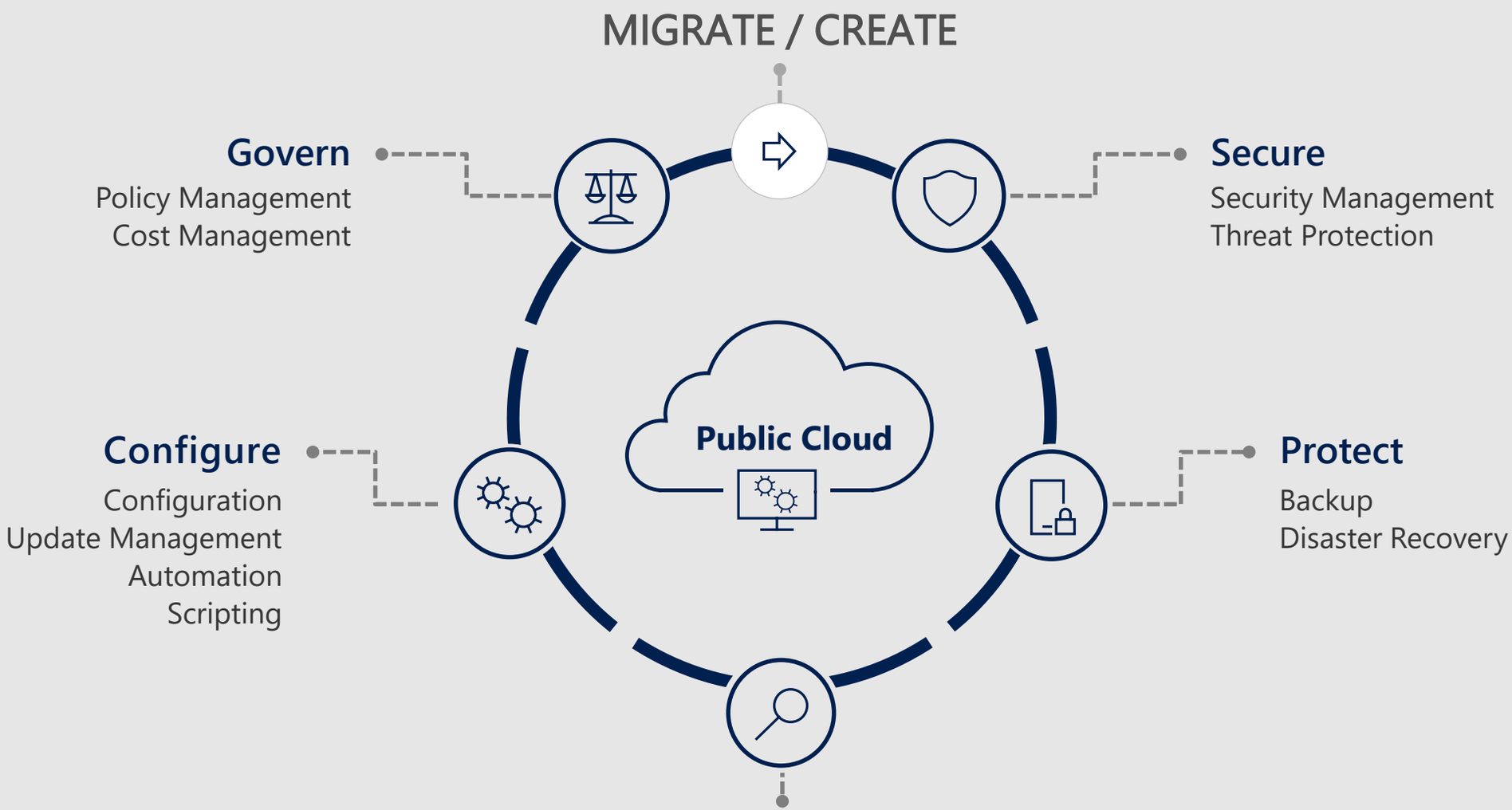
Microsoft

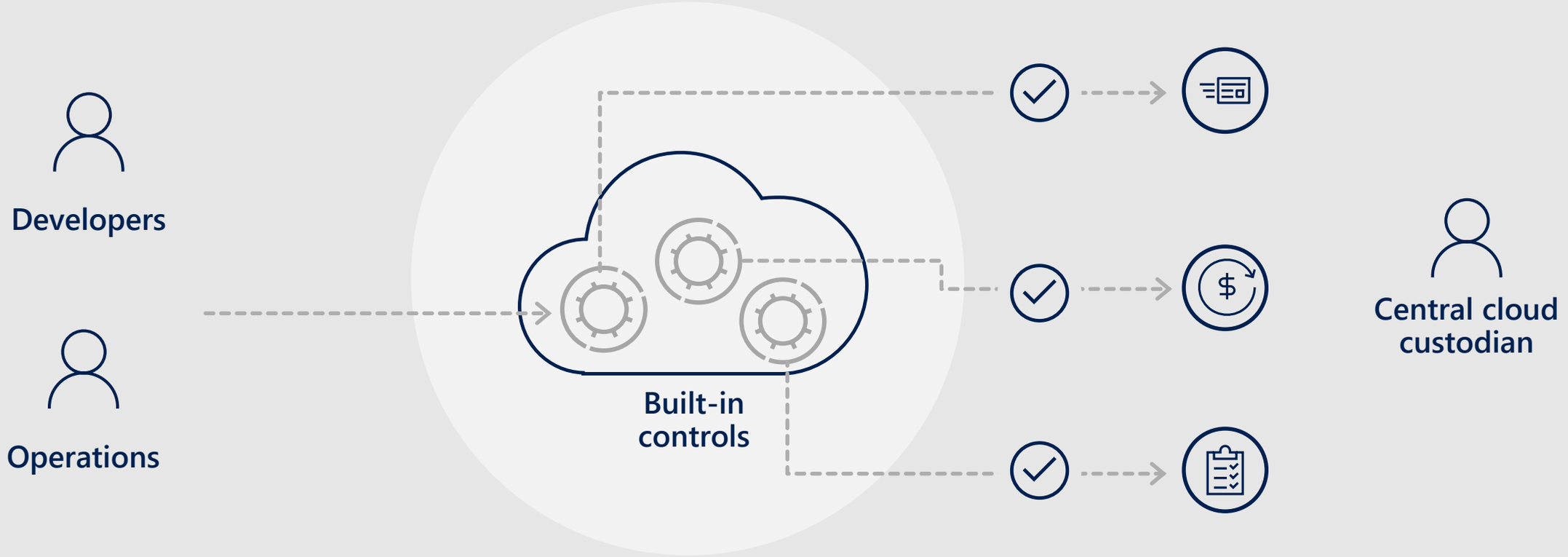
Cloud Governance

Maciej Sobianek
https://www.linkedin.com/in/maciejsobianek/

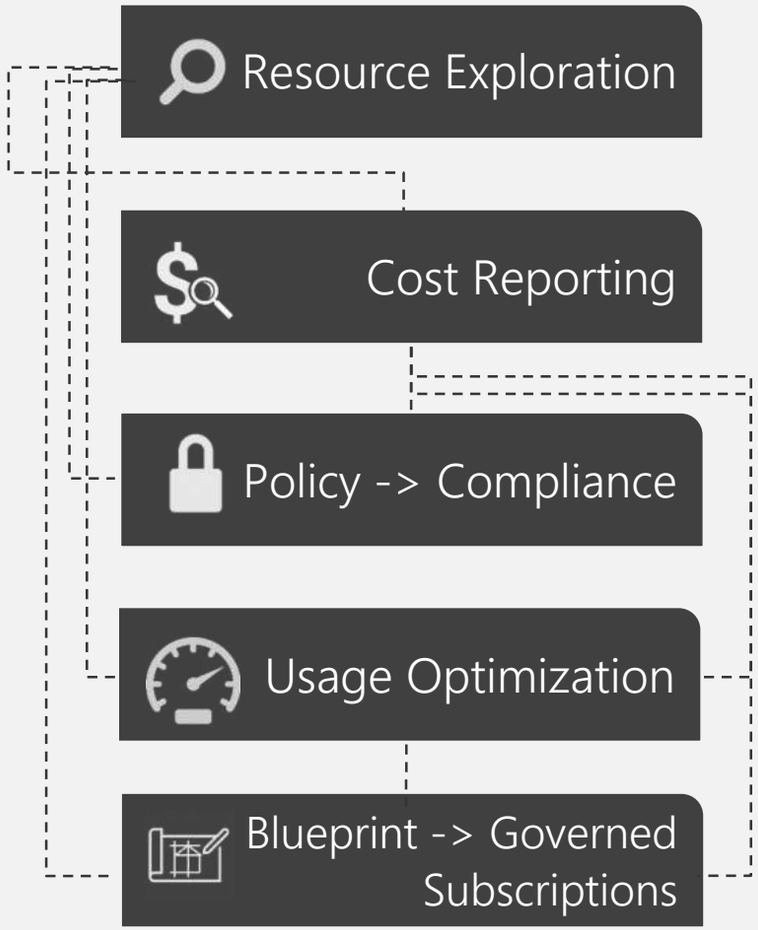

MIGRATE / CREATE
Govern
Policy Management
Cost Management
Secure
Security Management
Threat Protection
Public Cloud
Configure
Configuration
Update Management
Automation
Scripting
Protect
Backup
Disaster Recovery
Monitor
App, Infra, & Network Monitoring
Log Analytics and Diagnostics

Cloud-native governance

Removing barriers to compliance and enabling velocity



Governance capabilities



Business / Enterprise

App

Org

..metadata

Cloud Resource

Cloud Resource

Resource

Cloud Resource

Resource

Cloud Resource

Governance for the cloud

Quickly search and find resources across your organization and their relationships with query-based exploration

Resource visibility

Monitor cloud spend, drive organizational accountability, and optimize cloud efficiency

Cost management and optimization

Assess and enforce enterprise-wide governing standards across your cloud environment for proper control and compliance

Policy-based management

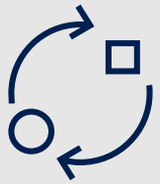
Create easy-to-use pre-defined templates for DevOps teams that meet organizational security and compliance requirements

Subscription governance

Azure policy for enterprise-level compliance

- Turn on built-in policies or build custom ones
- Enforce configurations like restricting deployment to specific datacenters
- Establish tagging standards to help drive accountability

Add policies to your resources



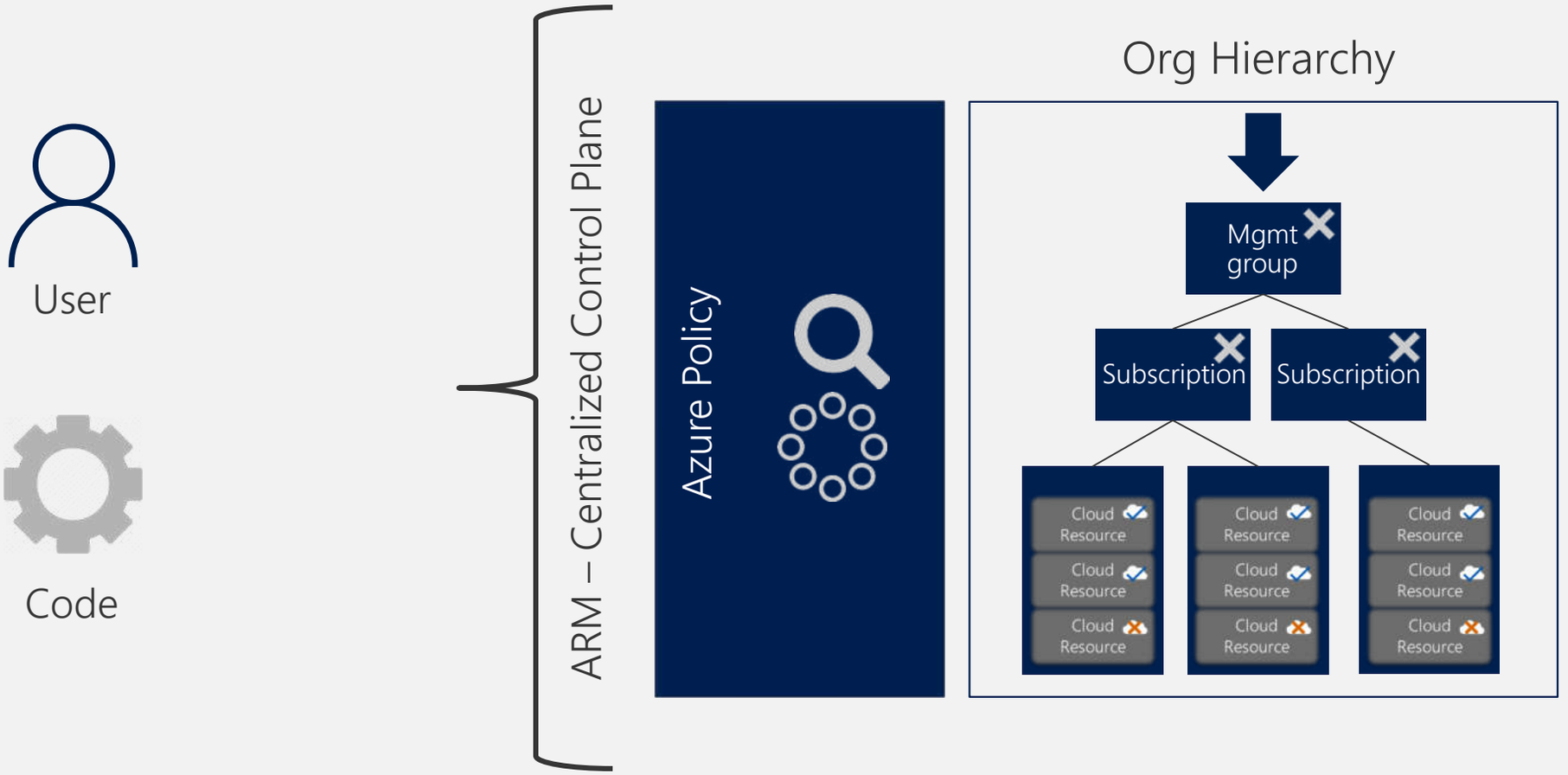
- Enable policy-based management for all your Azure resources
- Apply policies to a Management Group with control across your entire organization

Apply policies at scale

- Audit policy compliance against best practices
- View policy compliance and trends over time
- Aggregate multiple policies together to gain visibility on an initiative

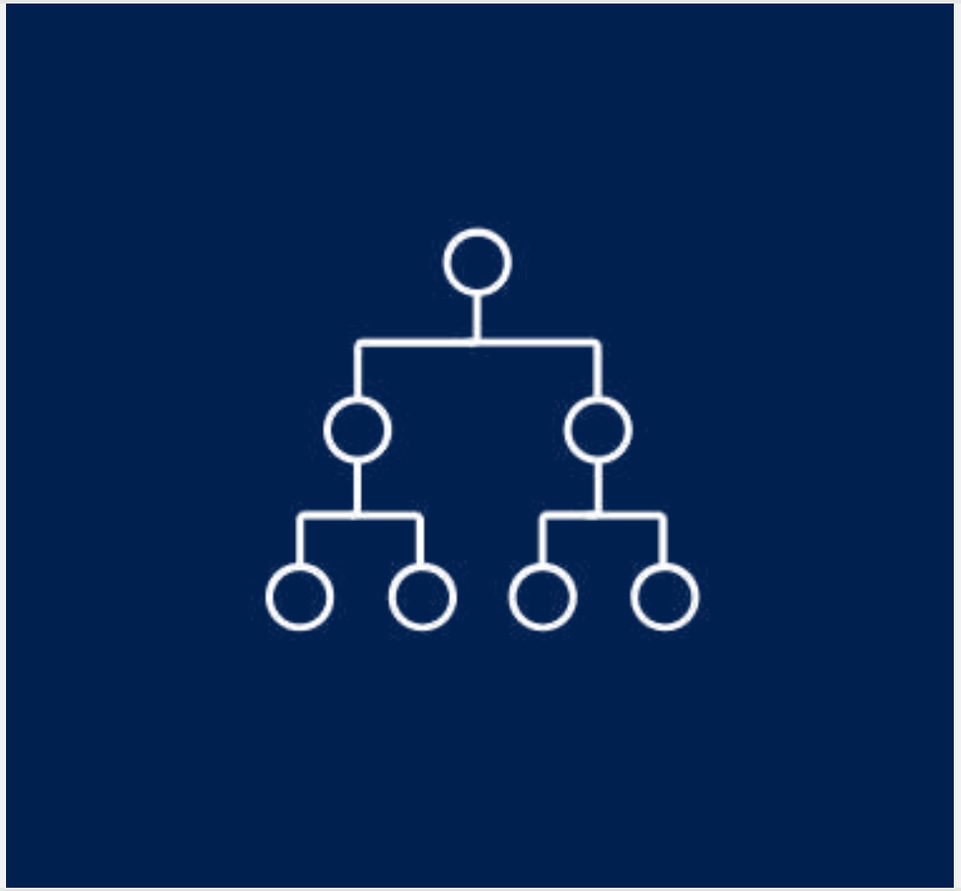
Monitor compliance

How it works at scale?



Management groups for enterprises

- Organizational alignment for your Azure subscriptions through custom hierarchies and grouping
- Enables targeting of policies and spend budgets across all subscriptions and inheritance down the hierarchies
- Enables compliance and cost reporting by organizations (business/teams)



Policy rule

Logical operators

"not": {condition or operator}
"allOf": [{condition or operator},
{condition or operator}]
"anyOf": [{condition or operator},
{condition or operator}]

Conditions

"equals": "value"
"like": "value"
"match": "value"
"contains": "value"
"in": ["value1","value2"]
"containsKey": "keyName"
"exists": "bool"

Fields

name
kind
type
location
tags
tags.*
property aliases

Effects

Deny,
Audit,
Append,
AuditIfNotExists,
DeployIfNotExists

Policy definition

```
$policy = New-AzureRmPolicyDefinition -Name
costCenterTagPolicyDefinition -Description "Policy to deny
resource creation if no costCenter tag is provided" -Policy '{
  "if": {
    "not" : {
      "field" : "tags",
      "containsKey" : "costCenter"
    }
  },
  "then" : {
    "effect" : "deny"
  }
}'
```

Standard Recommended Tags

Standard Tags	Tag Value Explanation
compositeApp	Any resources tagged with the same value are considered part of the same application service
businessowner	Contains name/UPN of the person that is responsible for the resource from a business perspective.
costCode	Uniquely identifies where the costs of the resource should be associated in an external financial system.
deploymentStage	Identifies which deployment stage a resources is in (e.g. production, development, UAT)
vmWorkload	Identifies the primary application workload running in the VM (e.g. SQL Server or Jenkins)
vmRole	Identifies the role the VM is delivering in the larger service or lab environment (e.g. Database or Build Server)

Enforce naming convention

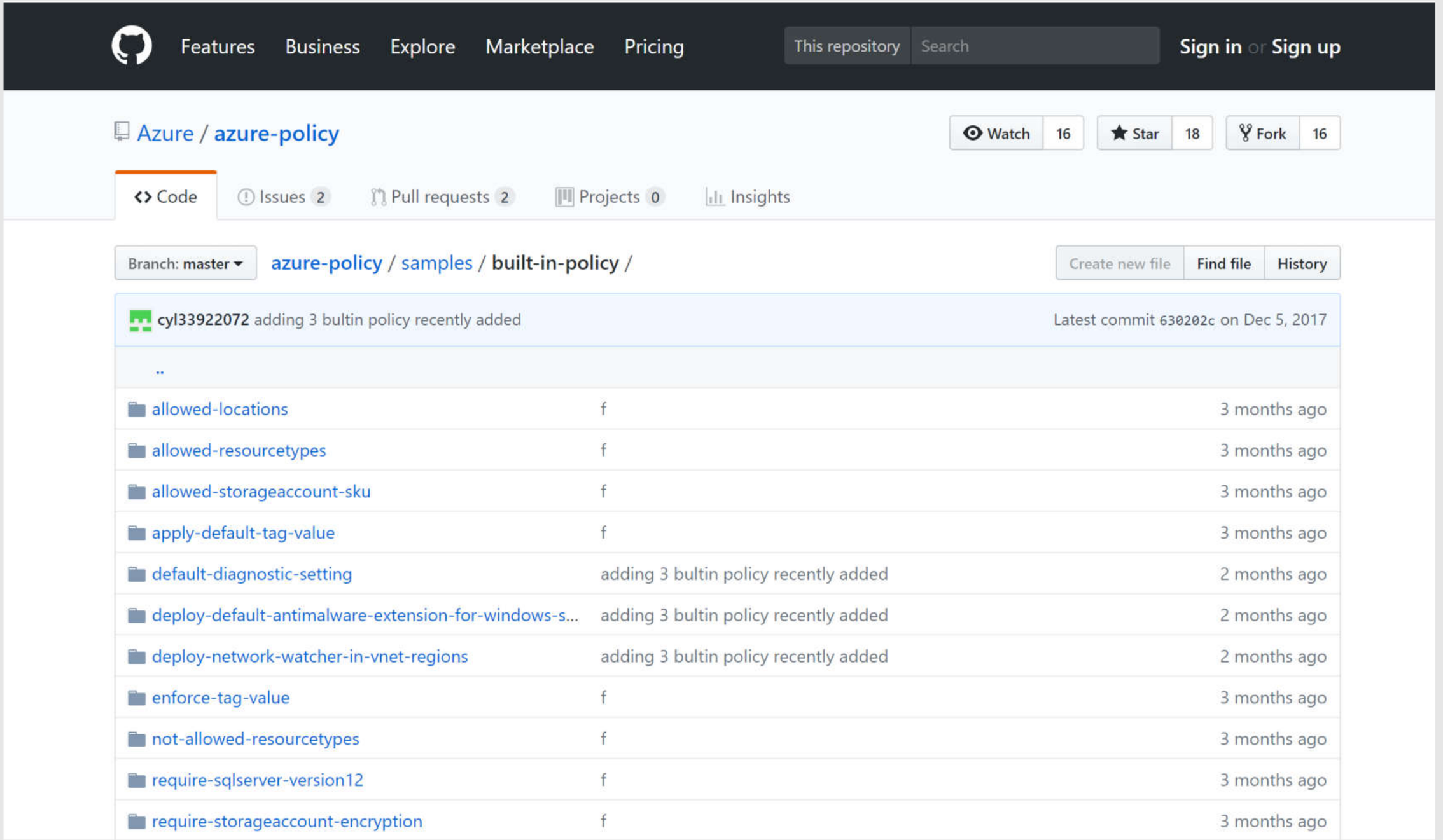
```
{
  "if": {
    "not": {
      "field": "name",
      "like": "namePrefix*nameSuffix"
    }
  },
  "then": {
    "effect": "deny"
  }
}
```

Enforce VM SKUs of basic A series

```
"properties": {
  "displayName": "Allowed VM Skus",
  "description": "This policy enables you to specify a set of virtual machine SKUs that your
  organization can deploy.“
},
"policyRule": {
  "if": {
    "allOf": [
      {
        "field": "type",
        "equals": "Microsoft.Compute/virtualMachines“
      },
      {
        "not": {
          "field":"Microsoft.Compute/virtualMachines/sku.name",
          "in": ["Basic_A0”,”Basic_A1”,”Basic_A2”,”Basic_A3”,”Basic_A4”]
        }
      }
    ]
  },
  "then": {
    "effect": "Deny“
  }
}
```

Policy Repository

https://github.com/Azure/azure-policy/


Features
Business
Explore
Marketplace
Pricing
This repository
Search
Sign in or Sign up
Azure / azure-policy
Watch 16
Star 18
Fork 16
Code
Issues 2
Pull requests 2
Projects 0
Insights
Branch: master
azure-policy / samples / built-in-policy /
Create new file
Find file
History
cyl33922072 adding 3 bultin policy recently added
Latest commit 630202c on Dec 5, 2017
..
allowed-locations f 3 months ago
allowed-resourcetypes f 3 months ago
allowed-storageaccount-sku f 3 months ago
apply-default-tag-value f 3 months ago
default-diagnostic-setting adding 3 bultin policy recently added 2 months ago
deploy-default-antimalware-extension-for-windows-s... adding 3 bultin policy recently added 2 months ago
deploy-network-watcher-in-vnet-regions adding 3 bultin policy recently added 2 months ago
enforce-tag-value f 3 months ago
not-allowed-resourcetypes f 3 months ago
require-sqlserver-version12 f 3 months ago
require-storageaccount-encryption f 3 months ago

Azure Cost Management from Cloudyn

- Track usage and cost trends
- Detect spending anomalies and usage inefficiencies
- Forecast future spend based on historical data
- Visualize data in consolidated or custom dashboards

Monitor cloud spend

- Allocate usage and costs to business units and projects
- Produce chargeback and showback reports
- Let teams access data and insights with Role-Based Access Control
- Automatically alert stakeholders of spending anomalies and risks

Drive organizational accountability

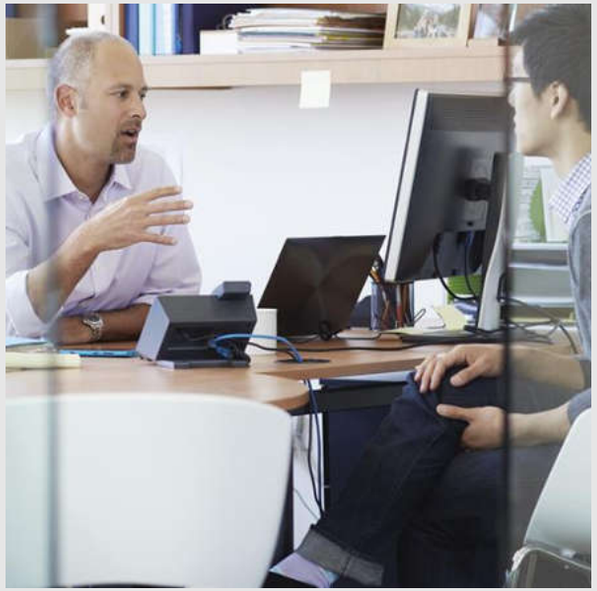
- Increase resource utilization with virtual machine right-sizing
- Eliminate idle resources
- Improve virtual machine reserved instances management

Optimize cloud efficiency

Managing cloud spend across the organization is becoming increasingly difficult

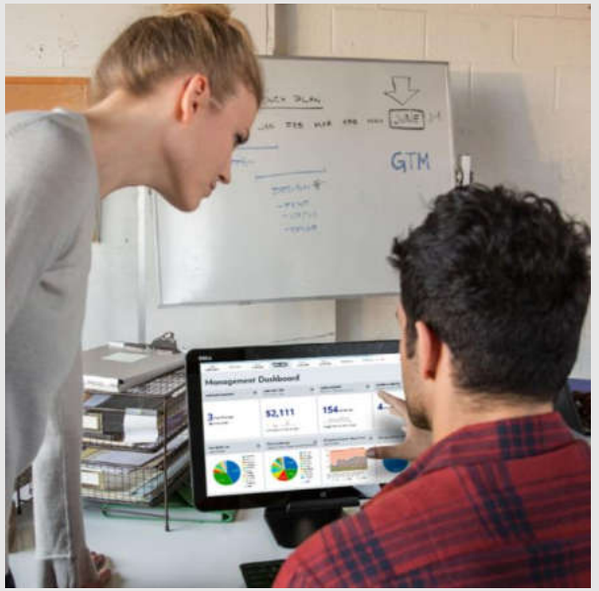
IT executives

We need to understand cloud spend across the organization to ensure the best ROI



Finance teams

We need to improve cloud spend forecasting and drive more accountability across teams



Project teams

We need to deliver more with the budget we have been given

How does Azure Cost Management work?

Customer portal: visualize data in dashboards and reports

Single Sign On

Role-Based Access Control

Cost analytics: produce insights, recommendations and alerts

Operational and financial insights
Optimization recommendations
Alerts and notifications

Organizational Hierarchy

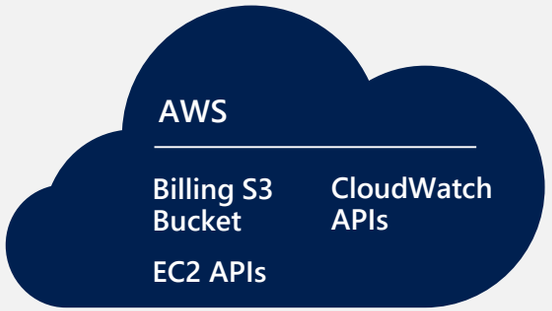
Budgets

Automated Analysis and Monitoring

Tag Enrichment

Customizable Chargeback

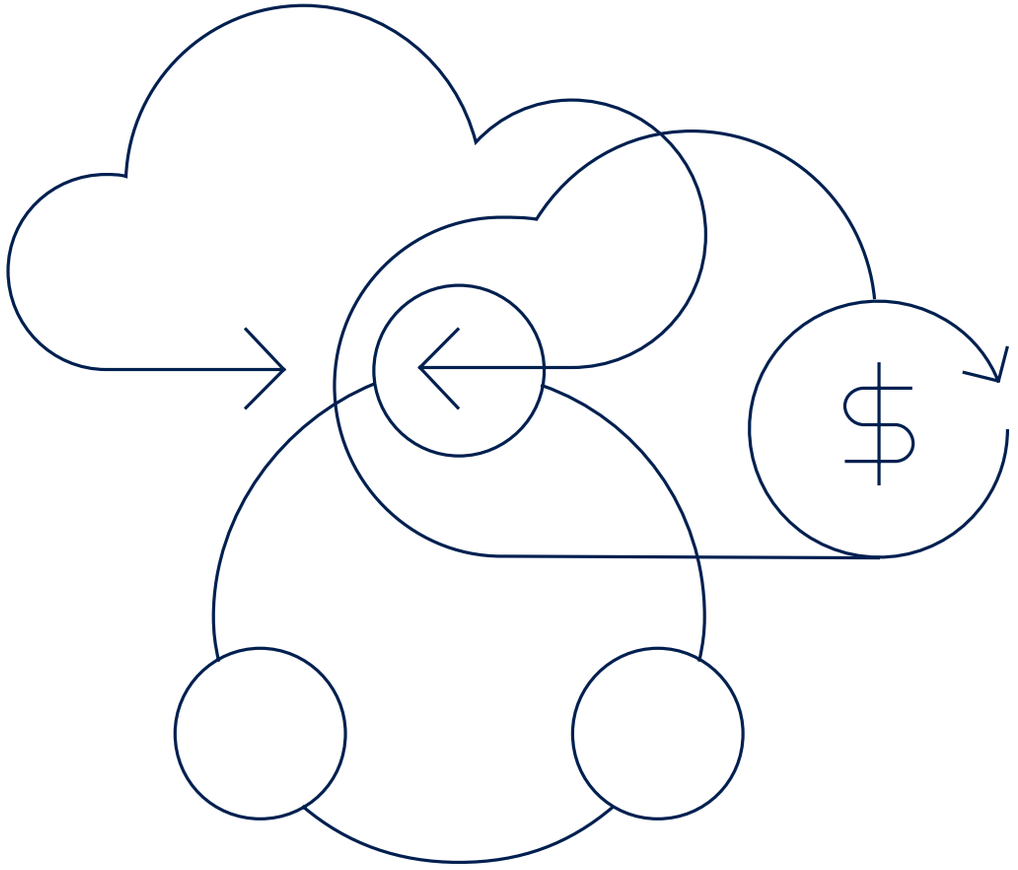
Cloud collectors: collect billing and utilization data from different clouds



Azure Cost Management can help you

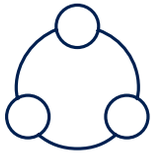
Customers see an average improvement of cloud efficiency by 20% - 25% within 3 - 6 months of using the service.

Based on customer data



With Cost Management, you can:

Monitor cloud spend



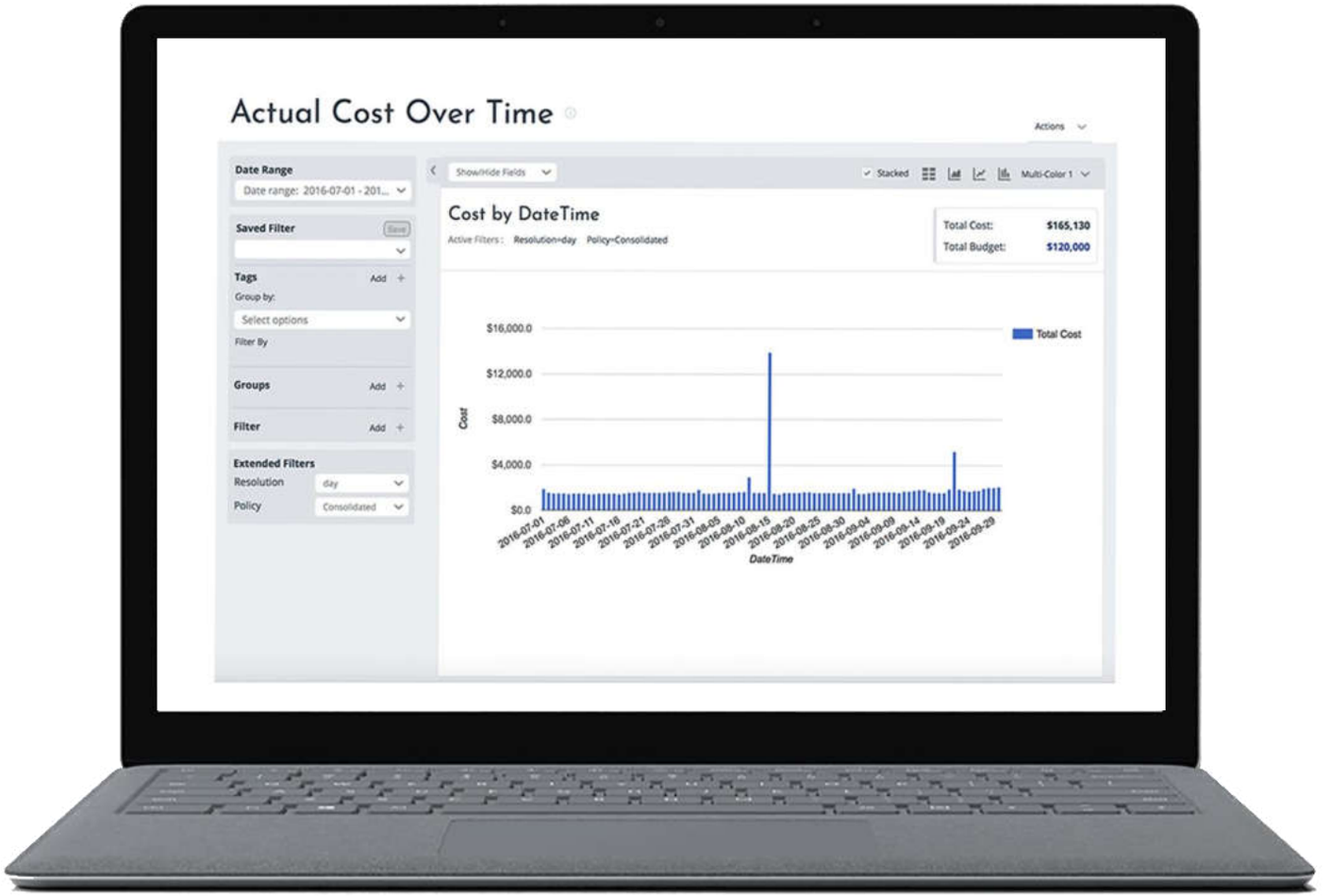
Drive organizational accountability

Optimize cloud efficiency

Across your multi-cloud environment

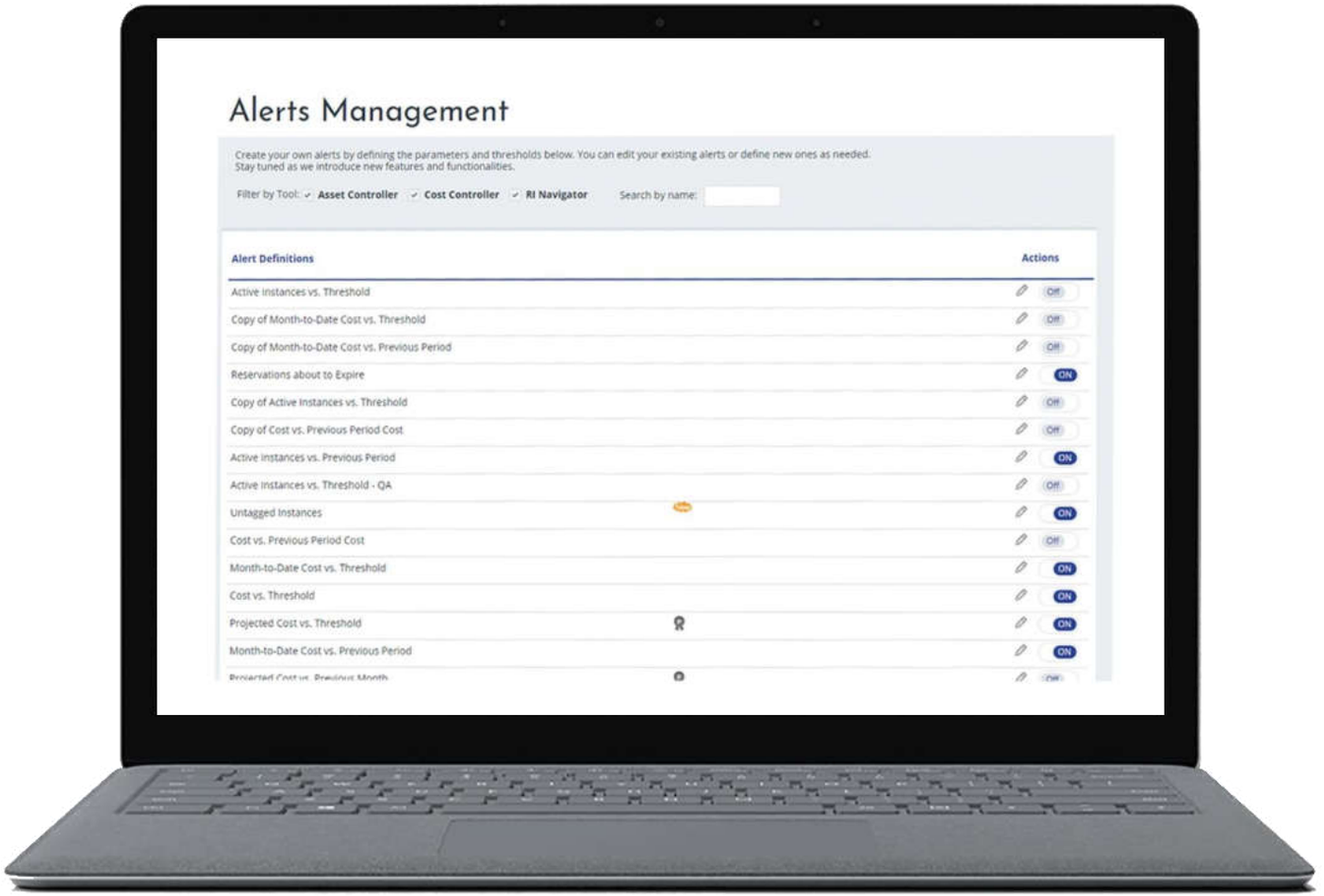
Monitor cloud spend

- Track usage and cost trends
- Detect spending anomalies and usage inefficiencies
- Forecast future spend using your historical data
- Visualize data in consolidated or custom dashboards



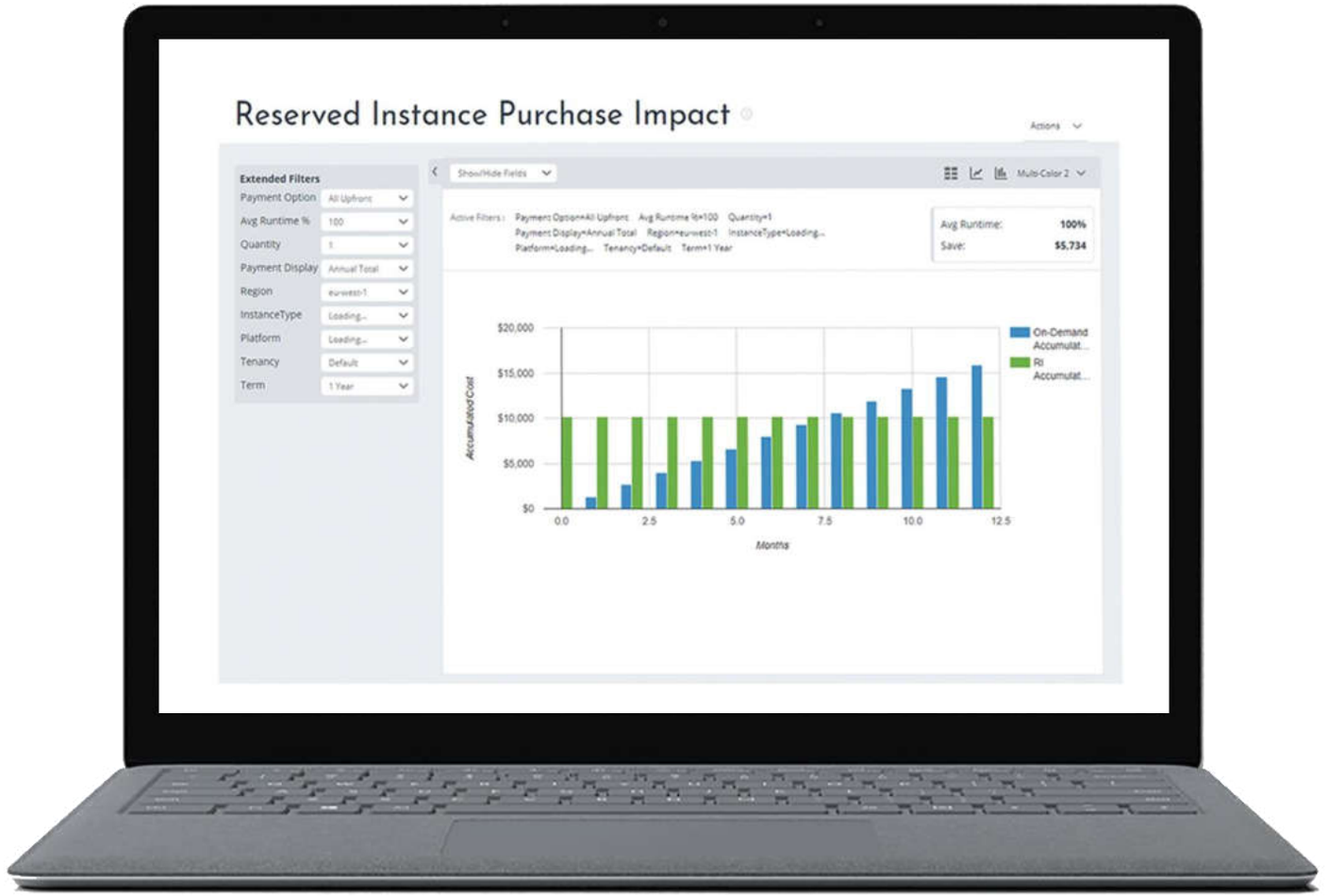
Drive organizational accountability

- Allocate usage and costs to business units and projects
- Produce chargeback and showback reports
- Let teams access data and insights with Role-Based Access Control
- Automatically alert stakeholders of spending anomalies and overspending risks



Optimize cloud efficiency

- Increase resource utilization with virtual machine right-sizing
- Eliminate idle resources
- Improve virtual machine reserved instances management



Cloud costs? The S.E.P. Field of IT

"An **S.E.P.** is something we can't see, or don't see, or our brain doesn't let us see, because we think that it's somebody else's problem.... The brain just edits it out, it's like a blind spot. If you look at it directly you won't see it unless you know precisely what it is. Your only hope is to catch it by surprise out of the corner of your eye."

- Douglas Adams, Hitchhiker's Guide to the Galaxy

S.E.P = Someone Else's Problem

Keys to accountability & governance

Extend visibility to stakeholders

Make them cost aware

Make them accountable

Set clear budgets

Set alerts
(be notified of any anomalies)

Challenge them to get better

Tagging is mandatory for better accountability

Tag your resources

Tags should be enforced by configuration policy

Use Azure Policy to set and track ARM tagging policies

Tags should include 3 types of information

Billing information: cost center, billing ID, etc.

Ownership information: whom should be contacted when needed

Purpose information: environment, application service, etc.

Cost Management can help

Discovers ARM Resource Group tags and automatically associate to underlying resources

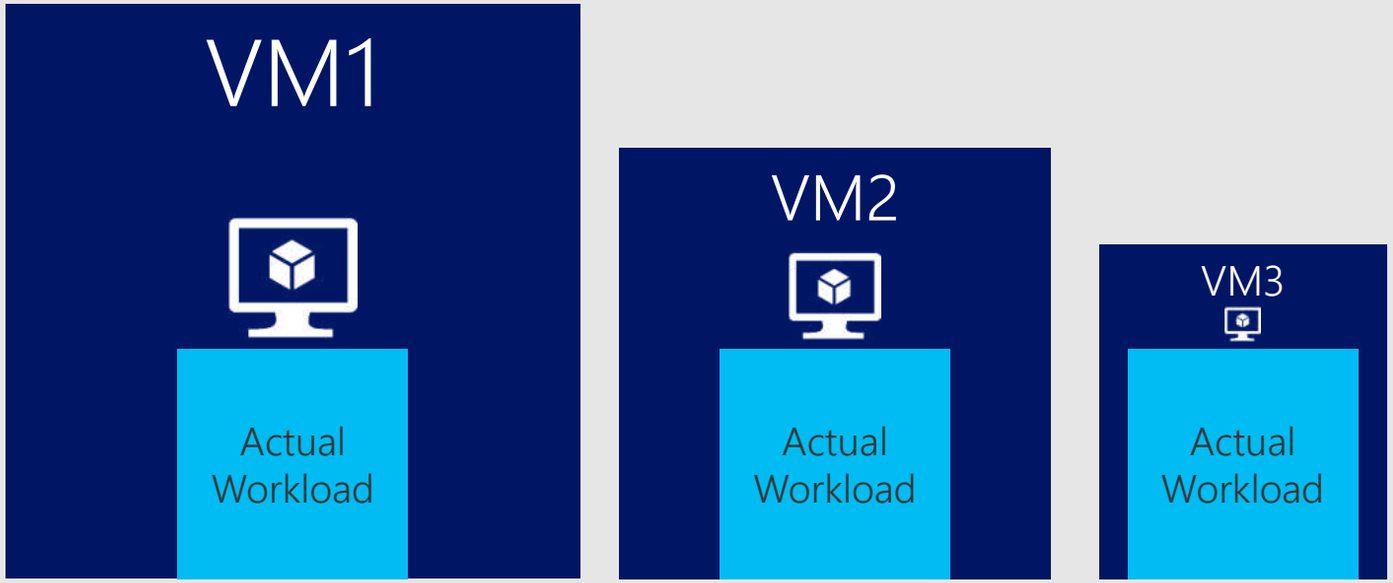
Has rules for standardizing, rewriting, adding meta-tag values

Cost is a difference between success and failure

A major operational metric with a friendly reminder every month and early indicator of anomalies

The workload will run fine in all three VM sizes

- Which will a developer naturally choose?
- Which will deliver more success to the business?
- Which one will make managers and finance want do more things in the cloud?



Optimization is the path to success

Optimization is not a one-time effort

Cloud is a constantly changing place

New projects, new applications, changing loads

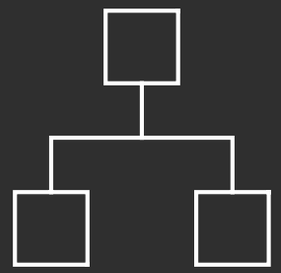
Resource optimization

Correct families & sizes

Correct resource/service types

Purchasing optimization

When to buy more/less Reserved Instances



Networking

Robust networking infrastructure services

Virtual Network

Provision private networks, optionally connect to on premise datacenters. NSG, User Defined Routes, & IP addresses.

Load Balancer

Deliver high availability and network performance to your applications

Application Gateway/WAF

Build scalable and highly-available web front ends in Azure

DDoS Protection

Protect your Azure resources from DDoS attacks

VPN Gateway

Establish secure, cross-premise connectivity

Azure DNS

Host your DNS domain in Azure

Content Delivery Network

Ensure secure, reliable content delivery with broad global reach

Traffic Manager

Route incoming traffic for high performance and availability

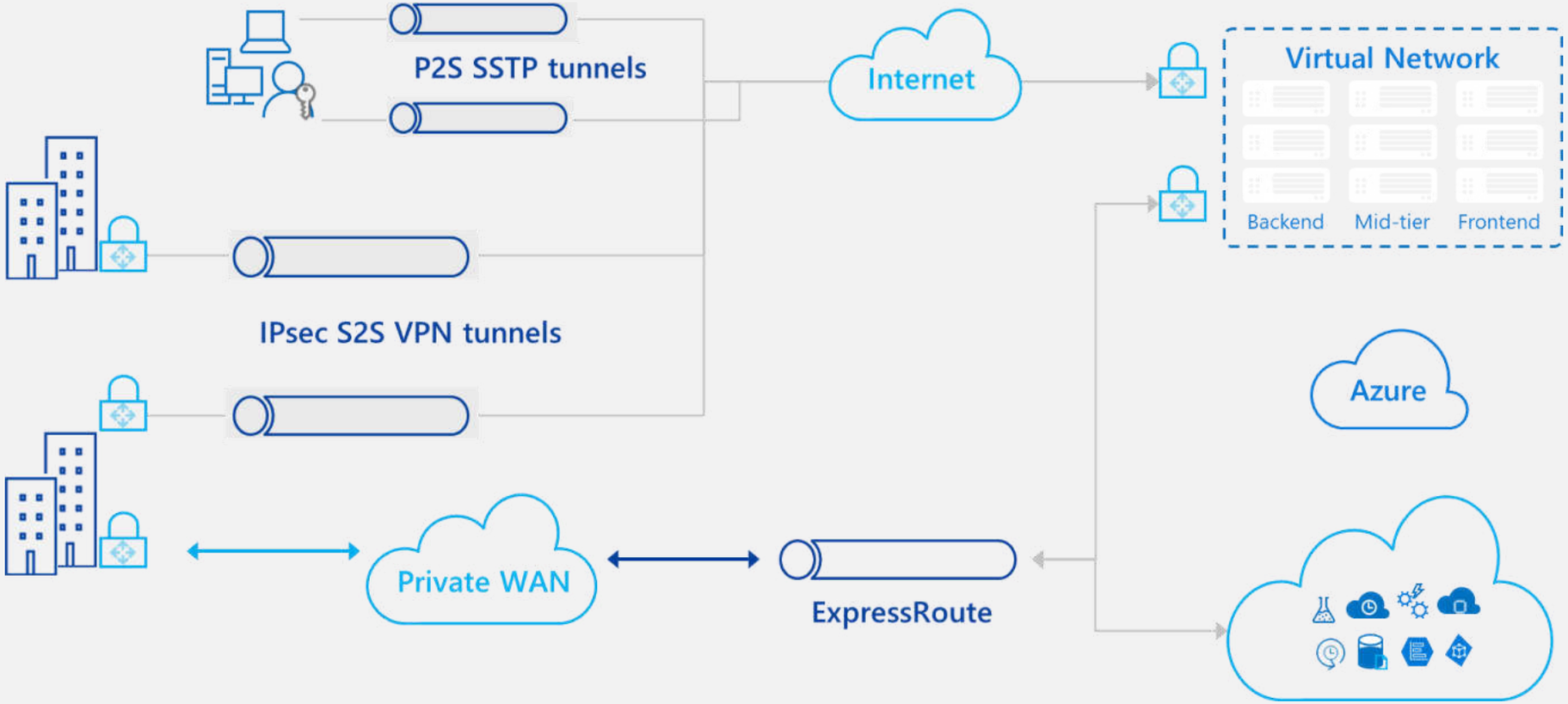
ExpressRoute

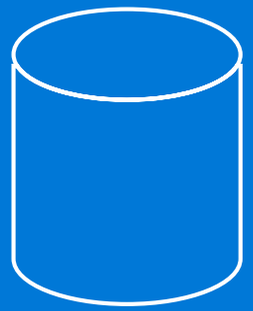
Dedicated private network fiber connections to Azure

Network Watcher

Network performance monitoring and diagnostics solution

Hybrid Connectivity Overview





Storage

Azure provides a unified distributed storage system offering durability, **encryption at rest**, strongly consistent **replication**, and auto load-balancing

Secure, scalable and highly available storage options for every use case

Disk Storage

Premium
Standard

Reliable, persistent, high performing storage for Virtual Machines

Object Storage

Azure Blobs

Secure, centralized storage target for backup/disaster recovery

File storage

Azure Files
Azure NetApp Files

Lift and shift of legacy applications that require file shares to the cloud

Data Transport

Azure Import/Export
Azure DataBox

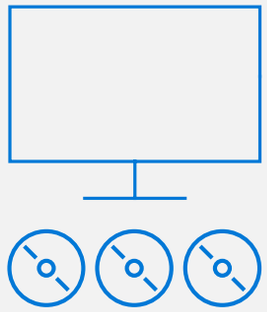
Move or migrate data into Azure

Hybrid Storage

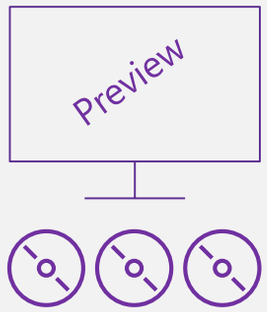
Azure StorSimple
Azure File Sync
Avere*
Secure, intelligent data tiering between on-premises and cloud storage

Azure Disks

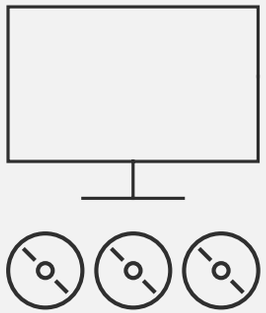
Performance Tiers



Premium SSD Disks
Provisioned performance for Enterprise Prod

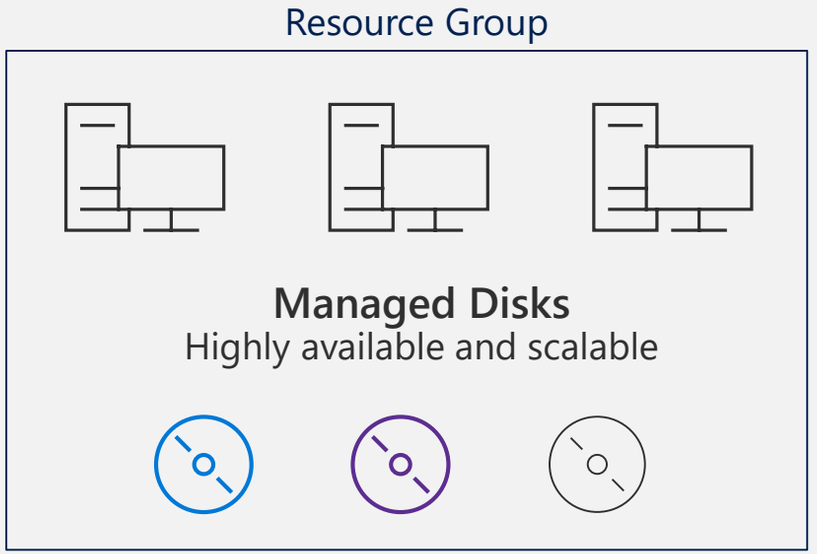


Standard SSD Disks
Cost effective performance for entry-level workloads



Standard HDD Disks
HDD based, cost effective for dev-test workloads

Simplified Management



Industry leading **ZERO %** Annual Failure Rate

Enterprise grade durability with 3 replicas

Best in class VMs with High IOPS/BW

80,000 IOPS & 2,000 MB/s Disk throughput per VM

< 1ms latency for cached operations

Blob Cache technology
Up to 160,000 IOPS

Developer Support

REST API Support
Easy Migration / DR / Backup
Rich partner ecosystem

Secure, scalable and highly available storage options for every use case

Disk Storage

Premium
Standard

Reliable, persistent, high performing storage for Virtual Machines

Object Storage

Azure Blobs

Secure, centralized storage target for backup/disaster recovery

File storage

Azure Files
Azure NetApp Files

Lift and shift of legacy applications that require file shares to the cloud

Data Transport

Azure Import/Export
Azure DataBox

Move or migrate data into Azure

Hybrid Storage

Azure StorSimple
Azure File Sync
Avere*
Secure, intelligent data tiering between on-premises and cloud storage

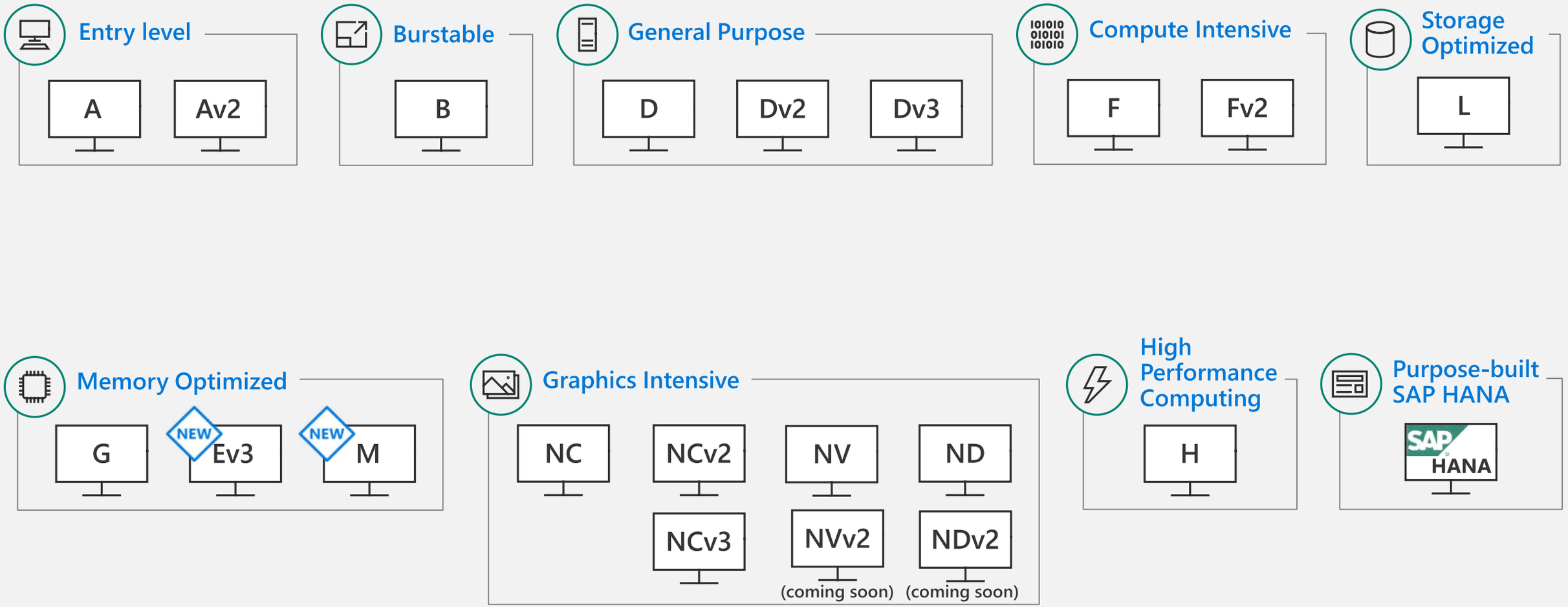
Object storage for every use case

Azure Blob

	Hot	Cool	Archive
	Frequently accessed data	Less frequently accessed data	Rarely accessed data
PER TB PER MONTH	$18.40	$10.00	$2.00
PER 10K WRITE OPERATIONS	$0.05	$0.10	$0.10
RETRIEVAL TIMES	Immediate	Immediate	Hours
USE CASES	Cloud native application data storage	Repository for server backups	Medical records archiving

Compute

Compute options for all types of apps



New VM Scale Sets enhancements

With VM Scale Sets, you can confidently deploy thousands of identical Virtual Machines in minutes and focus on what matters—your application.

- Provides auto scale-out and scale-in based on health checks
- Enables easy integration with Azure SLB or App Gateway
- Auto-OS image update for guest images
- Deploy low-priority VMs and realize cost savings
- Support for cross-zone deployment

Public Preview
April '18

Microsoft

Azure Reserved VM Instances

Committing to services through Reserved VM Instances

→ Reserve virtual machines in advance

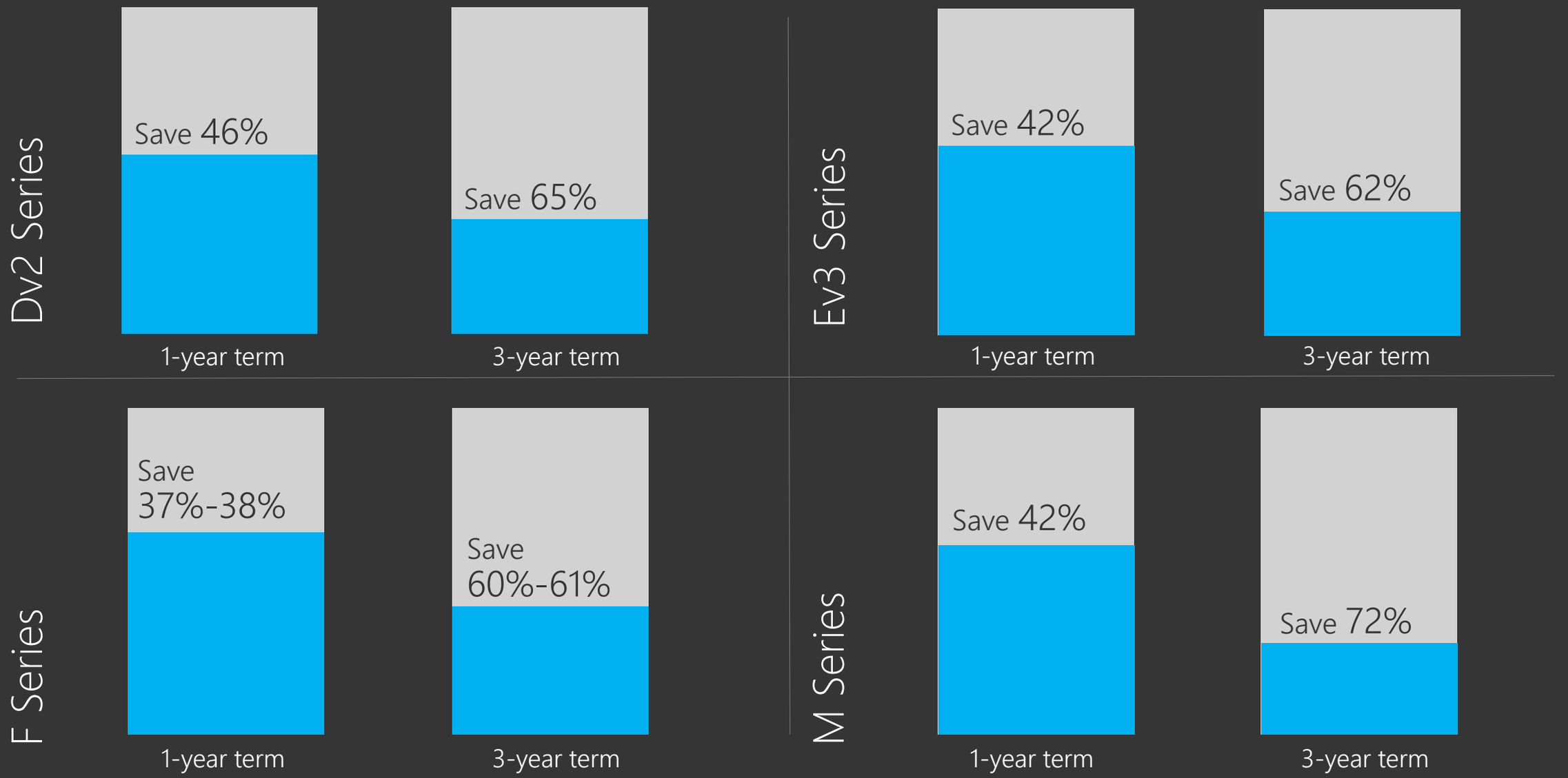
→ Select 1- or 3-year terms with significant benefits

Significant cost savings

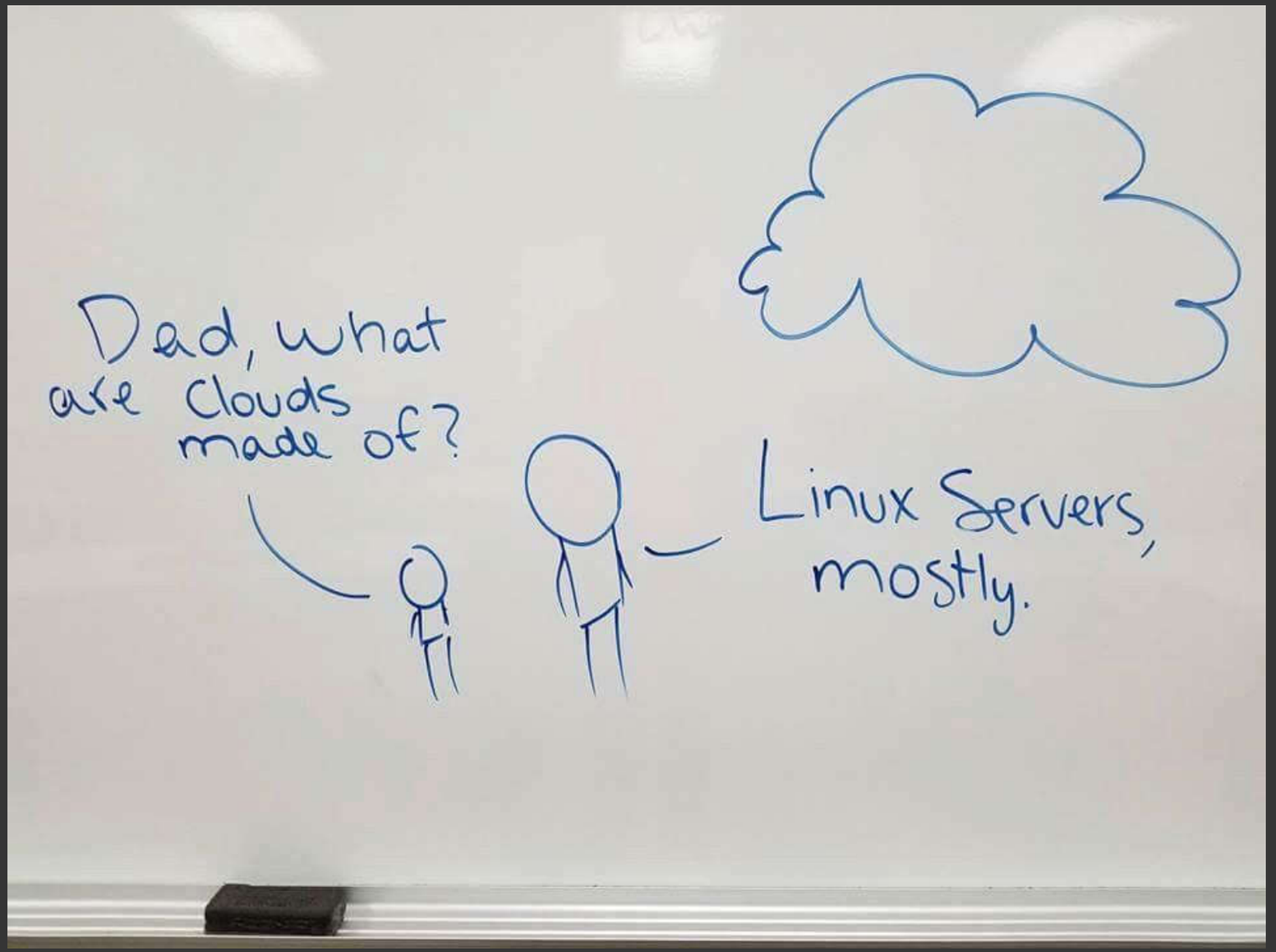
Budget predictability and prioritized compute capacity

Flexibility to modify reservations and simplicity of purchase

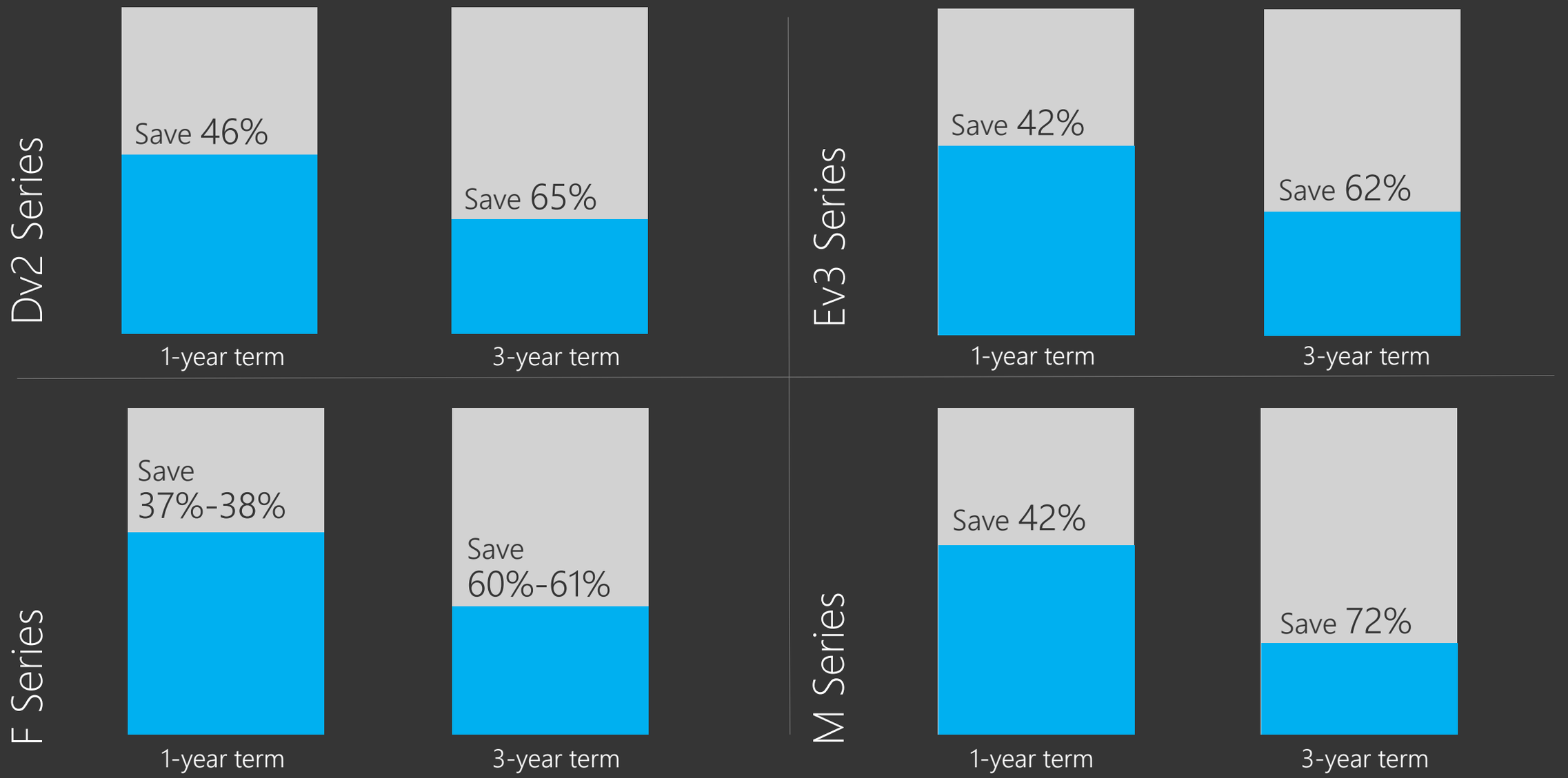
Typical savings with RI



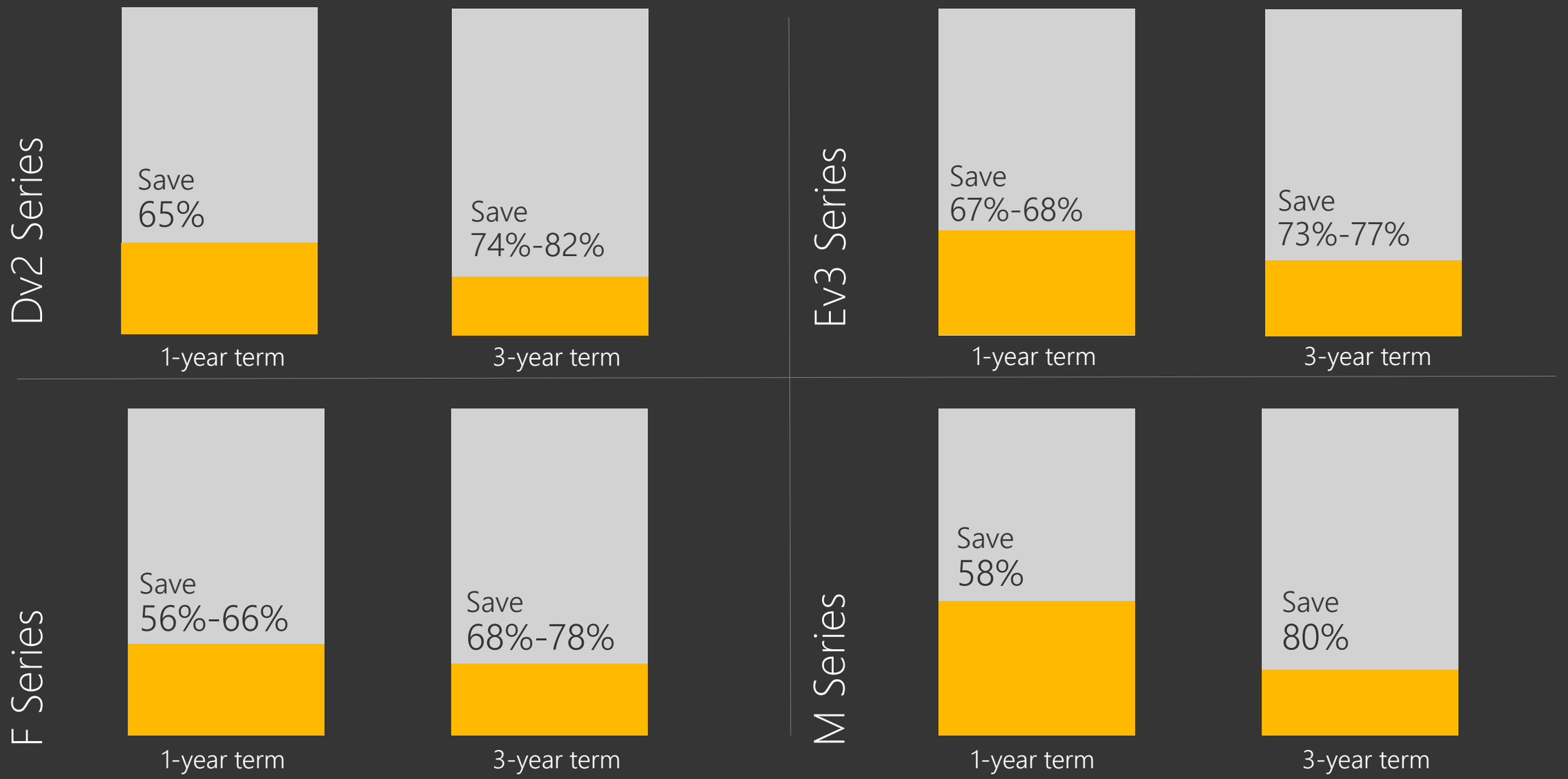
Typical savings with RI



Typical savings with RI



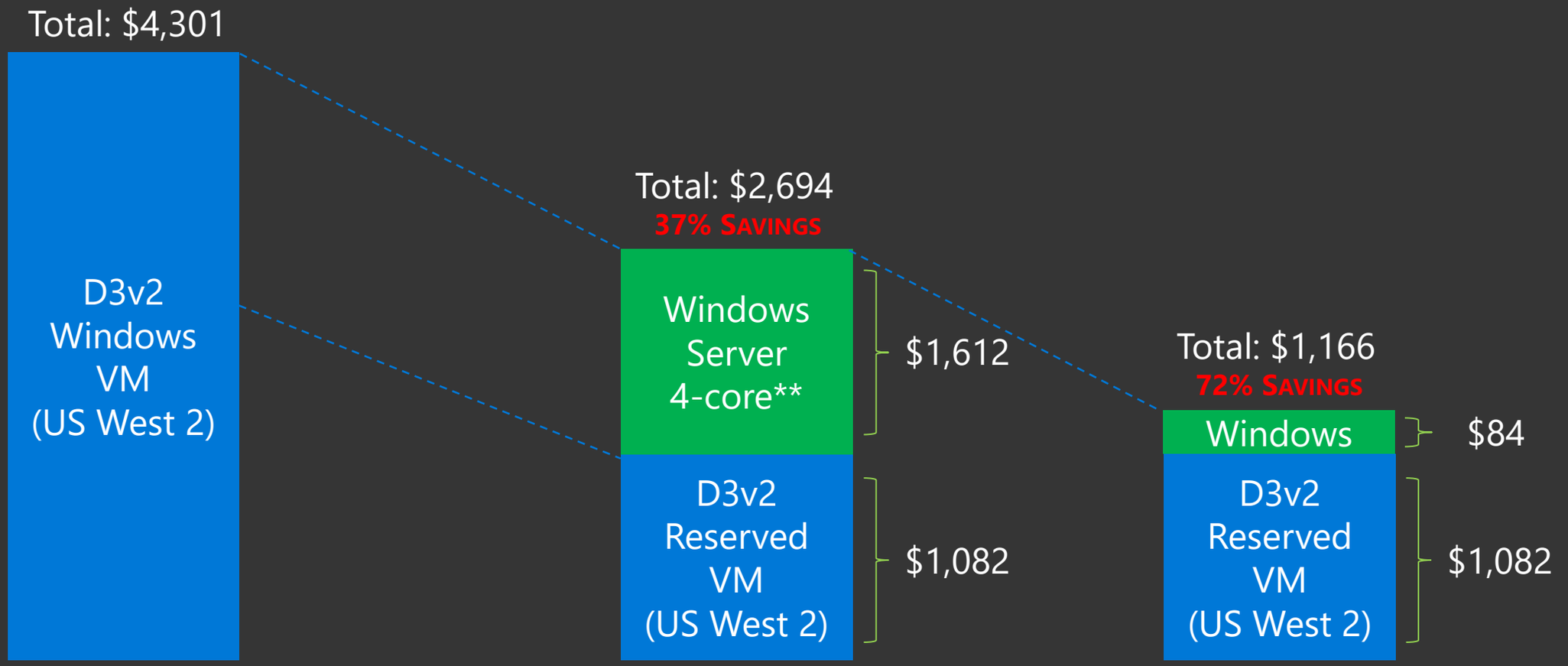
Typical savings with RI + Azure Hybrid Benefit



Base VM pay-as-you-go price Azure RI + Azure Hybrid Benefit price

1-year Reserved Virtual Machine Instance Savings

Scenario: Customer running a D3v2 Windows VM in US West 2 24x7x365



On-demand instance running 24x7x365

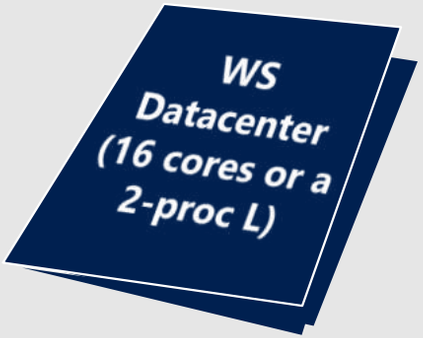
1-year Reserved Instance with Windows Subscription in Azure

1-year Reserved Instance + Azure Hybrid Benefit for Windows

*(2) 2-core Windows Server Standard Open Value Subscription

** Windows Server 4-core meter running 24x7x365 (only charged when VM is active)

Standard and Datacenter licenses with Software Assurance get up to two VMs per license

License with SA	VMs & cores granted	How they can be used
	Up to 2 VMs and up to 16 cores	Run virtual machines both on-premises and in Azure
	Up to 2 VMs and up to 16 cores	Run virtual machines either on-premises or in Azure

Flexibility to run configurations per your needs

With one two-Proc or 16-core license

Example 1: Maximize cores

VM #1 = D14 (16 vCore)

Total: 1 VM, 16 cores (max)

Example 2: Maximize VMs and cores

VM #1 = D13 (8 vCore)

VM #2 = D13 (8 vCore)

Total: 2 VMs (max), 16 cores (max)

Example 3: Mix VMs and cores

VM #1 = D2 (2 vCore)

VM #2 = D3 (4 vCore)

Total: 2 VMs (max), 6 cores

With two 2-Proc or 32 cores

Run VMs>16 cores by stacking licenses

Example: Stacking licenses with two 2-Proc or 32 cores

VM #1 = G5 (32 vCore)

Total: 1 VM, 32 cores (max)

Getting started with Azure Cost Management

Getting started with Azure Policy

https://aka.ms/GetPolicy

Azure Portal > Policy > Getting Started

Assign standard tier policy to enforce tags, policy to enable diagnostic logs & metrics & policy to audit use of managed disk

Assess state of compliance in Policy > Compliance view

Getting started with Azure Cost Management by Cloudyn

https://aka.ms/CloudynInfo

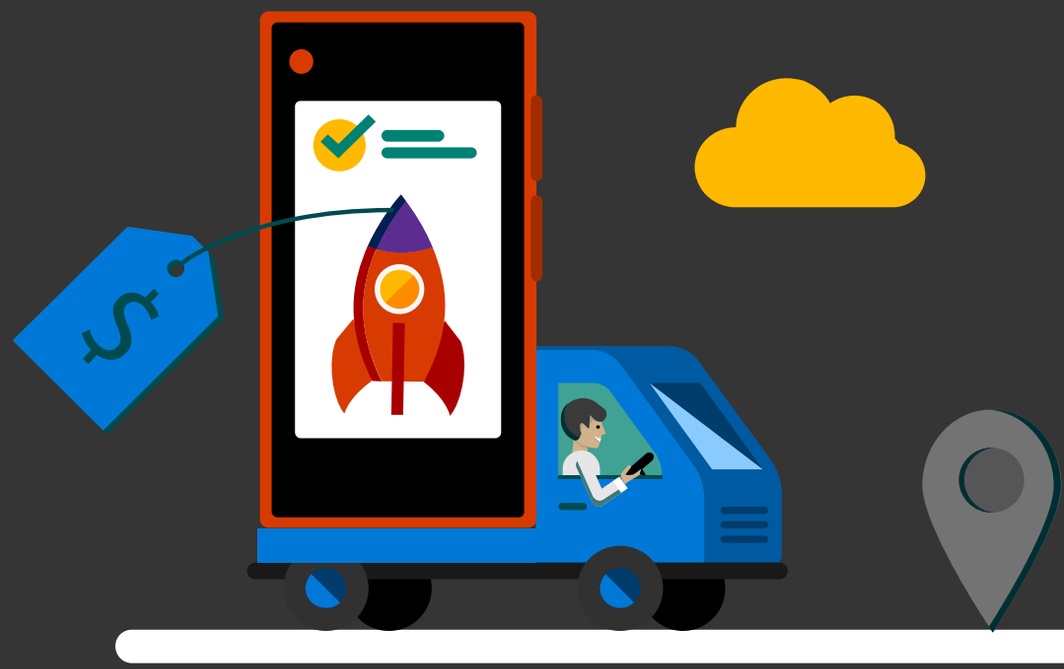
Azure Portal > Cost Management + Billing > Cost Management

Optimized onboarding experience for Azure customers and partners

Everybody starts with Azure free tier and a 30-day premium trial

Microsoft

Thanks!



Maciej Sobianek
https://www.linkedin.com/in/maciejsobianek/