Entrepreneur

founded three cloud startups - a multi-cloud backup/ recovery (sold 2013), cloud consulting (Avyan) helping enterprises with cloud adoption (AWS, Azure) and Cloudneeti

Cloud Architecture and Security Expert

key contributor to Center of Internet Security (CIS) benchmarks for Azure and M365, Azure Blueprints, speaker at security events

Product Engineering Leader

shipped large scale v1 cloud services at Microsoft (e.g. Microsoft Bing, integrations with Yahoo and Facebook, Azure Fabric, Windows Live ID, Directory Services)

✉ gururajp@cloudneeti.com

gnarlytweeter

in https://www.linkedin.com/in/gururajp/

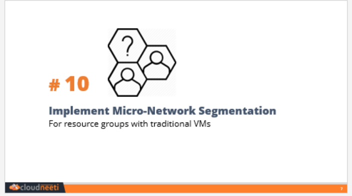
4the Year
Azure Bootcamp Speaker

Agenda

Az Security Primer

Azure Security – A Primer

Top 10 .. 9 .. 8



10

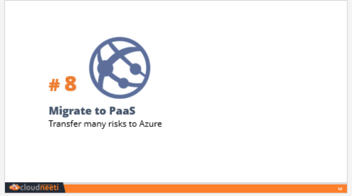
Implement Micro-Network Segmentation

For resource groups with traditional VMs

9

Implement Cloud Operations

Patching, Logging, Alerting



8

Migrate to PaaS

Transfer many risks to Azure

Top 7 .. 6 .. 5

7

Implement RBAC

Management Groups, Subscriptions, Resource Groups etc.

6

Implement Azure Policies

Security Guardrails

5

Infrastructure as Code

Check in to your Source control

Top 4 .. 3 .. 2

4

Enable Azure Security Center

Assessment, Visibility

3

Privileged Identity Management

PIM / PAM - Who has the Jam?

2

Conditional Access for Devices

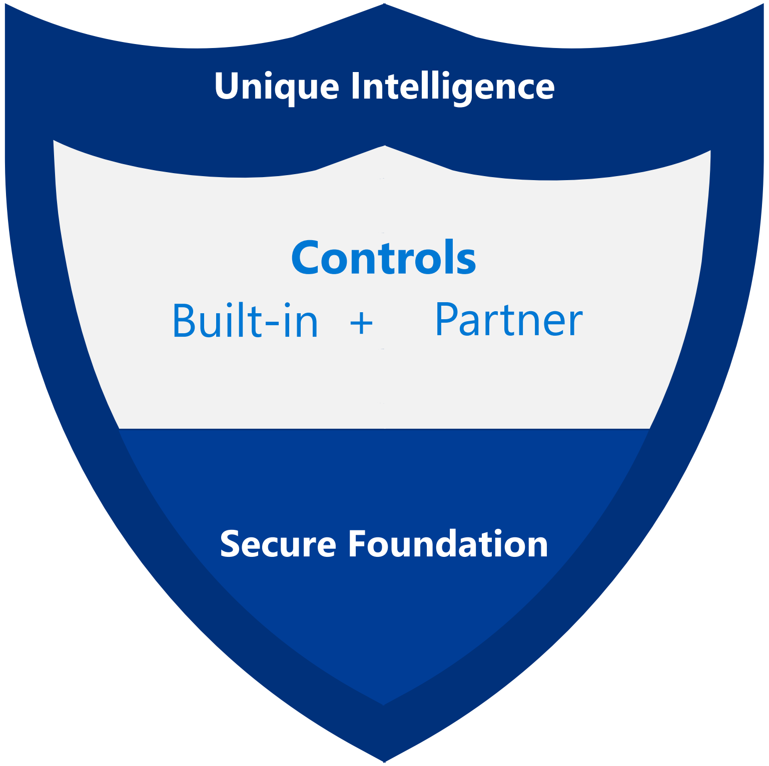
Top 1

1

Multi-Factor Authentication

Enforce for Admins and Contributors

Azure Security – A Primer



Unique Intelligence

Controls

Built-in + Partner

Secure Foundation

Defense in Depth

Identity & Access	Apps & Data Security	Network Security	Threat Protection	Security Management
Role based access	Encryption	DDoS Protection	Antimalware	Log Management
Multi-Factor Authentication	Confidential Computing	NG Firewall	AI Based Detection and Response	Security Posture Assessment
Central Identity Management	Key Management	Web App Firewall	Cloud Workload Protection	Policy and governance
Identity Protection	Certificate Management	Private Connections	SQL Threat Protection	Regulatory Compliance
Privileged Identity Management	Information Protection	Network Segmentation	IoT Security	SIEM

Microsoft + Partners

Quiz

Name four (4) Azure Network Security Services?

E.g. Azure Firewall, DDoS Protection, Azure WAF (App Gateway), Network Security Groups, Application Security Groups

Name four (4) Data Security Services?

E.g. Disk Encryption, Threat protection (SQL DB, Storage accounts), Always Encrypted, SQL DB Vulnerability Management

Name four (4) Compute Security Services?

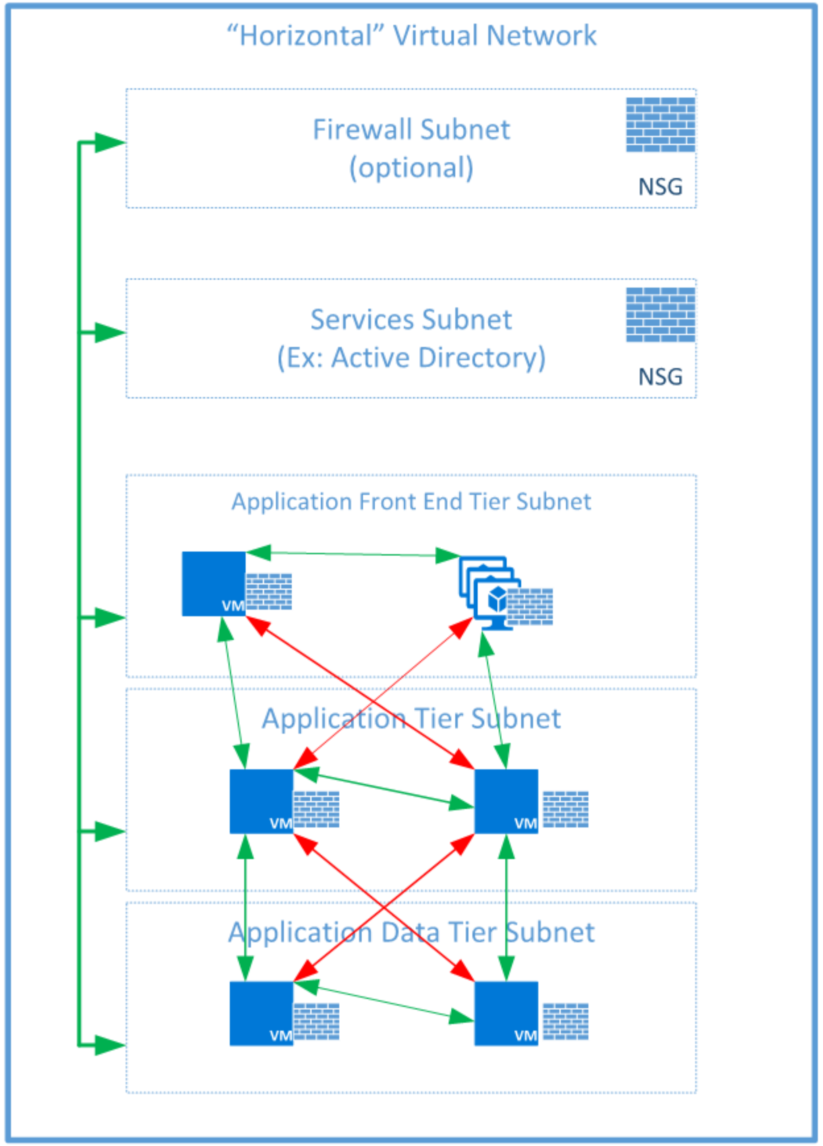
E.g. Azure Update Management, Shielded VMs, App Service Environments, End-point protection (Antivirus/malware)

10

Implement Micro-Network Segmentation

For resource groups with traditional VMs

Movement to vertical network design



“Horizontal” Virtual Network

Firewall Subnet (optional)

NSG

Services Subnet (Ex: Active Directory)

NSG

Application Front End Tier Subnet

VM

Application Tier Subnet

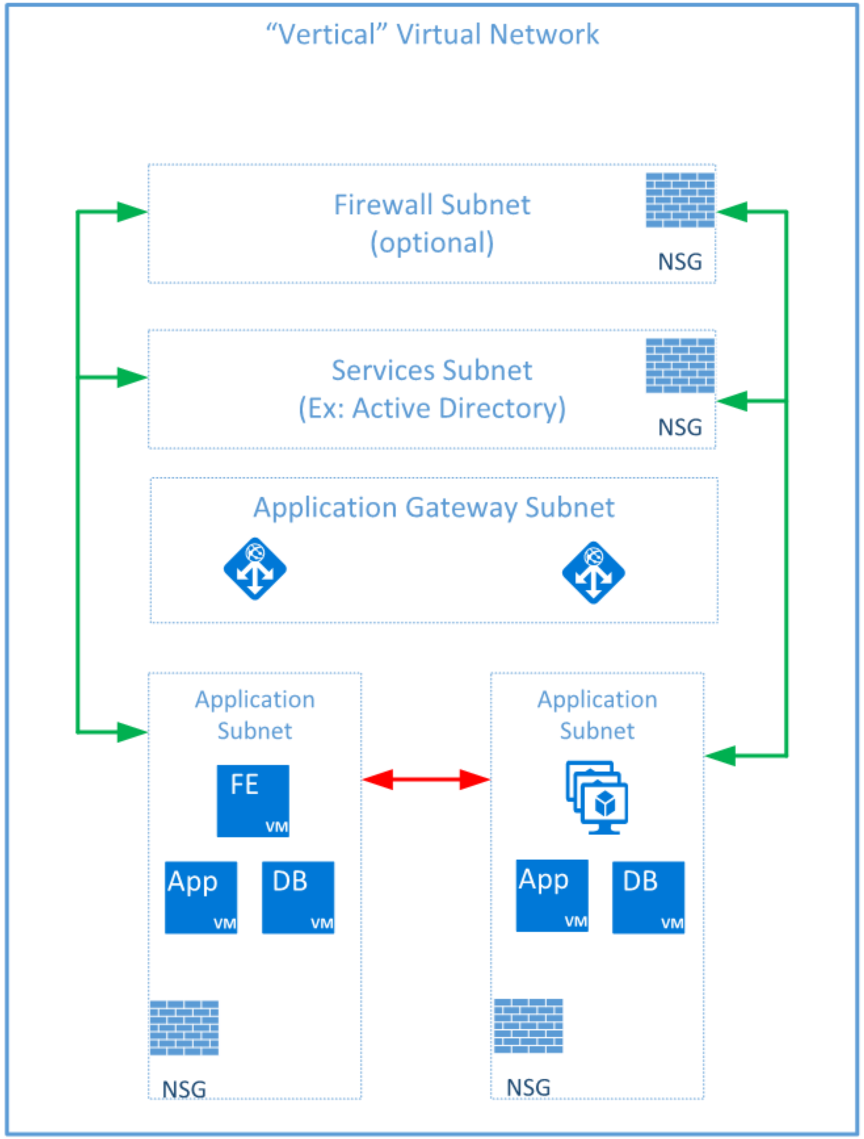
VM

VM

Application Data Tier Subnet

VM

VM



“Vertical” Virtual Network

Firewall Subnet (optional)

NSG

Services Subnet (Ex: Active Directory)

NSG

Application Gateway Subnet

Application Subnet

FE VM

App VM

DB VM

NSG

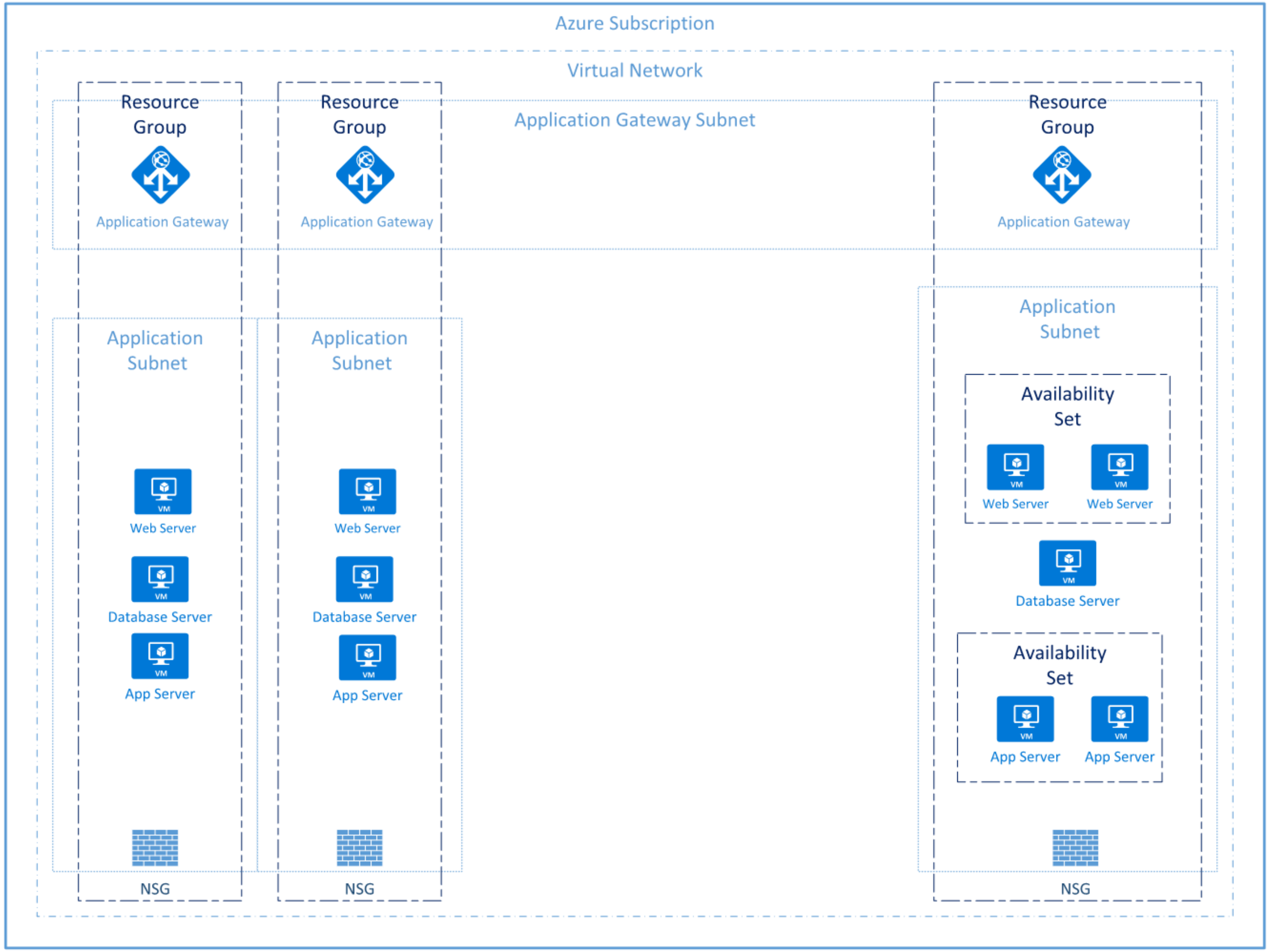
Application Subnet

App VM

DB VM

NSG

Another look at a vertical network



cloudneeti

9

Implement Cloud Operations

Patching, Logging, Alerting

Implement Cloud Operations to allow for Detection and Analysis

1

Azure Update & Automations Management

VM Patching, Desired State Automation

2

Azure Monitor

Log, Monitor & Alerts

3

Azure Log Analytics / Azure SIEM

Analytics & Alerts

8

Migrate to PaaS

Transfer many risks to Azure

Security Responsibilities Transfer to Azure

Responsibility	PaaS	IaaS
Information and Data	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦
Accounts and Identities	🟦	🟦
Identity and directory infrastructure	◩	🟦
Application	◩	🟦
Network controls	◩	🟦
Operating system	⬜	🟦
Physical hosts	⬜	⬜
Physical network	⬜	⬜
Physical datacenter	⬜	⬜

⬜ Microsoft 🟦 Customer

Transferred for PaaS

Security Patches

Feature Upgrades

VMs/Containers security –
OS and Middleware Installation, Maintenance, troubleshooting, etc.

Azure Marketplace
fits PaaS or IaaS model

Transferred for IaaS and PaaS

Denial of Service*

Racking/Stacking Servers, Delays in Adding Capacity

Fabric/Virtualization Patching, Maintenance & Troubleshooting

Fabric Availability / Uptime
→ SLA from Microsoft

Attacks on

- Physical Attacks
- Virtualization Fabric
- Hardware/Firmware
- Network Infrastructure

Azure App Service Plans transfer many risks to Azure. Choose wisely though …

Can host Windows Web apps, Linux web apps, Web Jobs, Docker containers, Mobile apps, Functions

General App Services

- Assume external internet access, very viable for production use case, **but missing isolation**
- You can apply IP restrictions, monitor access, leverage security center, etc.

App Service Environments

- **Provides Isolation**
- Can leverage **NSG**,
- **Deny** general internet access

7

Implement RBAC

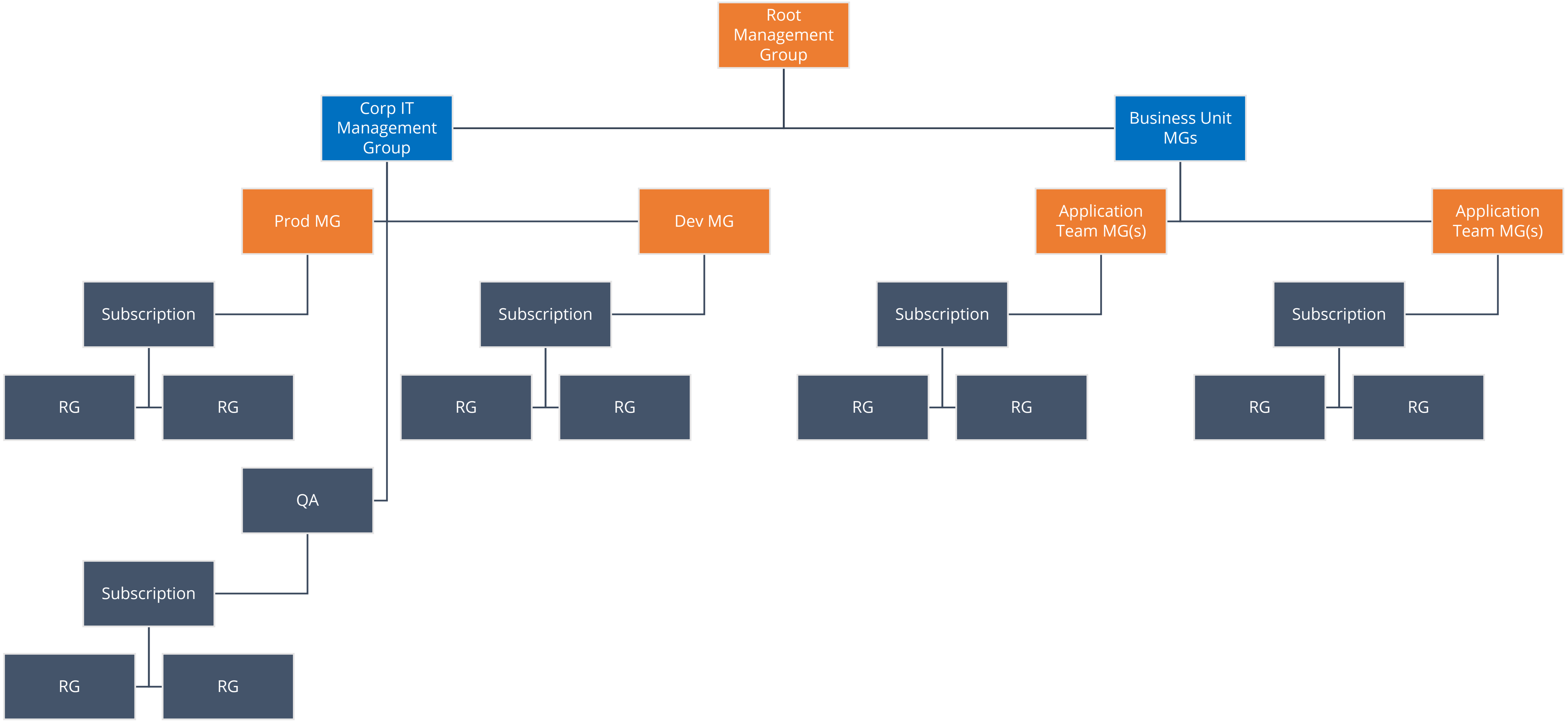
Management Groups, Subscriptions, Resource Groups etc.

Resource Group Isolation

RBAC applied to Applications

- Application teams **only access application RGs**
- Admin (owner) credentials are **different** than application credentials
- Deployments are encouraged to be automated from source code

Applying Permissions to Structure



6

Implement Azure Policies

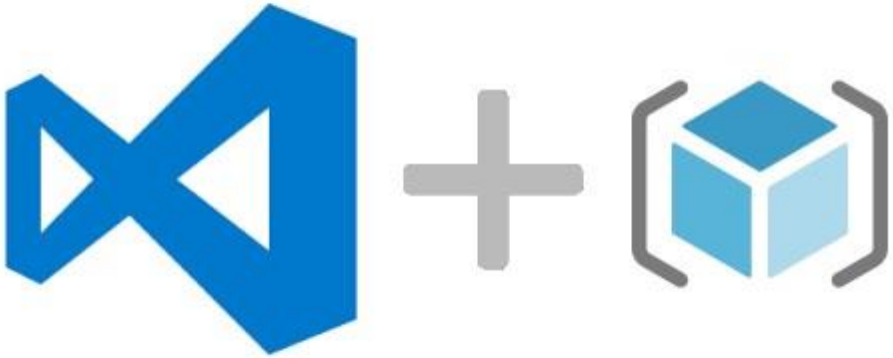
Security Guardrails

ARM and Azure Policy

Use platform to implement security controls

- Deployment **doesn’t happen without tagging**, application, app classification
- **Tagging applies policies**, audits, additional security controls
- Ensures **operational process is consistent**, but creativity exists

A possibility



5

Infrastructure as Code

Check in to your Source control

Infrastructure as Code

- Simplifies backup and recovery
- Allows re-deployability
- Enables DevSecOps

Avoid

4

Enable Azure Security Center

Assessment, Visibility

Enable visibility and control across hybrid workloads

Built-in Controls | Security Management

Enable centralized view of security state across cloud and on-premises workloads

Monitor security across all subscriptions and environments

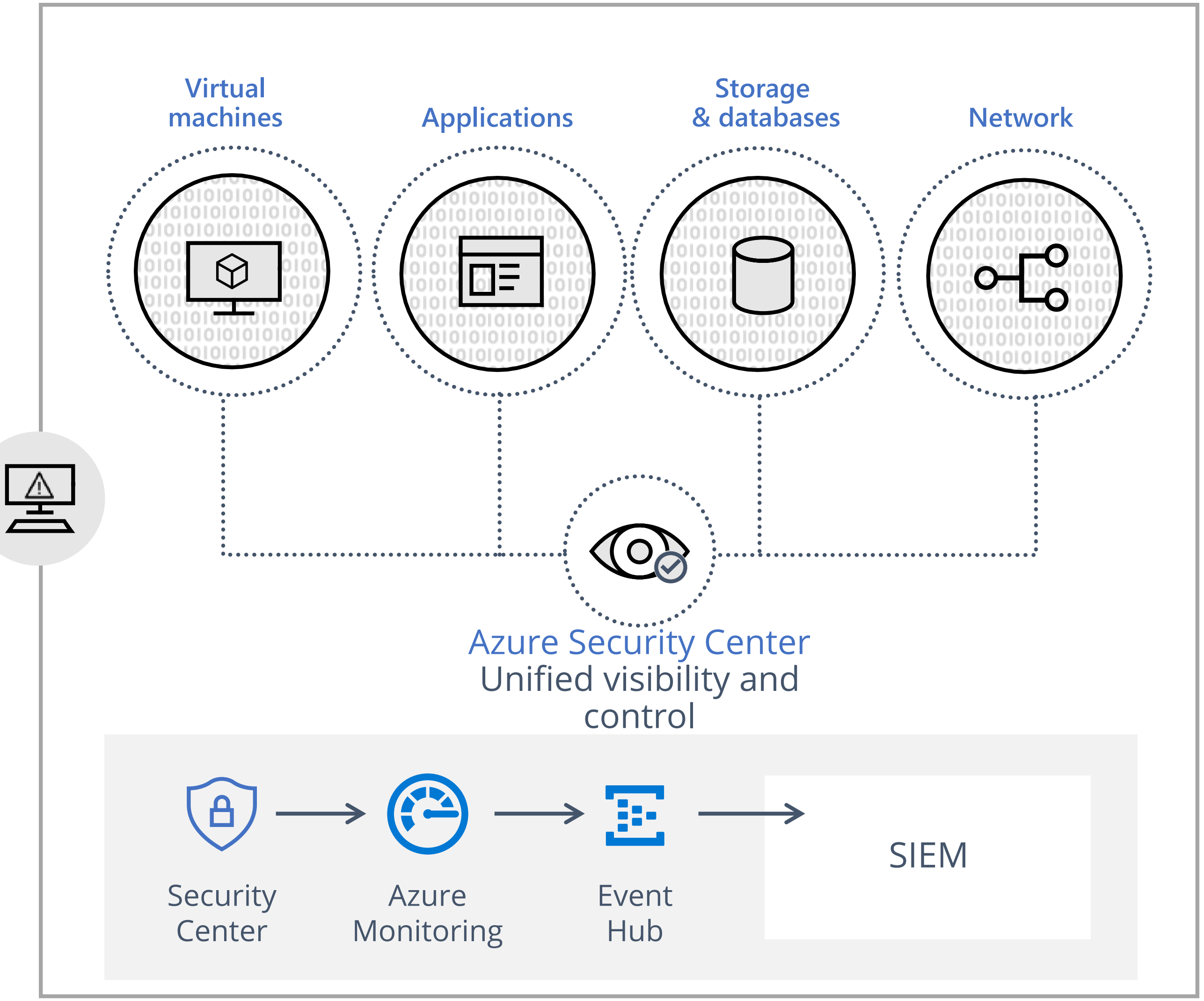
Ensure compliance to your requirements

Configure centralized security policy and view compliance score across different resources in a central dashboard

Integrate auditing, logging with existing processes

Configure auditing, logging and use Log Analytics for advanced analysis

Export security data to existing SIEM solutions



I SEE CYBER RISKS
EVERYWHERE
made on imgur

3

Privileged Identity Management

PIM / PAM - Who has the Jam?

Admin Accounts

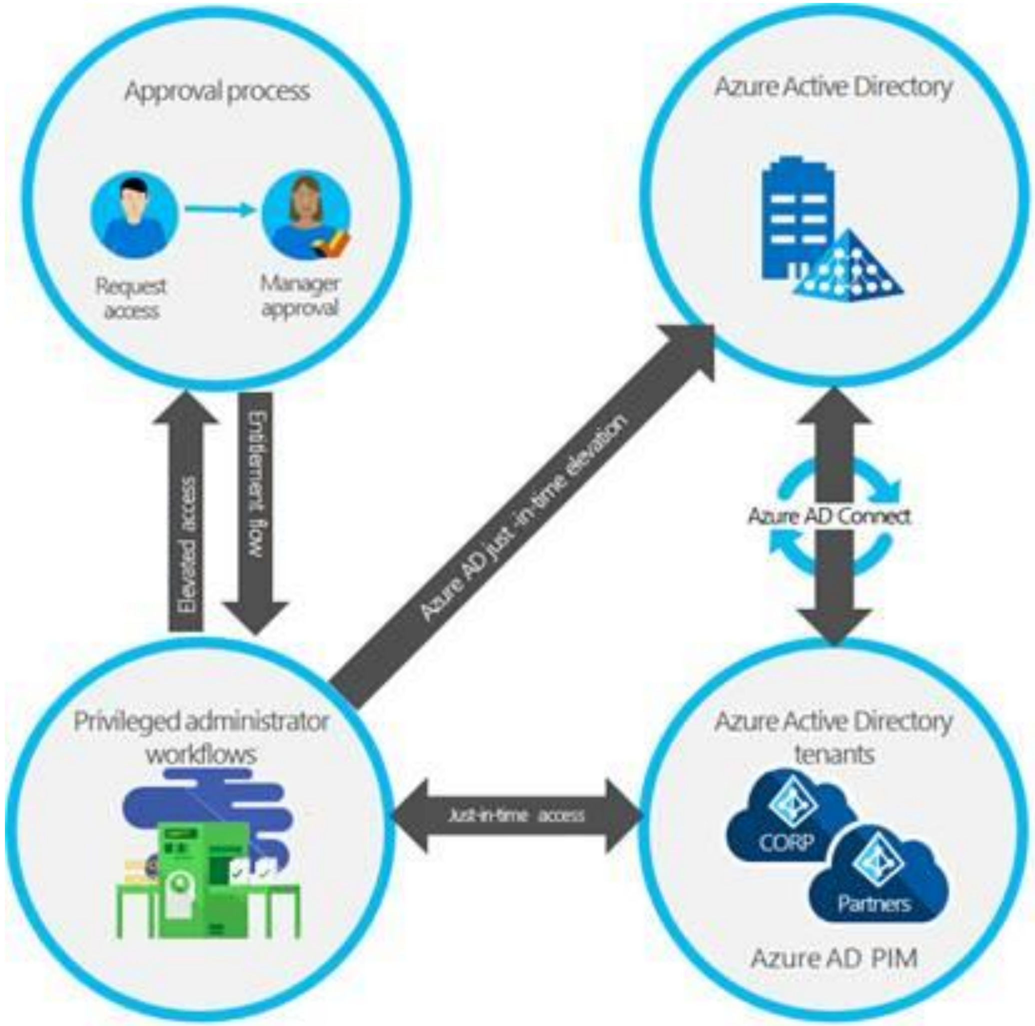
Don’t use your normal email for admin (owner) account

- Segment usage, you don’t need to be the owner often

When you do need roles, use Privileged Identity Management

- Request Just in Time access to roles

Azure Privileged Identity Management



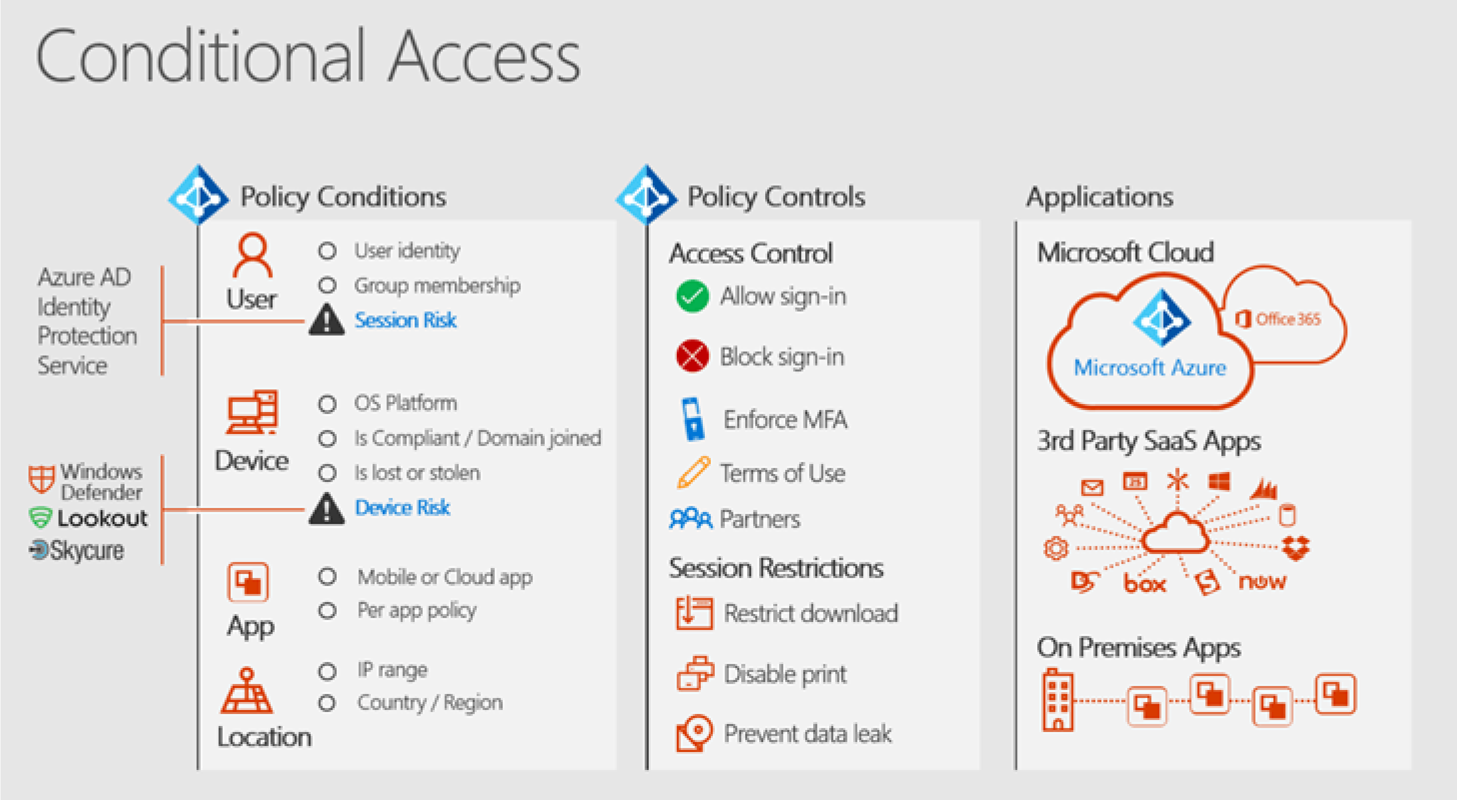
2

Conditional Access for Devices

Identity and Conditional Access ARE Your Firewall

- **Conditional Access**
  - Govern from what devices **certain functions** can be performed
  - Only healthy, managed devices can be used to perform activities
  - **Admin vs. non-admin** functions

- **Enable it with co-management or green field**
  - This is an important security barrier, not possible with SCCM alone



Conditional Access

Azure AD Identity Protection Service

Windows Defender
Lookout
Skycure

Policy Conditions

User
○ User identity
○ Group membership
⚠ Session Risk

Device
○ OS Platform
○ Is Compliant / Domain joined
○ Is lost or stolen
⚠ Device Risk

App
○ Mobile or Cloud app
○ Per app policy

Location
○ IP range
○ Country / Region

Policy Controls

Access Control
✓ Allow sign-in
Block sign-in
Enforce MFA
Terms of Use
Partners

Session Restrictions
Restrict download
Disable print
Prevent data leak

Applications

Microsoft Cloud
Microsoft Azure
Office 365

3rd Party SaaS Apps
box
now

On Premises Apps

You might need a manual

1

Multi-Factor Authentication

Enforce for Admins and Contributors

If you do one thing, do this...

Implement Multi-factor Authentication

- Use **Multifactor Authentication** in Azure AD at minimum for JIT and owner functions
- Combine with other conditional access functions
- **Single most important protection against administrative breach**

Cloudneeti is a security and compliance product that identifies and eliminates cloud risks

1000+ ways to secure your cloud infrastructure

Request A Free Trial:
https://www.cloudneeti.com/request-a-free-trial/