Microsoft

Azure

Azure Governance

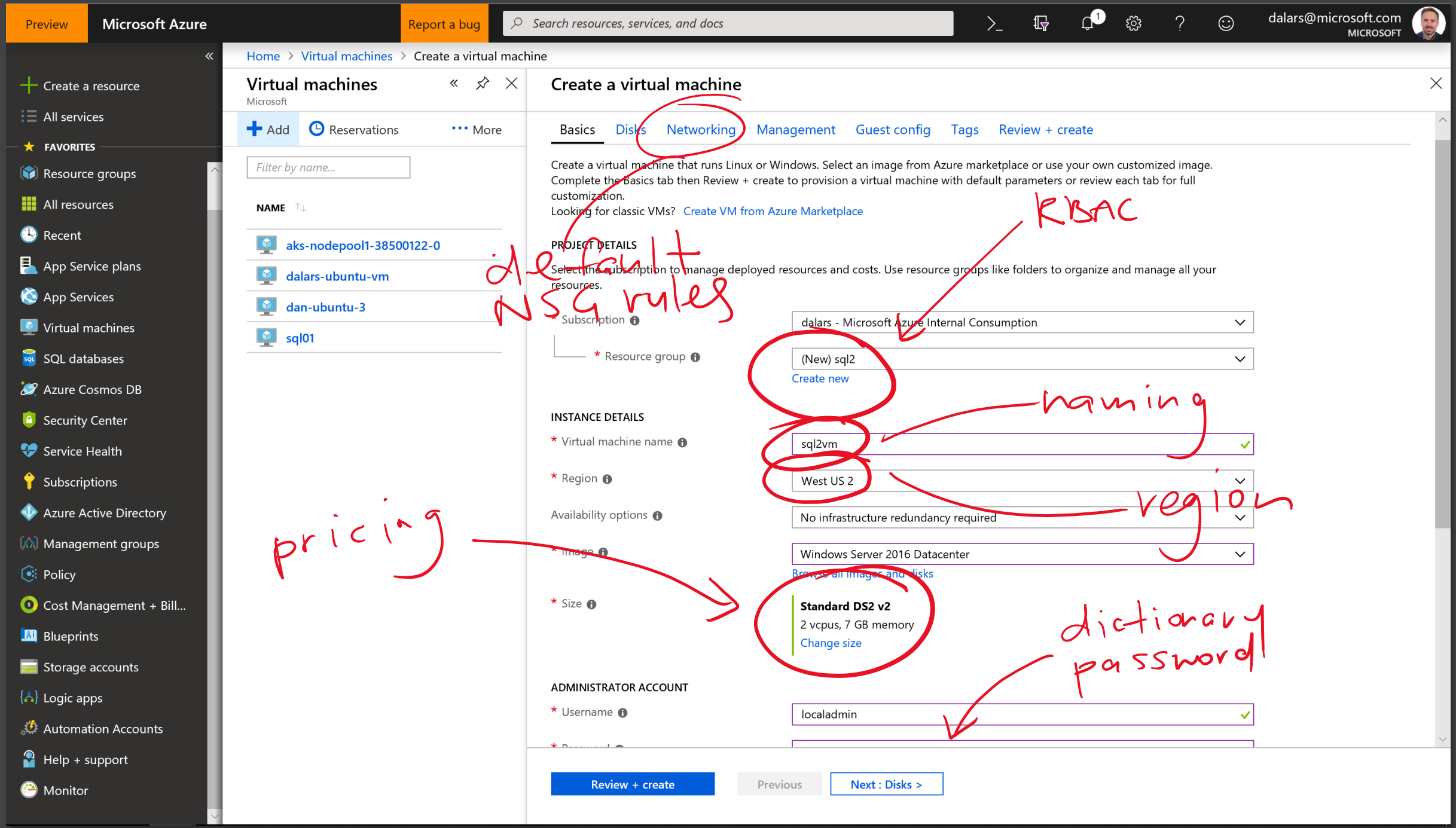
Operating Azure at Scale

Daniel Larsen

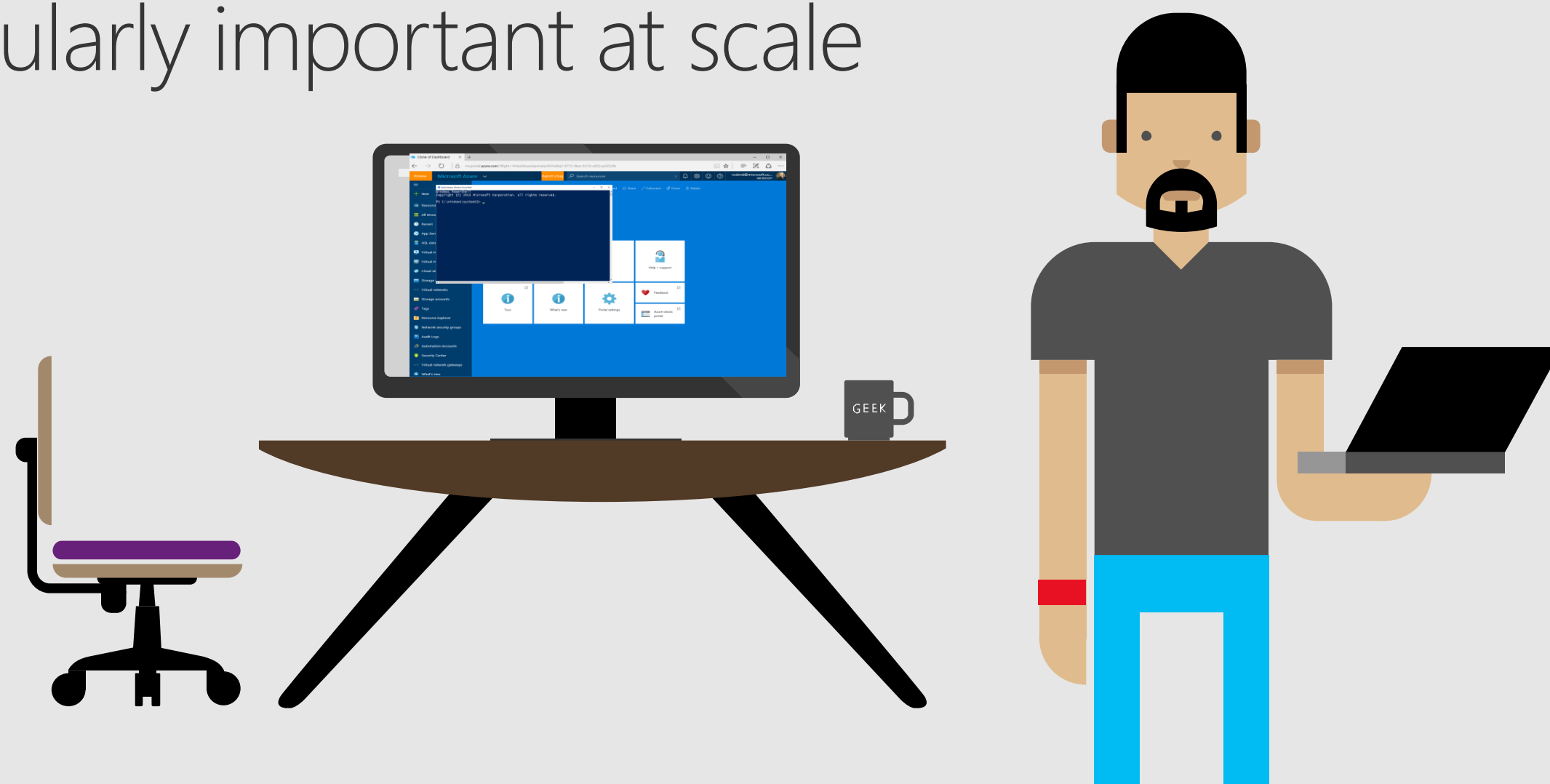
Senior Technical Evangelist

October 2018

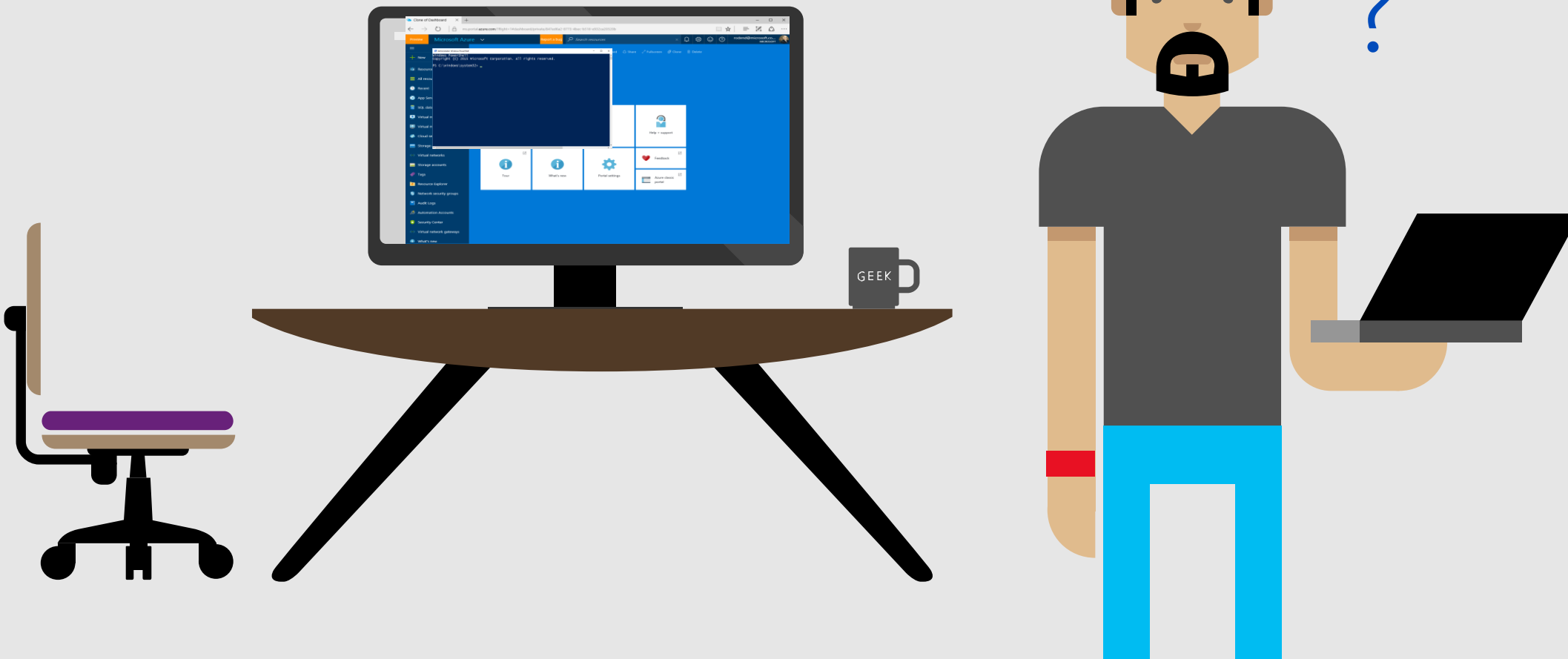
Hello VM


Preview
Microsoft Azure
Report a bug
Search resources, services, and docs
dalars@microsoft.com
MICROSOFT
Create a resource
All services
FAVORITES
Resource groups
All resources
Recent
App Service plans
App Services
Virtual machines
SQL databases
Azure Cosmos DB
Security Center
Service Health
Subscriptions
Azure Active Directory
Management groups
Policy
Cost Management + Bill...
Blueprints
Storage accounts
Logic apps
Automation Accounts
Help + support
Monitor
Home > Virtual machines > Create a virtual machine
Virtual machines
Microsoft
Add
Reservations
More
Filter by name...
NAME
aks-nodepool1-38500122-0
dalars-ubuntu-vm
dan-ubuntu-3
sql01
Create a virtual machine
Basics
Disks
Networking
Management
Guest config
Tags
Review + create
Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.
Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? Create VM from Azure Marketplace
PROJECT DETAILS
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
* Subscription
dalars - Microsoft Azure Internal Consumption
* Resource group
(New) sql2
Create new
INSTANCE DETAILS
* Virtual machine name
sql2vm
* Region
West US 2
Availability options
No infrastructure redundancy required
* Image
Windows Server 2016 Datacenter
Browse all images and disks
* Size
Standard DS2 v2
2 vcpus, 7 GB memory
Change size
ADMINISTRATOR ACCOUNT
* Username
localadmin
Review + create
Previous
Next : Disks >
default
NSG rules
RBAC
naming
region
pricing
dictionary
password

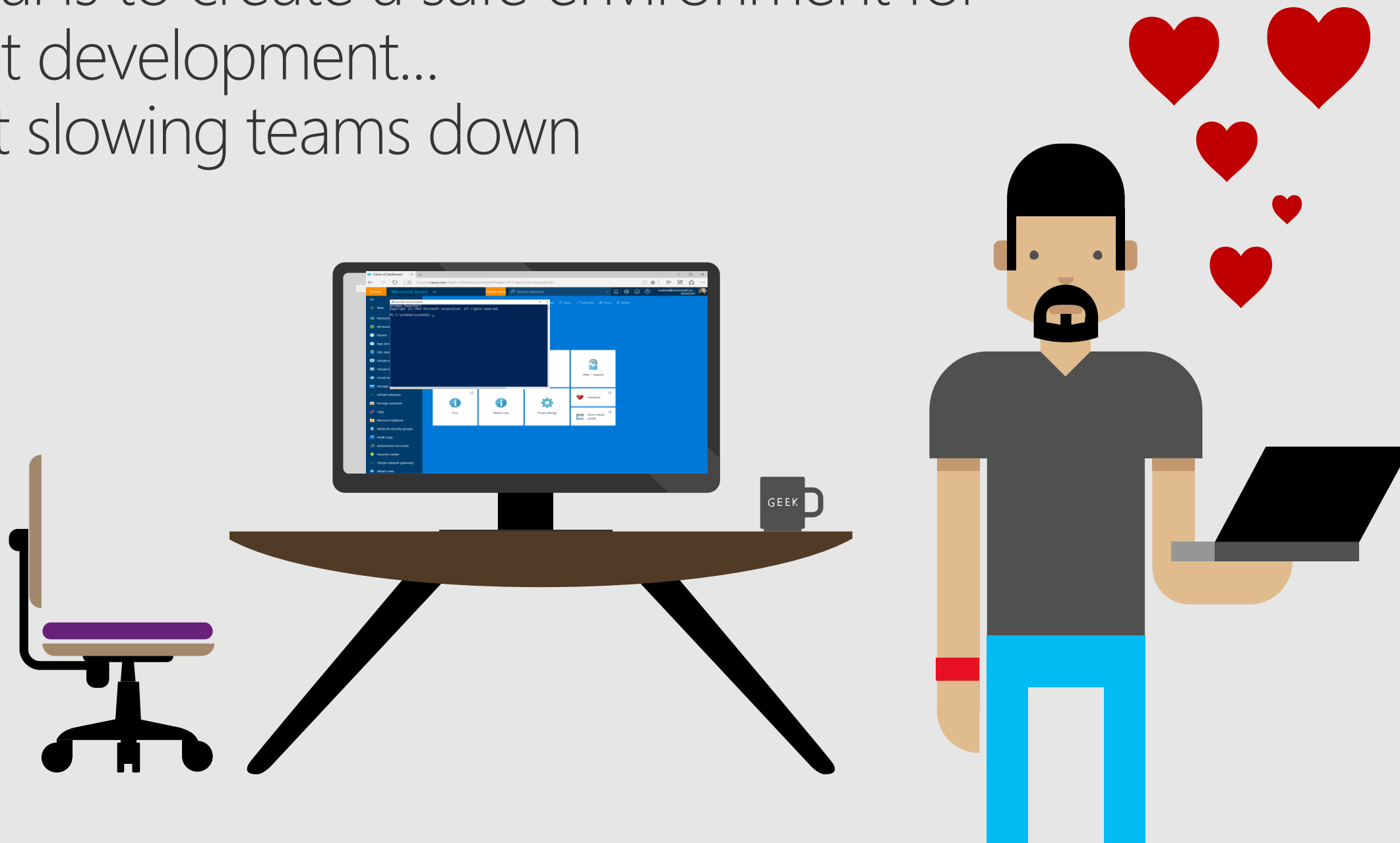
As the cloud becomes more important to the business we need governance. This is particularly important at scale



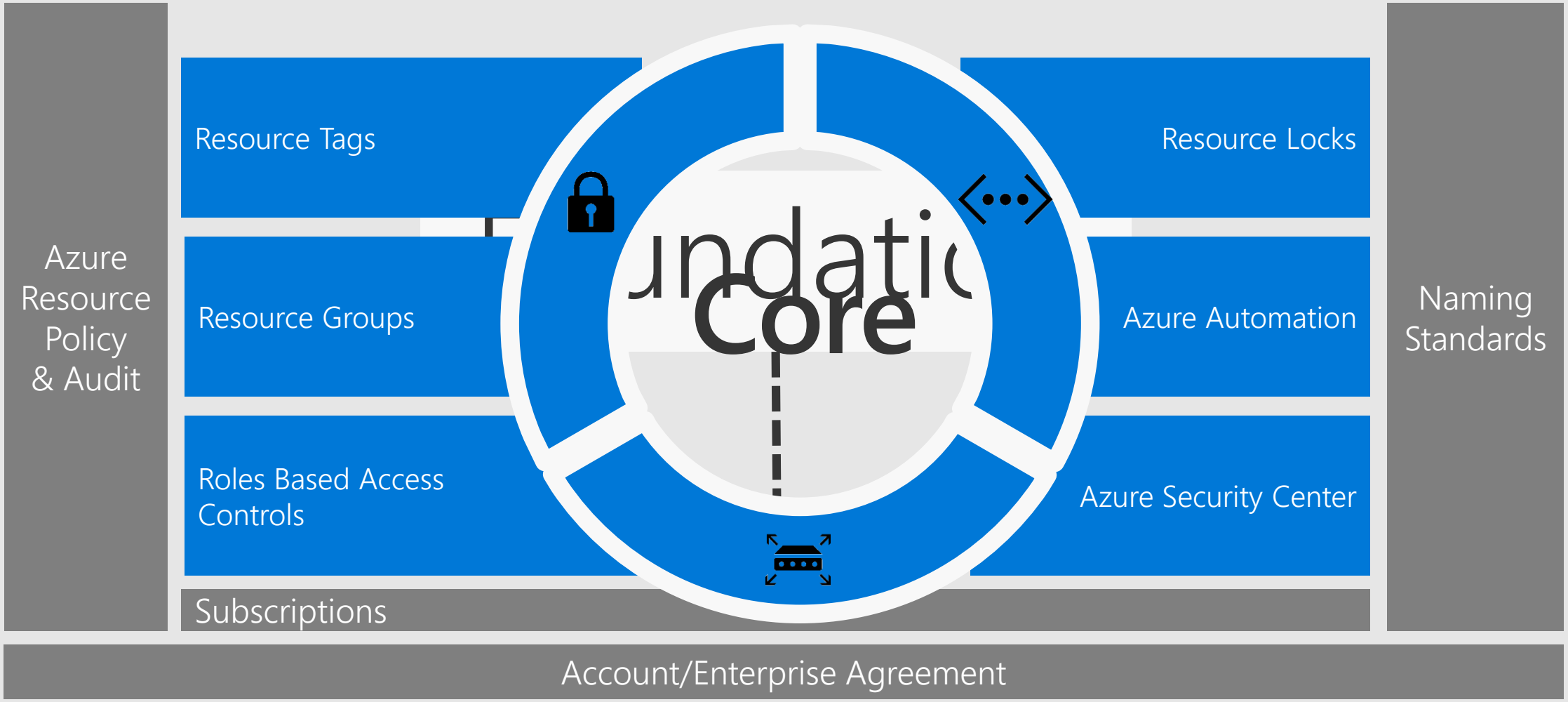
Governance includes policies, compliance, security and cost control.
Azure governance can be codified and automated



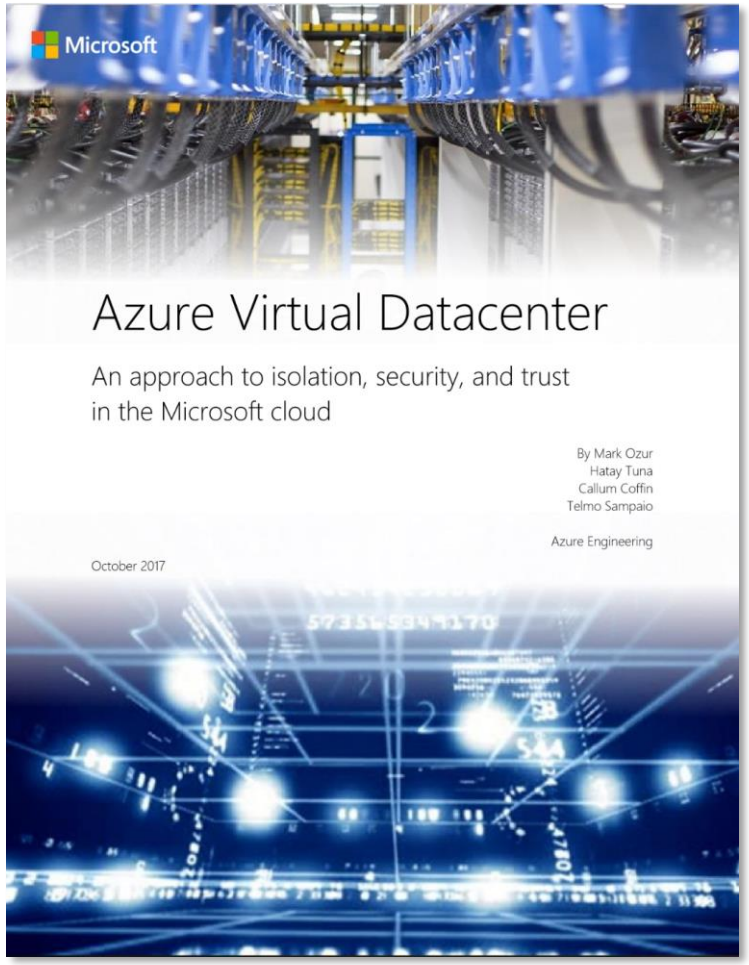
The goal is to create a safe environment for product development… without slowing teams down



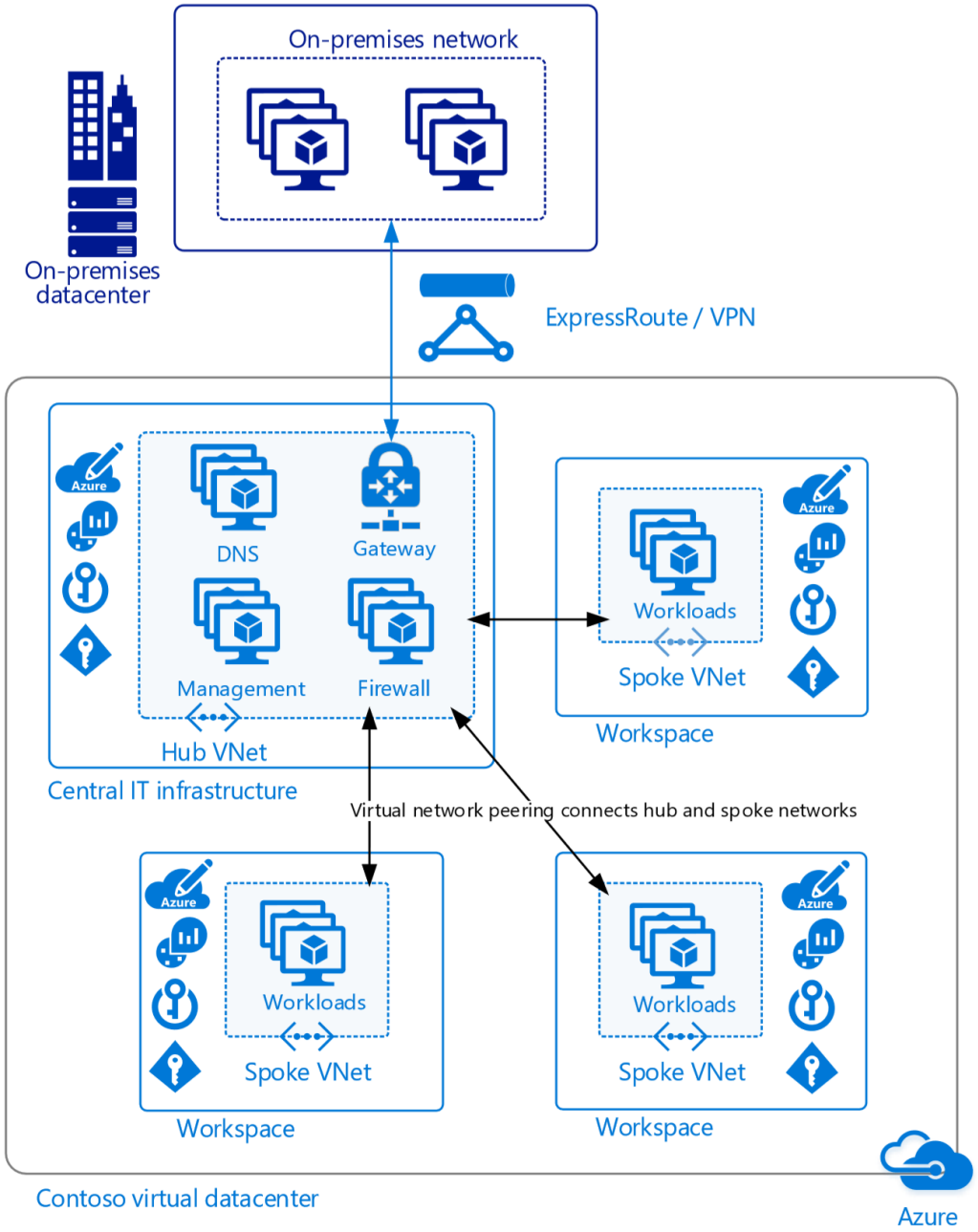
Azure Scaffold



Azure Virtual Datacenter



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



So much governance

Azure Security Center

Azure AD, Identity Protection, Privileged Identity Management, Access Reviews,

Multi-factor authentication

RBAC

Log Analytics

Azure Cost Management

Service Health

Management Groups

Network Watcher

DevTest Labs

Azure Advisor

Azure Monitor

VM Guest Policy

Azure Automation State Configuration (DSC)

Chef InSpec

Resource Graph

Diagnostics

Policy

Azure Blueprints

Metrics + Alerts

Automation accounts

and much more in the marketplace…

Introducing

Azure Governance

https://github.com/DanielLarsenNZ/talks

Governance for the cloud

Native platform controls

Policy

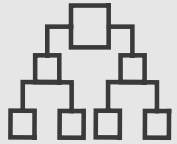
Real-time enforcement, compliance assessment and remediation

Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

Resource Graph

Query, explore & analyze cloud resources at scale



Management Group

Define organizational hierarchy

Cost

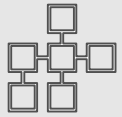
Monitor cloud spend and optimize resources

Azure Governance

Management Groups

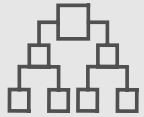
https://github.com/DanielLarsenNZ/talks

Introducing Azure Management Groups



Make environment management easier by grouping subscriptions together

- Grouping subscriptions into logical groups allow for new organization models
- Inheritance allows for single assignment of controls that apply to all subscriptions
- Aggregated views above the subscription level



Create a hierarchy of management groups that fit your organization

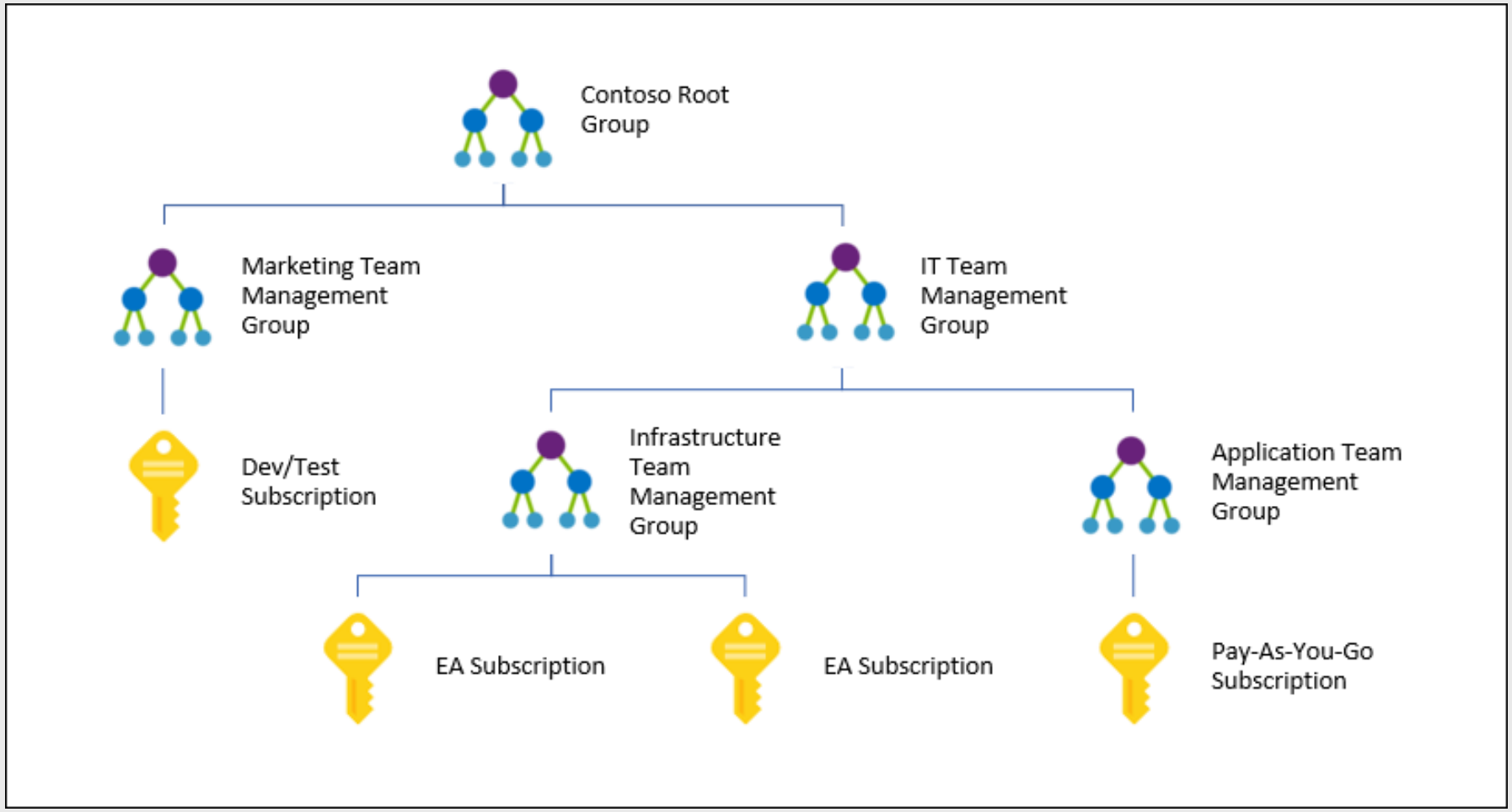
- Create a flexible hierarchy that can be updated quickly
- Hierarchy doesn't need to model the organizations billing hierarchy
- Can easily scale up or down depending on the organizational needs

Apply governance controls with policies and access controls along with other Azure services

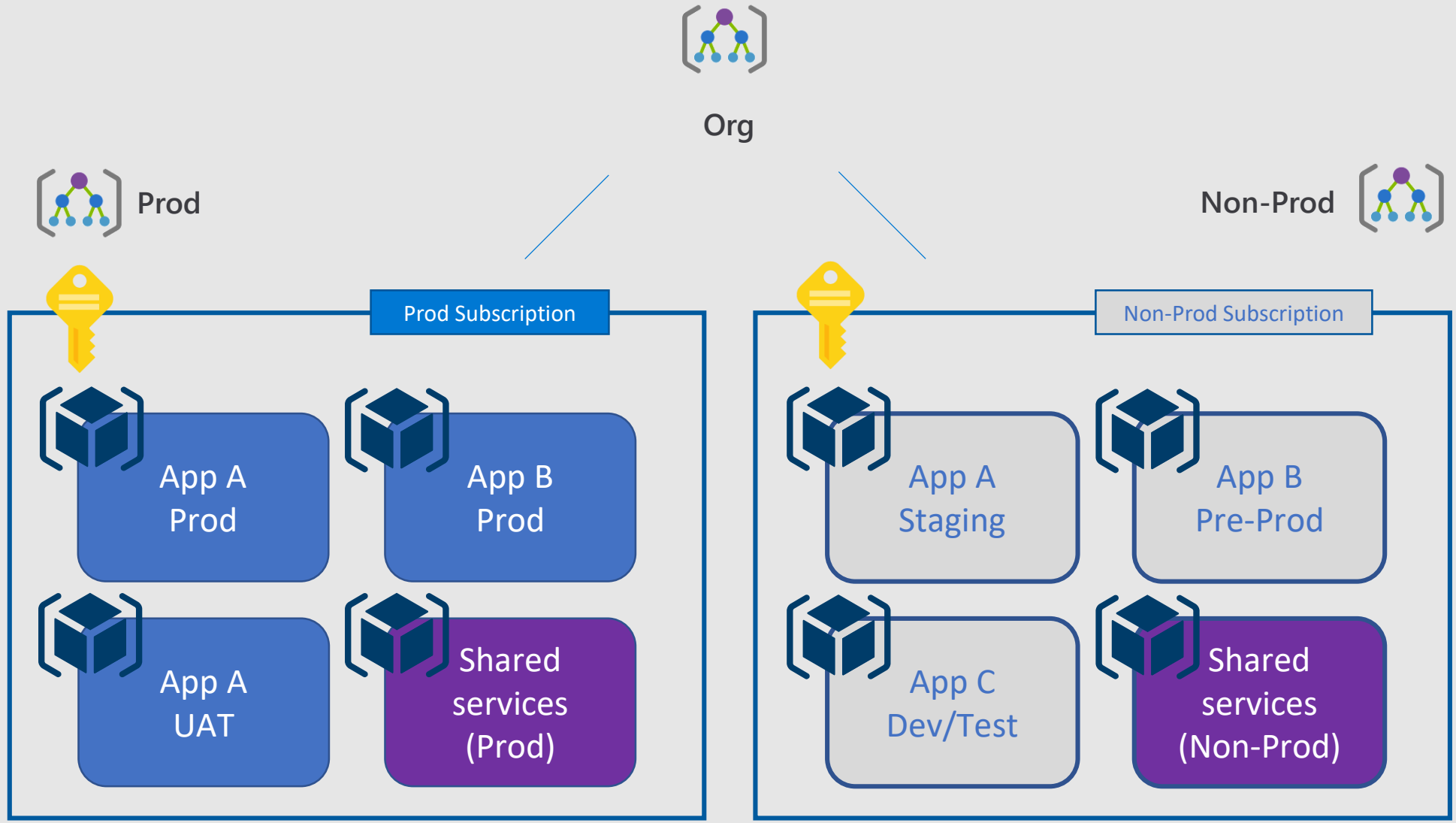
- Azure Resource Manager (ARM) objects that allow integrations with other Azure services
- Azure services:
  - Azure Policy
  - RBAC
  - Azure Cost Management
  - Azure Blueprints
  - Azure Security Center

Enterprise subscription model

Using Management Groups

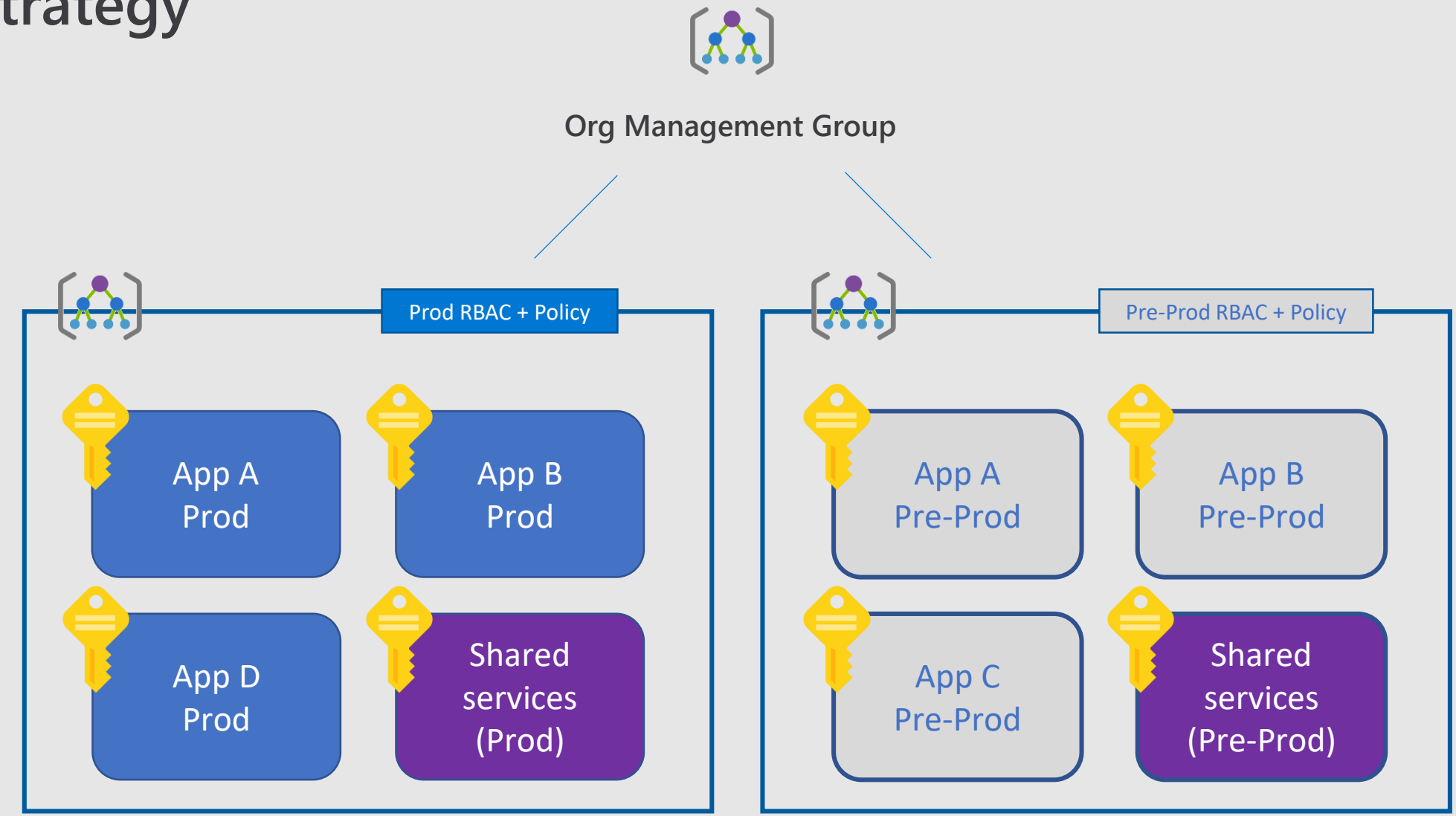


Prod / Non-prod subscription model



Management Group & Subscription Modeling Strategy

Microsoft Recommended



Demo

Management Groups

https://github.com/DanielLarsenNZ/talks

Azure Governance

Azure Policy

https://github.com/DanielLarsenNZ/talks

Azure Policy Journey

09/2017

Limited public preview

Introduced the new compliance engine (scans every 24 hours), UX and initiative

12/2017

Public preview

Introduced Management Group support

Compliance scan on resource change (delta scan)

Built-in definition support for remediation

05/2018

GA

Pricing details announcement (FREE!)

National clouds support

Introduced policy events view (count by user)

09/2018

Compliance percentage

Full fidelity of resources (store compliant resources)

'Last evaluated' timestamp

Trigger scan (on-demand scan) API

Custom definition support for remediation

Remediation on existing resources

'Denied due to policy' UX improvement

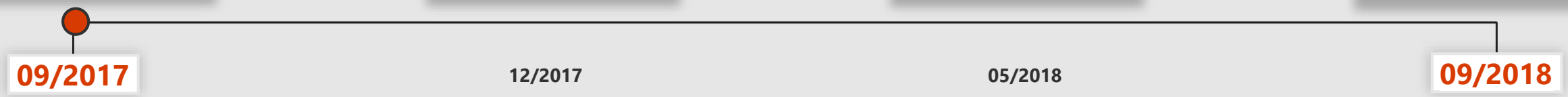
Progressive compliance results

In-guest Policy public preview

Default parameters

Azure DevOps integration

Azure Security Center integration



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 (NEW)

Enforcement & Compliance

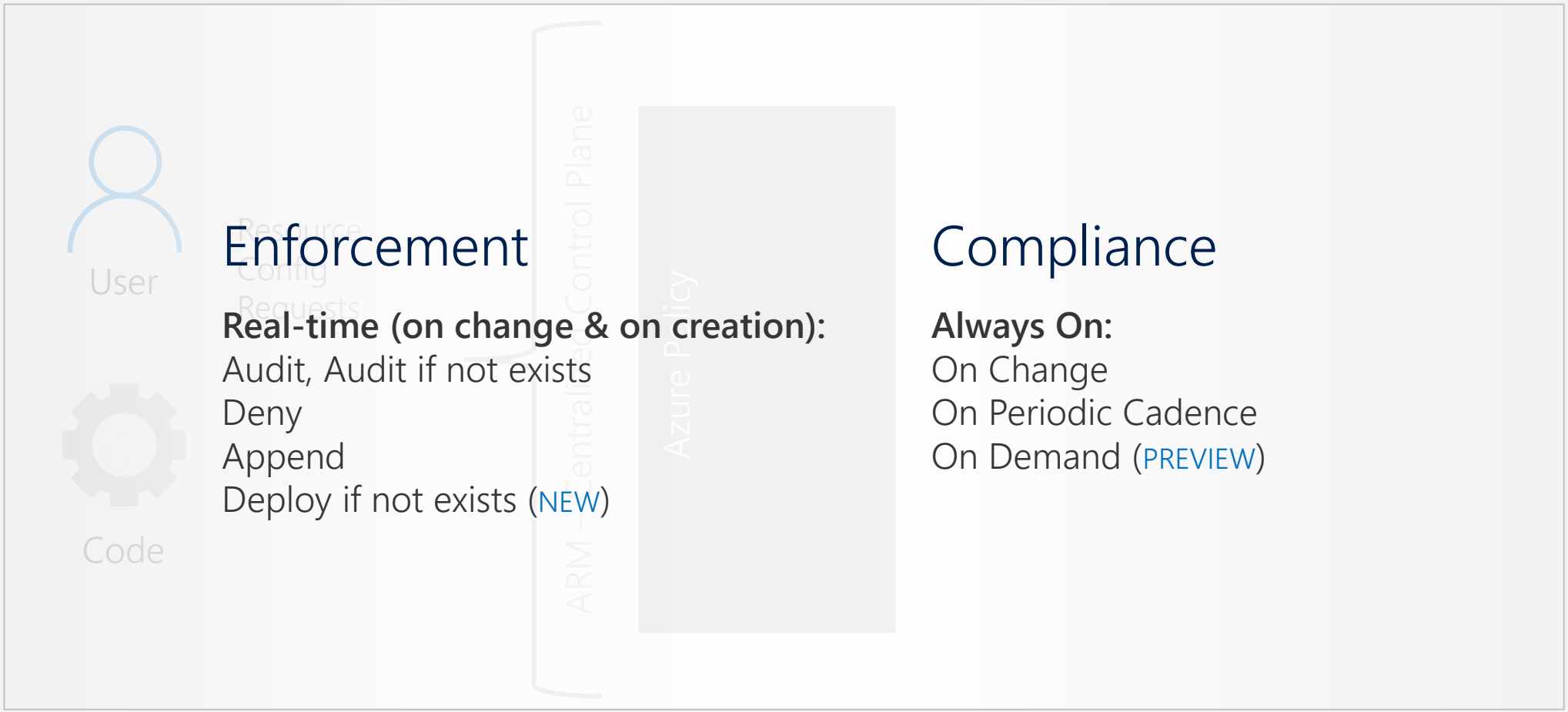
- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

Apply policies at scale

- Real time remediation
- Remediation on existing resources (NEW)

Remediation

How does it work?



Enforcement

Real-time (on change & on creation):
Audit, Audit if not exists
Deny
Append
Deploy if not exists (NEW)

Compliance

Always On:
On Change
On Periodic Cadence
On Demand (PREVIEW)

Demo

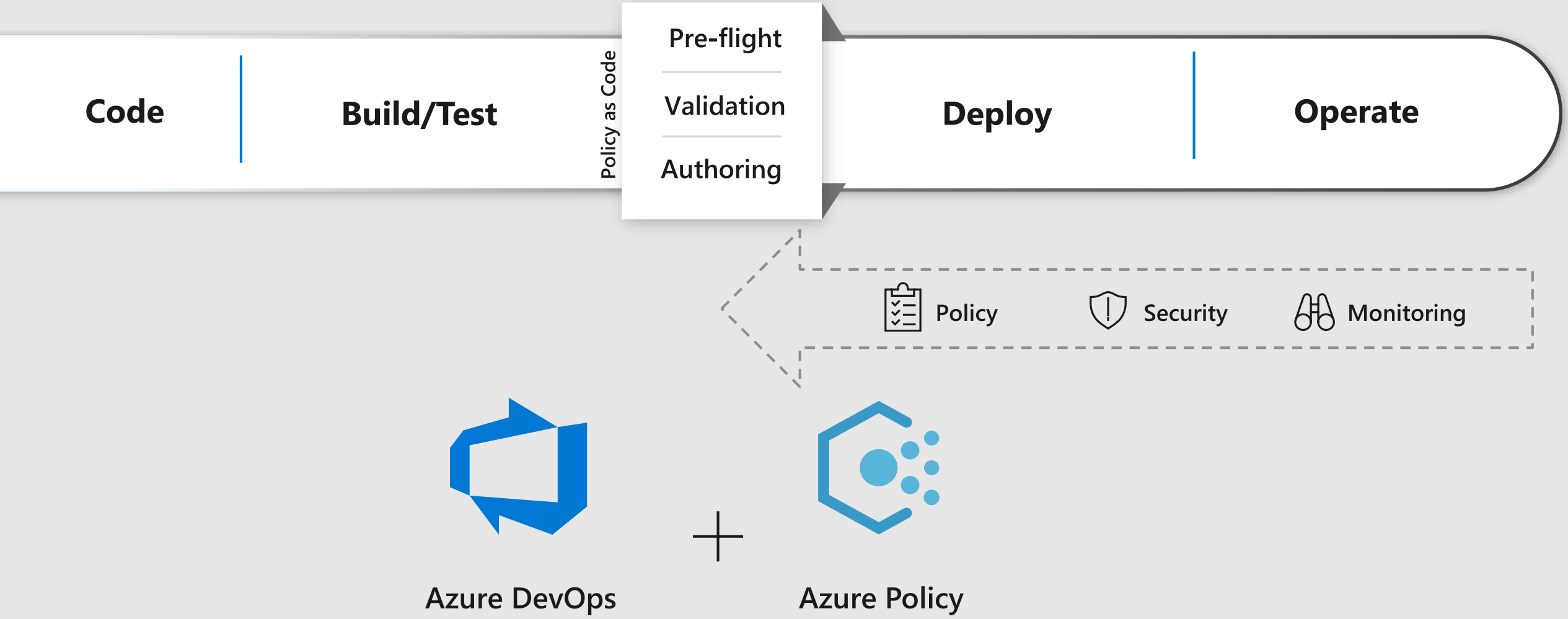
Azure Policy

Assign built-in policy definition
Exceptions
Create and assign custom policy definition
Compliance
Remediation

https://github.com/DanielLarsenNZ/talks

Enforce policies as part of the development process

Shift left to deliver compliant code faster



Azure Governance

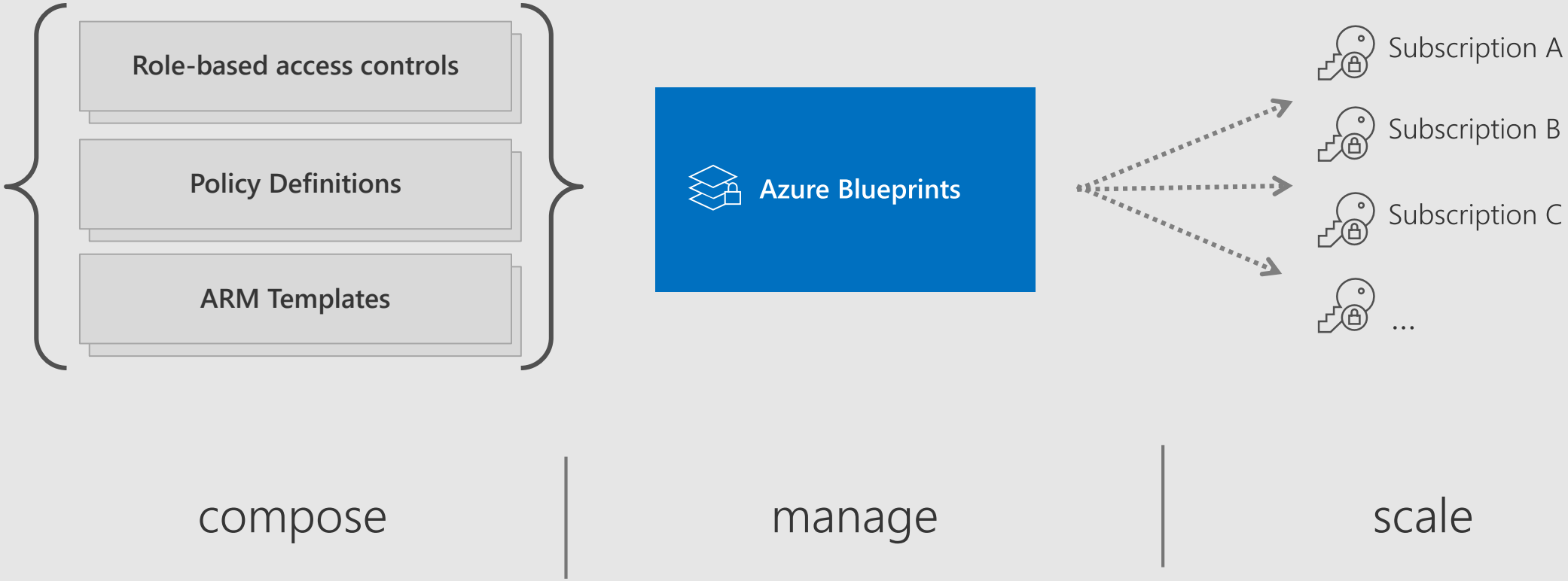
Azure Blueprints

https://github.com/DanielLarsenNZ/talks

Insert shot of Azure Scaffold repo in Azure DevOps

Azure Blueprints

deploy and update cloud environments in a repeatable manner using composable artifacts



compose | manage | scale

Demo

Azure Blueprints

Create a global Blueprint
- Environment tag
- Monitor missing system updates in Azure Security Center
- Assign SysOps group as Contributor
- Create Shared Infrastructure RG with KV (Key Vault) and auto (Automation account)

Create a Prod Blueprint
- Policy: Require Blob encryption for Storage account
- RG: app-prod-rg
- Apply `project-code` tag with default value to resources and RGs
- Add App Team as contributor

https://github.com/DanielLarsenNZ/talks

Azure Governance

Resource Graph

https://github.com/DanielLarsenNZ/talks

Demo

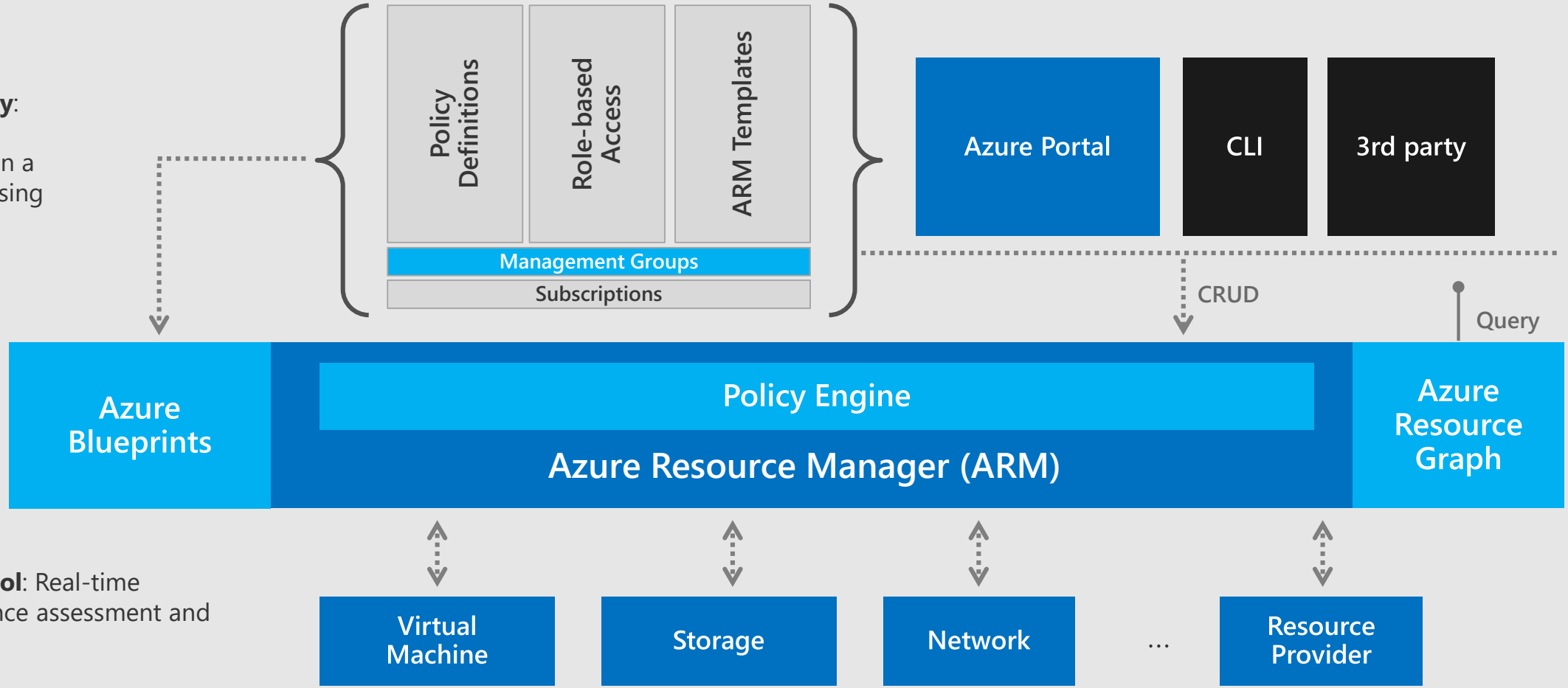
Resource Graph

https://github.com/DanielLarsenNZ/talks

Azure Governance Architecture

providing control over the cloud environment, without sacrificing developer agility

1. Environment Factory: Deploy and update cloud environments in a repeatable manner using composable artifacts



2. Policy-based Control: Real-time enforcement, compliance assessment and remediation at scale

3. Resource Visibility: Query, explore & analyze cloud resources at scale

Governance Roadmap- 6 to 8 months

Policy

- Auto-generation of aliases
- Partial RegEx support
- Multi-hop relationship
- 'What-if' evaluation powered by resource graph
- Sequence remediation actions
- More DevOps/Policy-as-code integrations

Blueprints

- Subscription creation as part of Blueprints deployment
- Apply Blueprints to one or more Resource Groups
- Sequence the deployment of artifacts
- Assess (what-if) the impact\change of Blueprint on an environment
- ISO, HIPAA solutions

Resource Graph

- Cross tenant queries at scale for MSP customers
- Microsoft Graph integration
- Query Explorer

Management Groups

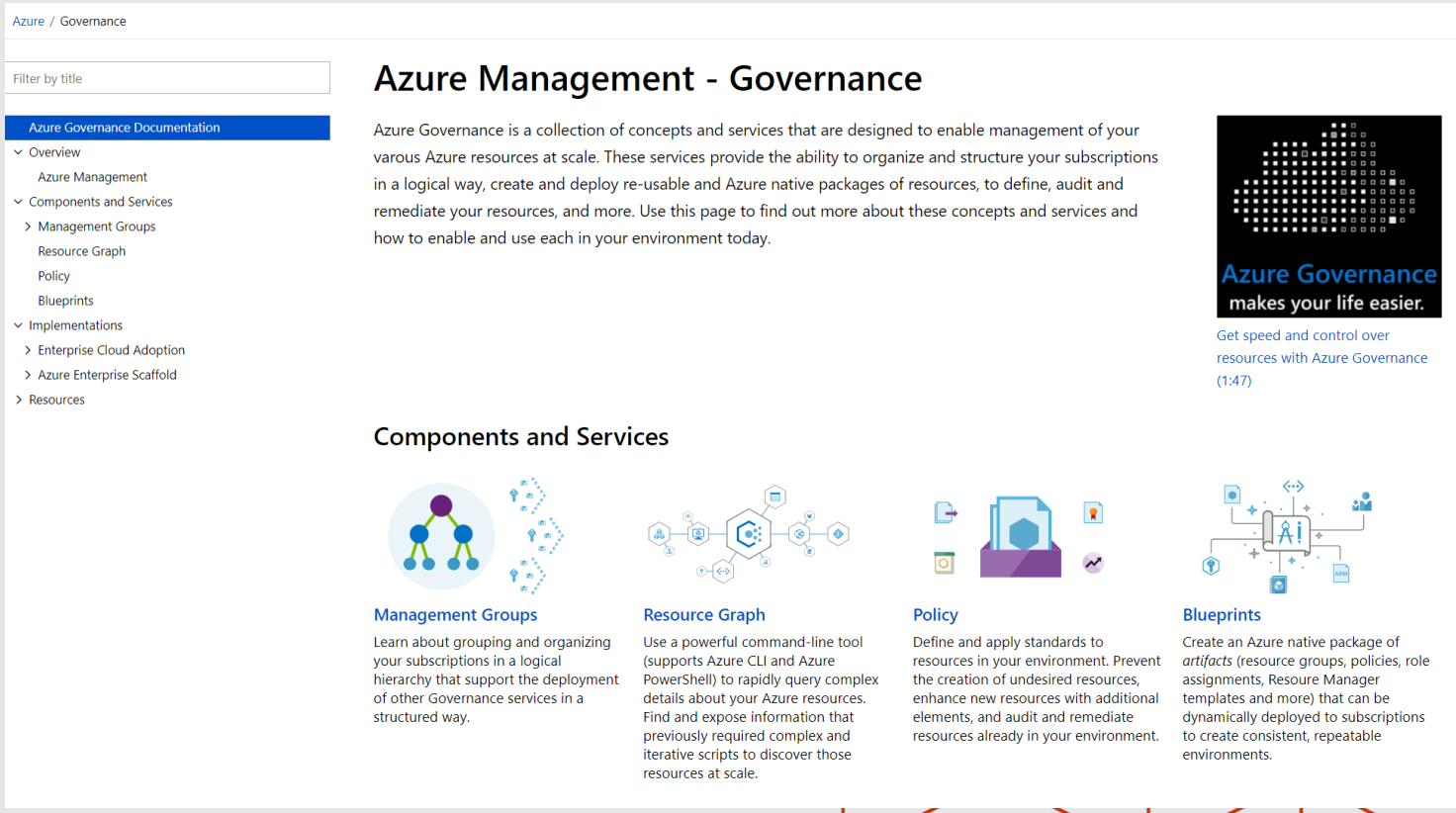
- Privileged Identity Management(PIM) integration and Just in Time(JIT) Capabilities
- Custom RBAC Support
- Custom settings for default parents of new Subscriptions and Management Groups
- Tagging Support

Governance services are available in all regions. Sovereign cloud support in progress

aka.ms/GovernanceDocs

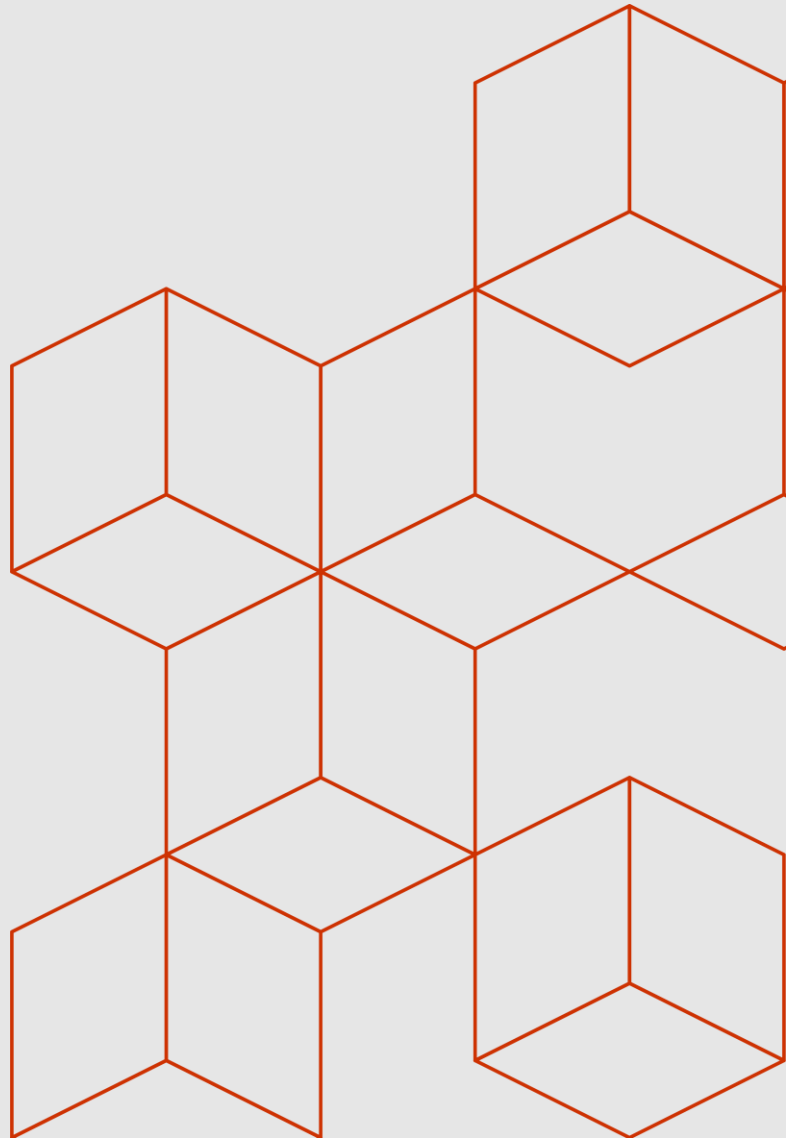
-or-

docs.microsoft.com/azure/governance



https://aka.ms/governancesurvey

What next? We want to hear from you!



Governance for the cloud

Native platform controls

Policy

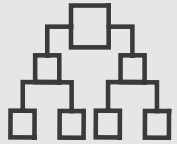
Real-time enforcement, compliance assessment and remediation

Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

Resource Graph

Query, explore & analyze cloud resources at scale



Management Group

Define organizational hierarchy

Cost

Monitor cloud spend and optimize resources

thank you!

https://github.com/DanielLarsenNZ/talks