



Secure and manage your Enterprise applications with Microsoft Azure



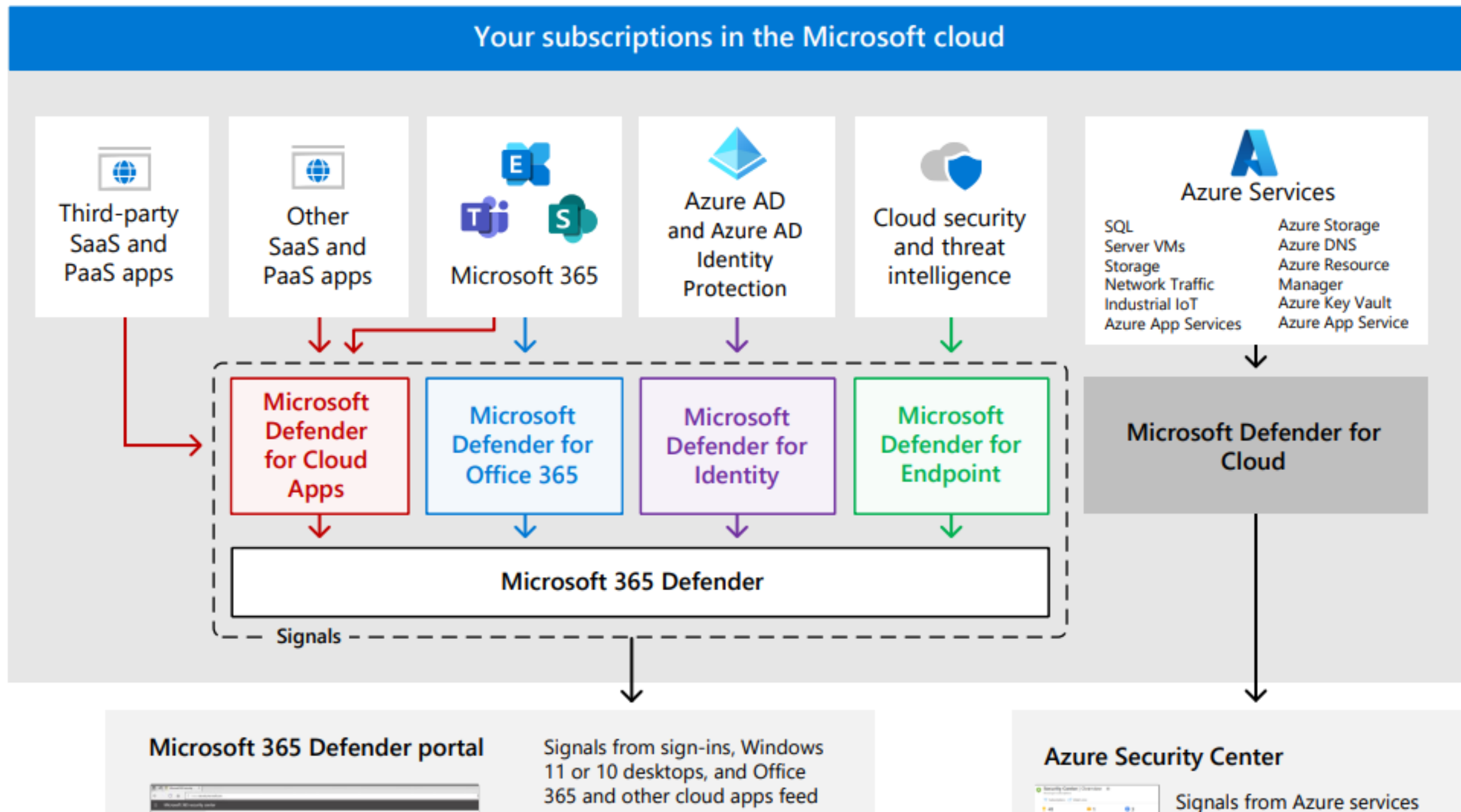
Martina Grom
Azure & Microsoft 365 MVP | Microsoft RD | CEO atwork
@magrom | martina.grom@atwork.at



Toni Pohl
Azure and Office Dev MVP | CTO atwork
@atwork | toni.pohl@atwork.at

Requirements and challenges

- Cloud apps can be a starting point for
 - Privilege escalation
 - Lateral movement
 - Exfiltration of data
- All or nothing does not work
- App governance
 - Visibility
 - Remediation
 - governance



App protection

- App governance provides detailed information about an app's activity at the API level.
- Azure AD provides foundational app metadata and detailed information on sign-ins to apps.
- Defender for Cloud Apps provides app risk information.

Demo

Application Governance

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](#)

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

Data usage (preview)

Total data usage

Month	Total data usage (GB)
July	0
August	100
September	60
October	25

Data usage by resource type



Month	File (GB)	Email (GB)
July	0	0
August	55	50
September	40	30
October	20	10



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](#)


- 
-  Home


 Incidents & alerts 




 Hunting 


 Actions & submissions 




 Threat analytics


 Secure score



 Learning hub



 Trials
-  Assets 

 Identities


 Device inventory
-  Endpoints 

 Device inventory

 Vulnerability management 

 Partners and APIs 

App governance

 Learn more about app governance

Get in-depth visibility and control over OAuth apps registered on Azure Active Directory.


Overview


Apps


Alerts

Policies

Apps

121 apps found 

39 overprivileged apps 

32 highly privileged apps 

[View all apps](#)

Incidents

2 unresolved incidents

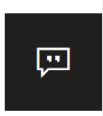
1 threat incidents

1 policy incidents

[View all incidents](#)

Latest incidents

Last Activity	Severity	Incident name	Source
5/13/2022	<div><div></div><div></div><div></div></div> Medium	App with numerous ...	Policy
4/4/2022	<div><div></div><div></div><div></div></div> Medium	App made unusual e...	Detection



Create rule

Select conditions

We will apply the policy to app

App details

+ Add condition

 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

rch

[Learn more about policies](#)

Save

Cancel

Filter  Save the query  Reset  Filters

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%)
appdracarbTecnicas	8/10/2021	8/10/2021	Admin (88)	0 B (0%)
appdracarbTecnicas1	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

Publisher verification	Certification
Contoso 	Not certified
Learn more about publisher verification	Learn more about Microsoft 365 certification 

1

Activity

1

Chat

Teams

Calendar

Calls

Files

Apps

Help

Join or create a team

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

!

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

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



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

391

IP addresses

188

Users

16

Devices

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 I...

Categories ▾

by

Traffic ▾



Traffic

from

high risk

apps

Traffic



“Microsoft Azure provides a secure foundation across physical, infrastructure, and operational security.”

- Azure compliance
<https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance>
- Compliance offerings
<https://docs.microsoft.com/en-us/azure/compliance>
- Microsoft Security Blog
<https://aka.ms/security>
- Microsoft Azure leads the industry in ISO certifications
<https://azure.microsoft.com/en-us/blog/microsoft-azure-leads-the-industry-in-iso-certifications>


Identify your use cases!


- Typical workloads types
- VM's (Lift & Shift)
- (Web) Apps
- PowerShell Scripts
- Business workflows


How to secure your Azure resources

Use Azure Advisor

This tool is helpful (and you can create exemptions)

 Search (Ctrl+/) <<

 Overview


 Advisor Score (preview)

Recommendations


 Cost

 Security


 Reliability

 Operational excellence

 Performance


 All recommendations


Monitoring

 Alerts (Preview)


 Recommendation digests





Settings


 Configuration

 **Successfully refreshed recommendations**

Successfully refreshed recommendations for Azure Advisor





-  Feedback
-  Download as CSV
-  Download as PDF
-  Try the new Advisor Score (preview)

 Your recommendations have been loaded

Subscriptions: tpe5 (MPN)


Active

 Cost



You are following all of our cost recommendations


[See list of cost recommendations](#)


 Security

30 Recommendations

11 High impact 15 Medium impact 4 Low impact


18 Impacted resources


 Reliability




You are following all of our reliability recommendations

[See list of reliability recommendations](#)

 Operational excellence

 Performance



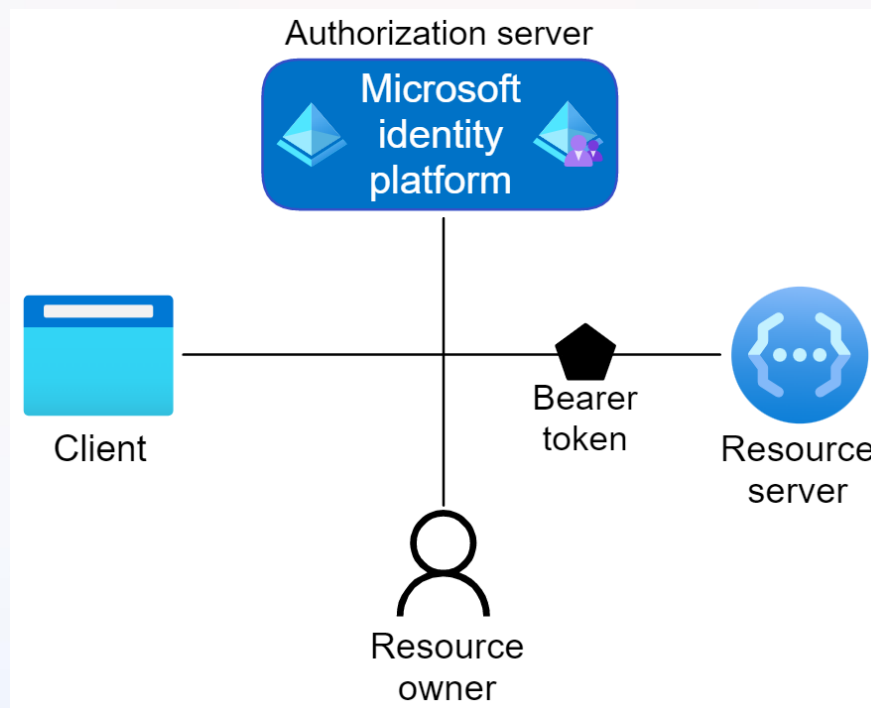
Identities on VMs, Azure Logic Apps, Azure Functions, Automation Accounts, Storages, ...

Use

- Firewalls / Network
- Managed Identities (System/User)
- Certificates
- Monitoring
- Alerting & reaction (Scripts/Logic Apps)

Identity – Modern Authentication

OAuth 2.0 is a method through which a third-party app can access web-hosted resources on behalf of a user.



VM's

Use Just-In-Time access, monitoring...

JIT creates a temporary rule in the Firewall

[Home](#) > [RG-SecureApps](#) > [VM1](#)

VM1 | Networking

Virtual machine

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Disks
- Size
- Security
- Advisor recommendations
- Extensions + applications
- Continuous delivery
- Availability + scaling

Attach network interface Detach network interface Feedback

vm1604

IP configuration ⓘ

ipconfig1 (Primary)

Network Interface: vm1604

[Effective security rules](#)

[Troubleshoot VM connection issues](#)

[Topology](#)

Virtual network/subnet: [RG-SecureApps-vnet/default](#)

NIC Public IP: **20.125.28.32**

NIC Private IP: **10.0.0.4**

Accelerated networking: **Enabled**

Inbound port rules

[Outbound port rules](#)

[Application security groups](#)

[Load balancing](#)

Network security group [VM1-nsg](#) (attached to network interface: [vm1604](#))

Impacts 0 subnets, 1 network interfaces

Add inbound port rule

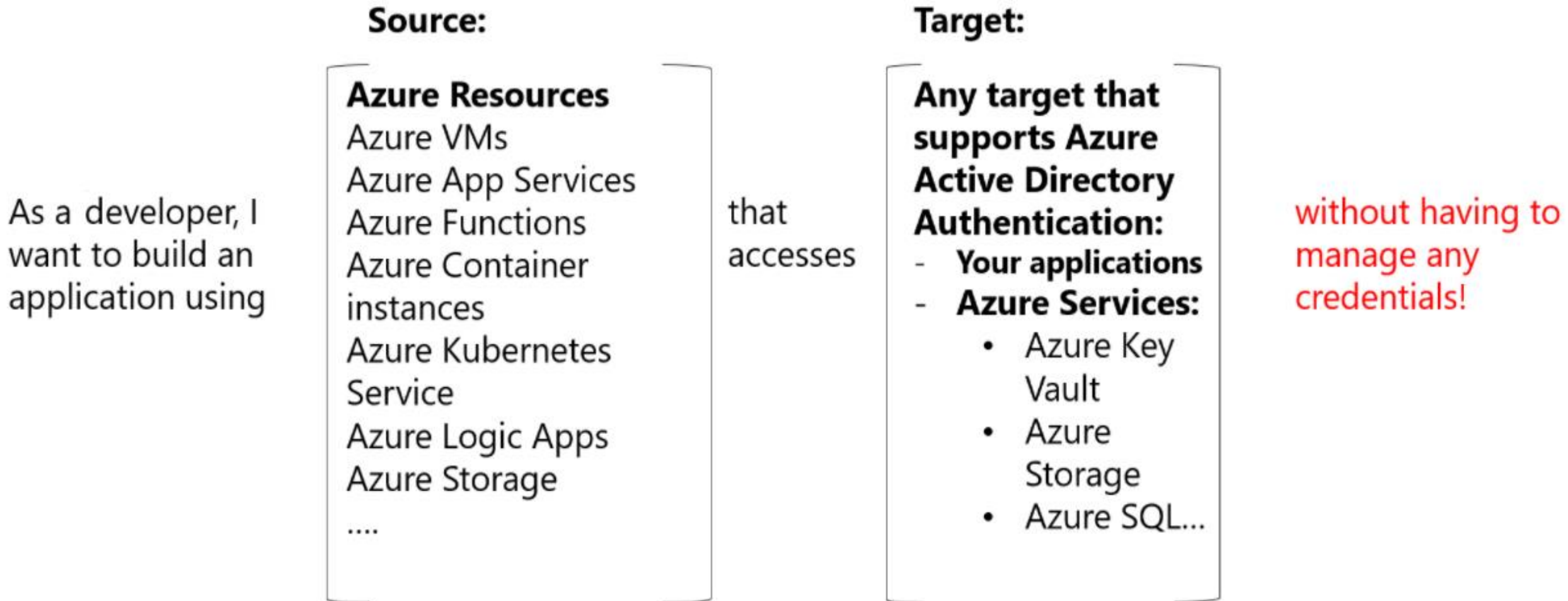
Priority	Name	Port	Protocol	Source	Destination	Action	
100	SecurityCenter-JITRule-567197904-...	3389	Any	89.185.116.247	10.0.0.4	✓ Allow	...
4096	⚠ SecurityCenter-JITRule_56719790...	3389	Any	Any	10.0.0.4	✗ Deny	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny	...

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...



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

Tip:
Use Secure Outputs
(Logging)

Settings for 'Get secret'

Secure Inputs

Secure inputs of the operation.

Secure Inputs

☐ Off

Secure Outputs

Secure outputs of the operation and references of output properties.

Secure Outputs

☒ On

Asynchronous Pattern

With the asynchronous pattern, if the remote server indicates that the request is accepted for processing with a 202 (Accepted) response, the Logic Apps engine will keep polling the URL specified in the response's location header until reaching a terminal state.

Asynchronous Pattern

☒ On

Automatic decompression

Automatically decompress gzip response.

Automatic decompression

☒ On

Action Timeout

Limit the maximum duration between the retries and asynchronous responses for this action. Note: This does not alter the request timeout of a single request.

Duration ⓘ

Example: P1D

Retry Policy

A retry policy applies to intermittent failures, characterized as HTTP status codes 408, 429, and 5xx, in addition to any connectivity exceptions. The default is an exponential interval policy set to retry 4 times.

Type

Default

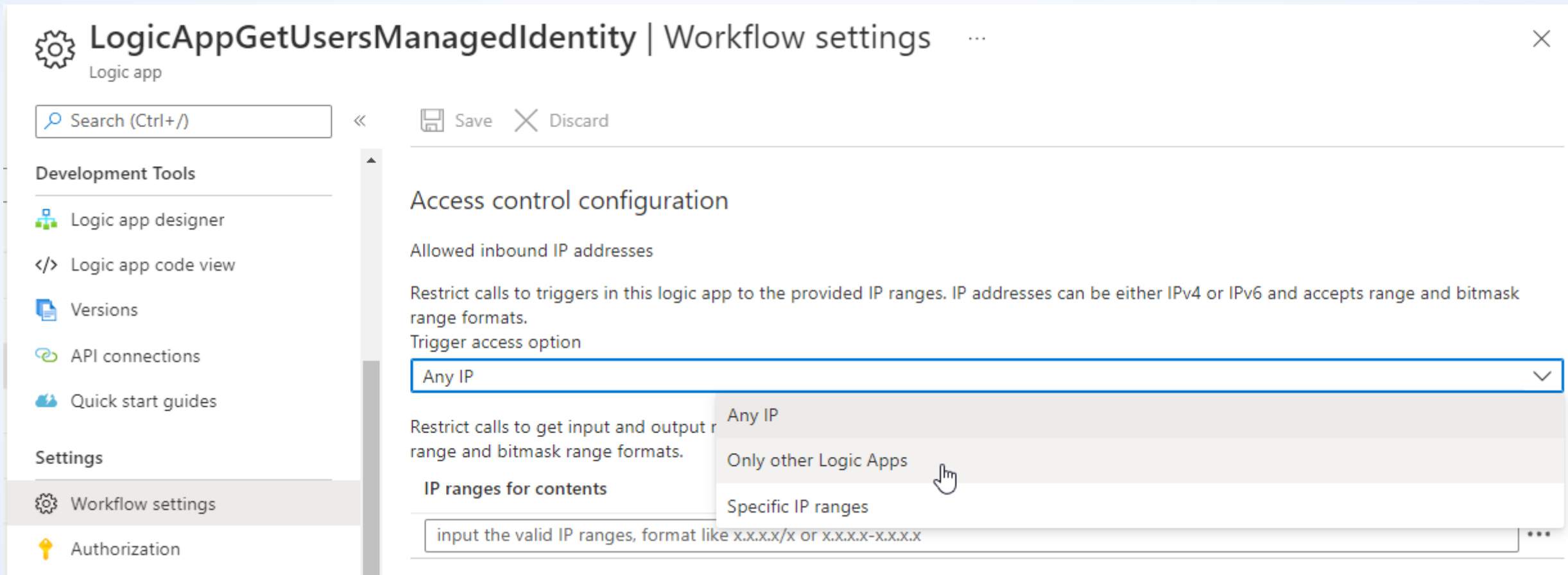
Tracked Properties

--	--

Done

Cancel

Azure Logic Apps: Secure the trigger



LogicAppGetUsersManagedIdentity | Workflow settings ...

Logic app

Search (Ctrl+ /)

Save Discard

Development Tools

- Logic app designer
- Logic app code view
- Versions
- API connections
- Quick start guides

Settings

- Workflow settings
- Authorization

Access control configuration

Allowed inbound IP addresses

Restrict calls to triggers in this logic app to the provided IP ranges. IP addresses can be either IPv4 or IPv6 and accepts range and bitmask range formats.

Trigger access option

Any IP

Restrict calls to get input and output ranges to the provided IP ranges. IP addresses can be either IPv4 or IPv6 and accepts range and bitmask range formats.

IP ranges for contents

input the valid IP ranges, format like x.x.x.x/x or x.x.x.x-x.x.x.x

Any IP

Only other Logic Apps

Specific IP ranges

Automation Accounts

Migrate your PowerShell scripts to the cloud

Secure the access

(Connections, Managed Identity, Key Vault, Firewall)

Access assets in scripts

Home > Automation Accounts > M365conf > test1 (M365conf/test1) >

Edit PowerShell Runbook test1 ...

Save Publish Revert to published Test pane Feedback

> RUNBOOKS

✓ ASSETS

- Variables
- Connections
 - m365conf5 ...
- Credentials
 - adelev@tpe5.onmicrosoft.com ...
- > Certificates

```
1 $user = Get-AutomationPSCredential -Name 'adelev@tpe5.onmicrosoft.com'
2
3 Write-Output $user
4
5 Write-Output $user.username
6 Write-Output $user.password
7
8
9
```


Create a self-signed certificate with PS

```
# Certificate (PFX)
```

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

App Services

Web sites

Web jobs

Azure Functions

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>

Search

Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Microsoft Defender for Cloud
- Events (preview)

Functions

- Functions
- App keys
- App files
- Proxies

Deployment

- Deployment slots
- Deployment Center

Settings

- Configuration
- Authentication
- Application Insights
- Identity

Click here to upg

Application settings

Application settings

Application settings display them in pla environment varia

+ New applicat

Filter applica

Name

AzureWebJobsDas
AzureWebJobsSto
FUNCTIONS_EXTE
FUNCTIONS_WOR
keyvault-secret
MICROSOFT_PRO
WEBSITE_RUN_FR

Connection str

Connection strings should only be use

Add/Edit application setting

Name

keyvault-secret

Value

@Microsoft.KeyVault(SecretUri=https:// m365conf.vault.azure.net/secrets/secr...

☐ Deployment slot setting

OK

Cancel

Logging + Monitoring

... should be part of every app or solution

KQL & Alerts

```
// Show errors
AzureDiagnostics
| where TimeGenerated > ago(1d)
| where resource_resourceGroupName_s == "RG-SecureApps"
| where Category == "WorkflowRuntime"
| where resource_workflowName_s == "GetUsers"
| where status_s == "Failed"
| order by TimeGenerated desc
```

```
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	08585167876653891612922812729CU42			
ResourceType	WORKFLOWS/RUNS			
OperationName	Microsoft.Logic/workflows/workflowRunCompleted			
Level	Error			
status_s	Failed			

 Search

<<

 Create

 Alert rules

 Action groups

 Alert processing rules


 Columns


 Refresh


 Export to CSV


 Open query





-  Overview


 Activity log


 Alerts


 Metrics


 Logs


 Change Analysis


 Service health


 Workbooks
- Insights


 Applications


 Virtual Machines


 Storage accounts


 Containers


 Networks


 SQL (preview)

 Azure Cosmos DB

 Key Vaults


 Azure Cache for Redis


 Azure Data Explorer Clusters


 Search

Directory : **tpe5**


Time range : **Past 7 days**

Alert condition : **Fired** 

Severity : **all** 

 Add filter

Total alerts

 **15**

Critical

0

Error

15

Warning


0































































Informational

0

Verbose

0

No grouping 

Name 	Severity 	Affected resource 	Alert condition 	User response 	Fire time 	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 10:45 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 10:40 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 10:35 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 10:30 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 10:25 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 10:20 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 10:16 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 10:10 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 10:05 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 10:01 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 9:55 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 9:50 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 9:45 AM	
<input type="checkbox"/> Error	 1 - Error	 response (getusers/...	 Fired	New	5/24/2023, 9:40 AM	

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

Links

- Shortcut to AppGovernance Dashboard
<https://aka.ms/appgovernance>
- App governance in Microsoft 365 | Microsoft Docs
<https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-manage-app-governance>
- Scripts & presentation
<https://github.com/tonipohl/SecureAppsWithAzure>
- Microsoft Graph Explorer
<https://aka.ms/ge>



Thank you



<https://github.com/tonipohl/SecureAppsWithAzure>

Let's connect!

@magrom @atwork



THRIVE
CONFERENCE

Sponsors



INTELLITY

