

Service Principals & Managed Identities – How to Properly Secure your Azure Resources



ESPC Community Webinar
October 12, 2022

About me



Shannon Kuehn (KEEN)

Identity and Network Access Digital Influence Team

Senior Program Manager



[@shankuehn](https://twitter.com/shankuehn)



<https://www.linkedin.com/in/shannonkuehn/>



Microsoft 425show

The Digital Influence team is looking for tech influencers!

Live Streamers

Content Creators

Social Media Influencers

Bloggers



YouTube



twitter

TikTok



Instagram

Learn More: <https://425show.com>

Opt-In: [Join the Digital Influence Program](#)

Contact: 425show@microsoft.com



Application Objects, Service Principals, & Managed Identities



Definitions

- Application object
- ServicePrincipal object
- Managed Identity

Types of Managed Identities

System-Assigned

- Tied to a specific resource, such as App Service or Virtual Machine
- Same lifecycle as the resource. Example: If a virtual machine is deleted, the managed identity is also deleted.
- Cannot be shared with or assigned to other resources

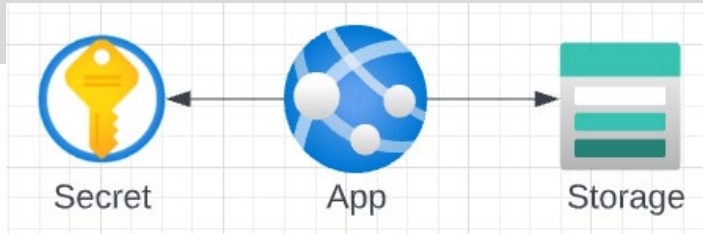
User-Assigned

- Created as a stand-alone resource
- Independent life cycle. Must be explicitly deleted.
- Can be assigned to multiple resources
- For cases such as:
 1. Multiple services require access to the same resource
 2. Need to maintain permissions even when resources are deleted and recreated
 3. Need to break up permissions across multiple identities

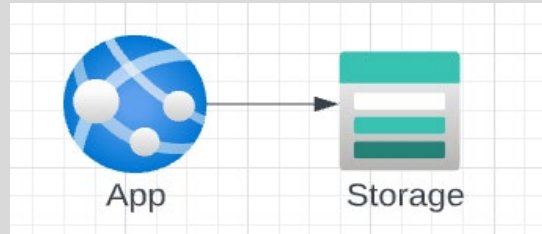
Managed Identities

Common Patterns

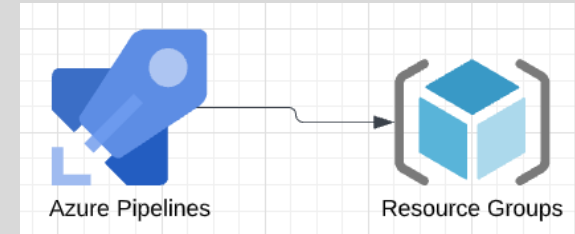
Securely store and access secrets from an Azure Key Vault store



Application access to resources such as storage accounts



Access for Azure Management (DevOps Pipeline, Terraform, ...)

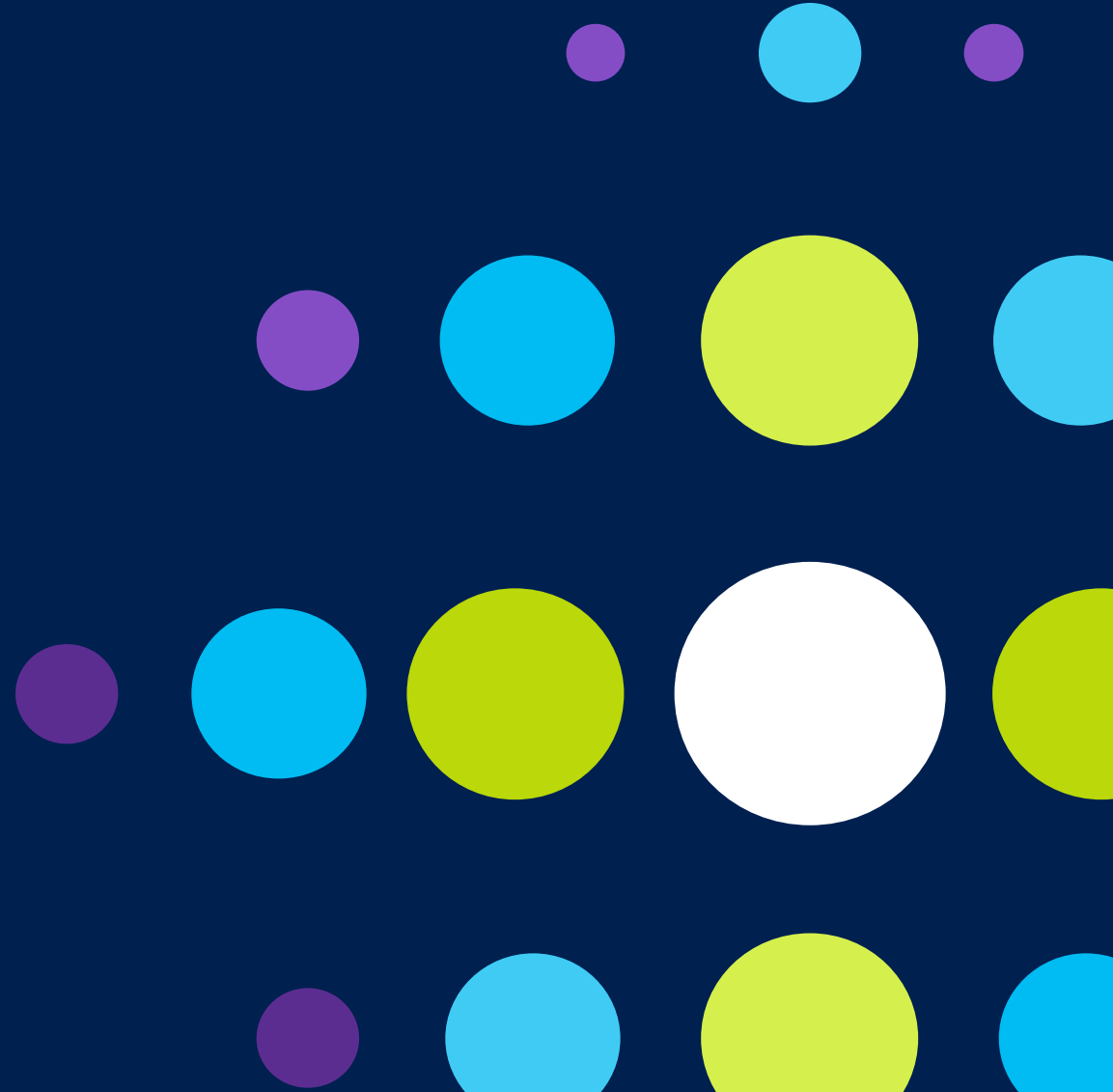


Access to
Azure AD tenant
(Home tenant only)



Service to Service
authorization
Ex: App Service+Key Vault References

Workload Identities



What are workload identities?

Definition: A workload identity is an identity used by a software workload (such as an application, service, script, or container) to authenticate and access other services and resources.

In Azure Active Directory (Azure AD), workload identities are:

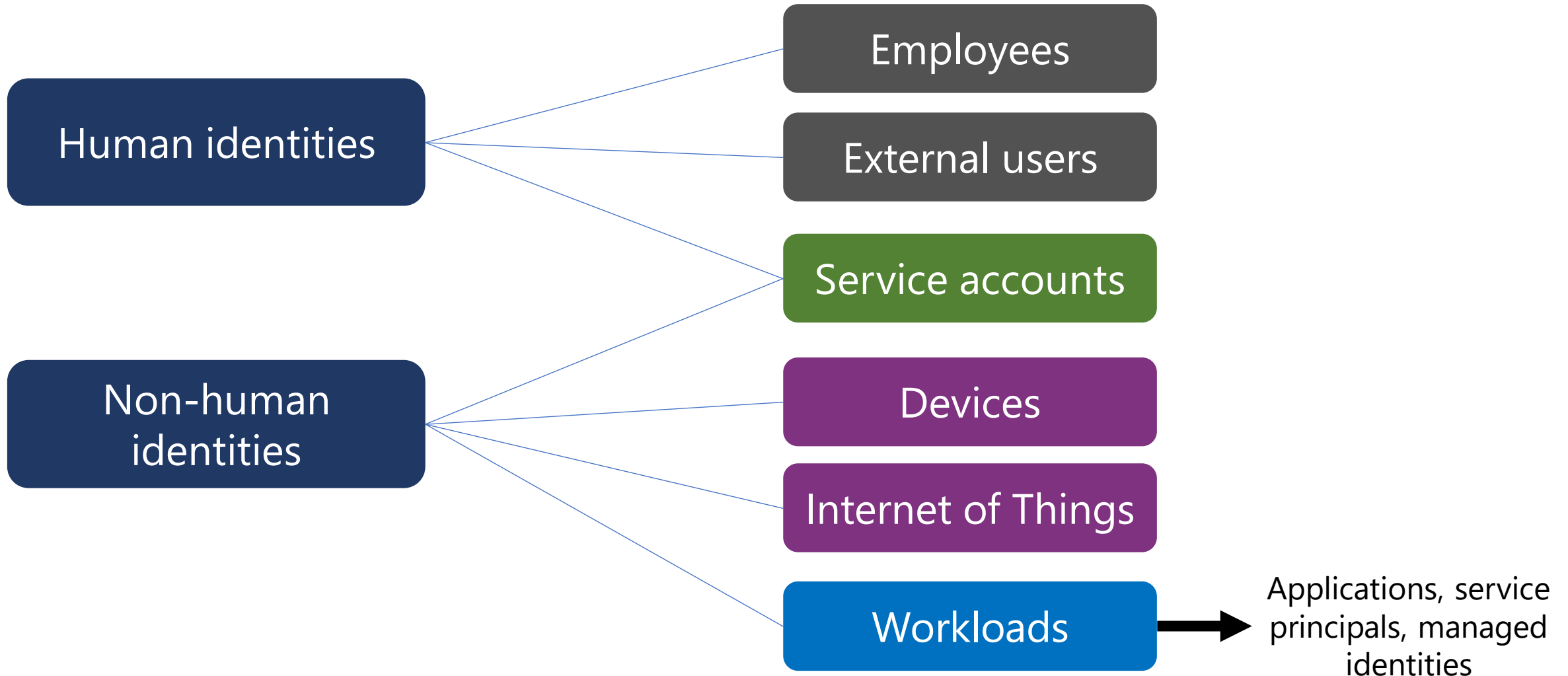
- An [application](#)
- A [service principal](#)
- A [managed identity](#)



Background

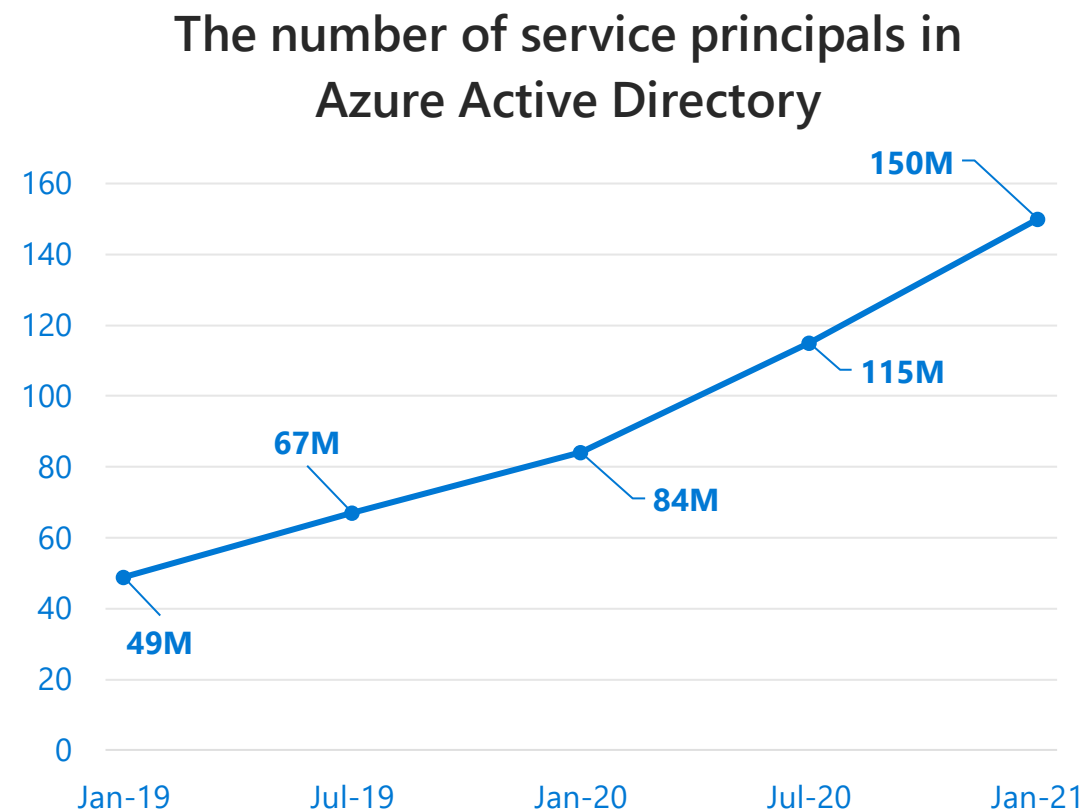
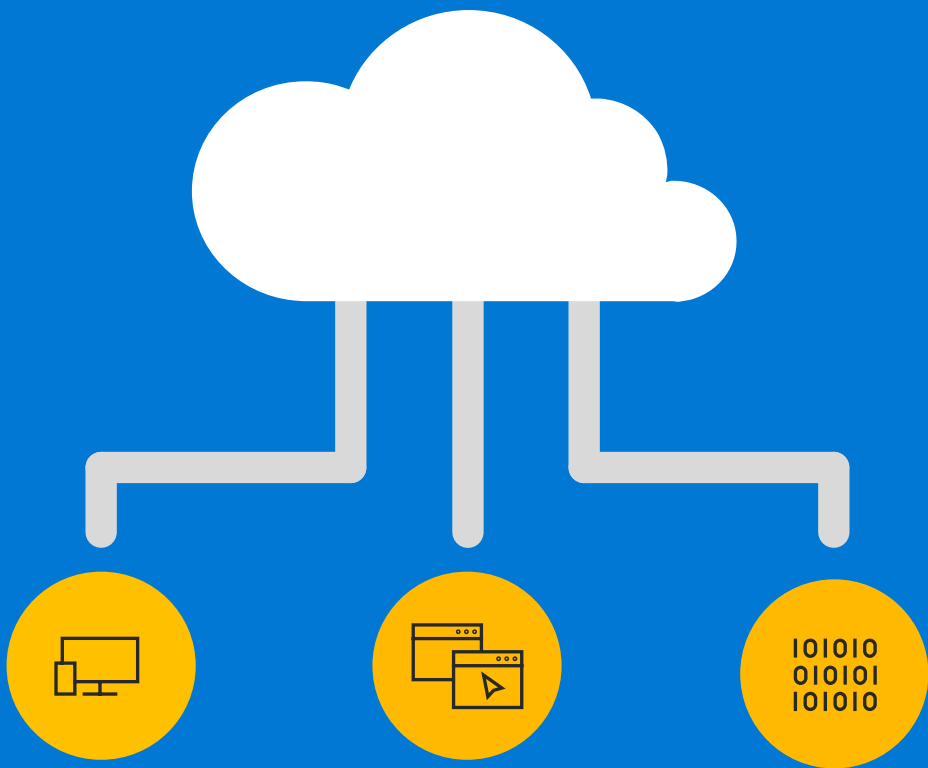
- Workloads continue to move to the cloud
- Many new enterprise solutions are cloud native
- Made up of:
 - Applications
 - Services
 - Scripts
 - Daemons
- Increase in needs of managing and securing “workload identities”

Taxonomy of identities in Azure AD



Growth of cloud service or application usage

More applications and services are continuing to move to the cloud



How are workload identities used?

Here are some ways that workload identities in Azure AD are used:



Web app



Key Vault



Azure Storage



GitHub – CI/CD Pipeline

Challenges of managing and securing workload identities

Many traditional IAM capabilities do not apply to workload identities



Difficult to manage lifecycle:

How to get a visibility into the activity of workload identities, that enables periodic cleanup



Higher potential for secrets or credentials to leak:

How to ensure that workload identities are not breached



Lacking capabilities for securing access:

How to remove unnecessary or overprivileged access

Do any of the following apply in your environment?

- Heavy app/workload identity integration with Azure AD
- Currently using Azure AD Conditional Access, Identity Protection, or Access Reviews to secure users
- Want to protect identities from compromise
- Subject to regulations and auditor visits

Introducing 4 new capabilities to protect workload identities

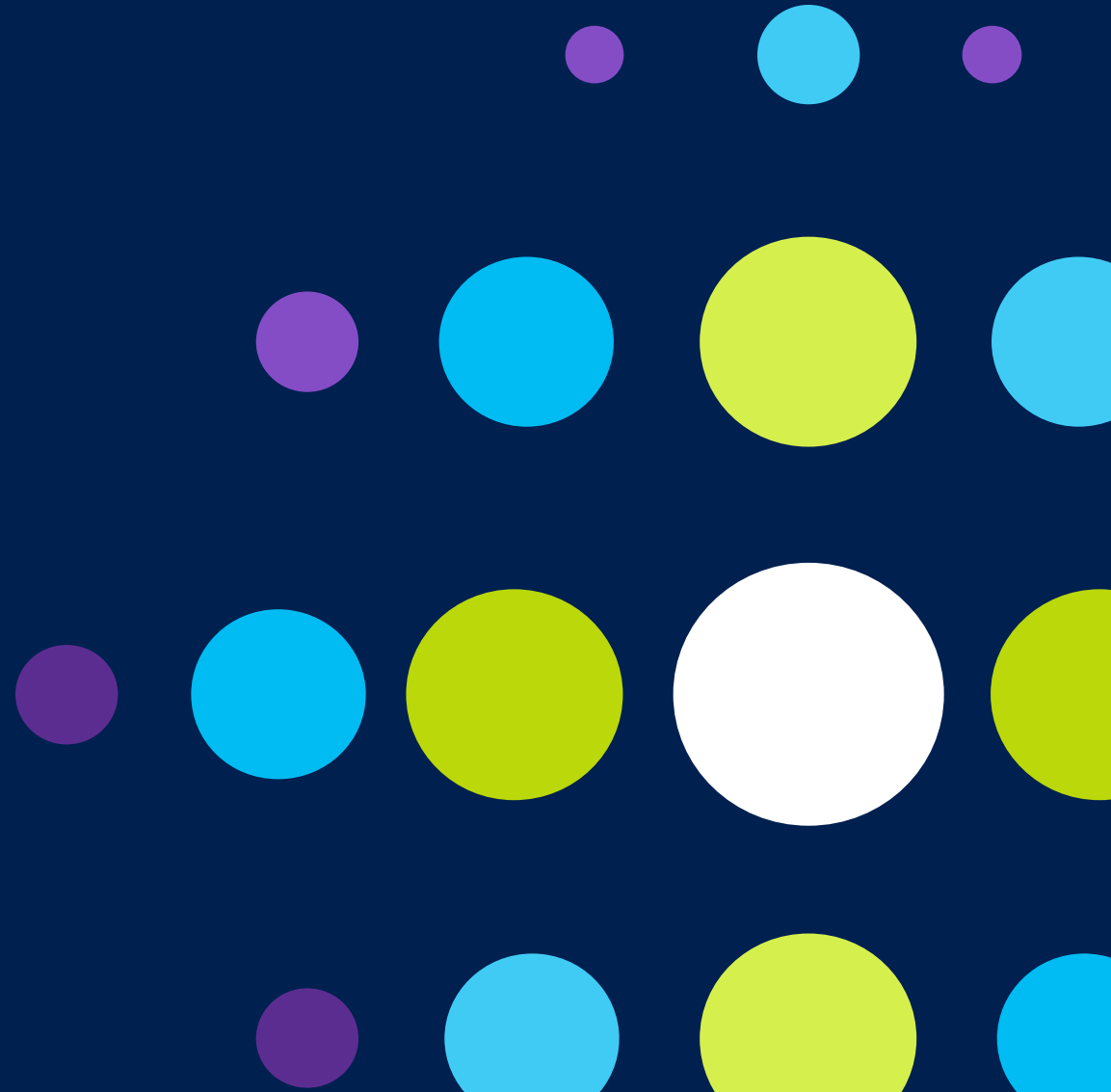
Conditional Access for workload identities

Identity Protection for workload identities

Access Reviews for workload identities

Workload Identity Federation

Conditional Access for workload identities



Conditional Access for workload identities

- Extend Conditional Access policies to apps and service principals
- Restrict access from named locations and Azure Virtual Networks
- View service principals blocked by policies using Insights and Reporting workbook

Public Preview

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more](#)

Name *

Example: 'Device compliance app policy'

Assignments

Users or workload identities ⓘ

0 users or workload identities selected

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.
[Learn more](#)

What does this policy apply to?

Workload identities (Preview) ▼

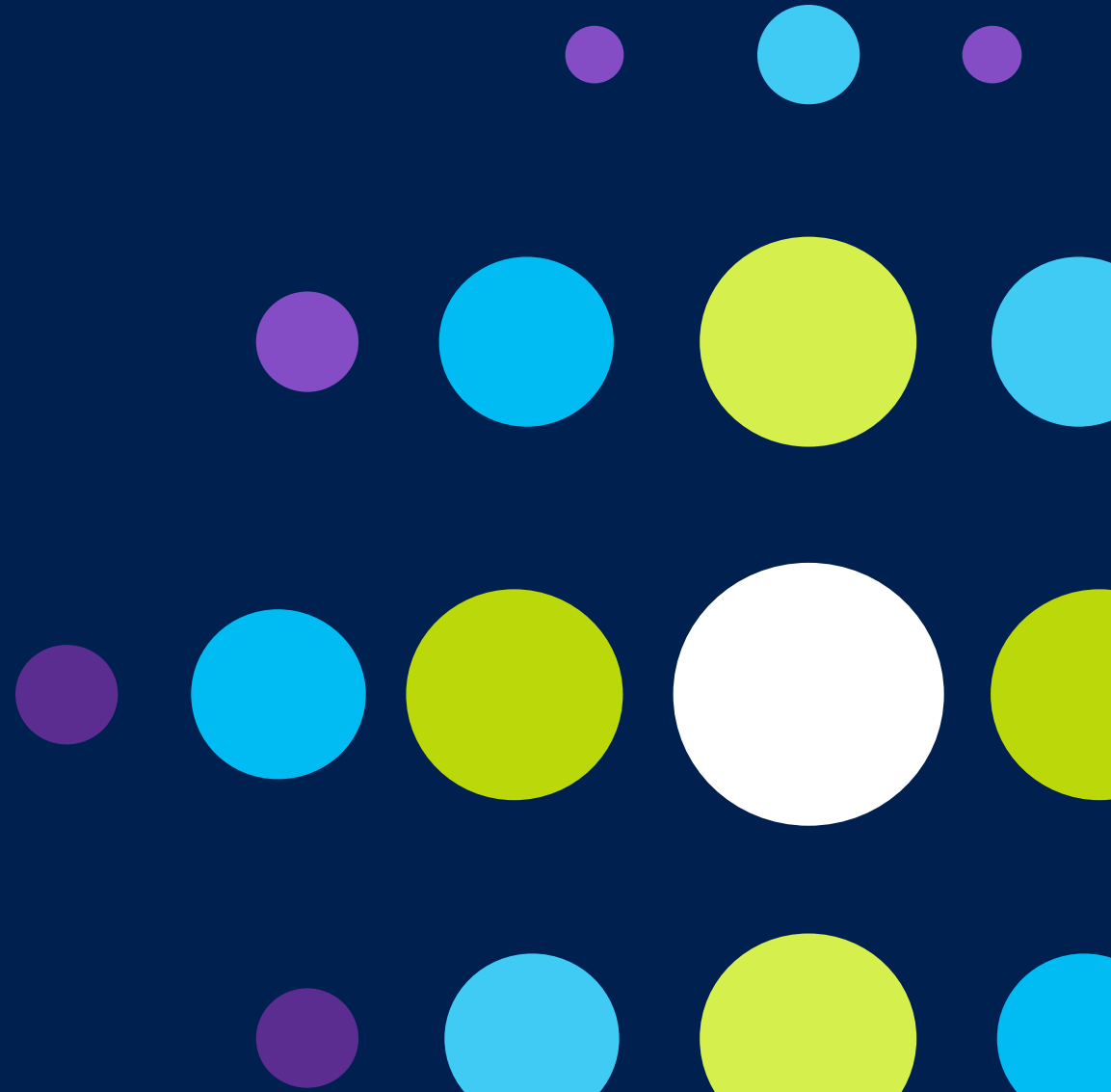
Users and groups

Workload identities (Preview)

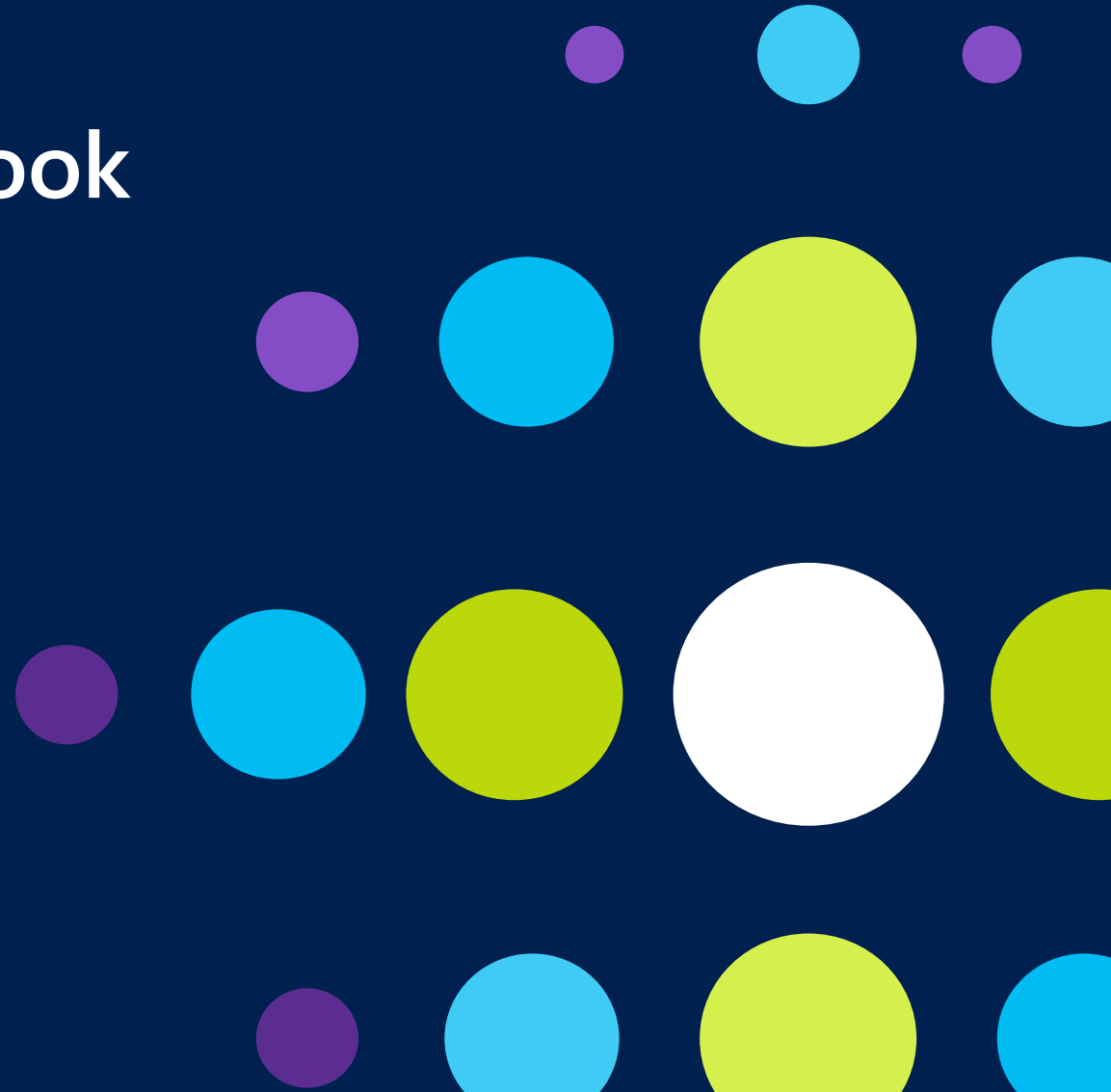
☐ All owned service principals

☐ Select service principals

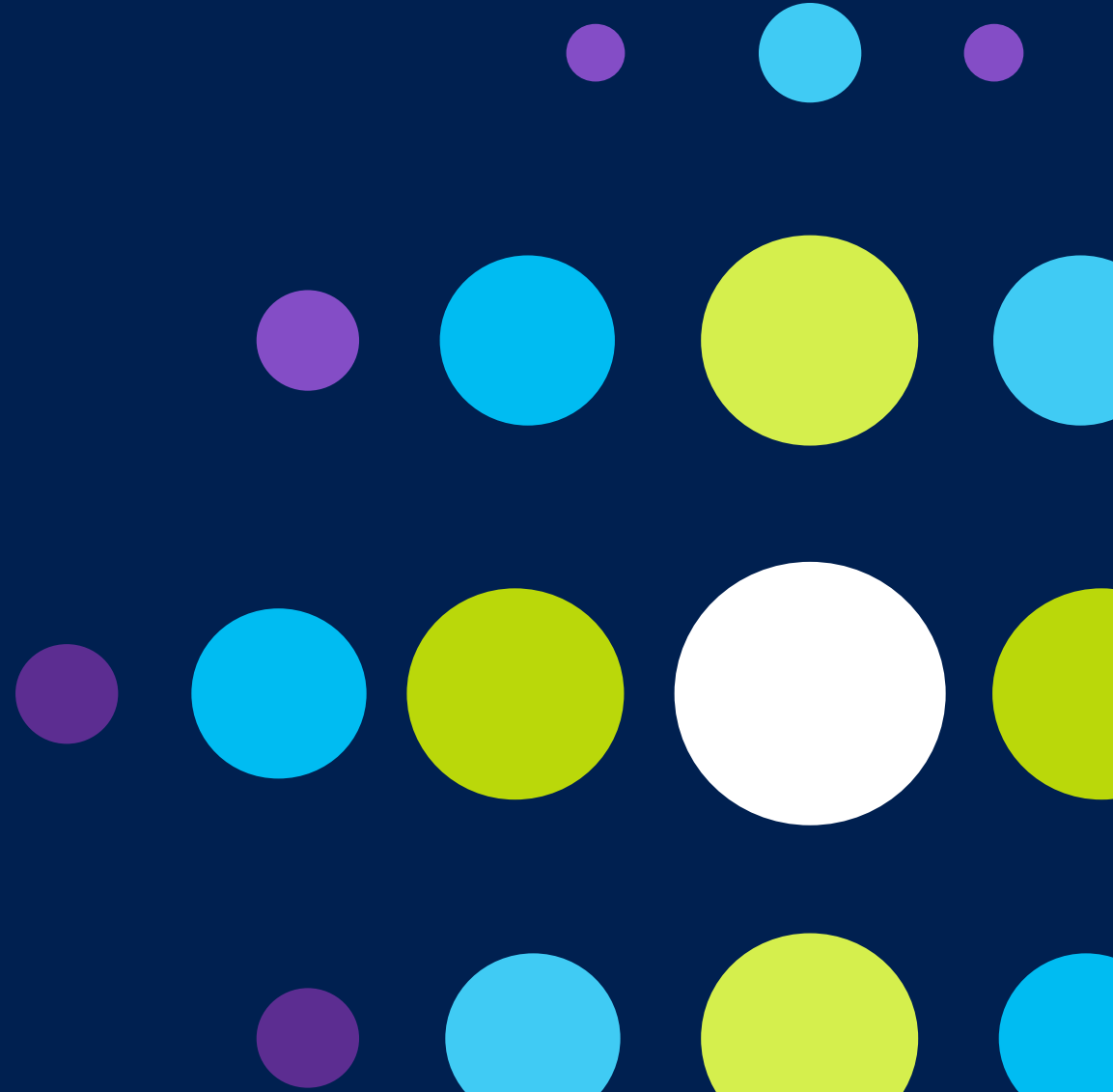
Creating a Conditional Access policy for workload identities Demo



Insights and Reporting workbook supports workload identities Demo



Identity Protection for workload identities







Identity Protection for workload identities





- Detect compromised apps and service principals
- Block access on risky workload identities in Conditional Access
- Export risk logs using Diagnostic Settings (e.g., for SIEM tools)

Public Preview

Risky workload identities (preview) ...

 Learn more  Download  Select all  Confirm service principal(s) compromised

Auto refresh : **Every hour** Show dates as : **Local** Risk state : **2 selected** 

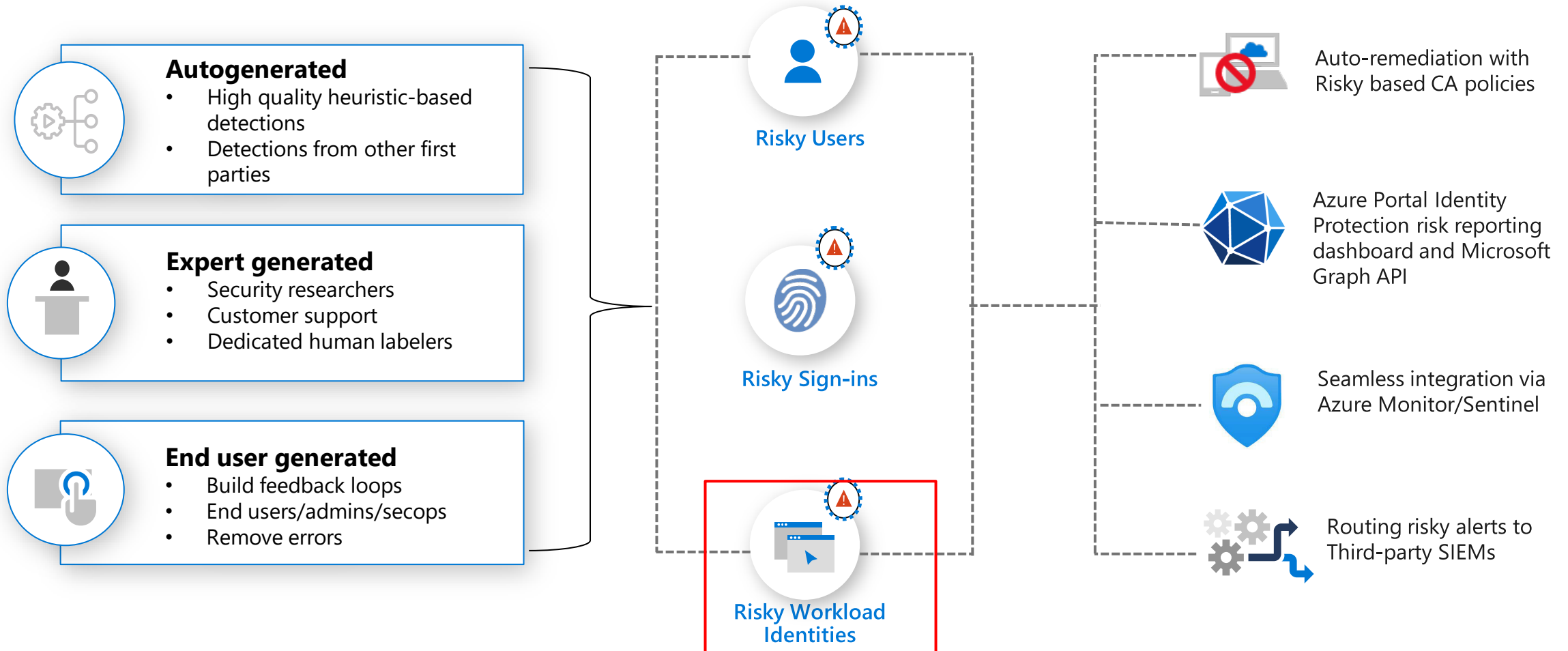
<input type="checkbox"/> Service principal 	App ID 	Risk state 	Risk level 
<input type="checkbox"/> Contoso Chat Bot	1e429928-7ff6-...	At risk	Medium
<input type="checkbox"/> Contoso Sales Tracker	971b68fa-7541-...	At risk	High
<input type="checkbox"/> ContosoDevOps	7b37ac67-48c3-...	At risk	High
<input type="checkbox"/> AutomateContoso	f91ebafb-19a8-...	At risk	High
<input type="checkbox"/> Contoso Expense	0feb38ac-a572-...	At risk	High
<input type="checkbox"/> Contoso HR App	ede08db0-9492...	At risk	High
<input type="checkbox"/> AppToTestLeakedCreds	752f776d-a403-...	At risk	High

Azure AD Identity Protection

Unique insights powered by trillions signal

Assess Risk Levels via real-time evaluation engine

Secure Access via policy enforcement and unified investigation experience

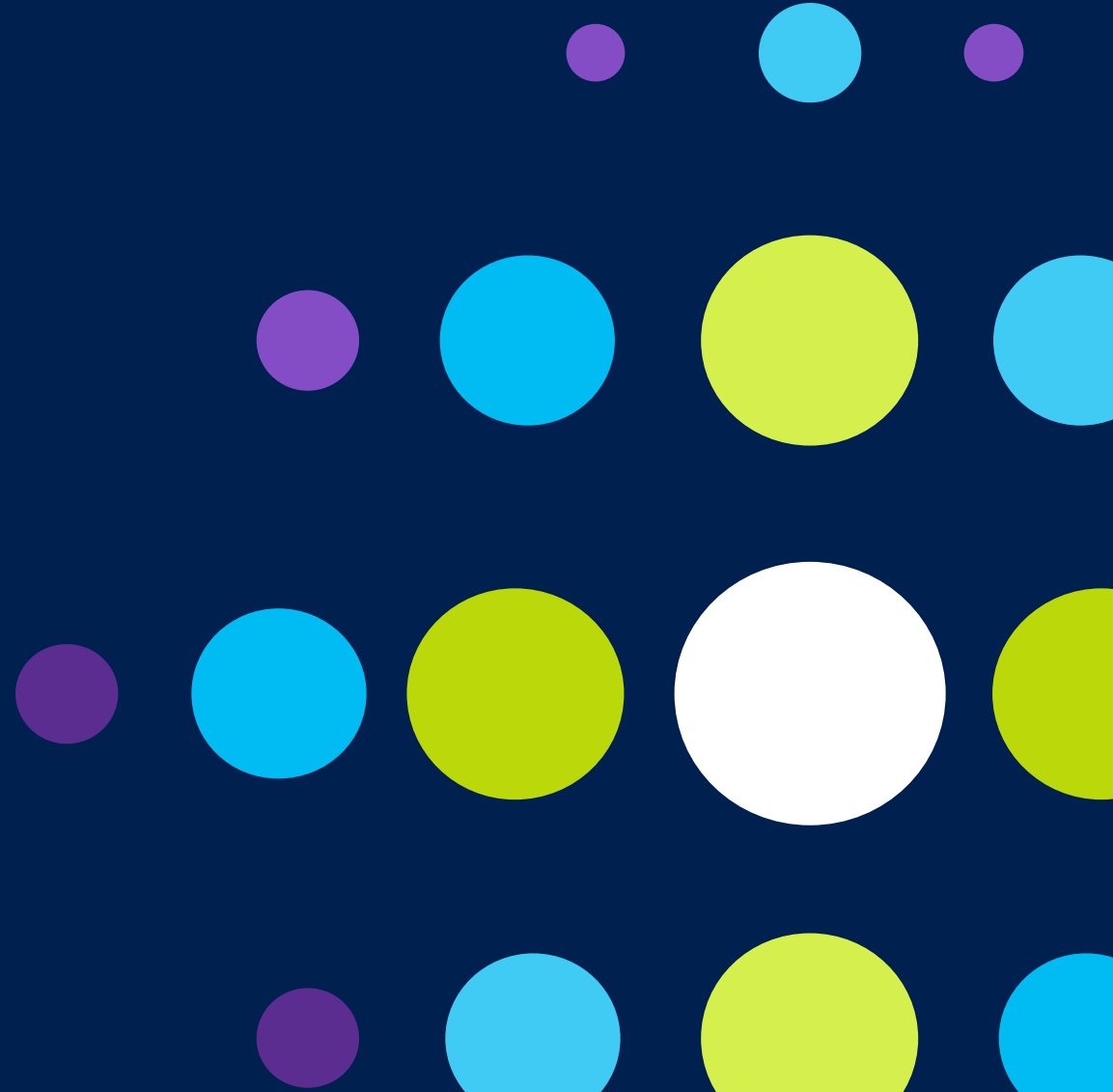


Identify risky workload identities

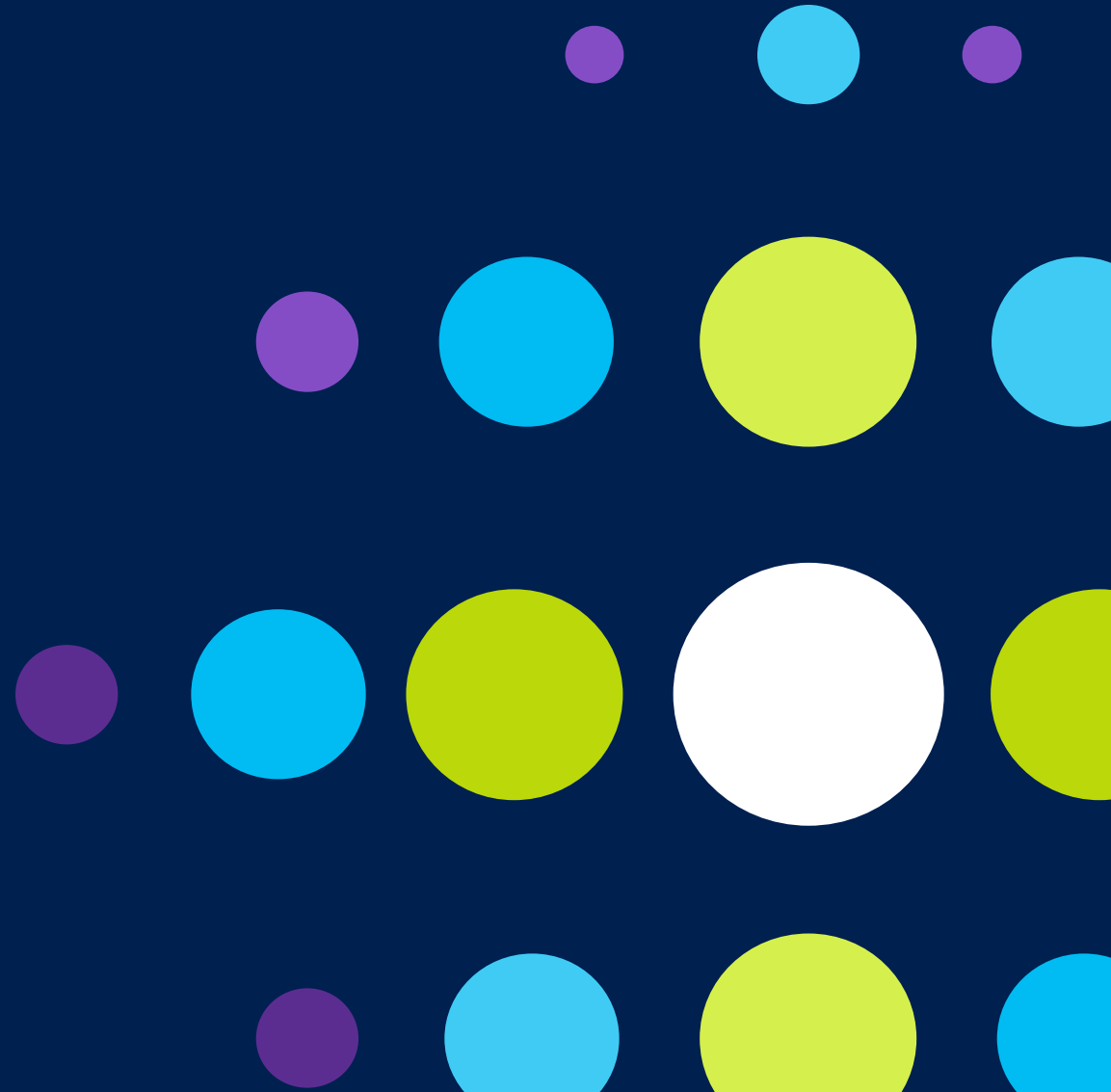
Demo



Configure a risk-based Conditional Access policy for workload identities Demo



Export risk data



Woodgrove | Diagnostic settings

Azure Active Directory

- Custom security attributes (Preview)
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security
- Monitoring
 - Sign-in logs
 - Audit logs

Refresh Feedback

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. [Learn more about diagnostic settings](#)

Diagnostic settings

Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
Woodgrove_Diagnostics_Setti...	woodgrovesigninstorage	woodgrove-eventhub	woodgrove-loganalyticsworkspc	-	Edit setting

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AuditLogs
- SignInLogs
- NonInteractiveUserSignInLogs
- ServicePrincipalSignInLogs
- ManagedIdentitySignInLogs
- ProvisioningLogs
- ADFSSignInLogs
- RiskyUsers
- UserRiskEvents
- NetworkAccessTrafficLogs
- RiskyServicePrincipals
- ServicePrincipalRiskEvents

Two new data sources
you can export

[Home](#) > [Woodgrove](#) >

Diagnostic setting ...



Save



Discard



Delete



Feedback

Diagnostic setting name

Woodgrove_Diagnostics_Settings

Logs

Categories

<input checked="" type="checkbox"/> AuditLogs	Retention (days) 180
<input checked="" type="checkbox"/> SignInLogs	Retention (days) 180
<input checked="" type="checkbox"/> NonInteractiveUserSignInLogs	Retention (days) 180
<input checked="" type="checkbox"/> ServicePrincipalSignInLogs	Retention (days) 180
<input checked="" type="checkbox"/> ManagedIdentitySignInLogs	Retention (days) 180
<input checked="" type="checkbox"/> ProvisioningLogs	Retention (days) 180
<input checked="" type="checkbox"/> ADFSSignInLogs	Retention (days) 180
<input checked="" type="checkbox"/> RiskyUsers	Retention (days) 180
<input checked="" type="checkbox"/> UserRiskEvents	Retention (days) 180
<input type="checkbox"/> NetworkAccessTrafficLogs	Retention (days) 0
<input type="checkbox"/> RiskyServicePrincipals	Retention (days) 0
<input type="checkbox"/> ServicePrincipalRiskEvents	Retention (days) 0

Destination details

☒ Send to Log Analytics workspace

Subscription

Woodgrove - GTP Demos (External/Sponsored) ▾

Log Analytics workspace

Woodgrove-LogAnalyticsWorkspace (westus2) ▾

☒ Archive to a storage account

Showing all storage accounts including classic storage accounts

Location

All

Subscription

Woodgrove - GTP Demos (External/Sponsored) ▾

Storage account *

woodgrovesigninstorage ▾

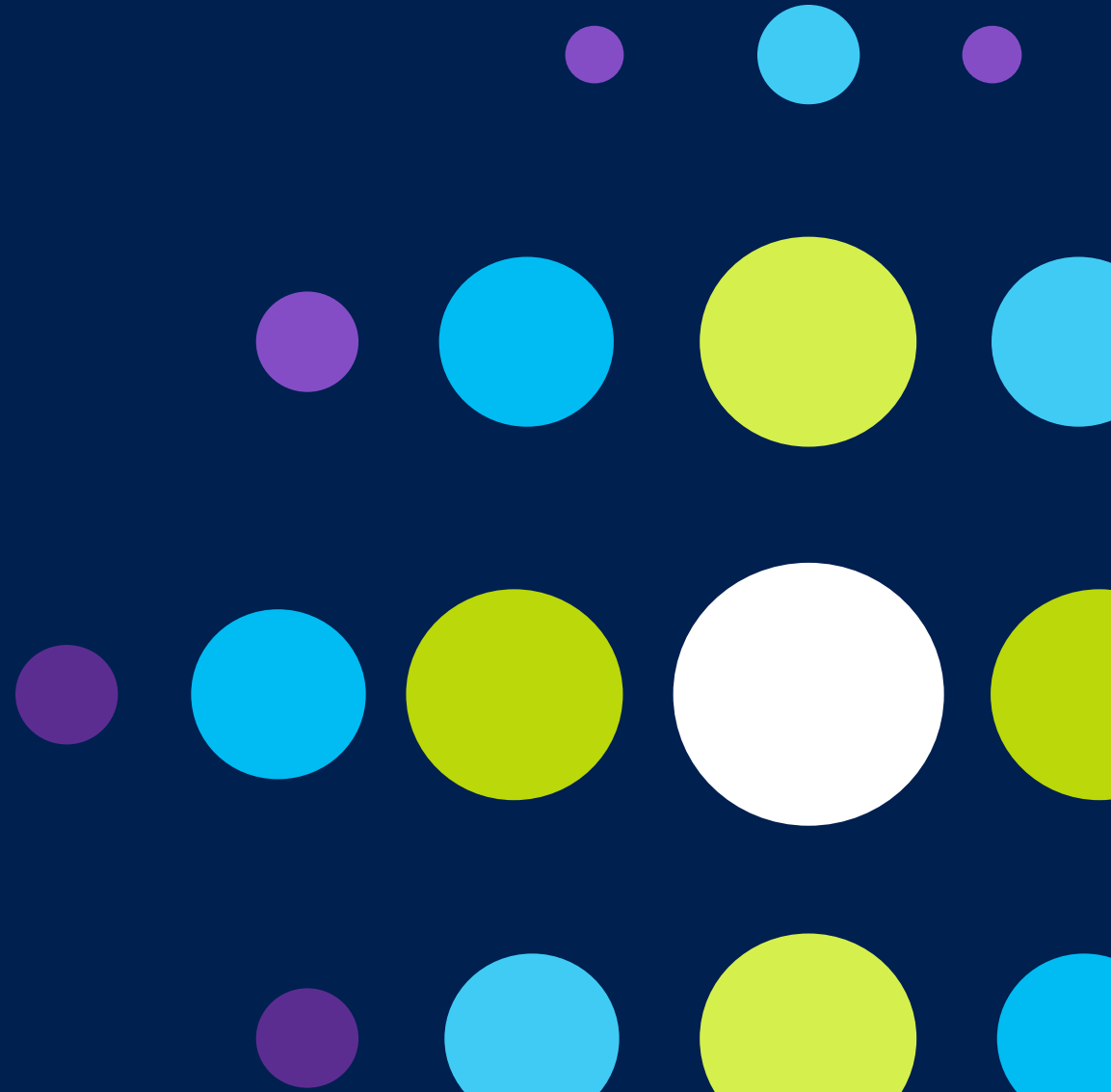
☒ Stream to an event hubFor potential partner integrations, [click to learn more about event hub integration.](#)

Subscription

Woodgrove - GTP Demos (External/Sponsored) ▾

Check the box and specify the retention period (if storing)

Access reviews for workload
identities assigned to privileged
roles



Access reviews for workload identities

- Schedule reviews of **service principal** assignment to **Azure AD roles** and **Azure subscription roles**
- Delegate the reviews to the right people, then automatically revoke access of service principals denied by reviewers

Public Preview

Home > Identity Governance >

New access review

[* Review type](#) [* Reviews](#) [Settings](#) [* Review + Create](#)

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles. [Learn more](#)

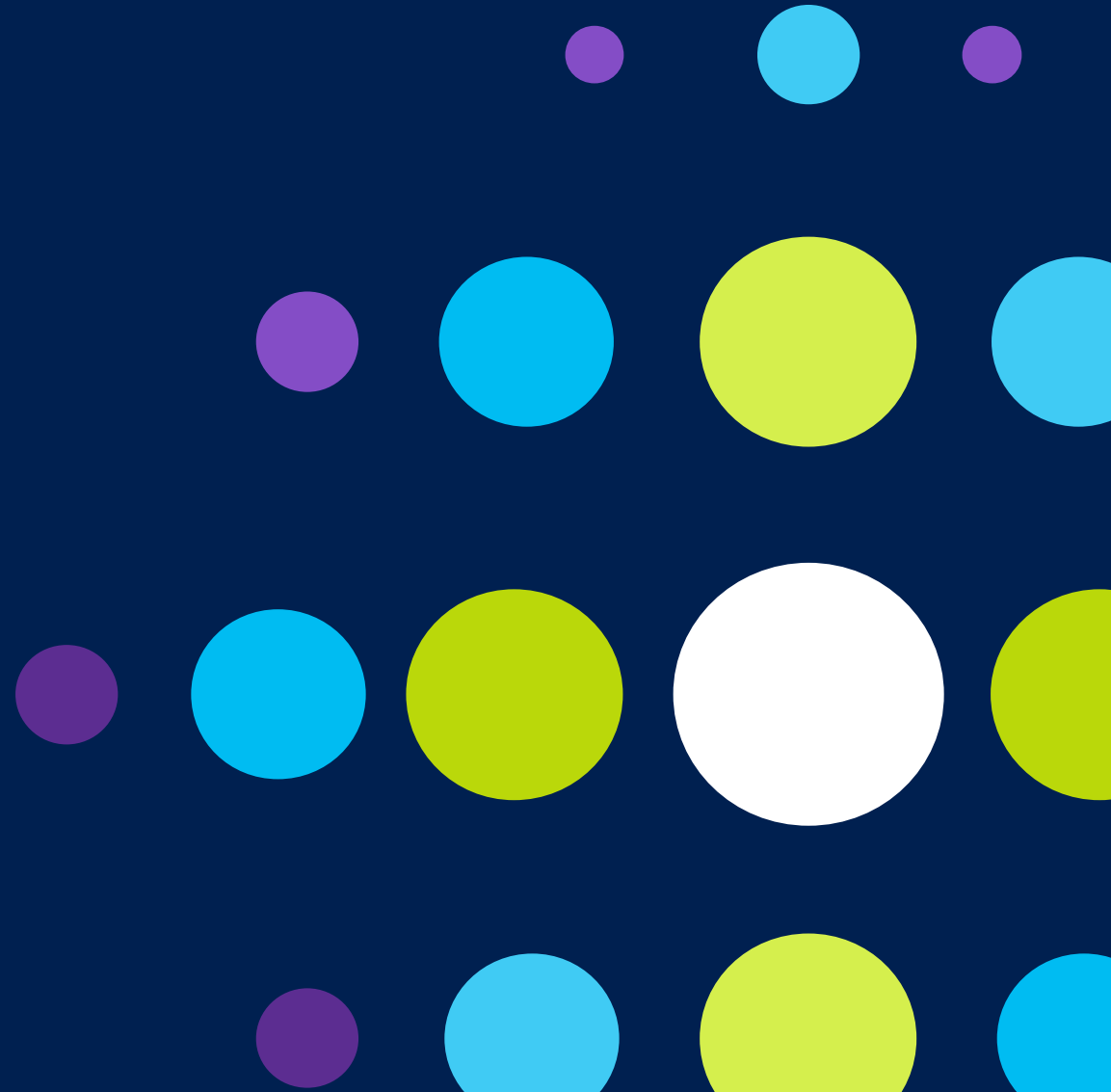
Select what to review * Azure AD Roles

Scope *
☐ All users and groups
☒ (Preview) Service Principals

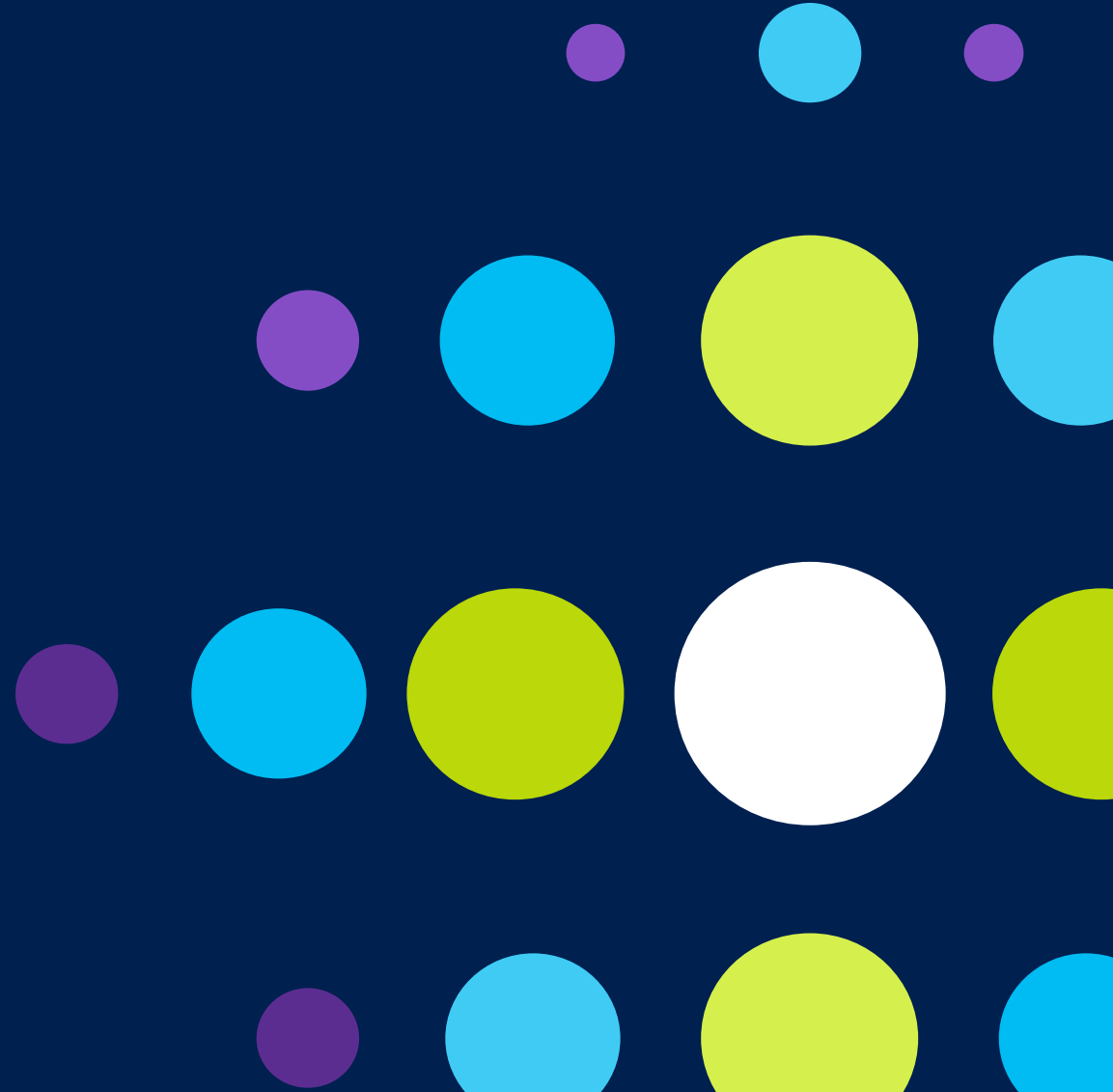
Assignment type
☒ Active ⓘ
☐ Eligible ⓘ
☐ Active And Eligible

Role * Global Administrator

Creating an access review for workload identities Demo



Workload Identity Federation



Background

- Managed identities
- Credentials NOT managed by developers
- Assign identity to Azure resources:
 - App Service
 - Functions
 - LogicApps
 - Storage
- Request tokens from Azure AD

What is “Workload Identity Federation”

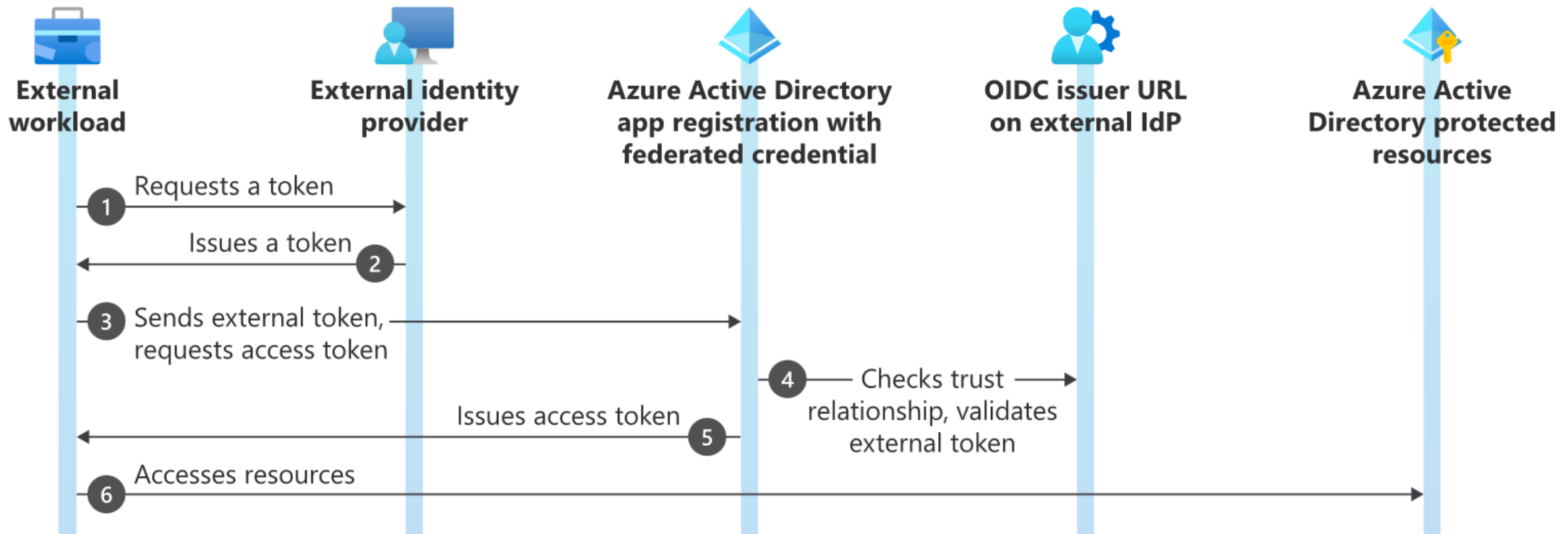
Several scenarios require developers to manage secrets for Azure AD service principals, where the secrets are stored securely and rotated regularly. Some examples are GitHub Actions, K8s pods. This can lead to:

- Security breaches due to secrets leaking
- Service downtime when secrets expire

Workload identity federation allows developers to use a 3rd party JWT token to get access tokens for Azure AD service principals, without needing secrets. Avoids issues around leaked or expiring secrets.

Workload Identity Federation

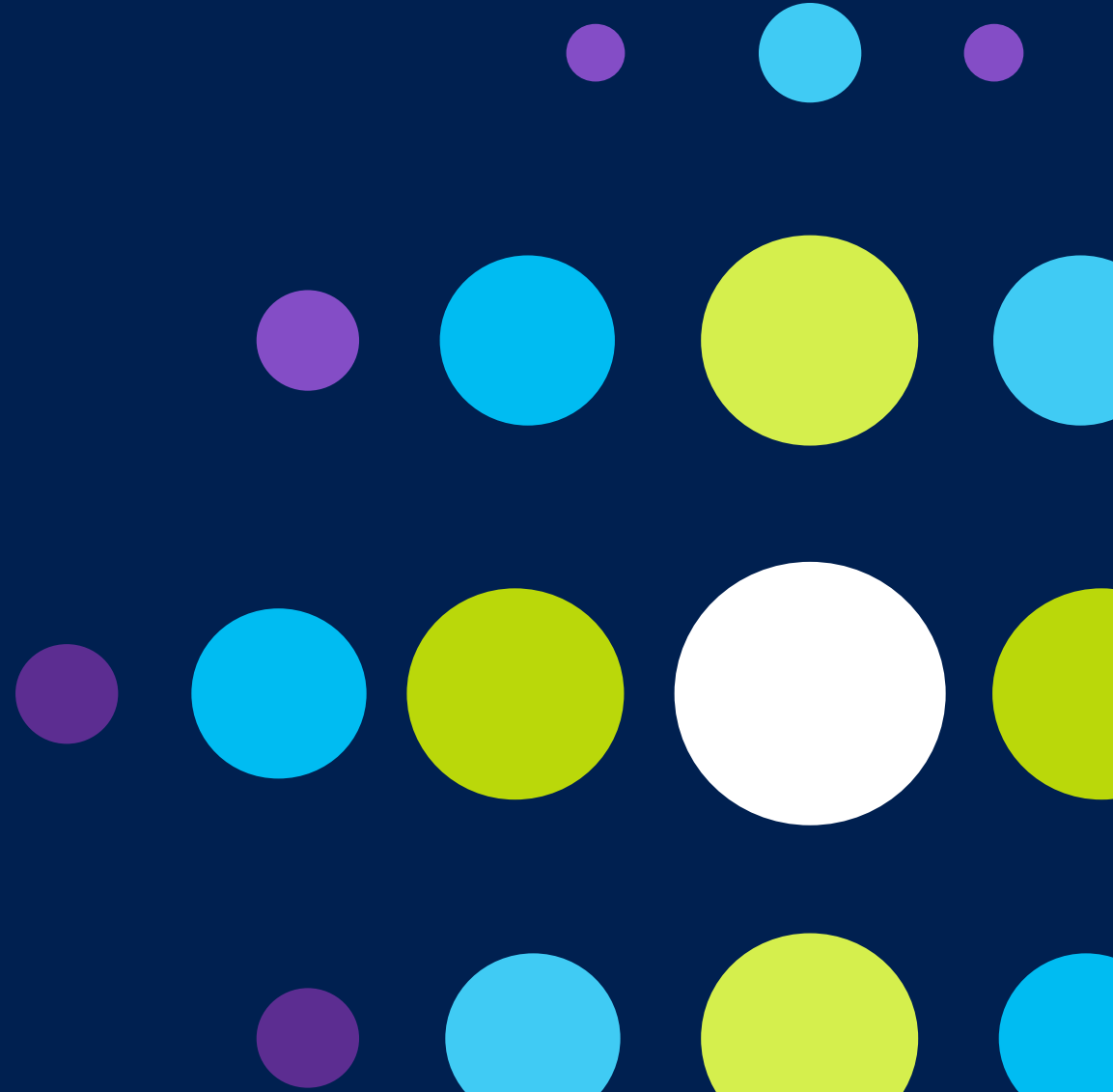
Allows you to access Azure Active Directory (Azure AD) protected resources without needing to manage secrets



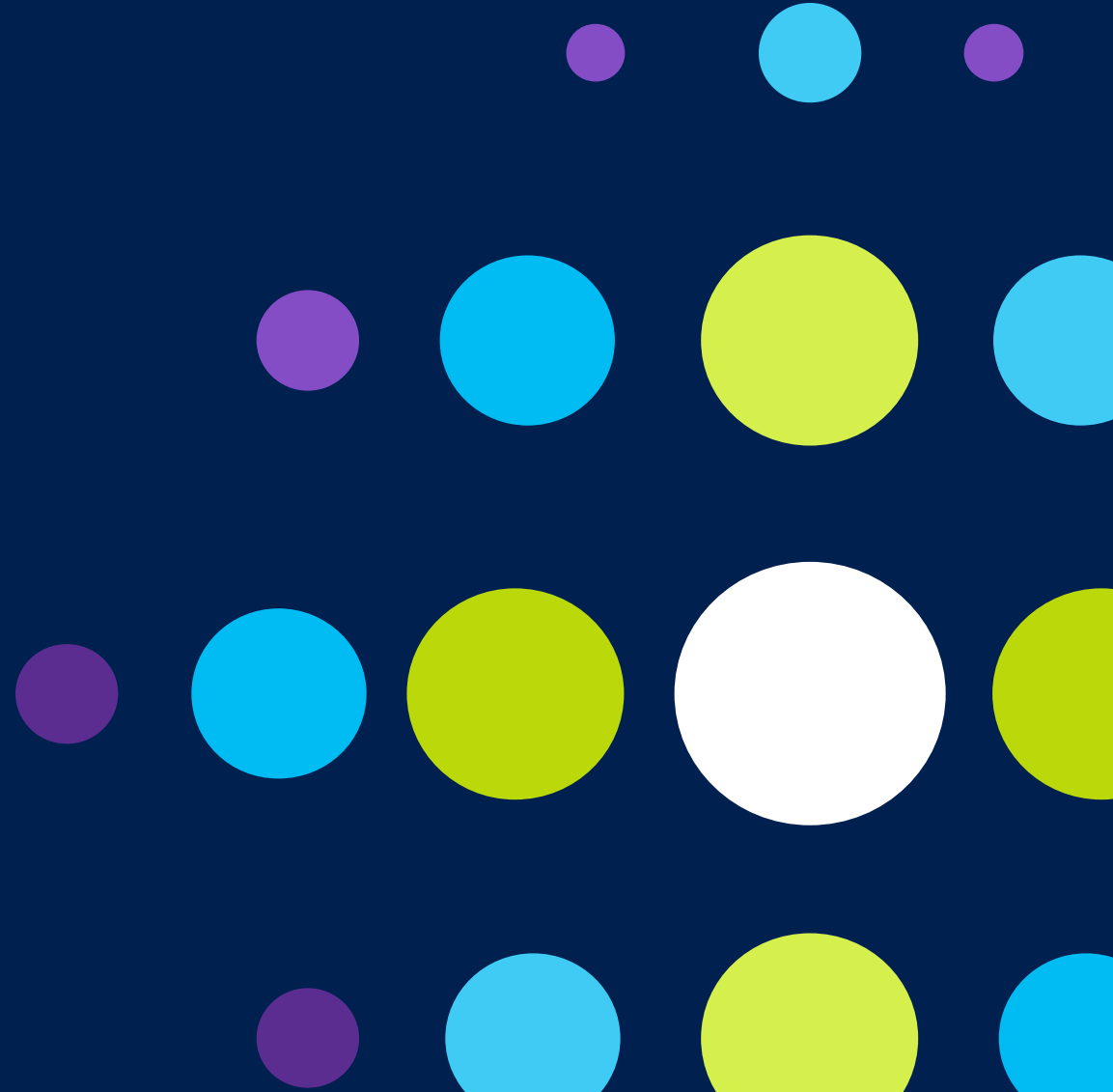
Workload Identity Federation – Supported Scenarios

- GitHub Actions
- Google Cloud
- Workloads running on Kubernetes
- Workloads running in compute platforms outside of Azure

Workload Identity Federation Demo



Resources



Takeaways

- Detect attacks against workload identities
- Control access based on risk
- Export the risk data to the platform of your choice
- Reduce risk and increase security by extending access reviews capabilities beyond user accounts
- Federate workload identities – token-based authentication

Resources

Microsoft docs pages:

- [Workload identities - Microsoft identity platform | Microsoft Docs](#)
- [Workload identity federation - Microsoft identity platform | Microsoft Docs](#)
- [Azure Active Directory Conditional Access for workload identities preview | Microsoft Docs](#)
- [Create an access review of Azure resource and Azure AD roles in PIM - Azure AD | Microsoft Docs](#)
- [Securing workload identities with Azure AD Identity Protection Preview | Microsoft Docs](#)

Workload Federation – GitHub Actions Documentation:

- [Microsoft Documentation](#)
- [GitHub Documentation](#)
- [Jon Gallant GitHub Code](#)



Thank you!



Questions?