Insight | Digital Innovation

Azure Governance

AN OVERVIEW WITH INSIGHT DIGITAL INNOVATION

Insight Presentation

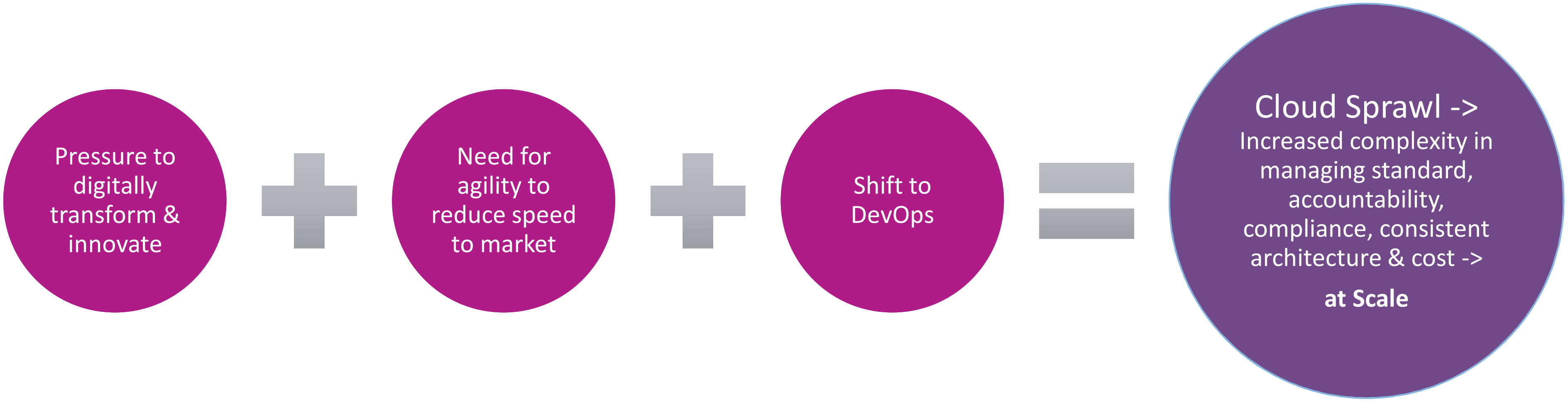
Today’s Agenda

- Governance Overview
- Azure Enterprise Scaffold

This is Cloud Governance baby, yeah!

… but it’s

Why Do We Need Governance?



Pressure to digitally transform & innovate

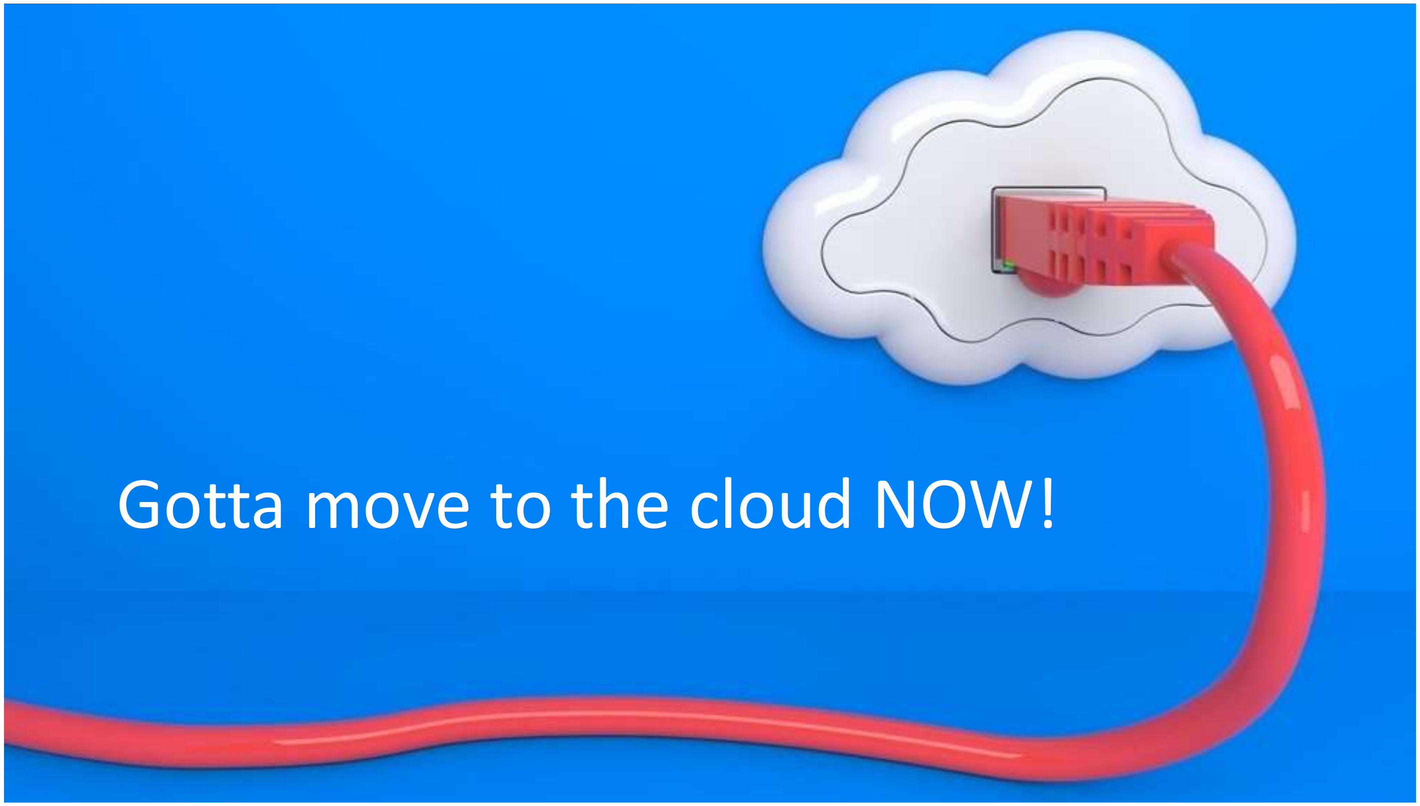
Need for agility to reduce speed to market

Shift to DevOps

Cloud Sprawl ->
Increased complexity in managing standard, accountability, compliance, consistent architecture & cost ->

at Scale

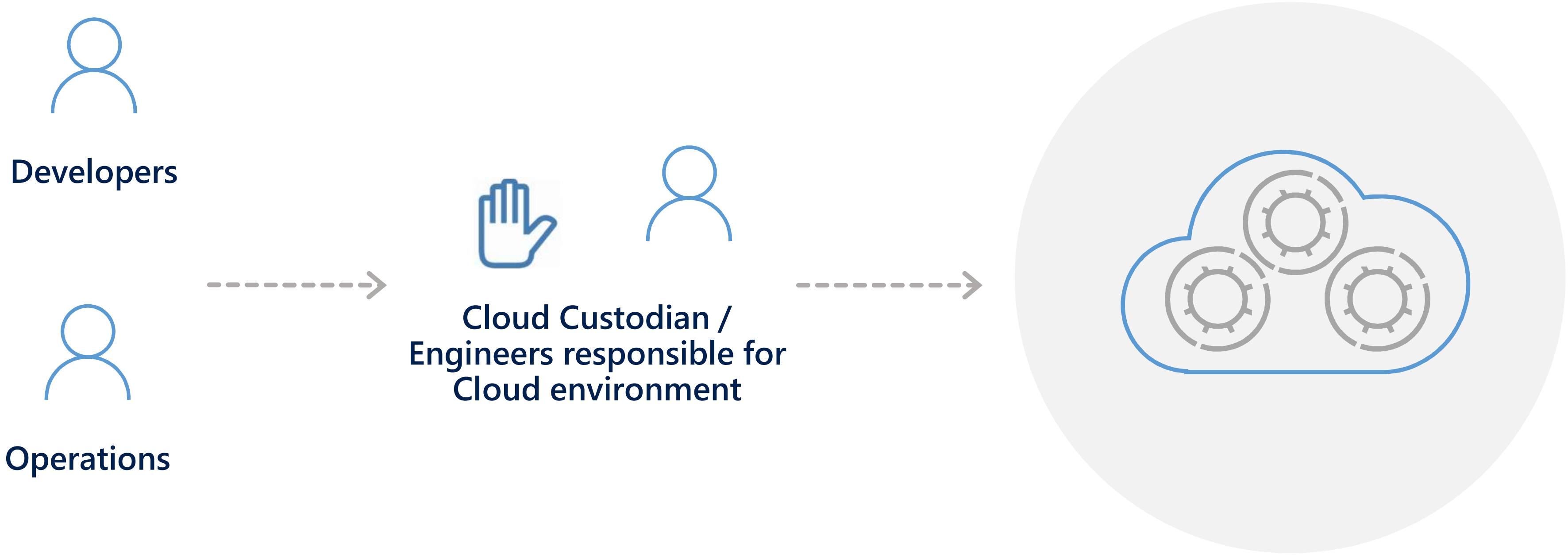
Traditional Approach



Gotta move to the cloud NOW!

Traditional Approach

Sacrifice Speed for Control



Developers

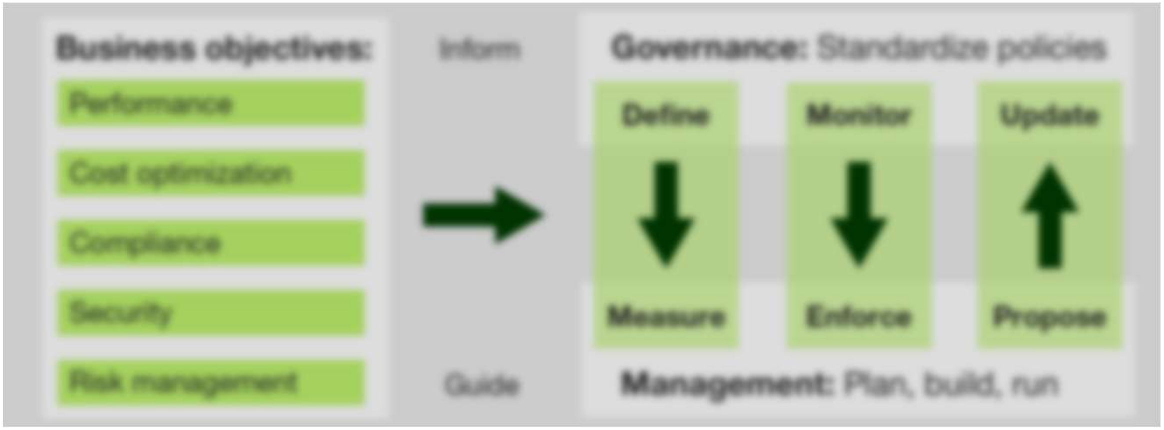
Operations

Cloud Custodian / Engineers responsible for Cloud environment

What about Cloud Agility?

The Current Trend

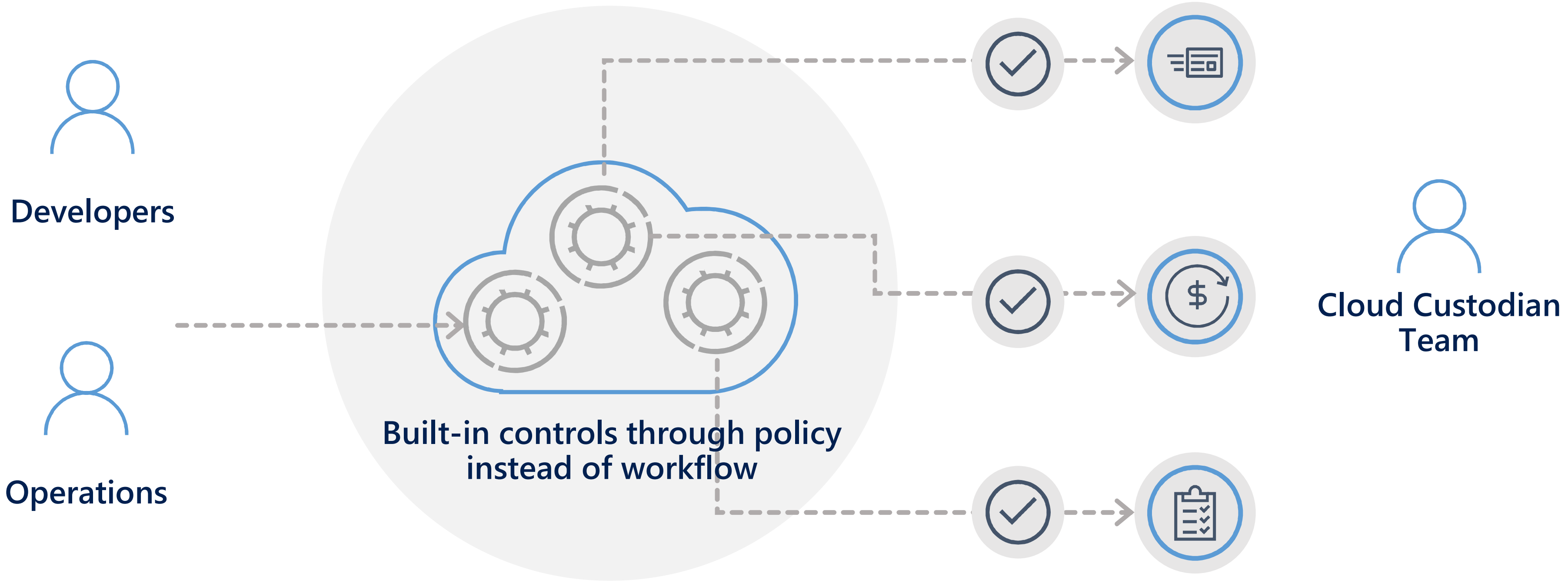
- Step 1) Cloud governance



- Step 2) Migrate workloads

Cloud-Native Governance

Speed AND Control



Developers

Operations

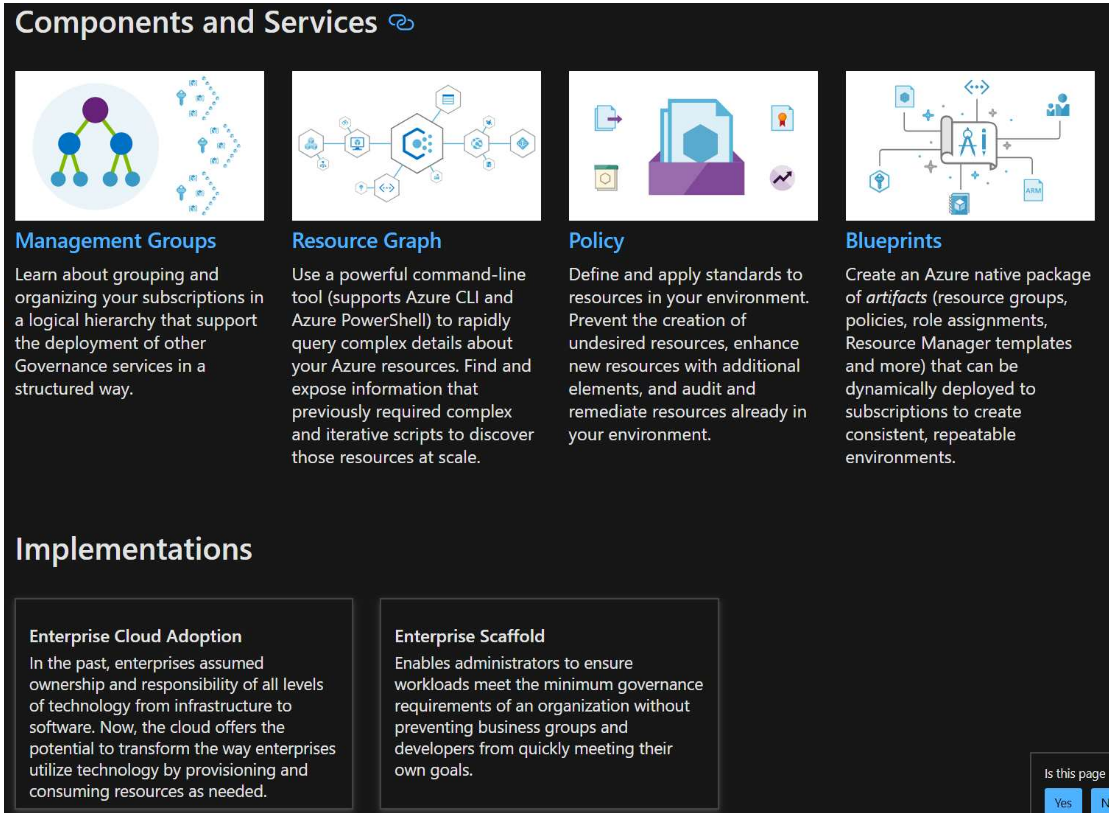
Built-in controls through policy instead of workflow

Cloud Custodian Team

Enterprise Governance in Azure

- RTFM: https://docs.microsoft.com/azure/governance

Enterprise Governance in Azure



Components and Services

Management Groups

Learn about grouping and organizing your subscriptions in a logical hierarchy that support the deployment of other Governance services in a structured way.

Resource Graph

Use a powerful command-line tool (supports Azure CLI and Azure PowerShell) to rapidly query complex details about your Azure resources. Find and expose information that previously required complex and iterative scripts to discover those resources at scale.

Policy

Define and apply standards to resources in your environment. Prevent the creation of undesired resources, enhance new resources with additional elements, and audit and remediate resources already in your environment.

Blueprints

Create an Azure native package of *artifacts* (resource groups, policies, role assignments, Resource Manager templates and more) that can be dynamically deployed to subscriptions to create consistent, repeatable environments.

Implementations

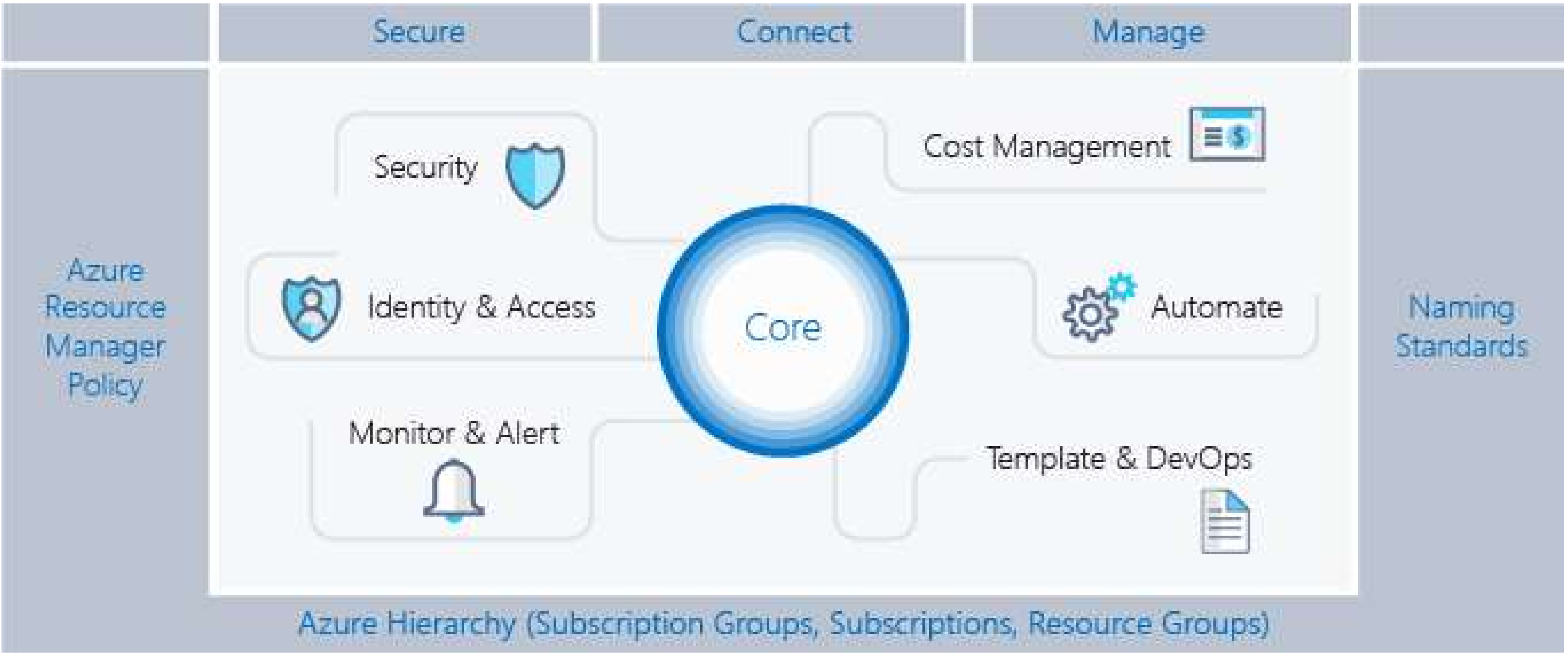
Enterprise Cloud Adoption

In the past, enterprises assumed ownership and responsibility of all levels of technology from infrastructure to software. Now, the cloud offers the potential to transform the way enterprises utilize technology by provisioning and consuming resources as needed.

Enterprise Scaffold

Enables administrators to ensure workloads meet the minimum governance requirements of an organization without preventing business groups and developers from quickly meeting their own goals.

Azure Enterprise Scaffold



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

Azure Enterprise Scaffold: Topics

- Hierarchy
- Naming Standards
- Policies
- IAM
- Security

- Monitoring & Alerting
- Cost Management

& DevOps

rk

All at the speed of cloud!

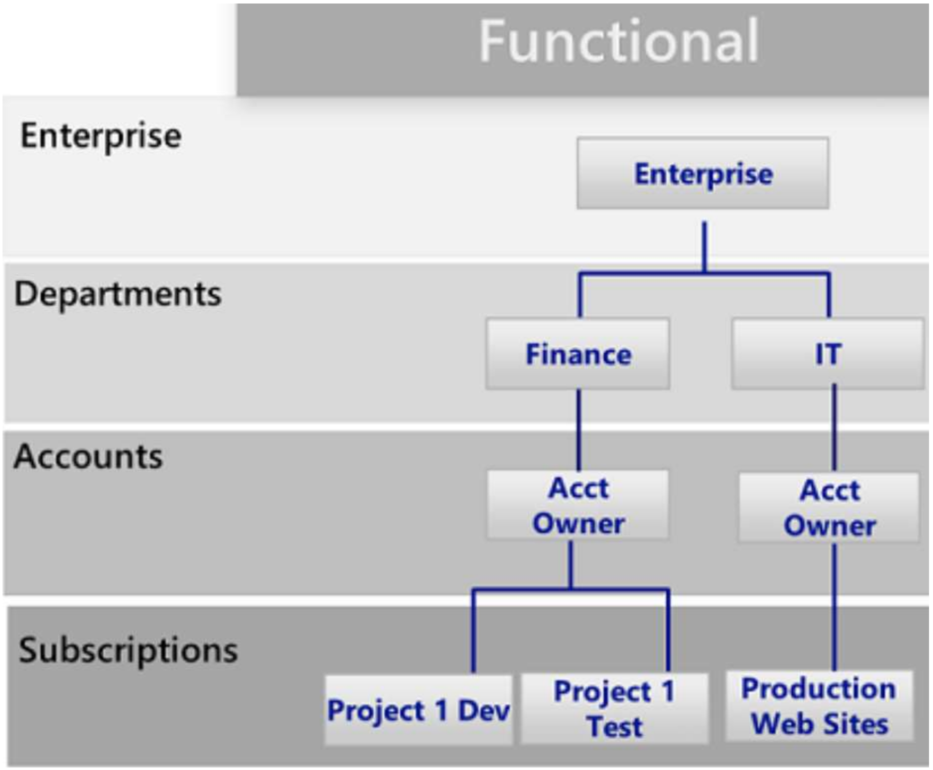
Hierarchy

Insight Presentation

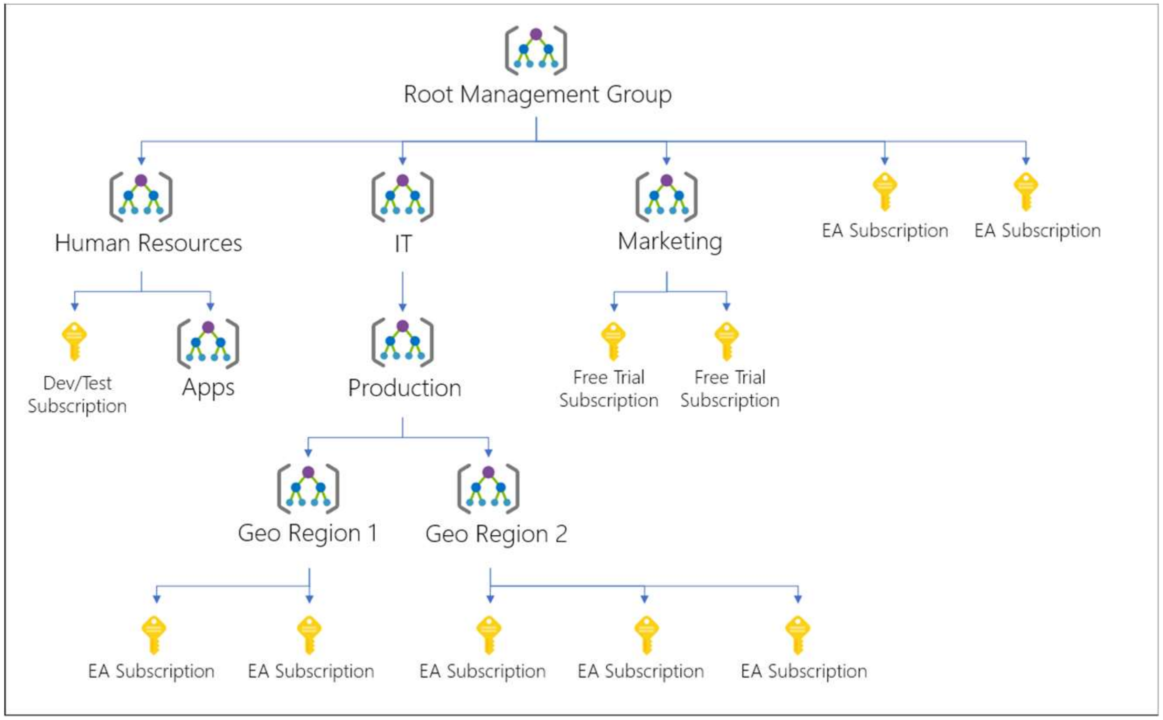
So many Azure subscriptions!

- How do you handle subscription sprawl?

Azure Enterprise Agreement Hierarchy

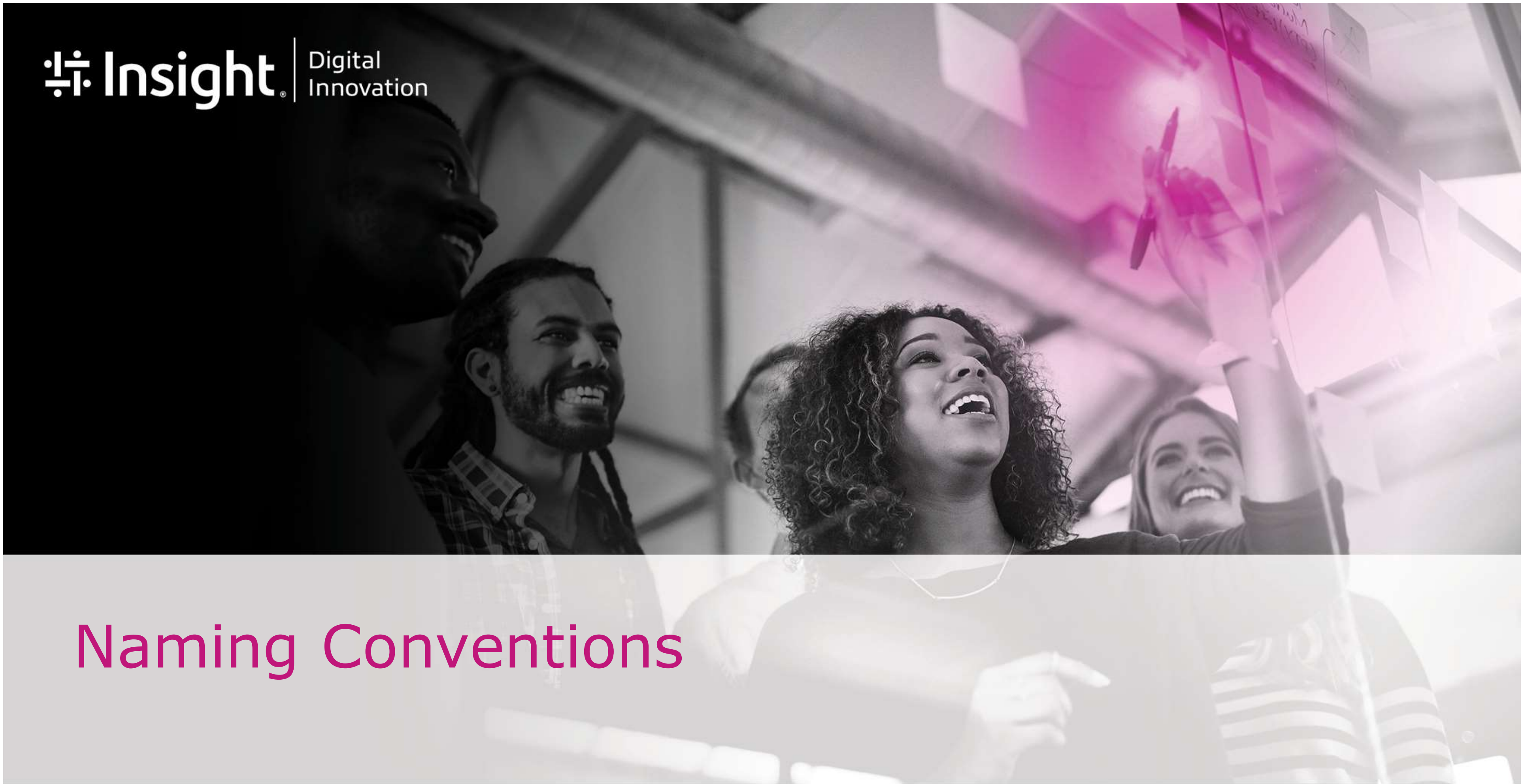


Azure Management Groups



Manage:

- Access Control
- Policies & Initiatives
- Activity Log
- Cost Management
- Blueprints



Naming Conventions

Insight Presentation

Naming Conventions

- Components of names
  - Environment (dev, test, prod)
  - Region
  - Application
  - Resource type
- Specific naming for certain resources
  - Resource Groups
  - Storage Accounts
- Generic formula for everything else

Subscription / Environment	Application / Platform	VNet ID	Region	Description	Sequence Number (opt)	Hyphen	Resource Type
np	ap	01	wu	webex	01	-	agw

Naming Conventions: Examples

	Description	Resource Name
Specific Rules	Resource Group	p1-pai-usw-web-rg
	VNet	management-dev-vnet
	Storage Account	P1ep01uswappstfabc123
	Virtual Machine	pgnsqlp001a
Generic Rule	Load balancer	p1pa01uswweb-lb
	Network Security Group	mduswapp-nsg
	SQL Server Availability Set	p1pluswsql-as
	Network Interface Card for Web Server	p4epuswweb01-nic

** And don’t forget about tagging resources!

Insight Digital Innovation

Policies and Initiatives

Insight Presentation

Azure Policy

- Turn on built-in policies or build custom ones for all resource types
- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation
- VM In-Guest Policy

Enforcement & Compliance

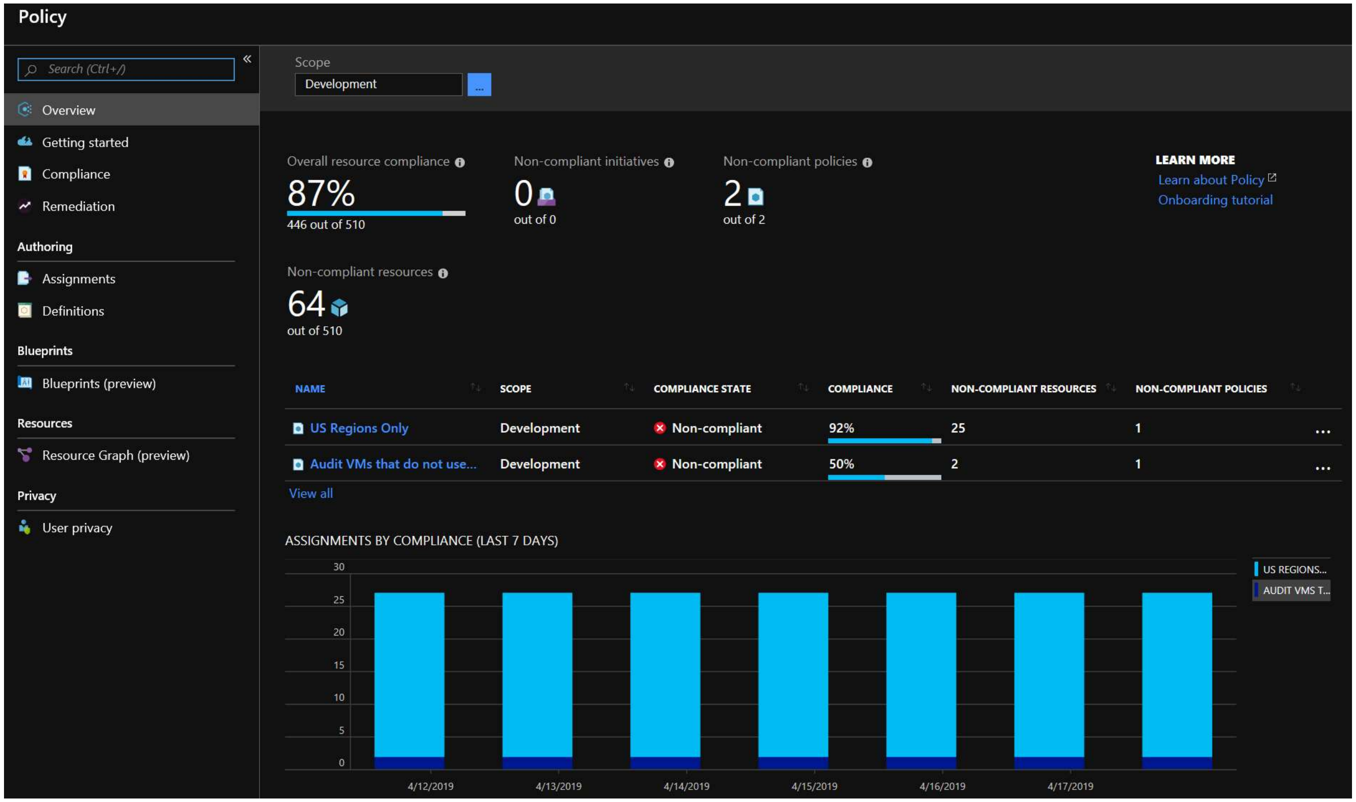
- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

Apply policies at scale

- Real time remediation
- Remediation on existing resources

Remediation

Policy Overview



Scope: Development

Overall resource compliance: 87% — 446 out of 510

Non-compliant initiatives: 0 — out of 0

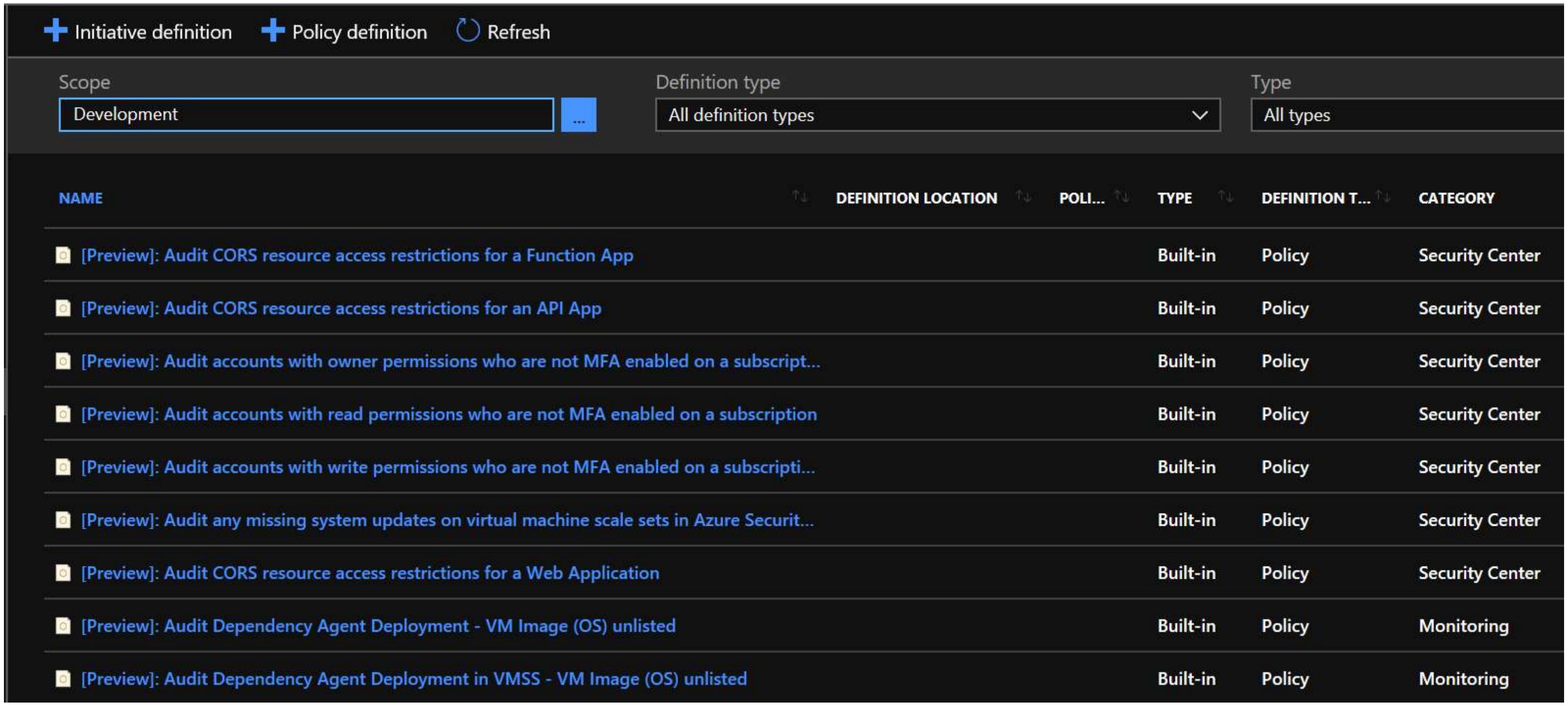
Non-compliant policies: 2 — out of 2

Non-compliant resources: 64 — out of 510

NAME	SCOPE	COMPLIANCE STATE	COMPLIANCE	NON-COMPLIANT RESOURCES	NON-COMPLIANT POLICIES
US Regions Only	Development	Non-compliant	92%	25	1
Audit VMs that do not use...	Development	Non-compliant	50%	2	1

ASSIGNMENTS BY COMPLIANCE (LAST 7 DAYS)

Policy Definitions



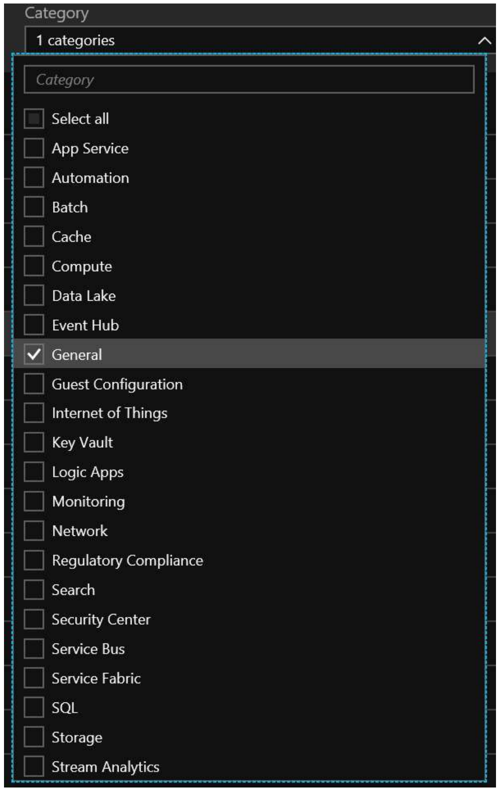
Scope: Development

Definition type: All definition types

Type: All types

NAME	DEFINITION LOCATION	POLI...	TYPE	DEFINITION T...	CATEGORY
[Preview]: Audit CORS resource access restrictions for a Function App			Built-in	Policy	Security Center
[Preview]: Audit CORS resource access restrictions for an API App			Built-in	Policy	Security Center
[Preview]: Audit accounts with owner permissions who are not MFA enabled on a subscript...			Built-in	Policy	Security Center
[Preview]: Audit accounts with read permissions who are not MFA enabled on a subscription			Built-in	Policy	Security Center
[Preview]: Audit accounts with write permissions who are not MFA enabled on a subscripti...			Built-in	Policy	Security Center
[Preview]: Audit any missing system updates on virtual machine scale sets in Azure Securit...			Built-in	Policy	Security Center
[Preview]: Audit CORS resource access restrictions for a Web Application			Built-in	Policy	Security Center
[Preview]: Audit Dependency Agent Deployment - VM Image (OS) unlisted			Built-in	Policy	Monitoring
[Preview]: Audit Dependency Agent Deployment in VMSS - VM Image (OS) unlisted			Built-in	Policy	Monitoring

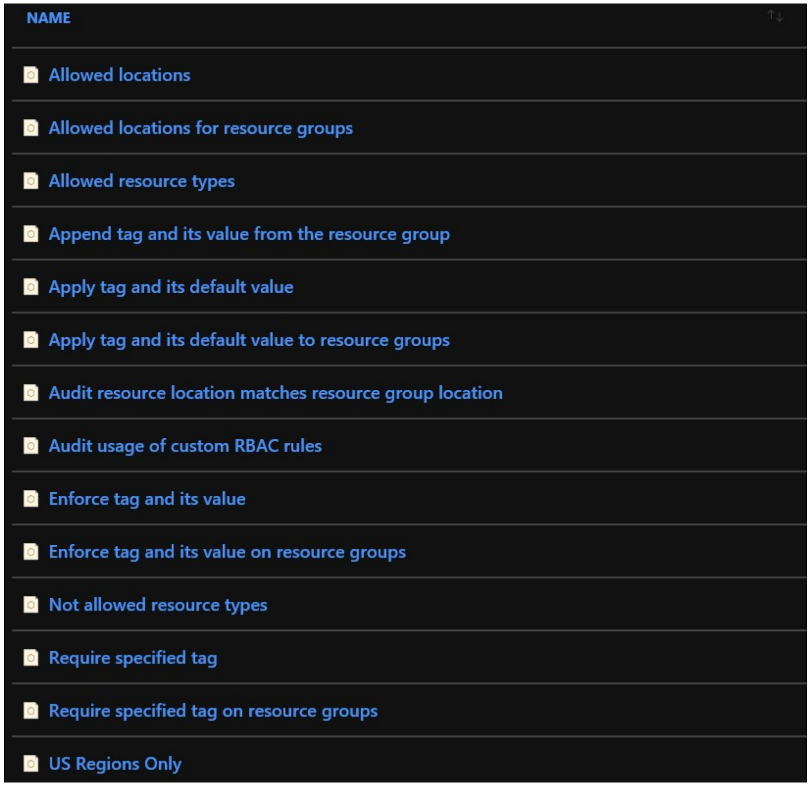
Policy Categories



Category

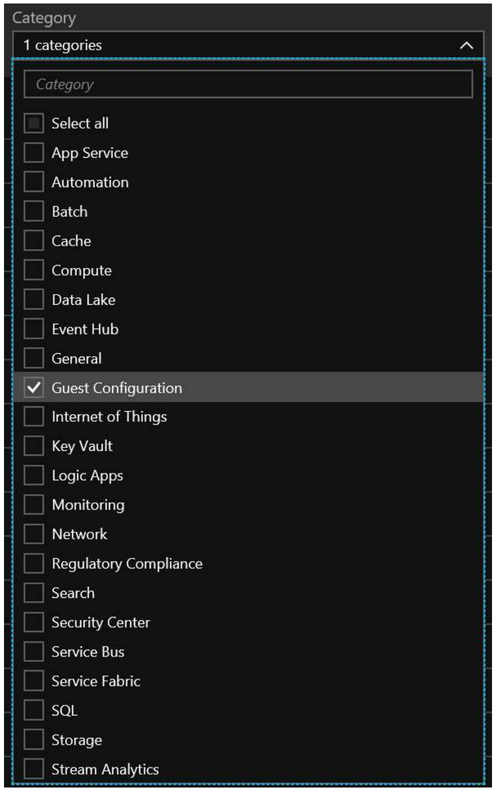
1 categories

- □ Select all
- □ App Service
- □ Automation
- □ Batch
- □ Cache
- □ Compute
- □ Data Lake
- □ Event Hub
- ☑ General
- □ Guest Configuration
- □ Internet of Things
- □ Key Vault
- □ Logic Apps
- □ Monitoring
- □ Network
- □ Regulatory Compliance
- □ Search
- □ Security Center
- □ Service Bus
- □ Service Fabric
- □ SQL
- □ Storage
- □ Stream Analytics



NAME
Allowed locations
Allowed locations for resource groups
Allowed resource types
Append tag and its value from the resource group
Apply tag and its default value
Apply tag and its default value to resource groups
Audit resource location matches resource group location
Audit usage of custom RBAC rules
Enforce tag and its value
Enforce tag and its value on resource groups
Not allowed resource types
Require specified tag
Require specified tag on resource groups
US Regions Only

Policy Categories

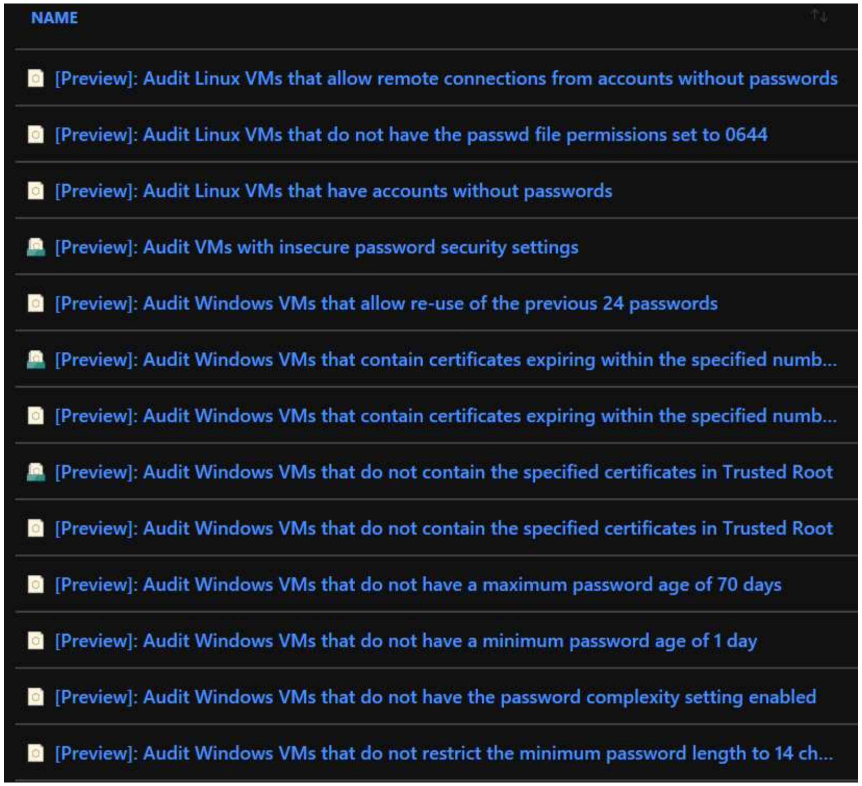


Category

1 categories

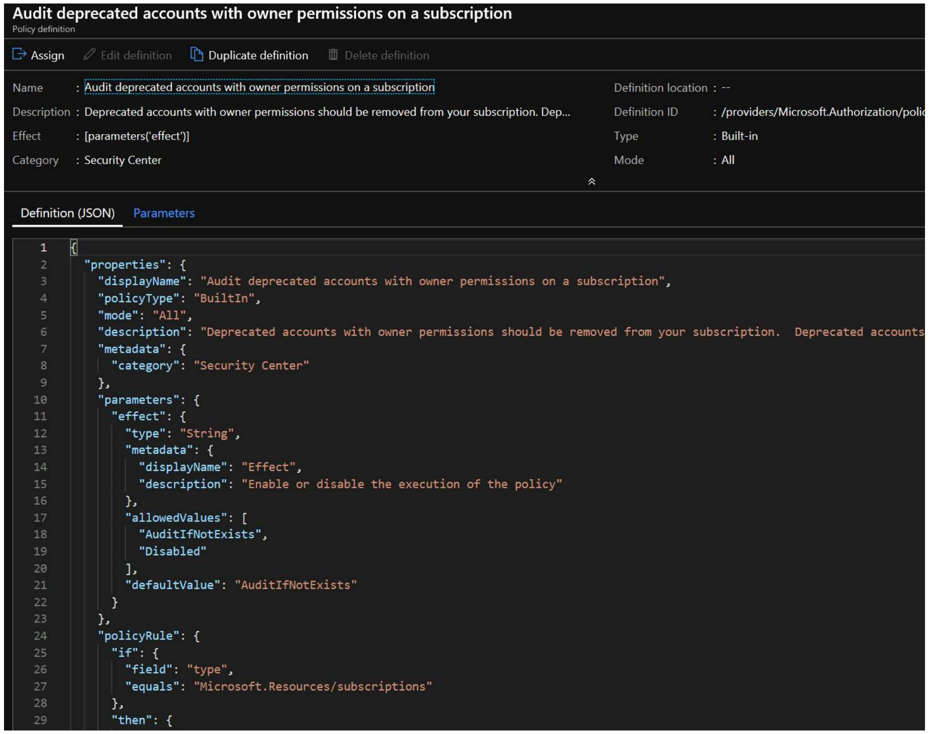
Category

- ■ Select all
- ☐ App Service
- ☐ Automation
- ☐ Batch
- ☐ Cache
- ☐ Compute
- ☐ Data Lake
- ☐ Event Hub
- ☐ General
- ☑ Guest Configuration
- ☐ Internet of Things
- ☐ Key Vault
- ☐ Logic Apps
- ☐ Monitoring
- ☐ Network
- ☐ Regulatory Compliance
- ☐ Search
- ☐ Security Center
- ☐ Service Bus
- ☐ Service Fabric
- ☐ SQL
- ☐ Storage
- ☐ Stream Analytics



NAME
[Preview]: Audit Linux VMs that allow remote connections from accounts without passwords
[Preview]: Audit Linux VMs that do not have the passwd file permissions set to 0644
[Preview]: Audit Linux VMs that have accounts without passwords
[Preview]: Audit VMs with insecure password security settings
[Preview]: Audit Windows VMs that allow re-use of the previous 24 passwords
[Preview]: Audit Windows VMs that contain certificates expiring within the specified numb...
[Preview]: Audit Windows VMs that contain certificates expiring within the specified numb...
[Preview]: Audit Windows VMs that do not contain the specified certificates in Trusted Root
[Preview]: Audit Windows VMs that do not contain the specified certificates in Trusted Root
[Preview]: Audit Windows VMs that do not have a maximum password age of 70 days
[Preview]: Audit Windows VMs that do not have a minimum password age of 1 day
[Preview]: Audit Windows VMs that do not have the password complexity setting enabled
[Preview]: Audit Windows VMs that do not restrict the minimum password length to 14 ch...

Policy Definition



Audit deprecated accounts with owner permissions on a subscription

Policy definition

Name : Audit deprecated accounts with owner permissions on a subscription

Description : Deprecated accounts with owner permissions should be removed from your subscription. Dep...

Effect : [parameters('effect')]

Category : Security Center

Definition location : --

Definition ID : /providers/Microsoft.Authorization/polic

Type : Built-in

Mode : All

```
{
  "properties": {
    "displayName": "Audit deprecated accounts with owner permissions on a subscription",
    "policyType": "BuiltIn",
    "mode": "All",
    "description": "Deprecated accounts with owner permissions should be removed from your subscription.  Deprecated accounts
    "metadata": {
      "category": "Security Center"
    },
    "parameters": {
      "effect": {
        "type": "String",
        "metadata": {
          "displayName": "Effect",
          "description": "Enable or disable the execution of the policy"
        },
        "allowedValues": [
          "AuditIfNotExists",
          "Disabled"
        ],
        "defaultValue": "AuditIfNotExists"
      }
    },
    "policyRule": {
      "if": {
        "field": "type",
        "equals": "Microsoft.Resources/subscriptions"
      },
      "then": {
```

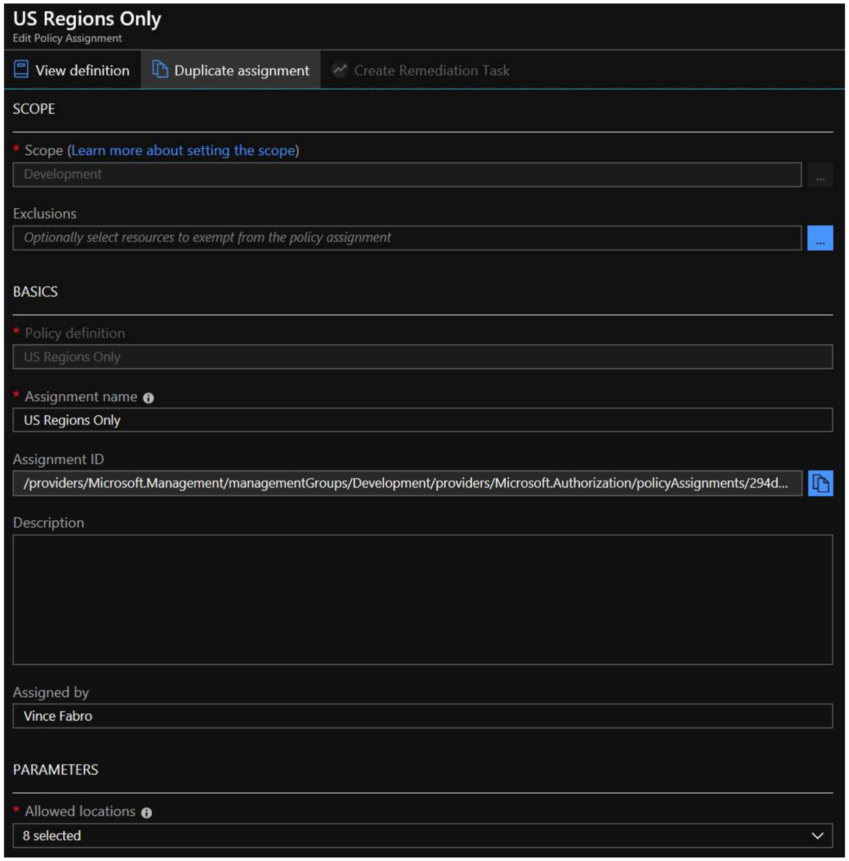
Effects

- deny
- audit
- append
- auditIfNotExists
- deployIfNotExists
- disabled

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

Policy Assignment

- Assign scope
  - Management Group ★
  - Subscription
  - Resource Group
- Specify parameters



US Regions Only
Edit Policy Assignment

SCOPE

* Scope (Learn more about setting the scope)
Development

Exclusions
Optionally select resources to exempt from the policy assignment

BASICS

* Policy definition
US Regions Only

* Assignment name
US Regions Only

Assignment ID
/providers/Microsoft.Management/managementGroups/Development/providers/Microsoft.Authorization/policyAssignments/294d...

Description

Assigned by
Vince Fabro

PARAMETERS

* Allowed locations
8 selected

Initiatives

- A group of policies to assign in bulk
- Definition includes
  - Policies
  - Parameters
  - Optional parameter assignments
- Assignment works same as w/policies

92 of the top 100 Azure Customers use policy

ASOS

“..we’re now confident that all of our IaaS is hardened to our very own standards”
“..continuously helping us to reduce our attack surface in our DevTest environments”

Ian Margetts, Platform Lead (ALM)
Leslie Lintott, Lead Platform Engineer

BP

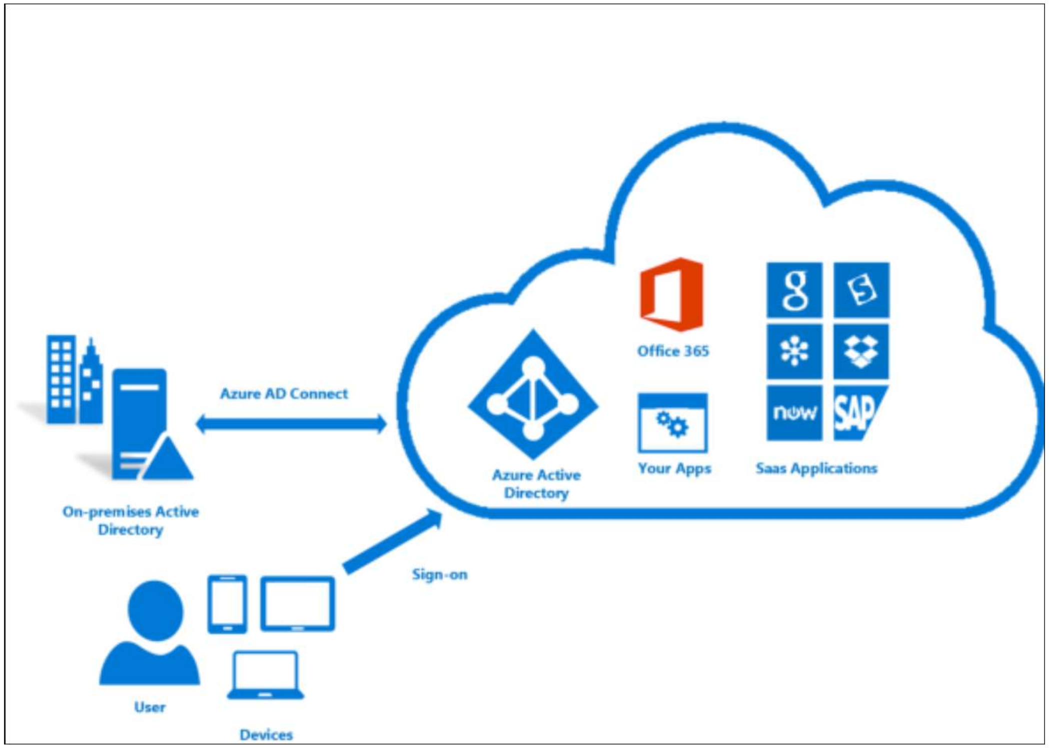
“..allowed BP to obtain a better security, compliance and audit profile”
“..found policies to be a game changer simply because they provide control in areas which protect compute, network, storage and various other Azure services″

John Maio, Chief Architect

Identity & Access Management

Insight Presentation

Identity and Access Management



Recommendations

- Always use MFA!!
- Consider using AD PIM and Conditional Access
- Don’t use classic Administrator/Co-Administrator
- Use management groups to scope RBAC
- Use AD groups instead of individual users
- Follow the principle of least privilege

Security

Insight Presentation

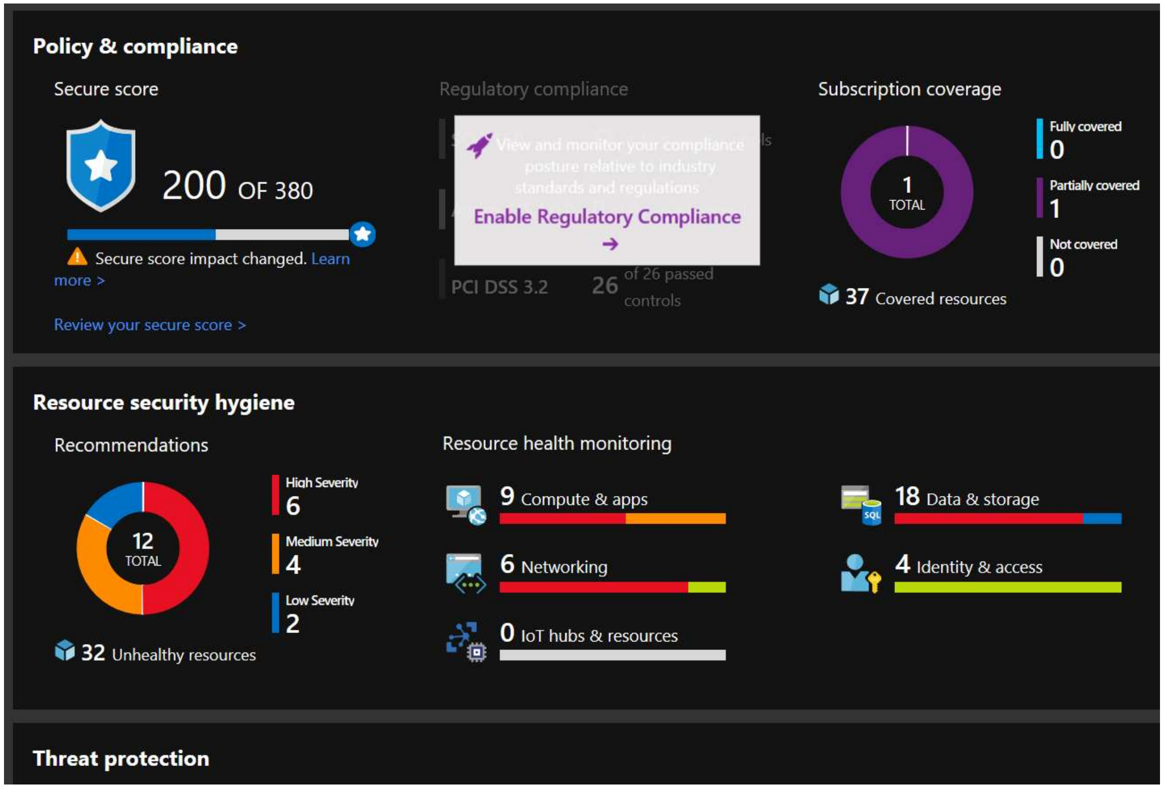
Security

- Security is really, really important in the cloud

Architect for Security!

** Networking section coming later

Azure Security Center



Policy & compliance

Secure score

200 OF 380

Secure score impact changed. Learn more >

Review your secure score >

Regulatory compliance

View and monitor your compliance posture relative to industry standards and regulations

Enable Regulatory Compliance →

PCI DSS 3.2 26 of 26 passed controls

Subscription coverage

1 TOTAL

Fully covered 0

Partially covered 1

Not covered 0

37 Covered resources

Resource security hygiene

Recommendations

12 TOTAL

High Severity 6

Medium Severity 4

Low Severity 2

32 Unhealthy resources

Resource health monitoring

9 Compute & apps

18 Data & storage

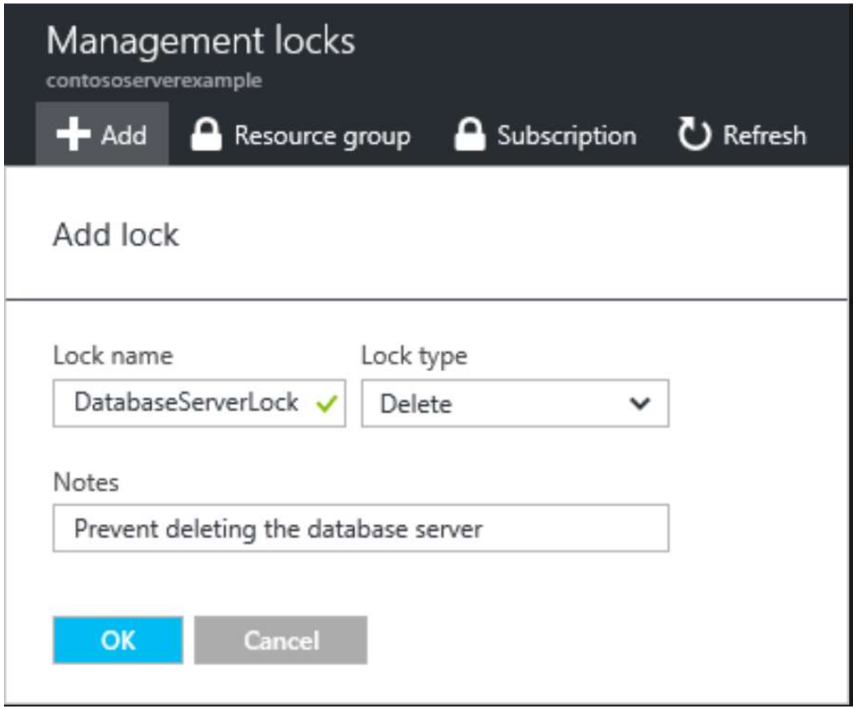
6 Networking

4 Identity & access

0 IoT hubs & resources

Threat protection

Resource Locks


Management locks
contososerverexample

Add lock

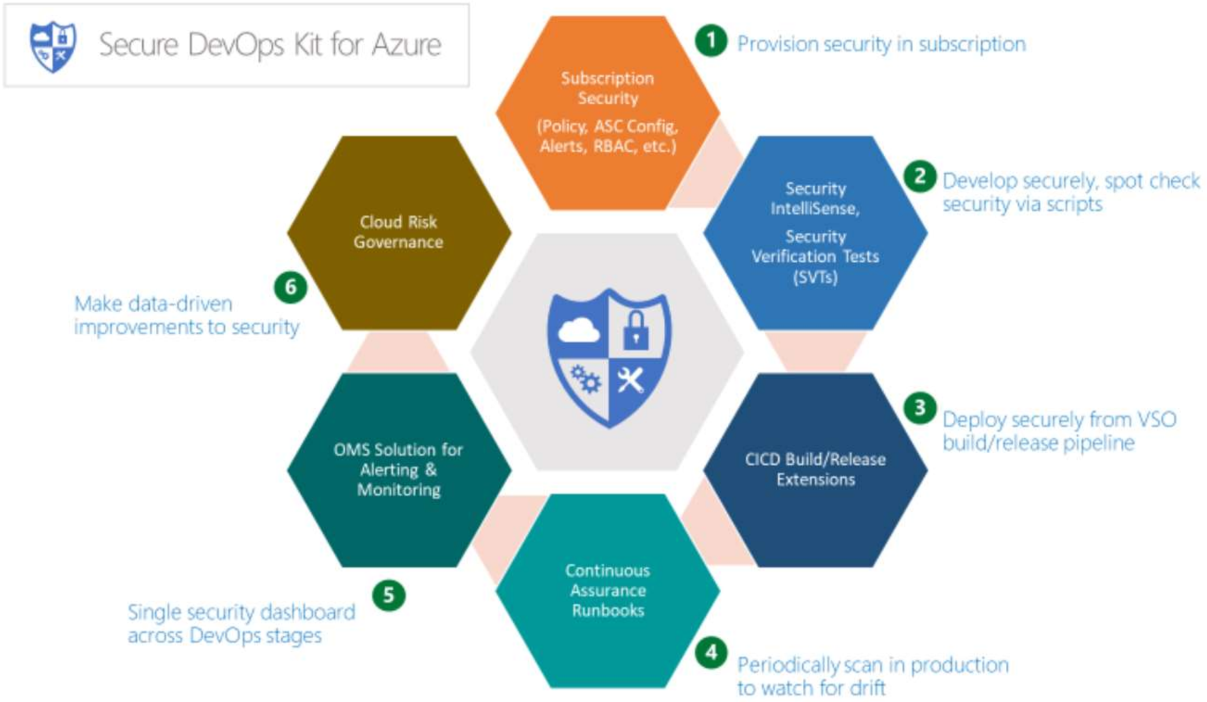
Lock name: DatabaseServerLock ✓

Lock type: Delete

Notes: Prevent deleting the database server

- Read-only
- Delete

Secure DevOps Toolkit


Secure DevOps Kit for Azure
Subscription Security
(Policy, ASC Config, Alerts, RBAC, etc.)
Security IntelliSense,
Security Verification Tests (SVTs)
CICD Build/Release Extensions
Continuous Assurance Runbooks
OMS Solution for Alerting & Monitoring
Cloud Risk Governance
1
2
3
4
5
6

1 Provision security in subscription

2 Develop securely, spot check security via scripts

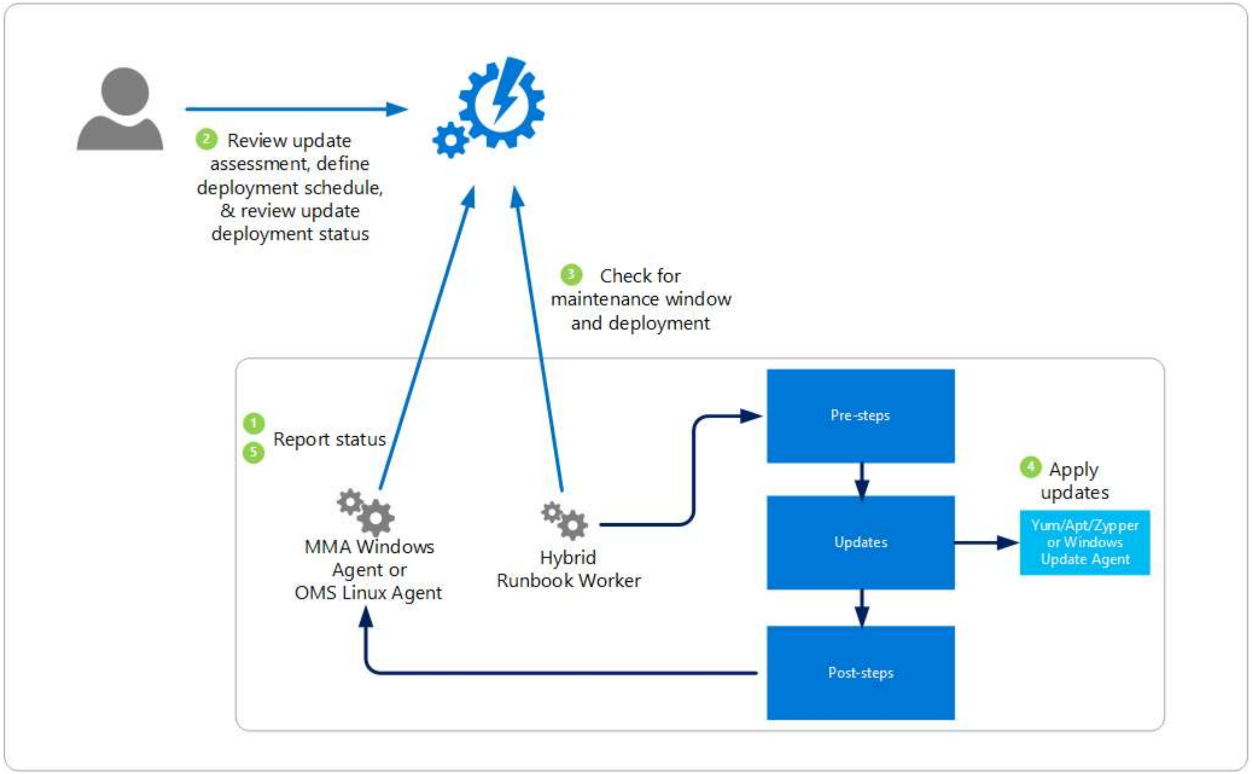
3 Deploy securely from VSO build/release pipeline

4 Periodically scan in production to watch for drift

5 Single security dashboard across DevOps stages

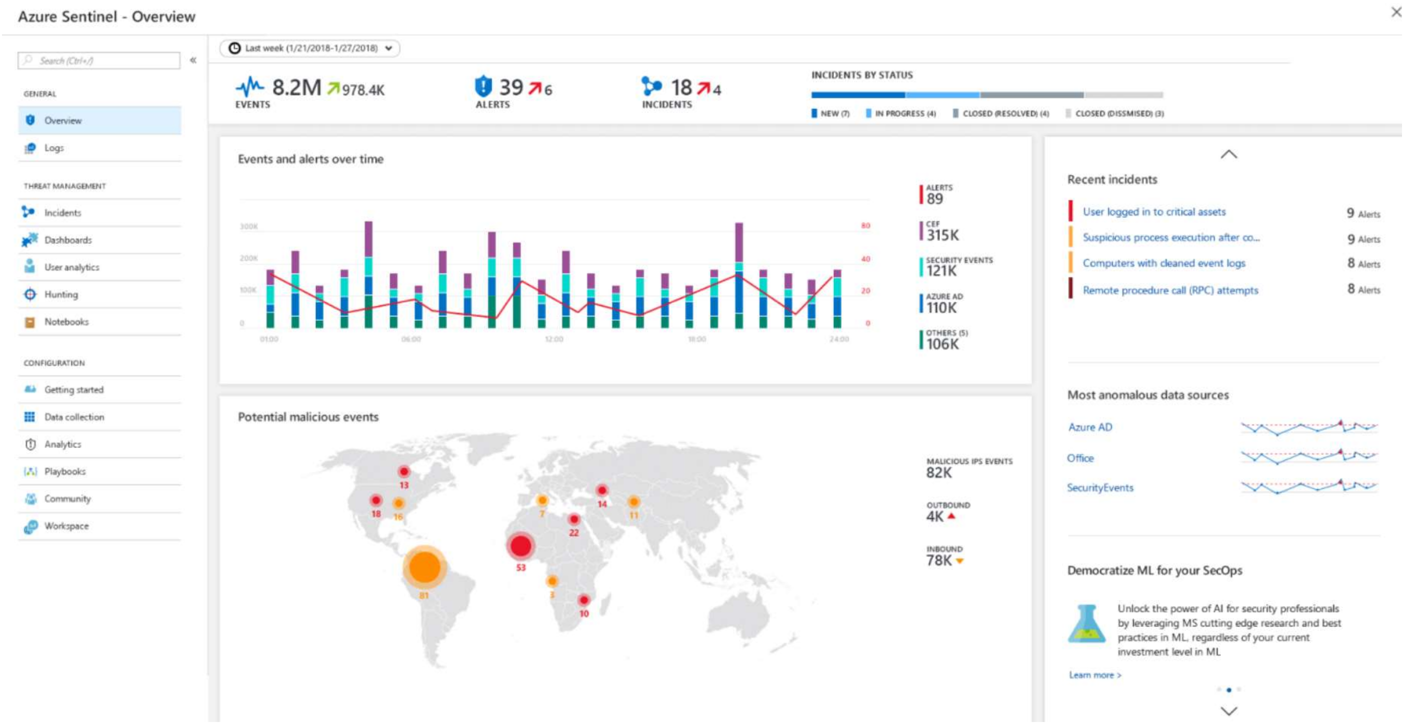
6 Make data-driven improvements to security

Azure Update Management


2 Review update assessment, define deployment schedule, & review update deployment status
3 Check for maintenance window and deployment
1 5 Report status
MMA Windows Agent or OMS Linux Agent
Hybrid Runbook Worker
Pre-steps
Updates
Post-steps
4 Apply updates
Yum/Apt/Zypper or Windows Update Agent

Azure Sentinel (Preview)

Microsoft’s Azure-native SIEM (Security Information and Event Management)



Azure Sentinel - Overview

8.2M ↗978.4K EVENTS

39 ↗6 ALERTS

18 ↗4 INCIDENTS

INCIDENTS BY STATUS

NEW (7) IN PROGRESS (4) CLOSED (RESOLVED) (4) CLOSED (DISMISSED) (3)

Events and alerts over time

ALERTS 89

CEF 315K

SECURITY EVENTS 121K

AZURE AD 110K

OTHERS (5) 106K

Potential malicious events

MALICIOUS IPS EVENTS 82K

OUTBOUND 4K ▲

INBOUND 78K ▼

Recent incidents

User logged in to critical assets	9 Alerts
Suspicious process execution after co...	9 Alerts
Computers with cleaned event logs	8 Alerts
Remote procedure call (RPC) attempts	8 Alerts

Most anomalous data sources

Azure AD

Office

SecurityEvents

Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML

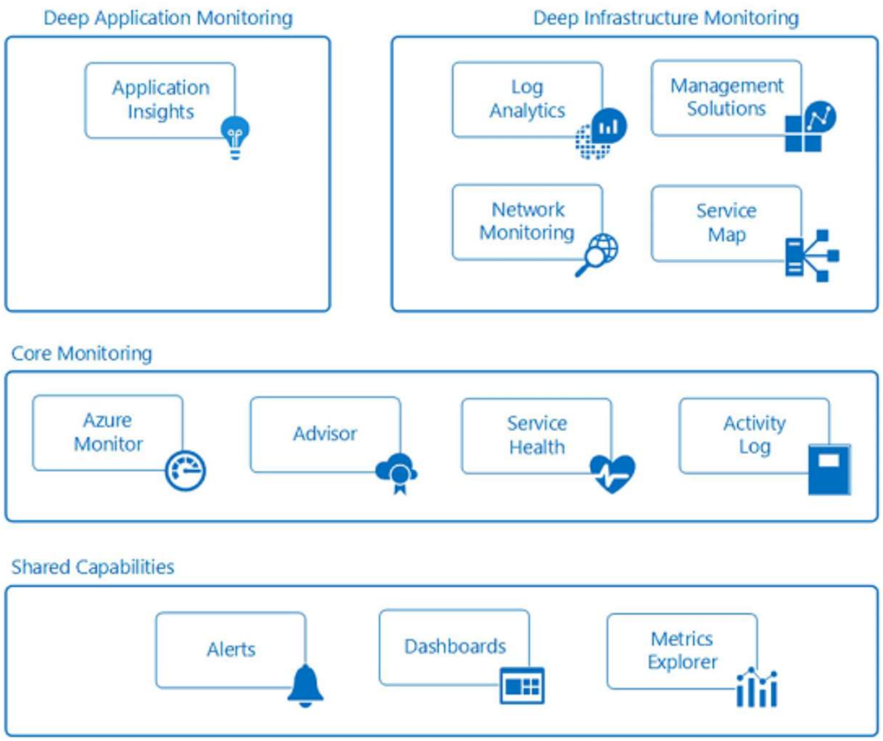
Learn more >

Insight Digital Innovation

Monitoring and Alerting

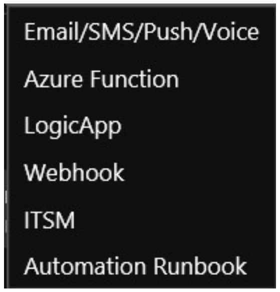
Insight Presentation

Monitoring and Alerting

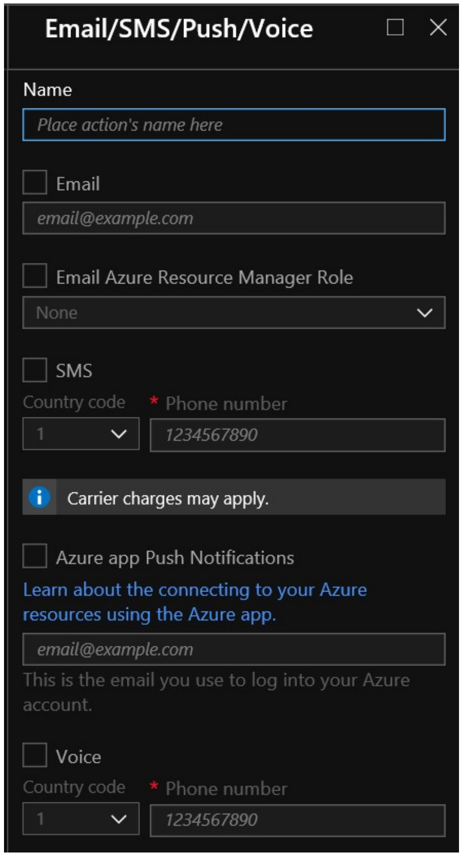


Monitoring and Alerting

Action Groups:



- Email/SMS/Push/Voice
- Azure Function
- LogicApp
- Webhook
- ITSM
- Automation Runbook



Name

Place action's name here

☐ Email

email@example.com

☐ Email Azure Resource Manager Role

None

☐ SMS

Country code: 1 | * Phone number: *1234567890*

Carrier charges may apply.

☐ Azure app Push Notifications

Learn about the connecting to your Azure resources using the Azure app.

email@example.com

This is the email you use to log into your Azure account.

☐ Voice

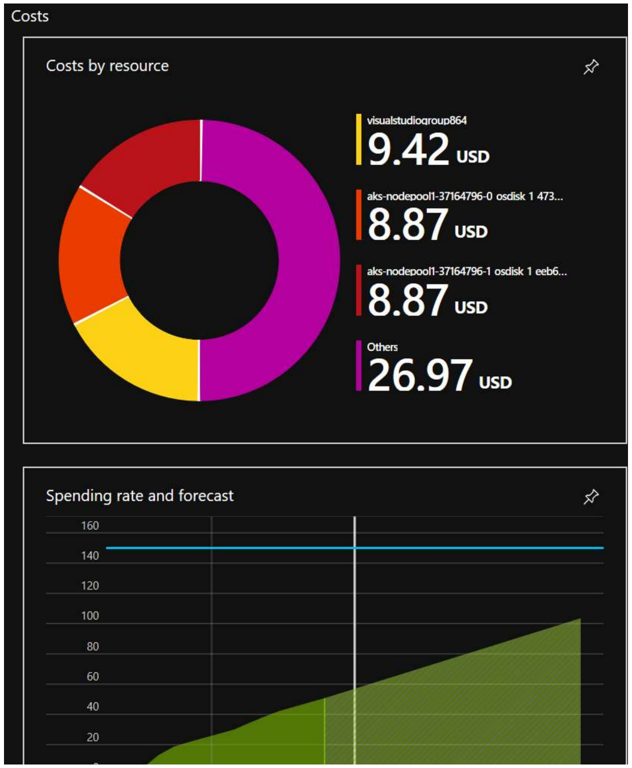
Country code: 1 | * Phone number: *1234567890*

Insight Digital Innovation

Cost Management

Insight Presentation

Cost Management: Subscription



Costs

Costs by resource

visualstudiogroup864
9.42 USD

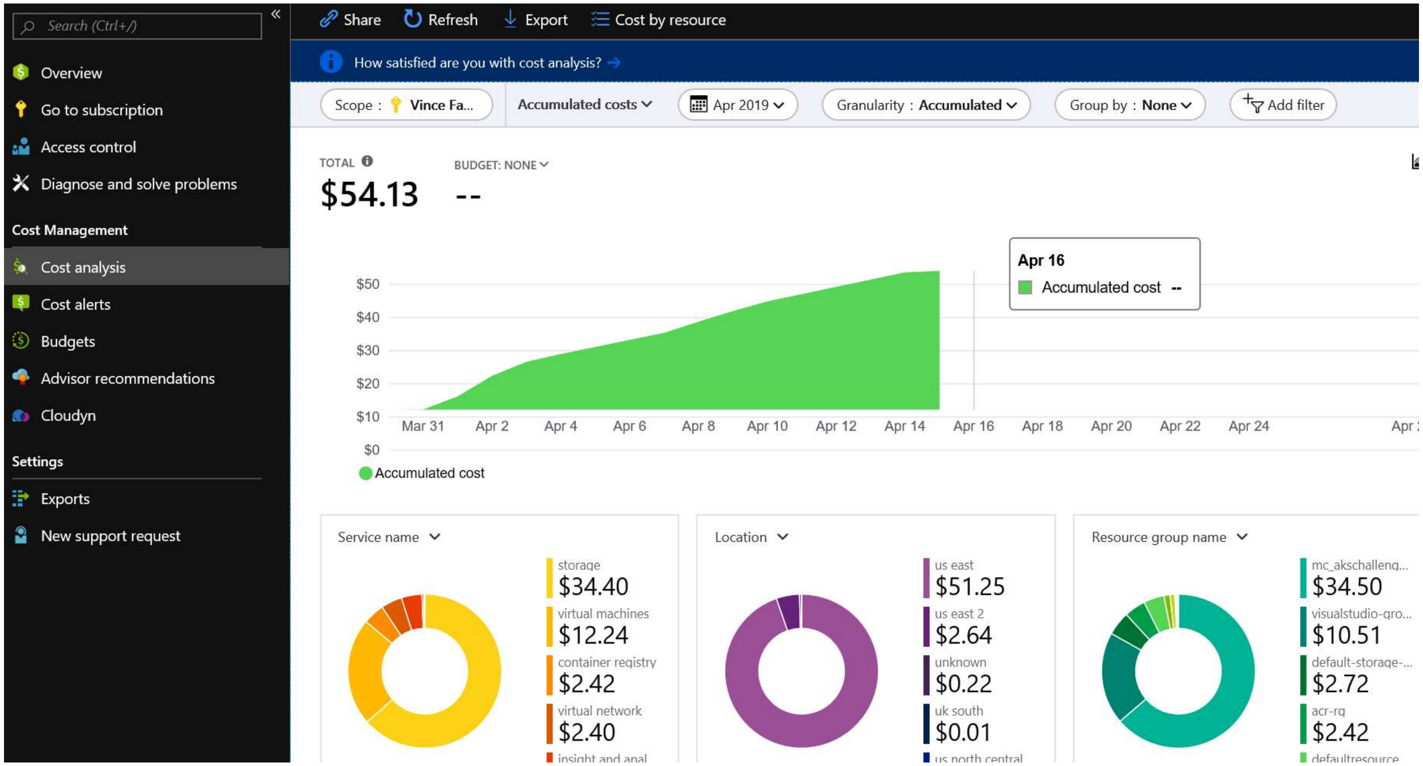
aks-nodepool1-37164796-0 osdisk 1 473...
8.87 USD

aks-nodepool1-37164796-1 osdisk 1 eeb6...
8.87 USD

Others
26.97 USD

Spending rate and forecast

Cost Management: Cost Management



Scope : Vince Fa...

Accumulated costs

Apr 2019

Granularity : Accumulated

Group by : None

TOTAL $54.13

BUDGET: NONE --

Apr 16
🟩 Accumulated cost --

Service name

storage $34.40
virtual machines $12.24
container registry $2.42
virtual network $2.40
insight and anal

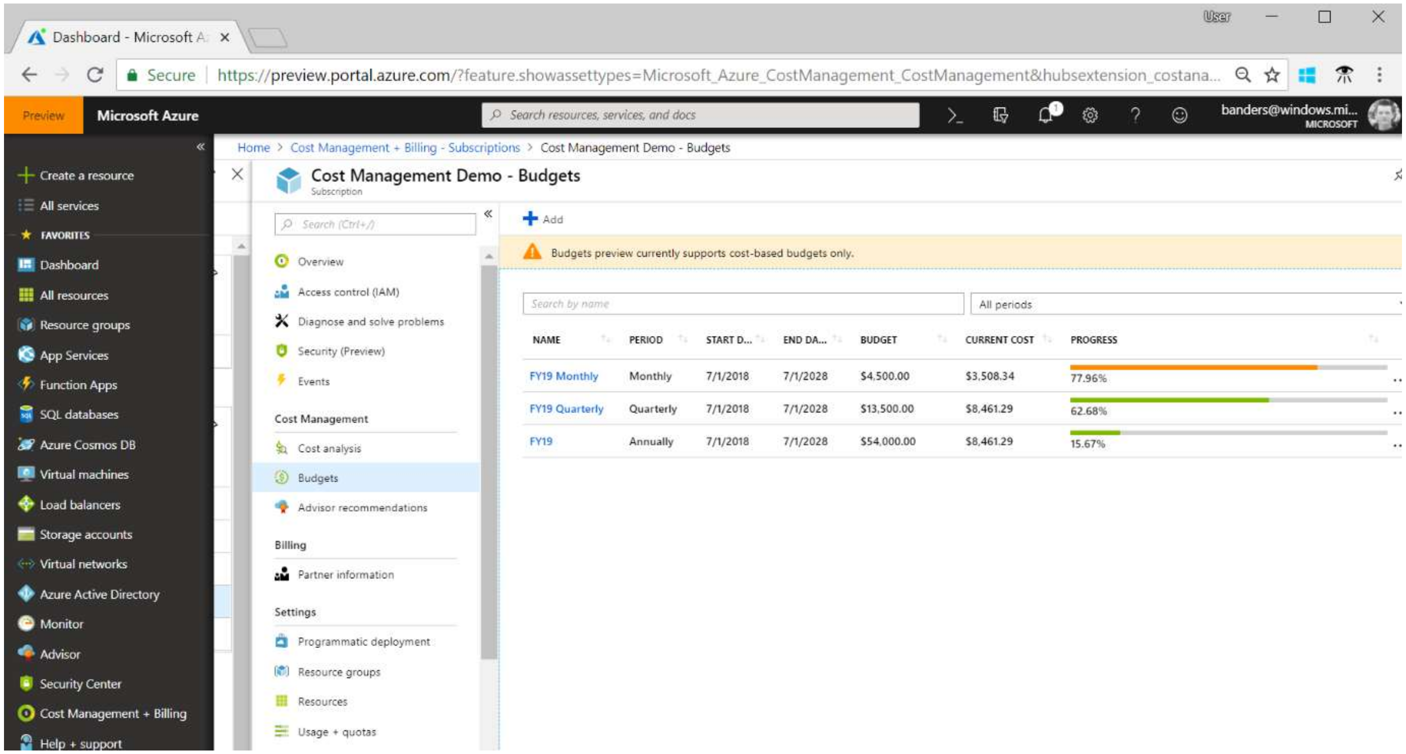
Location

us east $51.25
us east 2 $2.64
unknown $0.22
uk south $0.01
us north central

Resource group name

mc_akschalleng... $34.50
visualstudio-gro... $10.51
default-storage-... $2.72
acr-rg $2.42
defaultresource

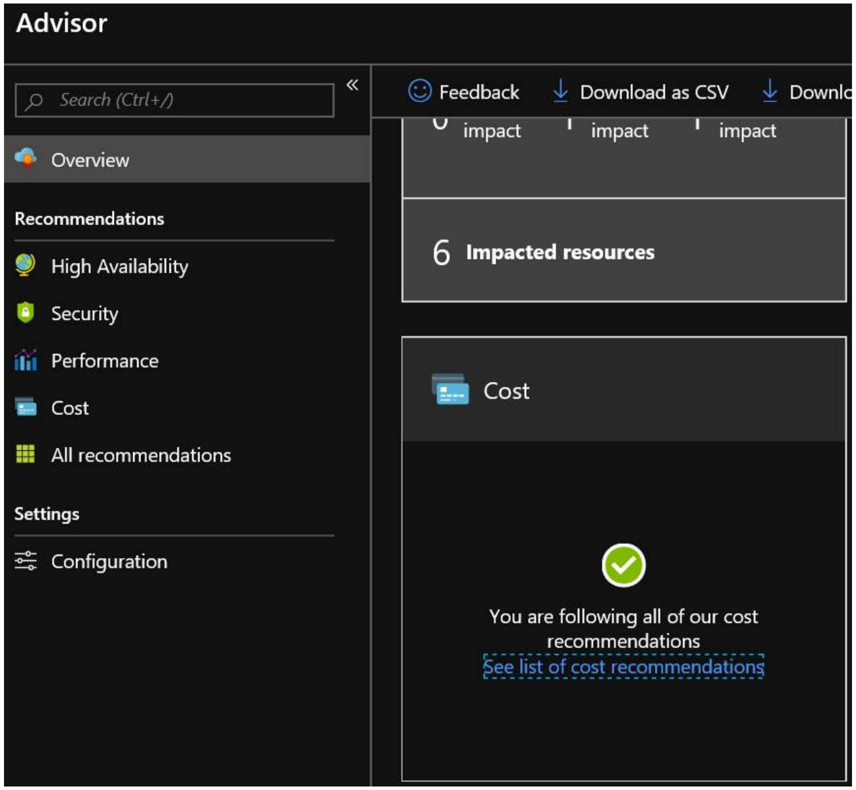
Cost Management: Budgets



Budgets preview currently supports cost-based budgets only.

NAME	PERIOD	START D...	END DA...	BUDGET	CURRENT COST	PROGRESS
FY19 Monthly	Monthly	7/1/2018	7/1/2028	$4,500.00	$3,508.34	77.96%
FY19 Quarterly	Quarterly	7/1/2018	7/1/2028	$13,500.00	$8,461.29	62.68%
FY19	Annually	7/1/2018	7/1/2028	$54,000.00	$8,461.29	15.67%

Cost Management: Advisor



You are following all of our cost recommendations
See list of cost recommendations

Cost recommendations:

- Optimize virtual machine spend by resizing or shutting down underutilized instances
- Reduce costs by eliminating unprovisioned ExpressRoute circuits
- Reduce costs by deleting or reconfiguring idle virtual network gateways
- Buy reserved virtual machine instances to save money over pay-as-you-go costs
- Delete unassociated public IP addresses to save money

Cost Management: Other Tools

- PowerBI Azure Consumption Insights
- Consumption API
- Licensing: AHUB and RIs
- Automation
- Resource tags

Insight | Digital Innovation

Automation

Insight Presentation

What to Automate?

- Tasks that you perform on a regular basis
- Might forget
- Want to avoid mistakes

Automate Using…

- Azure DevOps
- IaC: ARM templates, Terraform, etc.
- Azure Blueprints
- Azure Automation Accounts
- Event Grid, Logic Apps, Functions
- The many Azure SDKs and CLIs
- Cloud Shell

To Accomplish…

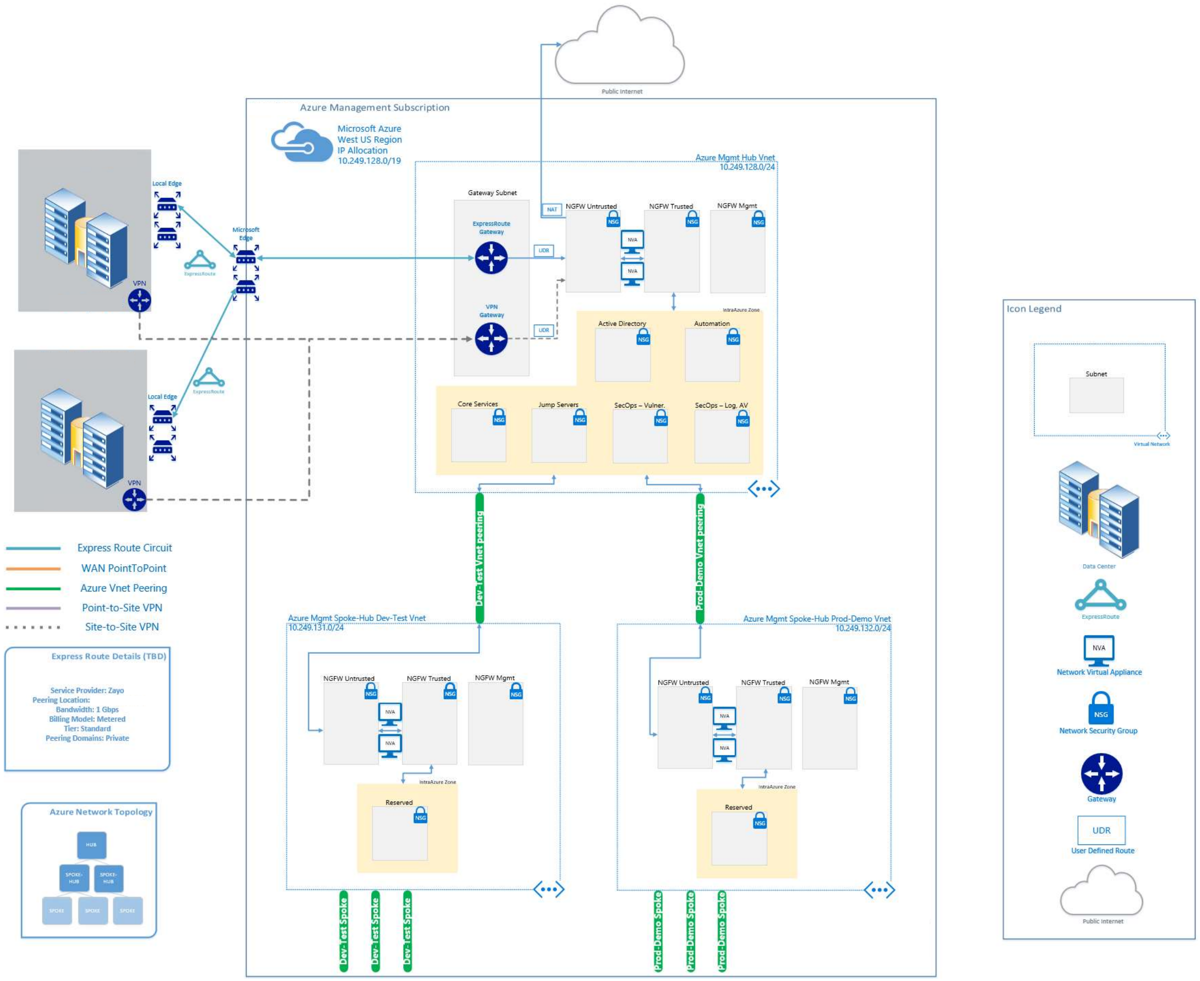
- Control cost
  - Shut down VMs
  - Control cloud sprawl
- Manage deployments/resources
  - Execute IaC deployments
  - Scale up and down
  - Perform backups
  - Execute DR failover

Core Network

Insight Presentation

Core Azure Network Technologies

- Virtual networks (VNets) and subnets
- Azure DNS
- Security groups (NSGs & ASGs)
- User-defined routes (UDRs)
- Virtual network peering
- VPNs (ExpressRoute, Site-to-site VPN)
- Load Balancers, App Gateways
- Azure Firewall, Azure Front Door, Virtual Appliances
- Service endpoints



Express Route Details (TBD)

Service Provider: Zayo
Peering Location:
Bandwidth: 1 Gbps
Billing Model: Metered
Tier: Standard
Peering Domains: Private

Insight | Digital Innovation

Questions? Thank You!

Relevant Links / Labs

- Azure Scaffold
  - https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/appendix/azure-scaffold
- Policies: https://docs.microsoft.com/en-us/azure/governance/policy/
- Secure DevOps Toolkit: https://github.com/azsk/DevOpsKit-docs
- Cost Management: https://docs.microsoft.com/en-us/azure/cost-management/
- Automation: https://docs.microsoft.com/en-us/azure/automation/
- Blueprints: https://docs.microsoft.com/en-us/azure/governance/blueprints/
- Networking: https://docs.microsoft.com/en-us/azure/virtual-network/