EUROPEAN CLOUD SUMMIT 2024

Enable compliant development with Azure

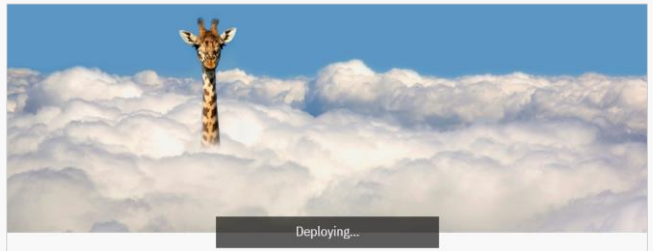
Martina Grom
Azure & Microsoft 365 MVP, Microsoft RD, CEO atwork
@magrom | martina.grom@atwork.at | www.atwork-it.com

Toni Pohl
Azure and Office Dev MVP, CTO atwork
@atwork | toni.pohl@atwork.at | www.atwork-it.com

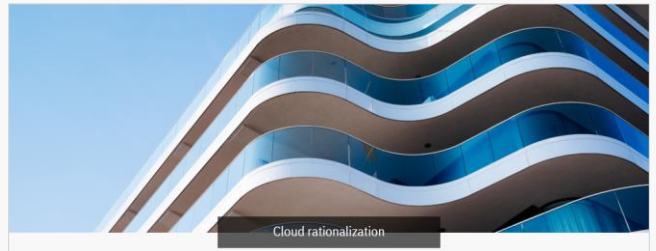
EUROPEAN CLOUD SUMMIT

EUROPEAN CLOUD SUMMIT

Agenda



How Azure works



Rationalization context

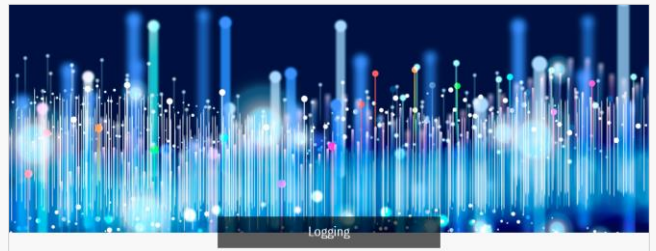
Microsoft Cloud Adoption Framework (CAF) for Azure

Set guardrails throughout your resources

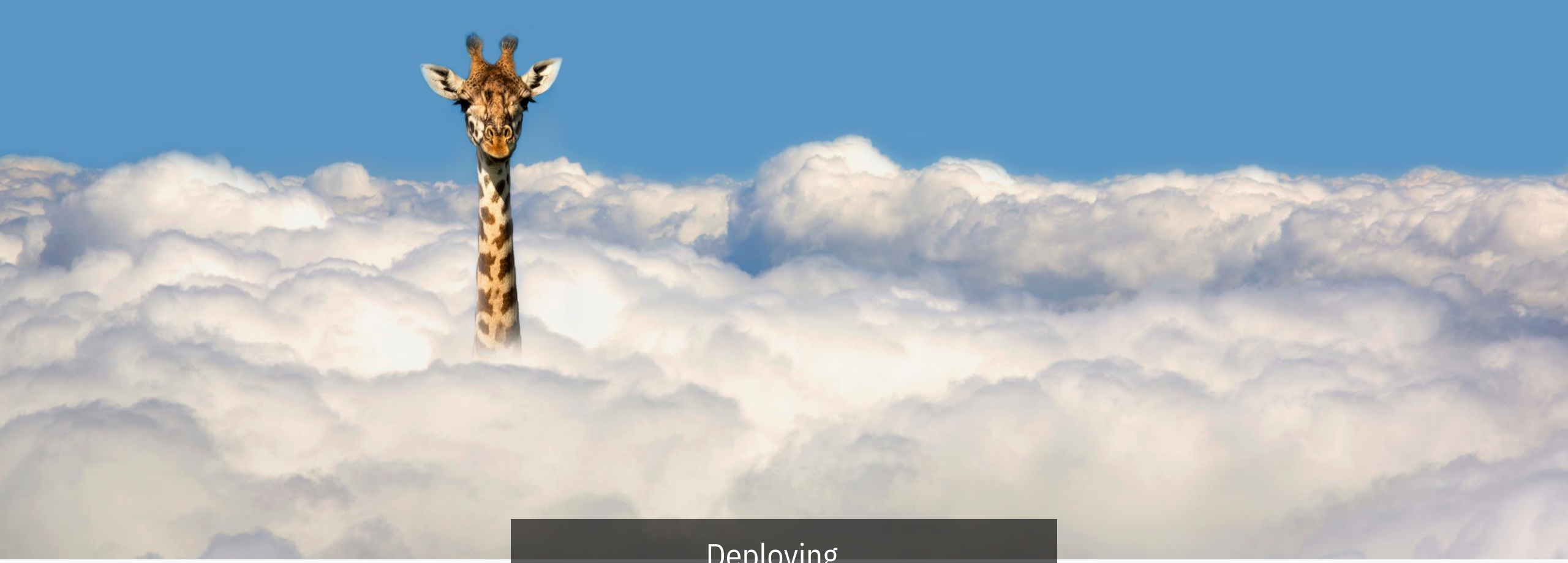
Requirements and challenges

Secure your Azure resources

Bicep & ARM

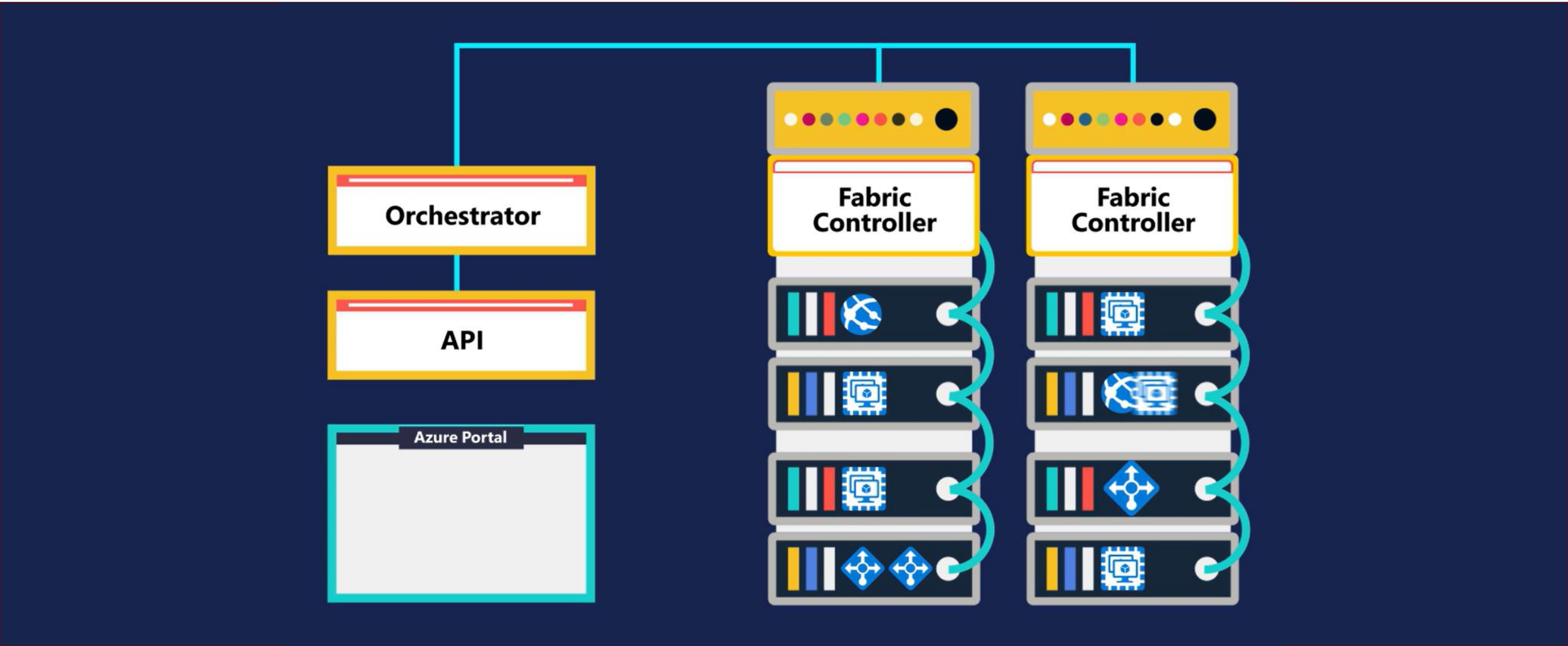


Monitoring & Alerts

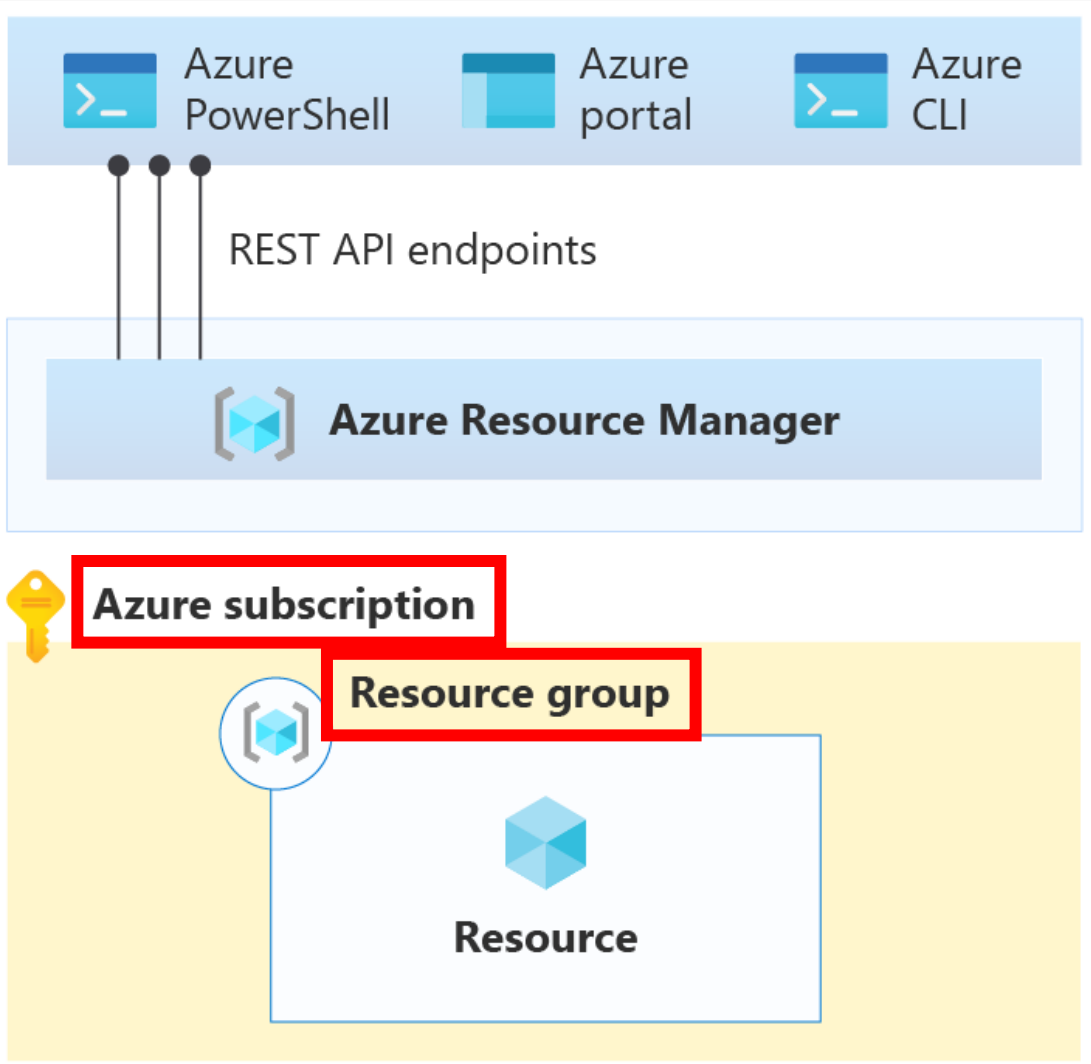


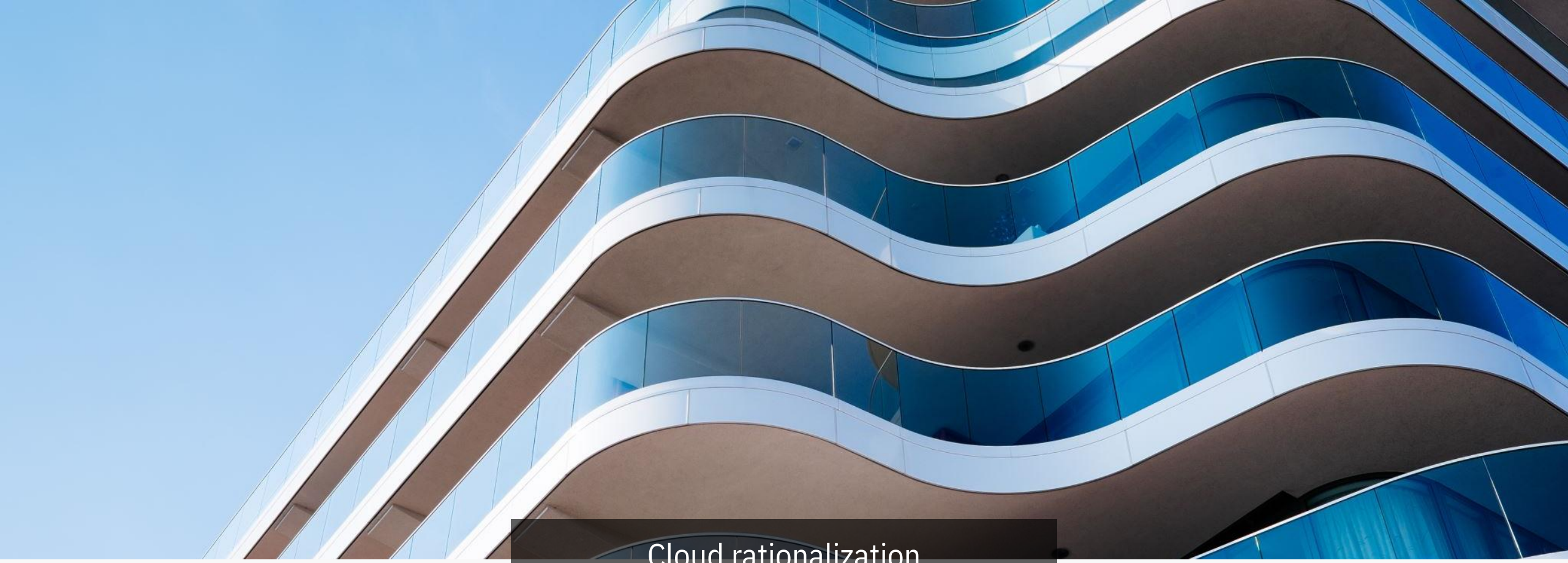
How Azure works

How Azure works



What does it mean for IT management



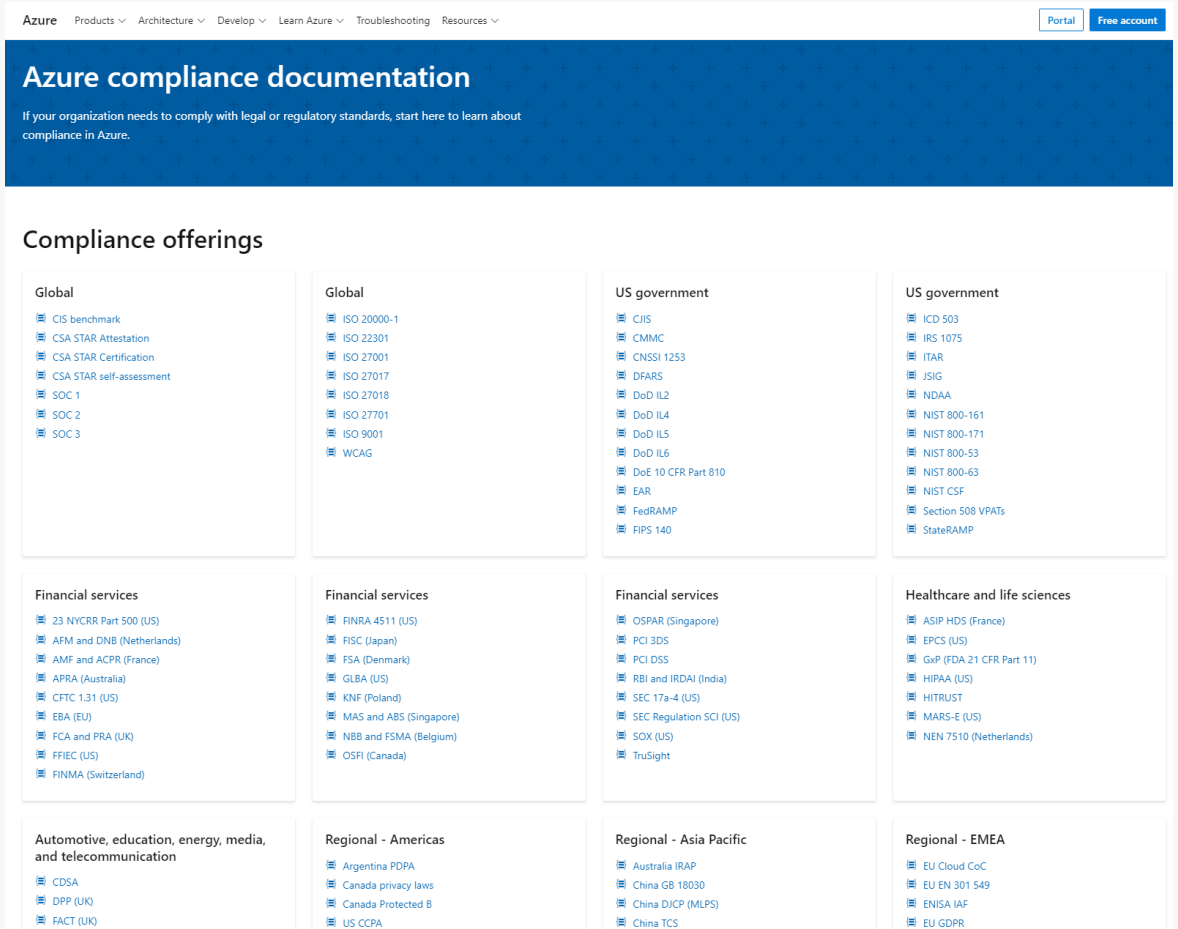


Cloud rationalization

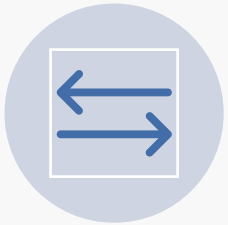
Rationalization context

Azure compliance documentation

https://learn.microsoft.com/en-us/azure/compliance/



Cloud rationalization with the 5 R´s



Rehost
Lift and shift migration

Refactor
Reduce the operational costs by using PaaS

Rearchitect
If some aging applications aren't compatible with cloud providers

Rebuild
For apps unsupported with the current business processes. Create a new code base to align with a cloud-native approach

Replace
Sometimes SaaS applications can provide all the necessary functionality

EUROPEAN CLOUD SUMMIT

Strategic Migration Assessment and Readiness Tool (SMART)

https://aka.ms/smarttool

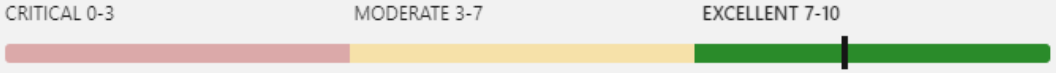
Understanding your SMART results

Based on your responses, the following results show your migration readiness across seven areas. The areas are chronological. Particularly focus on early phases, like business strategy, before moving on. Explore the recommendations to create your action plan and address gaps.

Your overall results

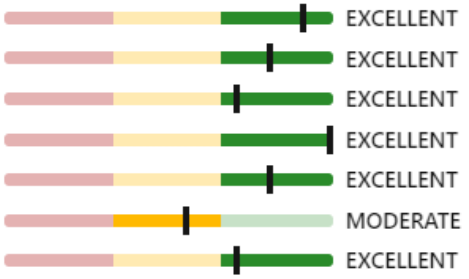
EXCELLENT

You are all set! Your results look strong and meet the necessary criteria for success.



Your result:
8/10

Categories that influenced your results



You can find out how to improve on individual categories by reviewing the recommendations below in the report.

Export to CSV

Improve your results

Our recommendations for improving your results are organized by category below.

Recommendations | Unanswered

Filter By- All

Business strategy EXCELLENT

1 recommended action — Show more

Planning EXCELLENT

3 recommended actions — Show more

Migration plan EXCELLENT

4 recommended actions — Show more

Technical skilling EXCELLENT

0 recommended actions — Show more

Landing zone EXCELLENT

4 recommended actions — Show more

Governance MODERATE

5 recommended actions — Show less

Results breakdown

CRITICAL 0-4 | MODERATE 4-7 | EXCELLENT 7-11

Your result: 6/11

5 recommended actions

	Recommendations	Priority	Notes
☐	Learn about Azure Cost Management and Billing.	0	Add a Note
☐	Learn about Azure Governance Visualizer (AzGovViz).	0	Add a Note
☐	Review the Cloud Adoption Framework governance methodology.	0	Add a Note
☐	Learn more at the FinOps Foundation.	0	Add a Note
☐	Learn how to incorporate Microsoft Defender for Cloud.	0	Add a Note

	A
1	Column1
2	Strategic Migration Assessment and Rea
3	
4	Understanding your SMART results
5	Your overall results
6	Business strategy
7	Planning
8	Migration plan
9	Technical skilling
10	Landing zone
11	Governance
12	Management
13	
14	Recommended next steps
15	Migration checklist
16	Azure migration and modernization cen
17	Microsoft Cloud Adoption Framework
18	
19	Category
20	Business strategy
21	Planning
22	Planning
23	Planning
24	Migration plan
25	Migration plan
26	Migration plan
27	Migration plan
28	Landing zone
29	Landing zone
30	Landing zone
31	Landing zone
32	Governance
33	Governance
34	Governance
35	Governance
36	Governance
37	----------
38	
39	Category
40	Business strategy

	G	H	I	
	olumn7	Column8	Column9	Colu
	eight	Context	CompleteY/N	Note
			N	
			N	
			N	
			N	
			N	
			N	
			N	
			N	
			N	
			N	
			N	
			N	
			N	
			N	
			N	
			N	

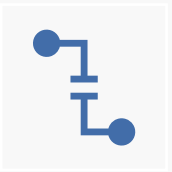
Microsoft Cloud Adoption Framework (CAF) for Azure

Start with Azure landing zones for modern application platforms

Guidance
The Cloud Adoption Framework guides the creation of all Azure environments using Azure landing zones.

Start (somewhere)
With Azure landing zones, you can start with a small implementation and expand over time.

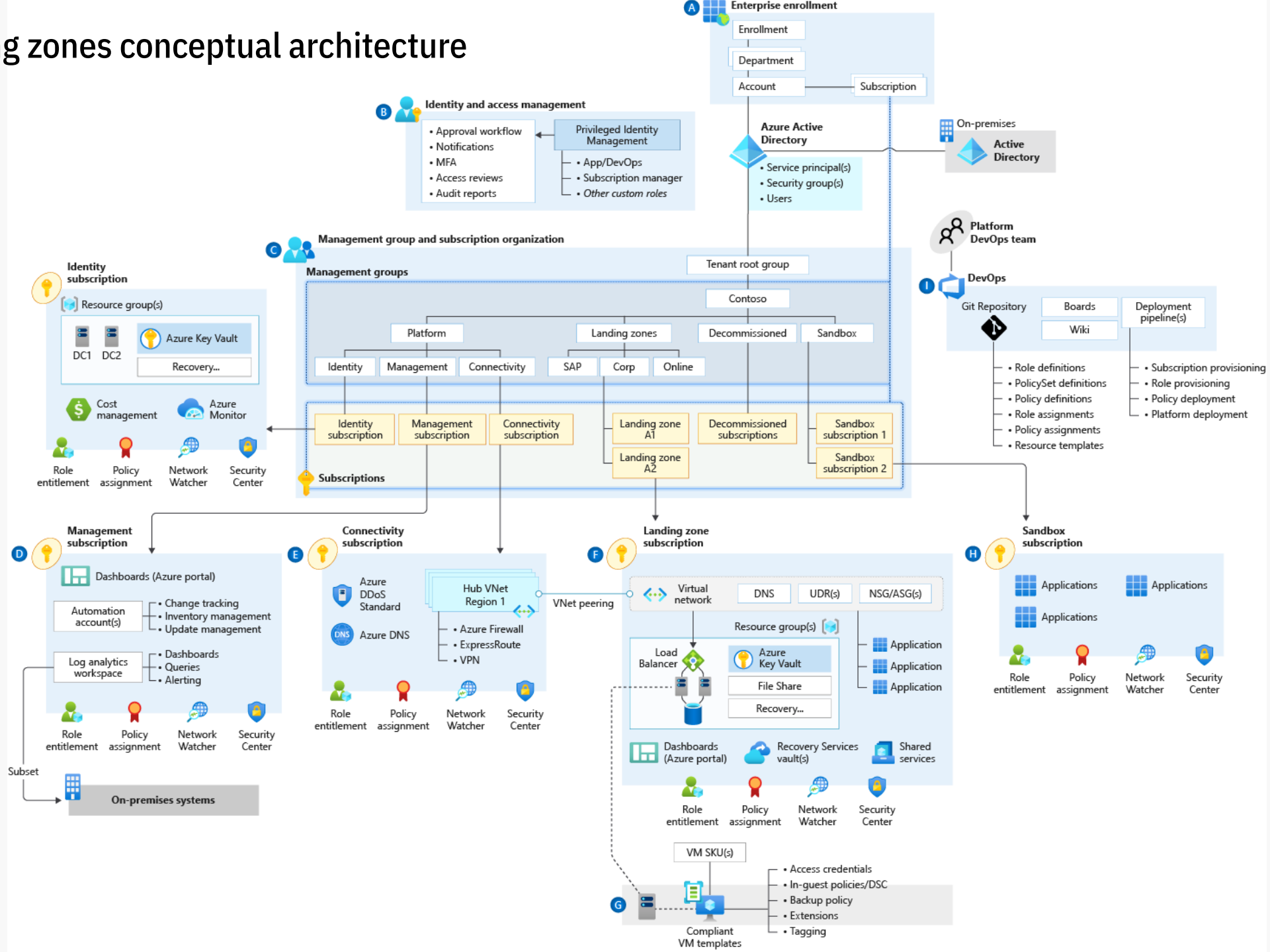
Strategy
Management groups and subscriptions are used to assign policies to the resources underneath them.



Separation
Subscriptions are the management boundary for governance and isolation of resources.

Standarization and Automation
Require developers to follow defined processes for deploying the hosts.

Azure landing zones conceptual architecture

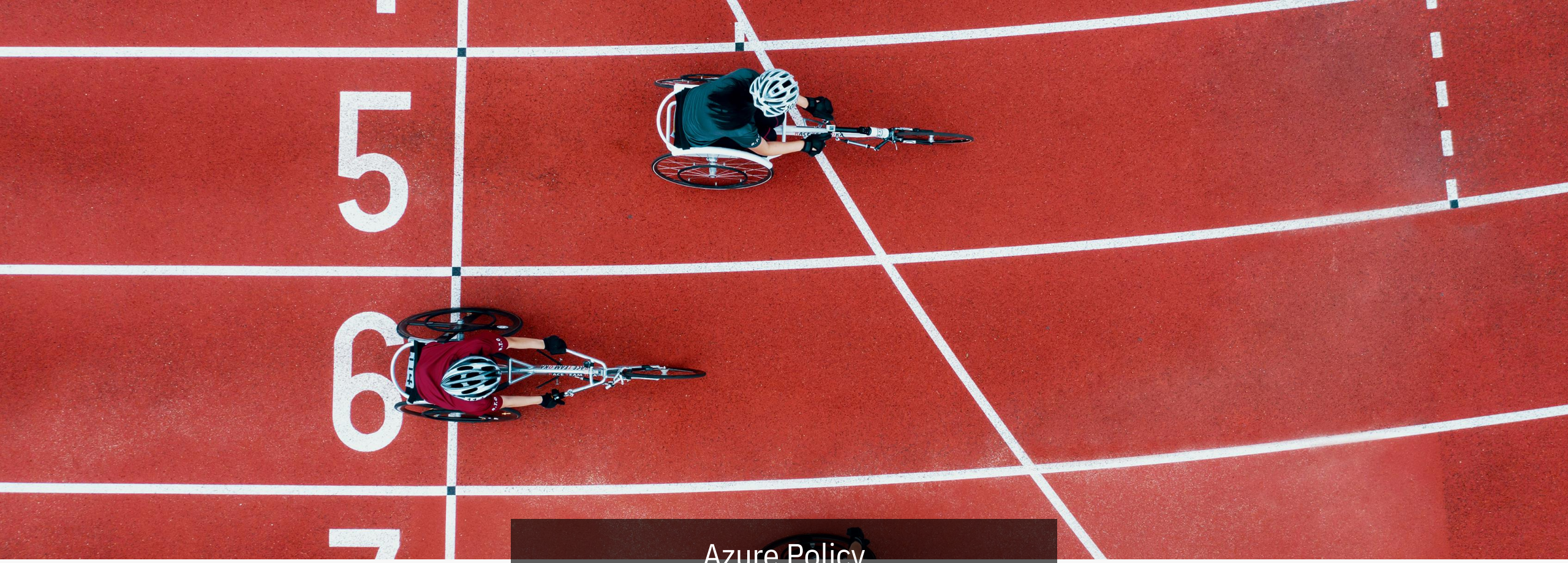


More resources

- Cloud Governance
  https://learn.microsoft.com/en-us/assessments/b1891add-7646-4d60-a875-32a4ab26327e/
- Cloud adoption antipatterns
  https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/antipatterns/antipatterns-to-avoid
- Azure compliance
  https://learn.microsoft.com/en-us/azure/compliance/
- SMART Tool
  https://aka.ms/smarttool

Management Groups

Name		Type	ID
Tenant Root Group	...	Management group	[redacted]
3 subscriptions			
2Disable	...	Management group	[redacted]
atwork root	...	Management group	[redacted]
MCPP Subscription	...	Subscription	[redacted]
PLAYGROUND	...	Management group	MPN
PROD	...	Management group	PROD



Azure Policy

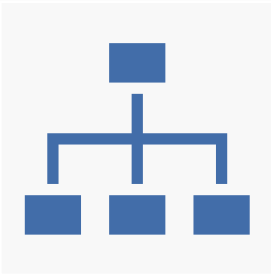
Set guardrails throughout your resources

EUROPEAN CLOUD SUMMIT

Best practices for working with Azure Policies to ensure effective governance, security, and compliance

Azure Policy
Implement proper guardrails and assess compliance across the organization.

Use RBAC
Remember that Azure Policy should not be used for tasks better handled by role-based access control (RBAC).



Define
It's essential to align policies with your organization's specific needs and compliance requirements.

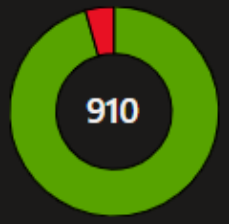
Azure Policies samples

Overall resource compliance ⓘ

96%

870 out of 910

Resources by compliance state ⓘ



870 - Compliant

40 - Non-compliant

Non-compliant initiatives ⓘ

0

out of 0

Non-compliant policies ⓘ

6

out of 10

Name ⇅	Scope ⇅	Compliance state ⇅	Resource compliance ⇅	Non-Compliant Re... ↓	Non-compliant pol...
ATW: Deploy Diagnostic Settings for Logic Apps to Log Analytics		Non-compliant	92% (321 out of 348)	27	1
ATW: App Service apps should use the latest TLS version		Non-compliant	89% (83 out of 93)	10	1
ATW: App Service Enforce HTTPS		Non-compliant	99% (109 out of 110)	1	1
ATW: Storage Account Require TLS 1.2		Non-compliant	99% (307 out of 308)	1	1
ATW: Storage accounts should have the specified minimum TLS v		Non-compliant	99% (307 out of 308)	1	1
ATW: Deploy - Configure diagnostic settings for Azure Key Vault t		Non-compliant	99% (68 out of 69)	1	1
ATW: Azure SQL Database should be running TLS version 1.2 or n		Compliant	100% (4 out of 4)	0	0
ATW: Audit SQL Database without elastic pool		Compliant	100% (69 out of 69)	0	0
ATW: Function apps should use the latest TLS version		Compliant	100% (19 out of 19)	0	0
ATW: Function apps should only be accessible over HTTPS		Compliant	100% (19 out of 19)	0	0

EUROPEAN CLOUD SUMMIT

Best practices for working with Azure Policies to ensure effective governance, security, and compliance

Use a Naming Convention for Policies
Consistently name your policies to make them easily identifiable and organized. A clear naming convention helps manage and maintain policies efficiently.

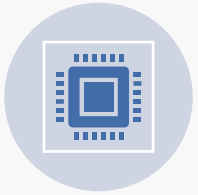
Block the Creation of Public IP Addresses
Set up an Azure Policy to prevent accidental creation of public IP addresses. This ensures that only authorized resources can have public endpoints.

Control Network Security Groups (NSGs)
Block NSGs from being applied to subnets directly. Instead, manage NSGs at the network interface or virtual machine level. This provides better control over network security.

Enforce Tagging Standards
Use Azure Policy to enforce tagging standards for resources. Tags help categorize and organize resources, making it easier to manage and track them.

Audit and Remediate Unused Resources
Regularly audit and remediate unused network interfaces, disks, or virtual machines. Azure Policy can help identify and enforce cleanup actions.

Monitor Changes to Critical Resources
Implement policies that monitor changes to critical resources. Detect unauthorized modifications promptly and take necessary actions.



Implement Just-in-Time (JIT) Access
Use Azure Security Center to enforce JIT access for virtual machines. This restricts access to specific time windows, reducing exposure to potential threats.

Azure Policies useful links

- Azure Policy Recommended Practices
  https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/azure-policy-recommended-practices/ba-p/3798024
- Insights and release/change tracking on Azure Governance capabilities
  https://www.azadvertizer.net/
- Policies included in Azure landing zones reference implementations
  https://github.com/Azure/Enterprise-Scale/wiki/ALZ-Policies
- Azure CAF Policies
  https://github.com/Azure/Enterprise-Scale

Azure Blueprints

- Simplify largescale Azure deployments by packaging key environment artifacts
- Can contain Azure Resource Manager templates, role-based access controls, and policies, in a single blueprint definition.

Important

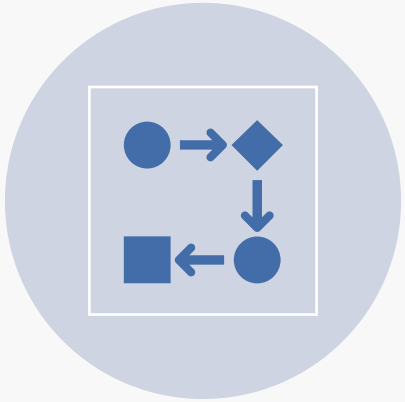
On July 11, 2026, Blueprints (Preview) will be deprecated. Migrate your existing blueprint definitions and assignments to Template Specs and Deployment Stacks. Blueprint artifacts are to be converted to ARM JSON templates or Bicep files used to define deployment stacks. To learn how to author an artifact as an ARM resource, see:

- Policy
- RBAC
- Deployments

Requirements and challenges

App Governance - Requirements and challenges

CLOUD APPS CAN BE A STARTING POINT FOR
PRIVILEGE ESCALATION
LATERAL MOVEMENT
EXFILTRATION OF DATA

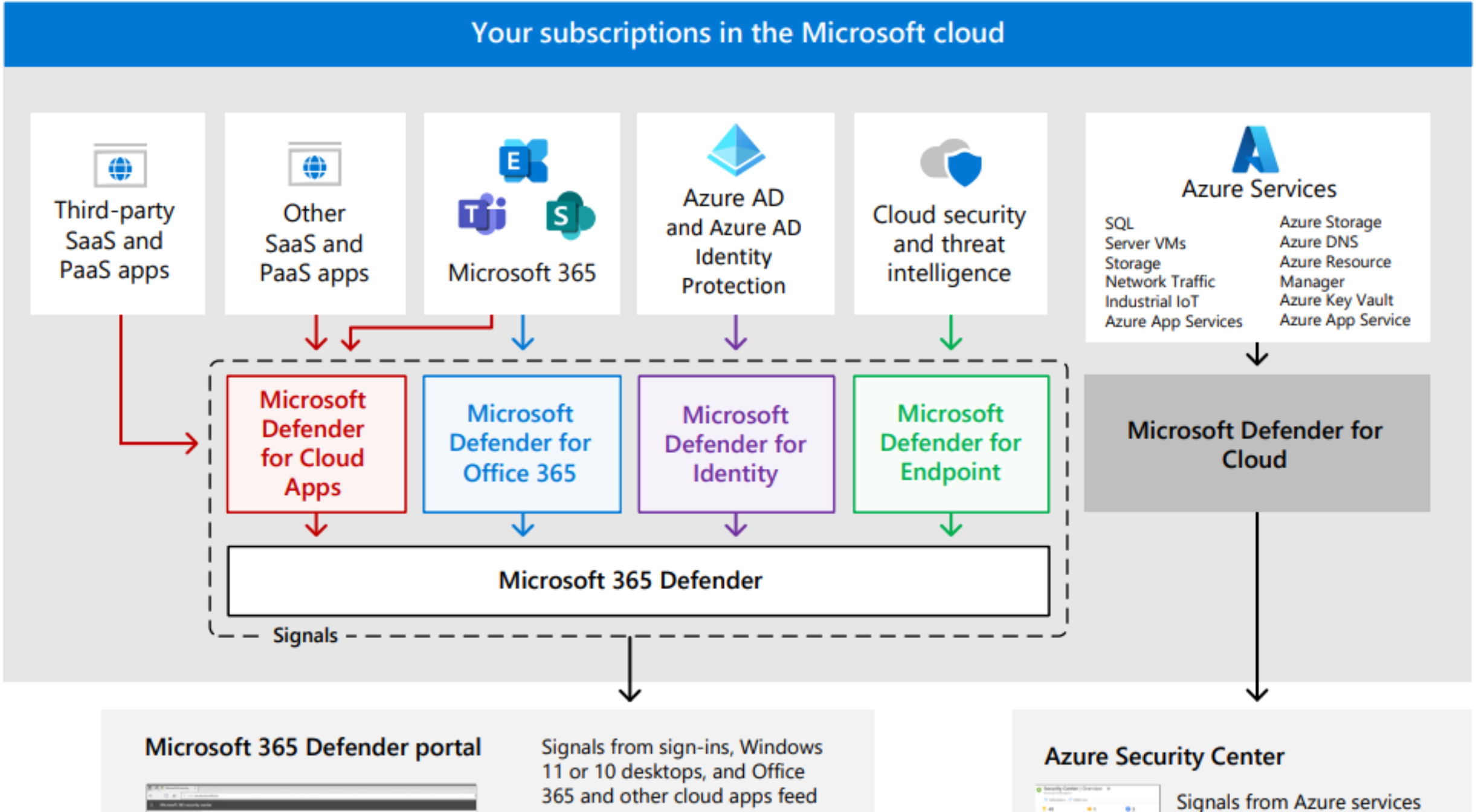


ALL OR NOTHING DOES NOT WORK
STAY CURRENT
START SMALL (BUT START)

APP GOVERNANCE
VISIBILITY
REMEDIATION
GOVERNANCE

Signals and security portals

Components and relationships



App protection

App governance
provides detailed information about an app's activity at the API level.

Entra ID
provides foundational app metadata and detailed information on sign-ins to apps.

Defender for Cloud Apps
provides app risk information.

Home
Incidents & alerts
Hunting
Action center
Threat analytics
Secure score
Learning hub

Endpoints
Search
Device inventory
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management

Email & collaboration
Investigations
Explorer
Submissions
Review
Campaigns
Threat tracker
Attack simulation training
Policies & rules

Cloud apps

App governance

Learn more about app governance

Overview | Apps | Alerts | Policies

Apps

70 apps in Microsoft 365
30 overprivileged apps
56 highly privilege apps

View all apps

Alerts

3K unresolved alerts
22 threat alerts
3K policy alerts

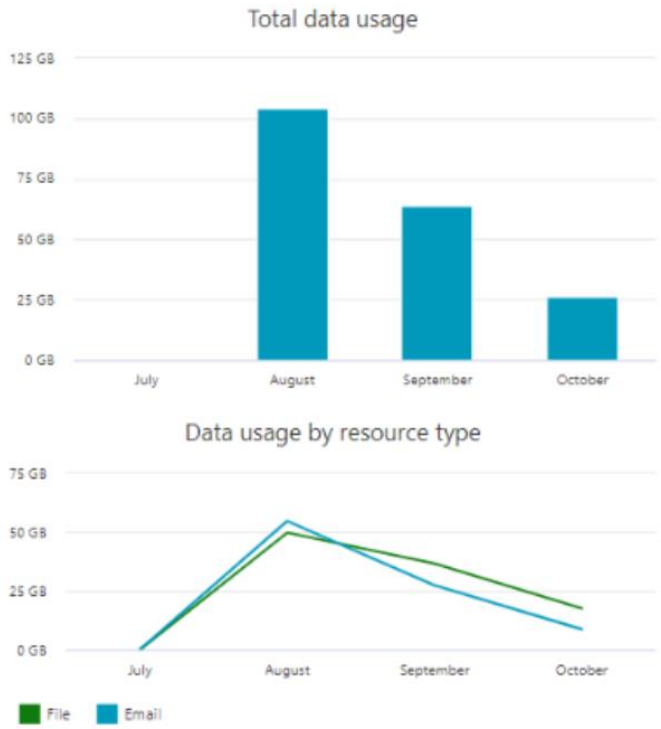
View all alerts

Latest alerts

Generated	Severity	Alert name	Source
10/28	Low	Policy [Sumit] Over...	Policy
10/28	Medium	Policy DemoPolicyT...	Policy
10/28	Medium	Policy Overprivileg...	Policy
10/28	Medium	Policy Overprivileg...	Policy
10/28	Medium	Policy DemoPolicyT...	Policy
10/28	Low	Policy Increase in a...	Policy
10/28	Low	Policy Overprivileg...	Policy
10/28	Low	Policy Overprivileg...	Policy
10/28	Medium	Policy Custom poli...	Policy
10/28	Medium	Policy DemoPolicyT...	Policy

View all alerts

Data usage (preview)



App categories

All apps | Highly privileged | Overprivileged | Unverified publisher | App-only permissions | New apps

App	Certification	Consent type	Privilege level	Data usage	Last modified
PostmanGraph	NA	Admin (88)	High	0 B	Aug 2, 2021 2:59 AM
AadAuditPipelineApp	NA	Admin (88)	High	0 B	Oct 4, 2021 3:52 PM
MaliciousApp	NA	Admin (88)	High	0 B	Oct 7, 2021 9:38 AM

Optimize app governance with policies

Secure app permissions
Find and stop apps that have unused permissions or permissions that might be too powerful.

Create policy

App governance

What's new Learn more

Get in-depth visibility and control over OAuth apps integrated with Azure Active Directory, Google, and Salesforce.

We've automatically turned on app governance. Learn more about our data security and privacy practices

Starting June 1, 2023, management of unused apps, unused credentials, and expiring credentials will only be available to app governance customers with Microsoft Entra Workload Identities Premium. Try Workload Identities

Overview | Azure AD | Alerts | Policies

Apps

207 apps found

44 overprivileged apps

41 highly privileged apps

View all apps

Incidents

4 unresolved incidents

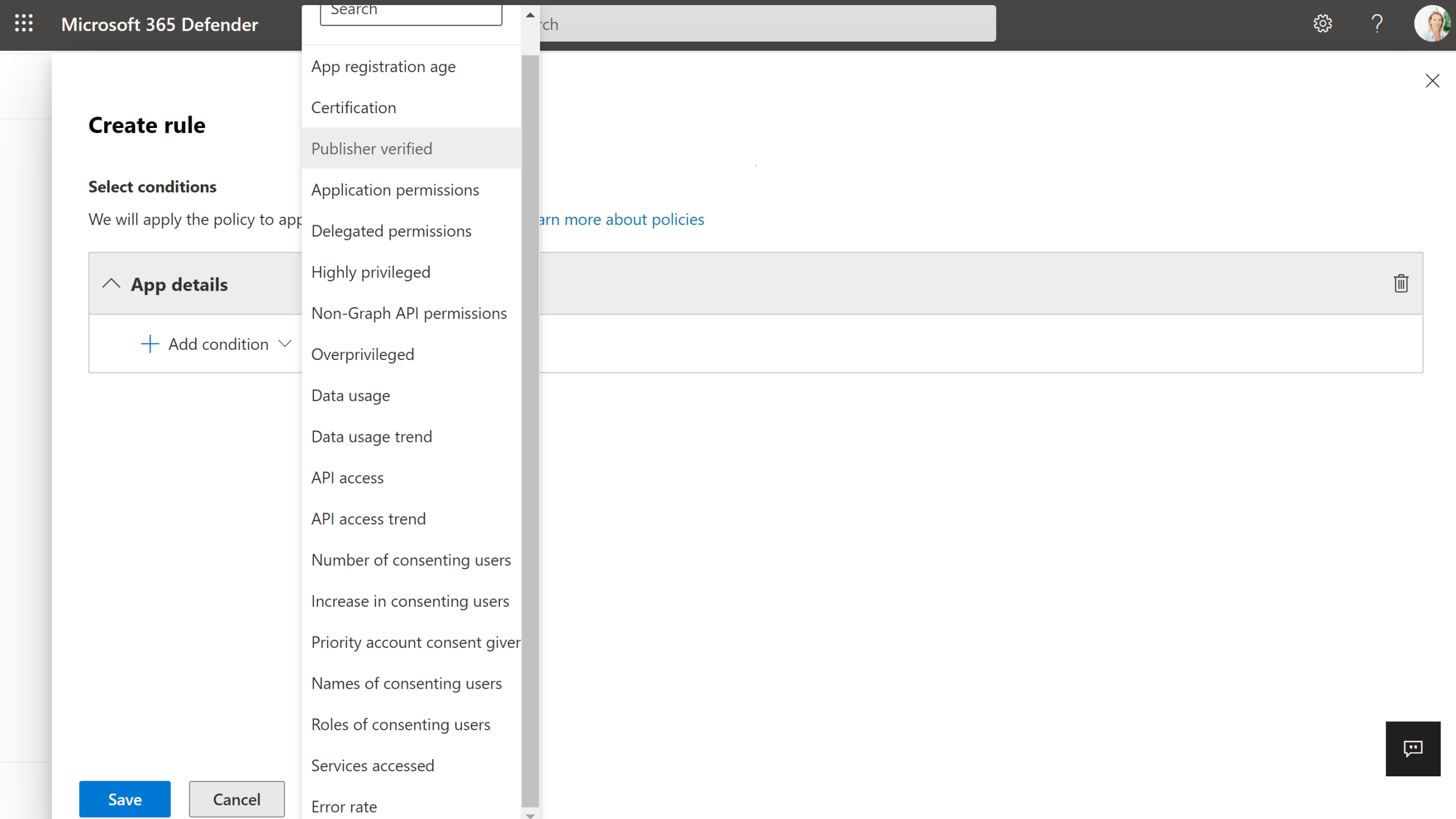
3 threat incidents

1 policy incidents

View all incidents

Latest incidents

Last Activity	Severity	Incident name	Source
5/14/2024	Medium	High volume of emai...	Detection
5/5/2024	Medium	App metadata associ...	Detection
1/16/2024	Medium	Unusual activity from...	Policy
12/11/2023	Medium	App metadata associ...	Detection


Microsoft 365 Defender
Search
App registration age
Certification
Publisher verified
Application permissions
Delegated permissions
Highly privileged
Non-Graph API permissions
Overprivileged
Data usage
Data usage trend
API access
API access trend
Number of consenting users
Increase in consenting users
Priority account consent giver
Names of consenting users
Roles of consenting users
Services accessed
Error rate
Create rule
Select conditions
We will apply the policy to app
arn more about policies
App details
Add condition
Save
Cancel

Cloud Hub	Enabled	Yes	Mixed	Admin	atwork GmbH	Jul 17, 2023 7:03 AM

Home
Incidents & alerts
Hunting
Action center
Threat analytics
Secure score
Learning hub

Endpoints
Search
Device inventory
Vulnerability management
Partners and APIs
Evaluation & tutorials
Configuration management

Email & collaboration
Investigations
Explorer
Submissions
Review
Campaigns
Threat tracker
Attack simulation training

App governance

Overview | Apps | Alerts | Policies

Filter | Save the query | Reset | Filters

Category: **All apps**

App name	Added on	Last modified	Consent type	Data usage (previe
AadAuditPipelineApp	3/7/2020	10/4/2021	Admin (88)	0 B (0%)
Adobe Sign for Micro...	8/3/2021	8/4/2021	User (1)	0 B (0%)
alfalfa4	9/3/2020	7/15/2021	Admin (88)	0 B (0%)
app	8/12/2020	7/7/2021	Admin (88)	0 B (0%)
appadracarbTecnicas	8/10/2021	8/10/2021	Admin (88)	0 B (0%)
appadracarbTecnicas1	8/10/2021	8/10/2021	Admin (88)	4.18 GB (-64.4%)
Audit Log Generator	2/22/2021	7/7/2021	Admin (88)	0 B (0%)
AuditGapClientApp	3/16/2021	7/7/2021	Admin (88)	0 B (0%)
AuditLogsConnector	3/24/2021	8/2/2021	Admin (88)	0 B (0%)
AZ500 app1	8/10/2021	9/22/2021	Admin (88)	4.83 GB (0%)
callingapp	7/29/2020	7/7/2021	Admin (88)	0 B (0%)
Cloud Sync	8/27/2020	7/7/2021	User (1)	0 B (0%)
Contoso File Parser	7/27/2021	9/27/2021	Admin (88)	0 B (0%)
Contoso Organizer	4/1/2021	7/7/2021	User (1)	0 B (0%)

Contoso Organizer

Details | Data usage (preview) | Users | Permissions

App name
Contoso Organizer

App ID
043768e9-2b46-4bee-9d73-0ee5b140a2dd
View in Azure AD

Added on
4/1/2021

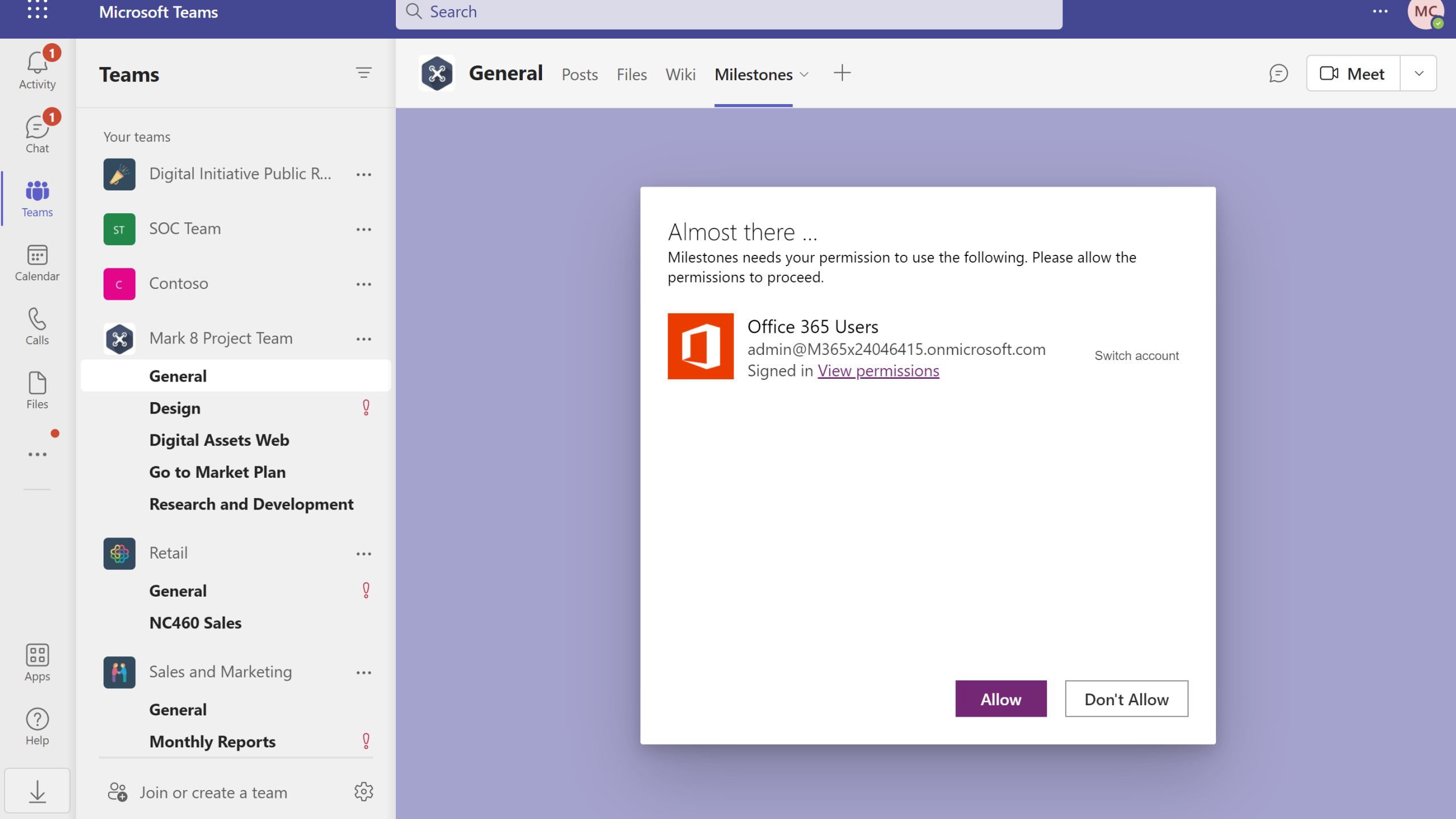
Last modified
7/7/2021

App status
Enabled

Last action
-

Publisher verification
Contoso
Learn more about publisher verification

Certification
Not certified
Learn more about Microsoft 365 certification


Microsoft Teams
Search
MC
Activity
Chat
Teams
Calendar
Calls
Files
Apps
Help
Teams
Your teams
Digital Initiative Public R...
SOC Team
Contoso
Mark 8 Project Team
General
Design
Digital Assets Web
Go to Market Plan
Research and Development
Retail
General
NC460 Sales
Sales and Marketing
General
Monthly Reports
Join or create a team
General
Posts
Files
Wiki
Milestones
Meet
Almost there ...
Milestones needs your permission to use the following. Please allow the permissions to proceed.
Office 365 Users
admin@M365x24046415.onmicrosoft.com
Signed in View permissions
Switch account
Allow
Don't Allow

Home
Incidents & alerts
Hunting
Actions & submissions
Threat analytics
Secure score
Learning hub
Trials
Assets
Identities
Endpoints
Device inventory
Vulnerability management
Partners and APIs
Evaluation & tutorials

Incidents

Email notification | New incidents queue

Most recent incidents and alerts

Export | Search for name or ID | Filter | Customize columns | 1 Week

Filters: Status: New +1 | Severity: High +2 | Service sources: App governance Policy +1

Incident name	Incident Id	Tags	Severity	Investigation state	Categories
App with numerous errors	703		Medium	1 investigation states	Suspicious activi
App made unusual email searches activities	685		Medium	1 investigation states	Collection

- **Policy template**
- Name and severity
- Scope and conditions
- Actions
- Status
- Review and finish

Choose a policy template

Create your policy from a template or choose "Custom" to start from scratch. You'll be able to add conditions and specify actions.

Search by template name

Category	Template
Usage	Overprivileged app
Permissions	New app with non-Graph API permissions
Certification	New highly privileged app
Activity	
Custom	

Next

Cancel

Explorer
Review
Campaigns
Threat tracker
Exchange message trace
Attack simulation training
Policies & rules

Cloud apps
Cloud discovery
Cloud app catalog
OAuth apps
App governance
Files
Activity log
Governance log

Cloud Discovery

Win10 Endpoint Users | Last 30 days | Actions

Updated on May 30, 2023, 4:05 PM

Dashboard | Discovered apps | Discovered resources | IP addresses | Users | Devices

Apps	IP addresses	Users	Devices
391	188	16	14

Traffic

224.9 GB

44.8 GB

180.0 GB

App categories 1-5 of 40 Traffic

Sanctioned Unsanctioned Other

Collaboration	57.5 GB
Hosting services	38.5 GB
Webmail	20.9 GB
Cloud storage	12.3 GB

Risk l... ategories by Traffic

Traffic from high risk apps

Traffic

Discove... of 391 >

All categories | Traffic

Sanctioned | Unsanctioned | Other

Microsoft SharePo...	53.4 GB
Azure CDN Edge ...	34.7 GB
Microsoft Exchang...	20.9 GB
Microsoft OneDriv...	12.2 GB
Garmin	9.7 GB
Netflix	9.2 GB
CloudFlare	9.1 GB
Microsoft Online S...	9.0 GB
Azure DevOps Ser...	7.1 GB
GitHub	5.3 GB
Adobe	5.3 GB
Fastly	5.0 GB
Microsoft Support	4.4 GB

Top e... User by Traffic

User	Total
[redacted]	49.2 GB
[redacted]	32.9 GB
[redacted]	24.2 GB
[redacted]	24.1 GB
[redacted]	23.4 GB

Apps headquart... All categories

Moving workloads and data to the cloud?

CUSTOMER:
"THE (PUBLIC) CLOUD IS NOT SAFE."

CONSULTANT:
"AZURE IS SECURE BY DEFAULT."

MICROSOFT:
"WE HAVE ENTRA ID, AZURE SECURITY CENTER, KEY VAULT, VNETS, BASTION, WAF, & MANY MORE SERVICES..."

Managed Identities

Secure your Azure resources

Azure Key Vault & Managed Identities

- The safe place to store credentials and secrets like certificates and connection strings.
- Use Managed identities if possible

I can use Managed Identities when…

As a developer, I want to build an application using

Source:

Azure Resources
Azure VMs
Azure App Services
Azure Functions
Azure Container instances
Azure Kubernetes Service
Azure Logic Apps
Azure Storage
….

that accesses

Target:

Any target that supports Azure Active Directory Authentication:
- **Your applications**
- **Azure Services:**
  - Azure Key Vault
  - Azure Storage
  - Azure SQL…

without having to manage any credentials!

For example, I want to build an application using ***Azure App Services*** that accesses **Azure Storage** without having to manage any credentials.

Managed Identity types – when use what?

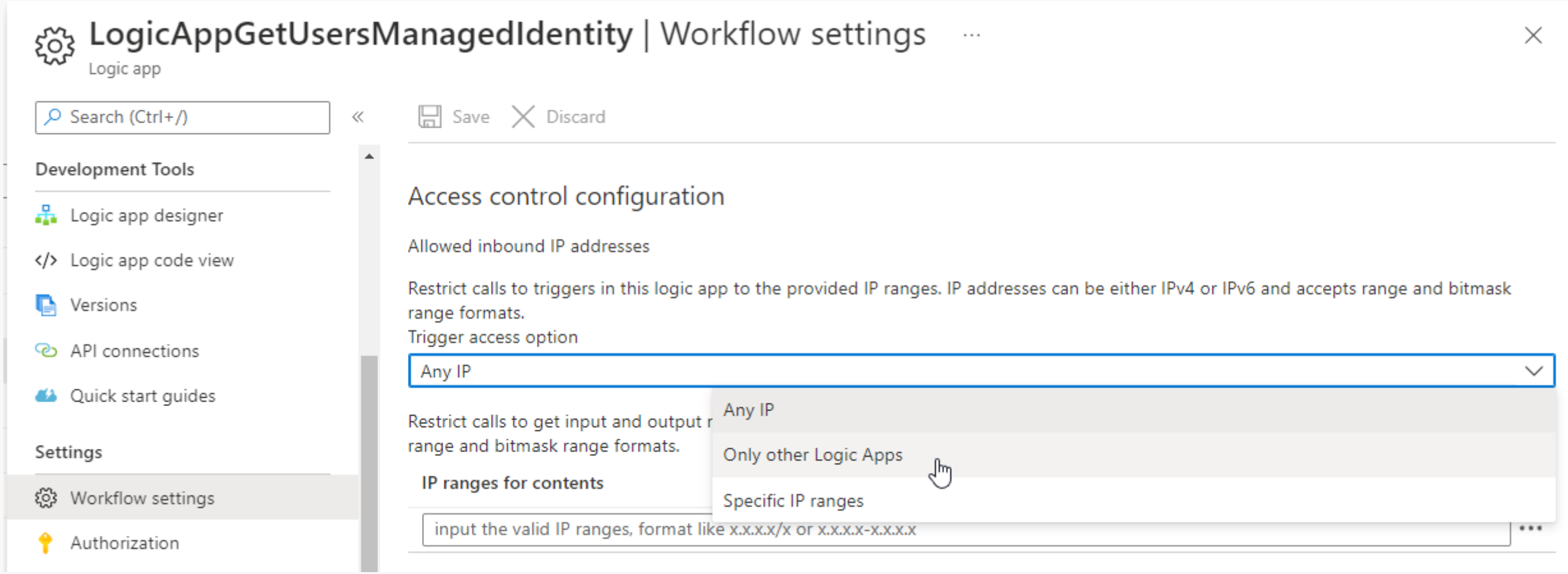
System-assigned
Tied to the lifecycle of that service instance.
Only that Azure resource can use this identity to request tokens from Azure AD.

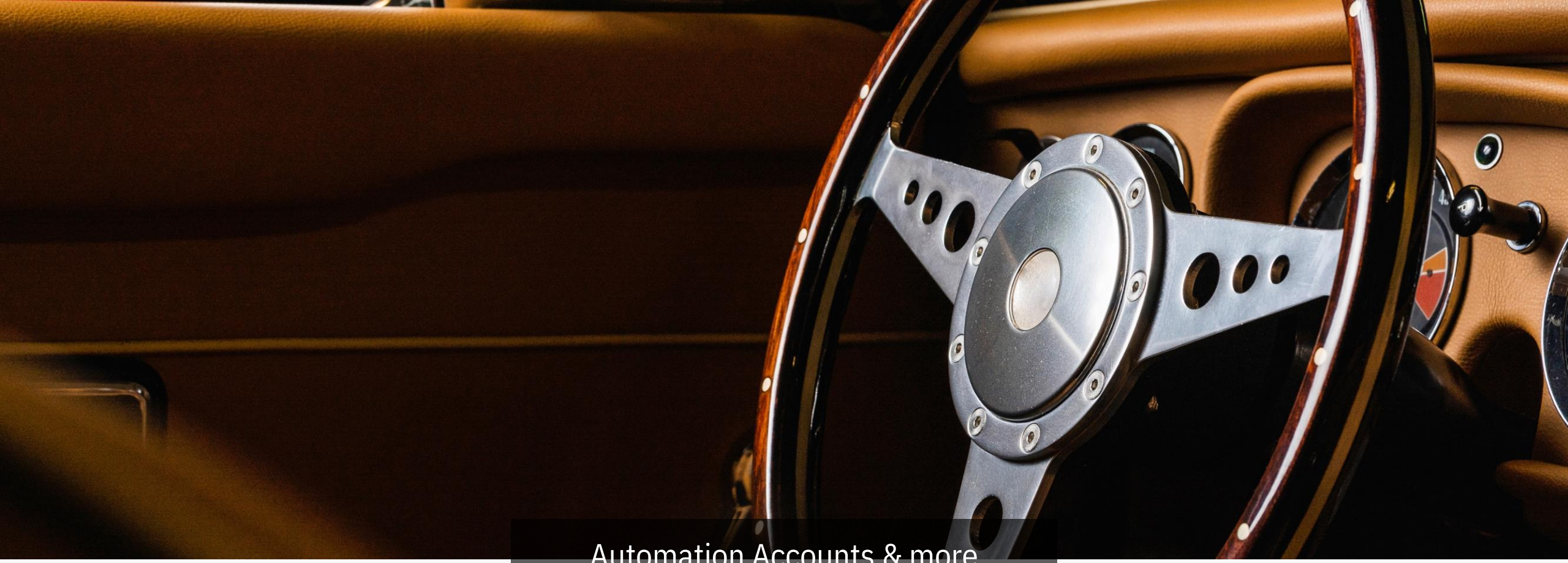
User-assigned
Managed identity as a standalone Azure resource managed separately from the resources that use it.
Assign it to one or more instances of an Azure service

Azure Logic Apps

- Perfect for no/low code business processes
- Secure connections + Managed Identity + Key Vault

Azure Logic Apps: Secure the trigger





Automation Accounts & more

Apps & Scripts Security & Deployment

Automation Accounts

- Migrate your PowerShell scripts to the cloud
- Secure the access
  (Connections, Managed Identity, Key Vault, Firewall)

Create a self-signed certificate with Powershell

```
# Certificate (PFX)
$cert = New-SelfSignedCertificate `
    -NotAfter $(Get-Date).AddYears($certYears) `
    -Type SSLServerAuthentication `
    -FriendlyName 'MyAuthCert' `
    -Subject 'CN=MyCompany' `
    -CertStoreLocation 'Cert:\CurrentUser\My' `
    -KeySpec KeyExchange
```

Access Key Vault from App config settings

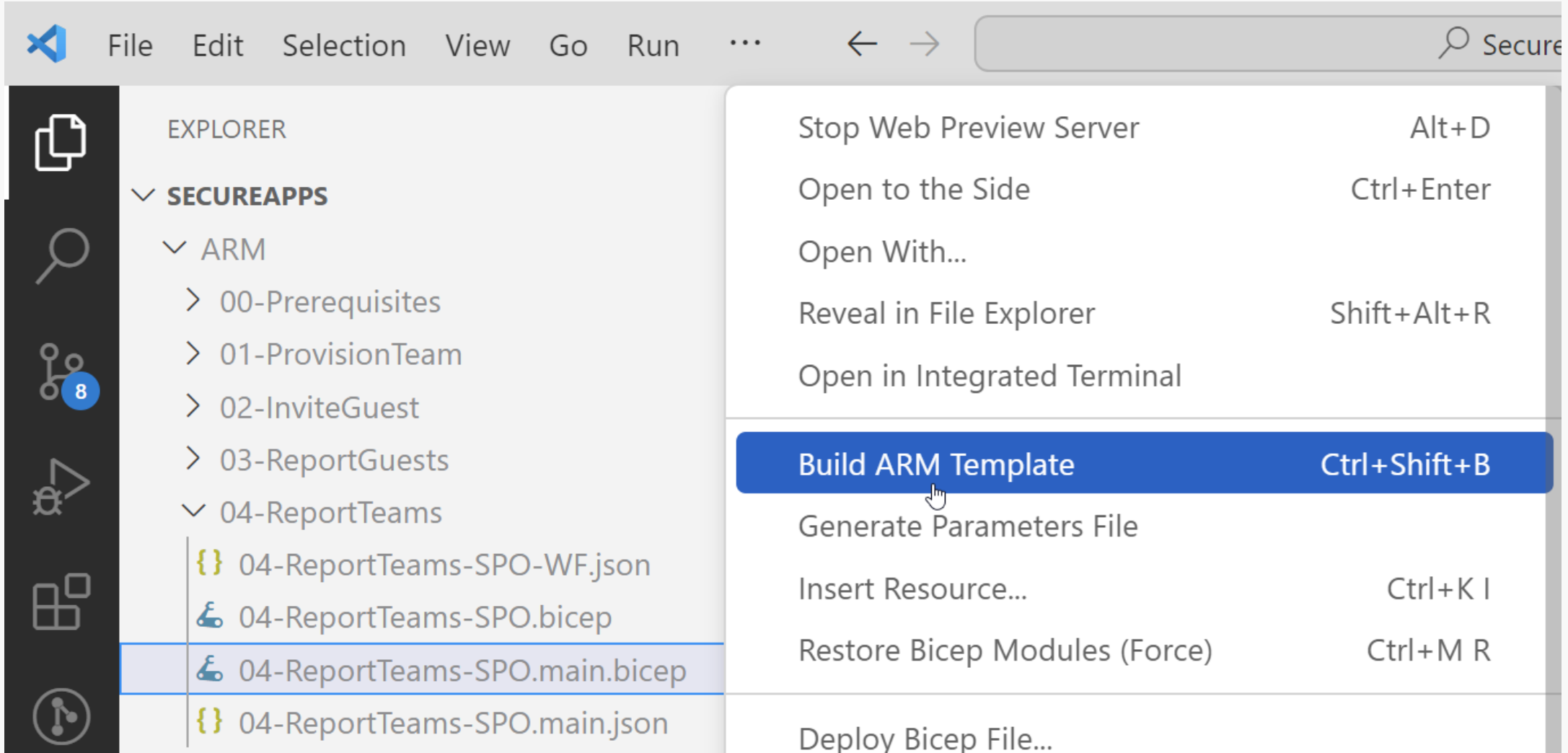
```
@Microsoft.KeyVault(SecretUri=https://
m365conf.vault.azure.net/secrets/secret1/)
```

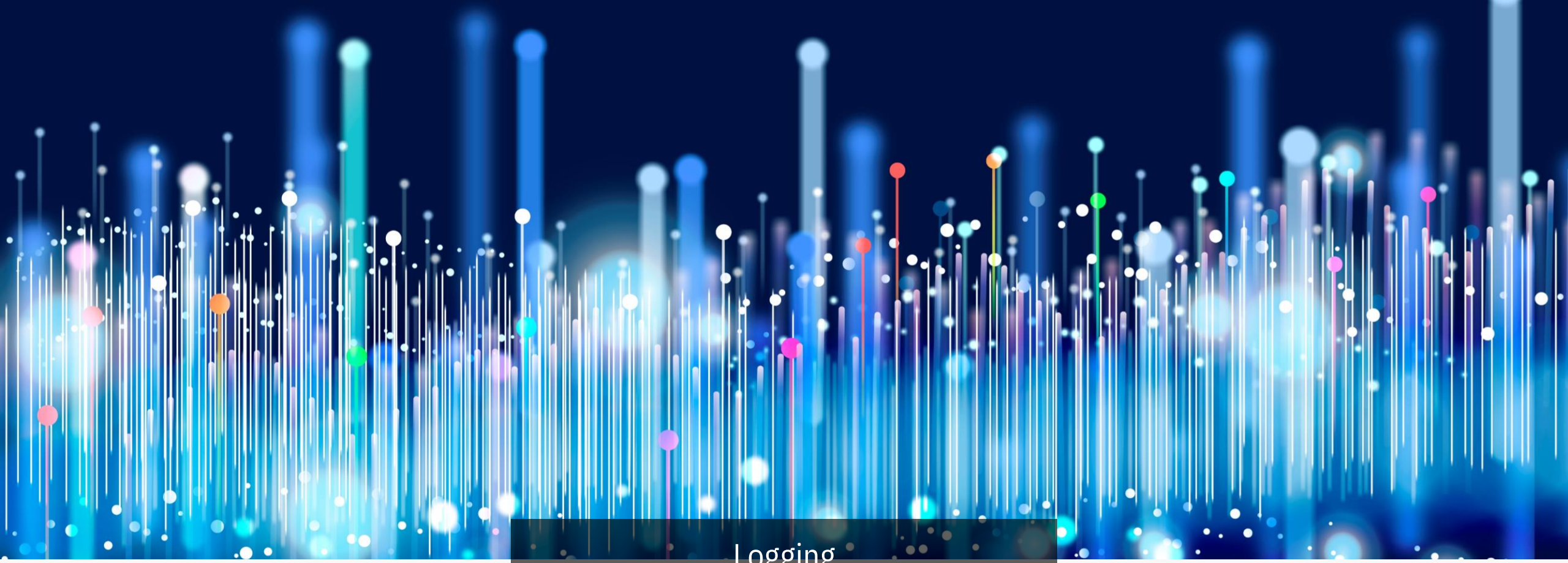
https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references

Deployment

Bicep & ARM

Build ARM template from a bicep script





Logging

Monitoring & Alerts

collabsummit | Logs

Log Analytics workspace

Errors - collabsu... *

Feedback | Queries

collabsummit | Select scope | Run | Time range : Set in query | Save | Share | New alert rule | Export | Pin to

```
1  // Errors
2  AzureDiagnostics
3  | where TimeGenerated > ago(30d)
4  | where resource_resourceGroupName_s == "RG-CollabSummit"
5  | where Category == "WorkflowRuntime"
6  | where resource_workflowName_s == "GetUsers"
7  | where status_s == "Failed"
8  | order by TimeGenerated desc
9
```

Results | Chart

TimeGenerated [Amsterdam, Berlin, Bern, Rome, Stockh...	ResourceId	Category	ResourceGroup	SubscriptionId
5/23/2023, 10:46:17.001 AM	/SUBSCRIPTIONS/0C5D1D4F-64E3-47A0-ACE1-25494A794C...	WorkflowRuntime	RG-COLLABSUMMIT	0c5d1d4f-64e3-47a0-ace1-254
5/23/2023, 7:20:20.795 AM	**/SUBSCRIPTIONS/0C5D1D4F-64E3-47A0-ACE1-25494A794...**	**WorkflowRuntime**	**RG-COLLABSUMMIT**	**0c5d1d4f-64e3-47a0-ace1-254**

TenantId	1633320f-2c09-4824-a4aa-f3b1281626ba
TimeGenerated [UTC]	2023-05-23T05:20:20.795587Z
ResourceId	/SUBSCRIPTIONS/0C5D1D4F-64E3-47A0-ACE1-25494A794CBF/RESOURCEGROUPS/RG-COLLABSUMMIT/PROVIDERS/MICROS
Category	WorkflowRuntime
ResourceGroup	RG-COLLABSUMMIT
SubscriptionId	0c5d1d4f-64e3-47a0-ace1-25494a794cbf
ResourceProvider	MICROSOFT.LOGIC
Resource	0858516787665389161292281272 9CU42
ResourceType	WORKFLOWS/RUNS
OperationName	Microsoft.Logic/workflows/workflowRunCompleted
Level	Error
status_s	Failed

Schema and Filter | Columns

1s 88ms | Display time (UTC+02:00) | Query details | 2 - 3 of 14

Summary

Staying compliant and secure in Azure

Secure your Enterprise applications with Azure

IDENTIFY YOUR USE CASES

USE BUILT-IN SERVICES & AZURE ADVISOR

ALWAYS CONSIDER PAAS

APPS (MANAGED IDENTITIES, CERTIFICATES, ...)

KEY VAULT FOR SECRETS

USE BUILT-IN FUNCTIONALITY (AUTOMATION ACCOUNTS, CONNECTIONS ...)

LOGGING & MONITORING / ALERTS

Best practises

- Secure your Entra ID (MFA, MFA, MFA ☺)
- Zero Trust
- Secure your Azure subscriptions
- Implement the Azure Cloud Adoption Framework (CAF)
- Work with Azure policies (best on Management Groups)
- Use a central code repository
- Use Build and Deploy Pipelines in Azure DevOps (or GitHub Actions, or other CI/CD pipelines)
- Train your users / developers how to use the deployment processes
- Automate as much as possible
- Have monitoring & alerting tools in place (Security is not a permanent state, but a living process)

THANK YOU,
YOU ARE AWESOME ❤️

PLEASE RATE THIS SESSION IN THE MOBILE APP.

Martina Grom
Azure & Microsoft 365 MVP, Microsoft RD, CEO atwork
@magrom | martina.grom@atwork.at | www.atwork-it.com

Toni Pohl
Azure and Office Dev MVP, CTO atwork
@atwork | toni.pohl@atwork.at | www.atwork-it.com | github.com/tonipohl/SecureAppsWithAzure