Microsoft Security

Entra the Matrix

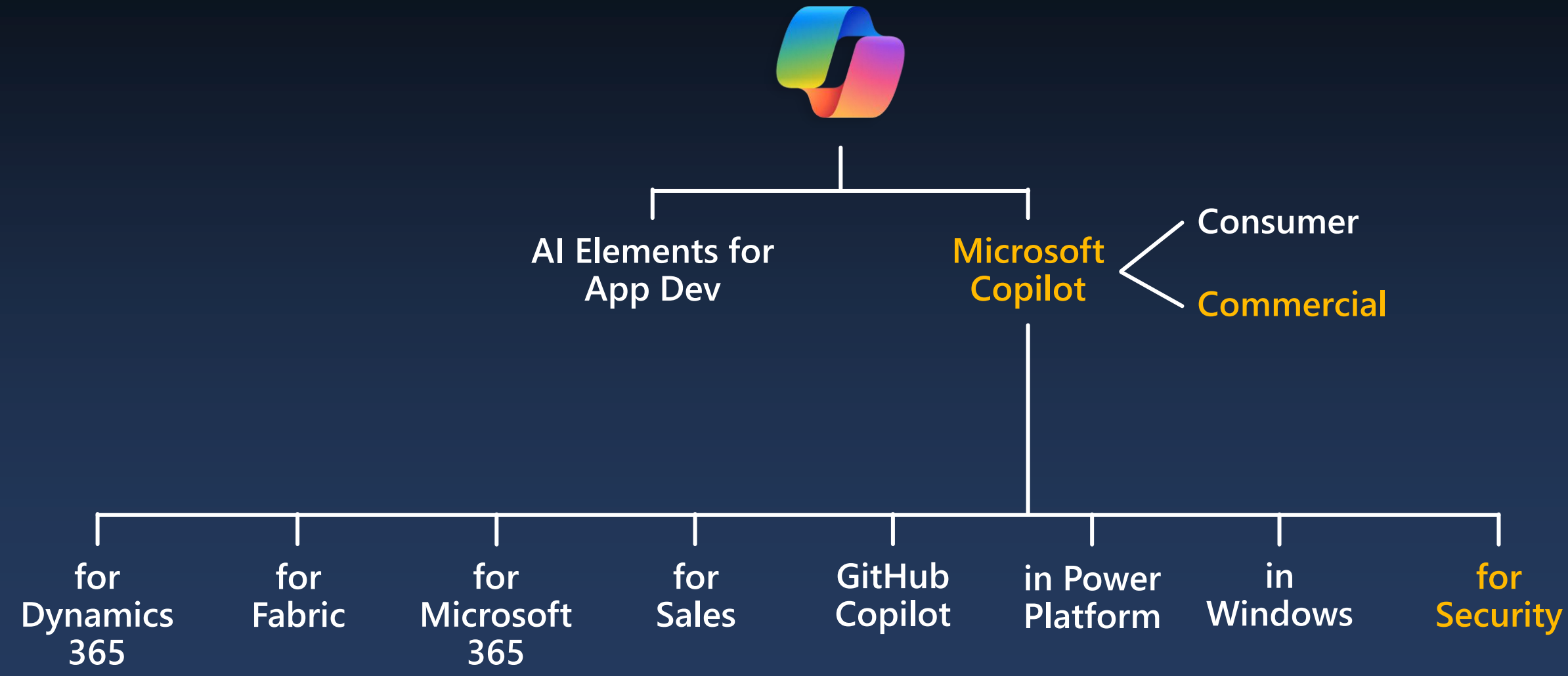
Where Security Copilot is your Neo!

Ronny de Jong
Security Technical Specialist | CCSP CISSP CISM

Agenda

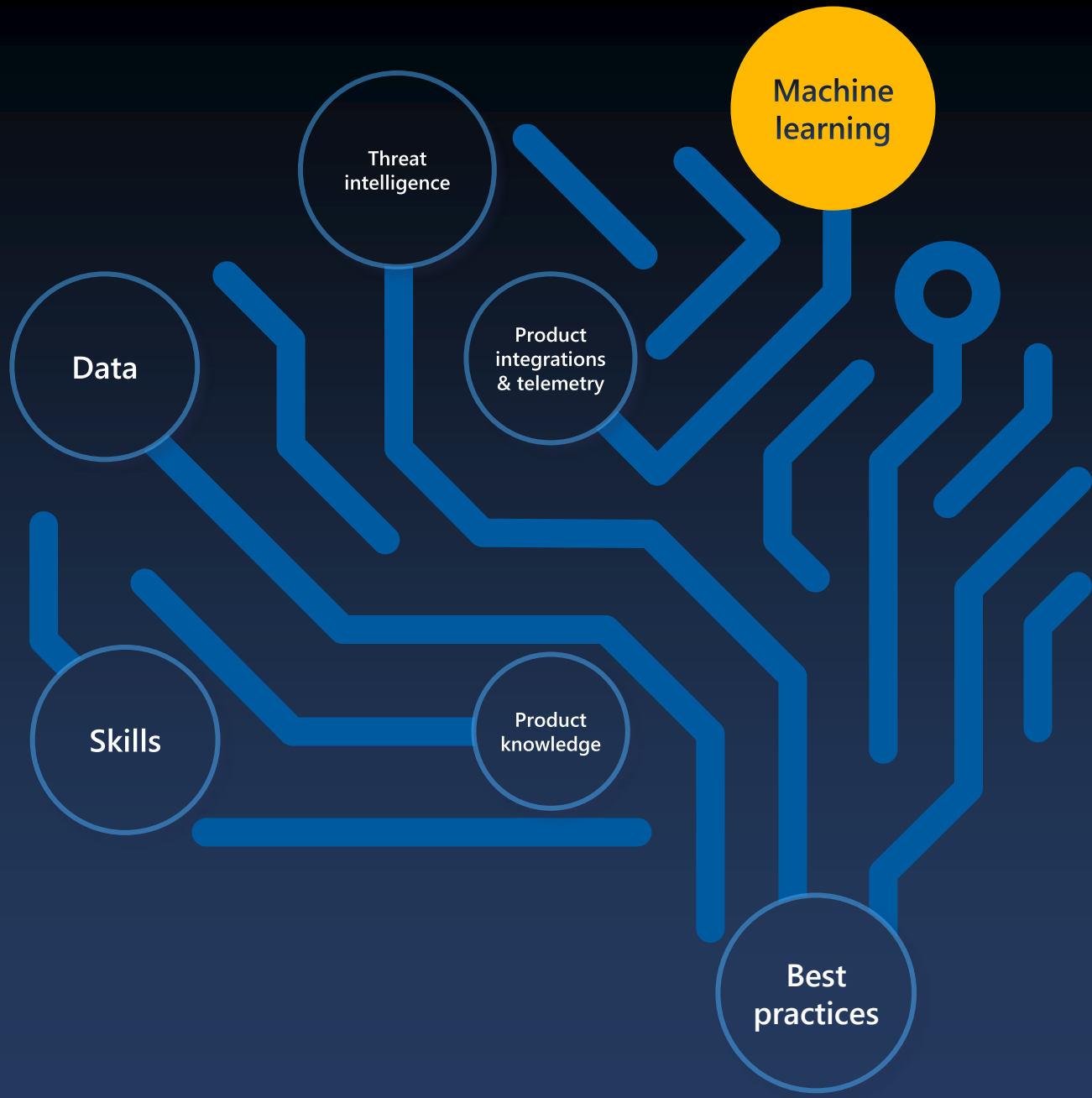
Introduction Security Copilot
Explore Security Copilot in Entra
Unlock hidden identity features

The Microsoft AI Landscape



Microsoft Security Copilot

The first generative AI security product that empowers security and IT teams to defend at the speed and scale of AI



End-to-end security at machine speed and scale

Microsoft Security Solutions	Available in the standalone experience	Available as an embedded experience
Microsoft Defender XDR	✓	✓
Microsoft Sentinel	✓	✓*
Microsoft Intune	✓	✓
Microsoft Entra	✓	✓
Microsoft Purview	✓	✓
Microsoft Defender for Cloud	✓	✓

Rapid investigation and response

Investigate with AI-assisted insights and quickly pivot to remediation with actionable, prioritized recommendations

Scaled visibility

Quickly assess security posture, threats and policy or compliance gaps. Access summaries with context to understand the potential impacts.

Faster troubleshooting

Get deep understanding of device, user, access, and app status to resolve issues quickly. Find and remediate policy issues faster with natural language prompts.

Advanced skills unlocked

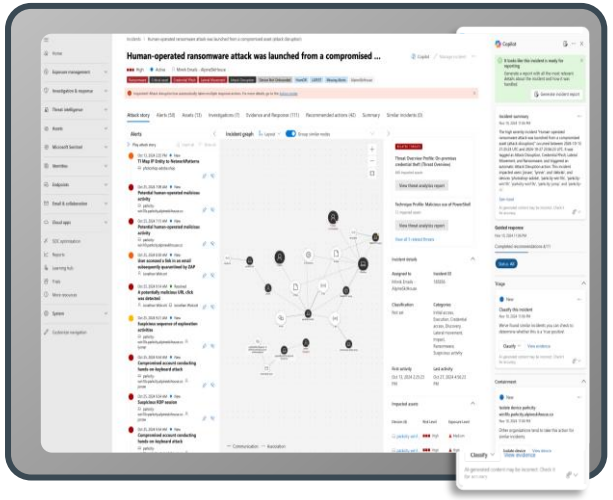
Script analysis and natural language to KQL and KeyQL empower any team member to complete complex tasks with confidence.

*Available as part of the Unified Security Operations Platform.

Evolution of Security Copilot

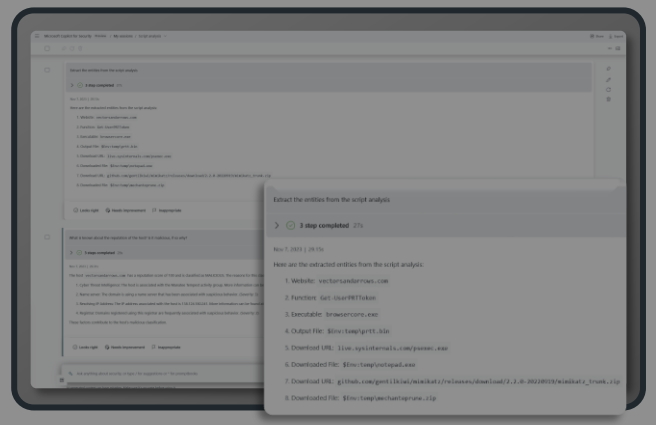
Embedded

Offers the intuitive experience of getting Copilot guidance natively within the products that your team members already work from and are familiar with



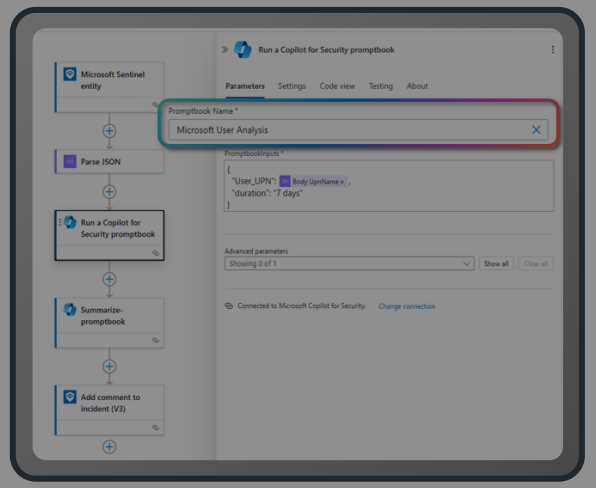
Standalone

Helps teams gain a broader context to troubleshoot and remediate incidents faster within Copilot itself, with many use cases in one place, enabling enriched cross-product guidance



Automation

Helps teams accelerate response with built-in and custom promptbooks as well as integration with Logic Apps



Security Copilot Platform

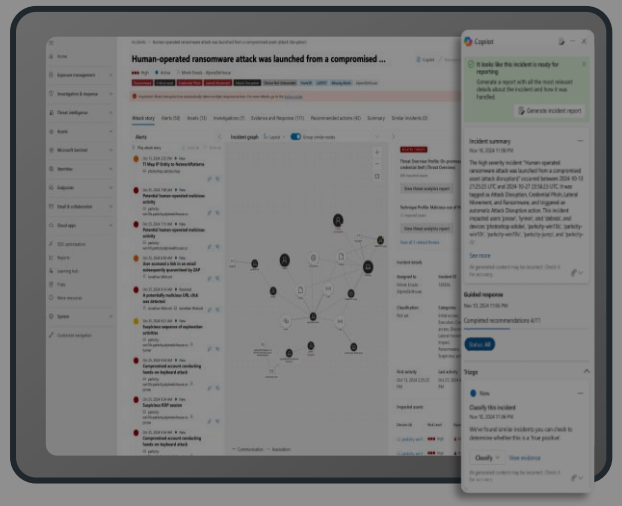
Demo #1

Setup Security Copilot & integration in Microsoft Entra

Evolution of Security Copilot

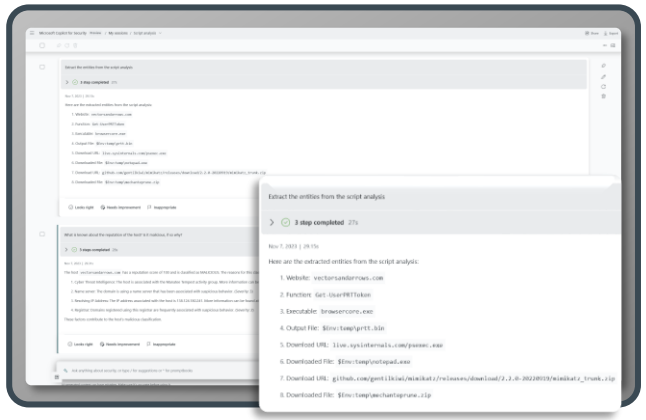
Embedded

Offers the intuitive experience of getting Copilot guidance natively within the products that your team members already work from and are familiar with



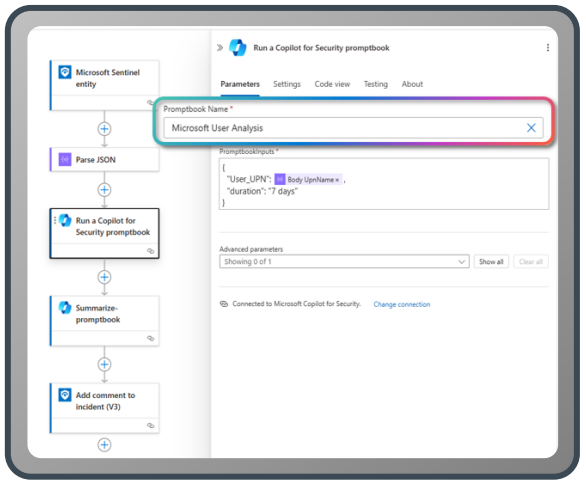
Standalone

Helps teams gain a broader context to troubleshoot and remediate incidents faster within Copilot itself, with many use cases in one place, enabling enriched cross-product guidance



Automation

Helps teams accelerate response with built-in and custom promptbooks as well as integration with Logic Apps



Security Copilot Platform

Elements of effective prompts

Goal

What is the specific security-related information you need?

"Give me information about Simon Templar..."

+

Context

What is the workflow focus or analysis for a tailored response?

"...that includes the most recent risky sign-ins..."

+

Source

Is there a plugin, known info, or data source Security Copilot should use?

"...in Entra..."

+

Expectations

How will the information be used and what is the desired format?

"...summarize into a list of recommendations that I can submit to my manager."

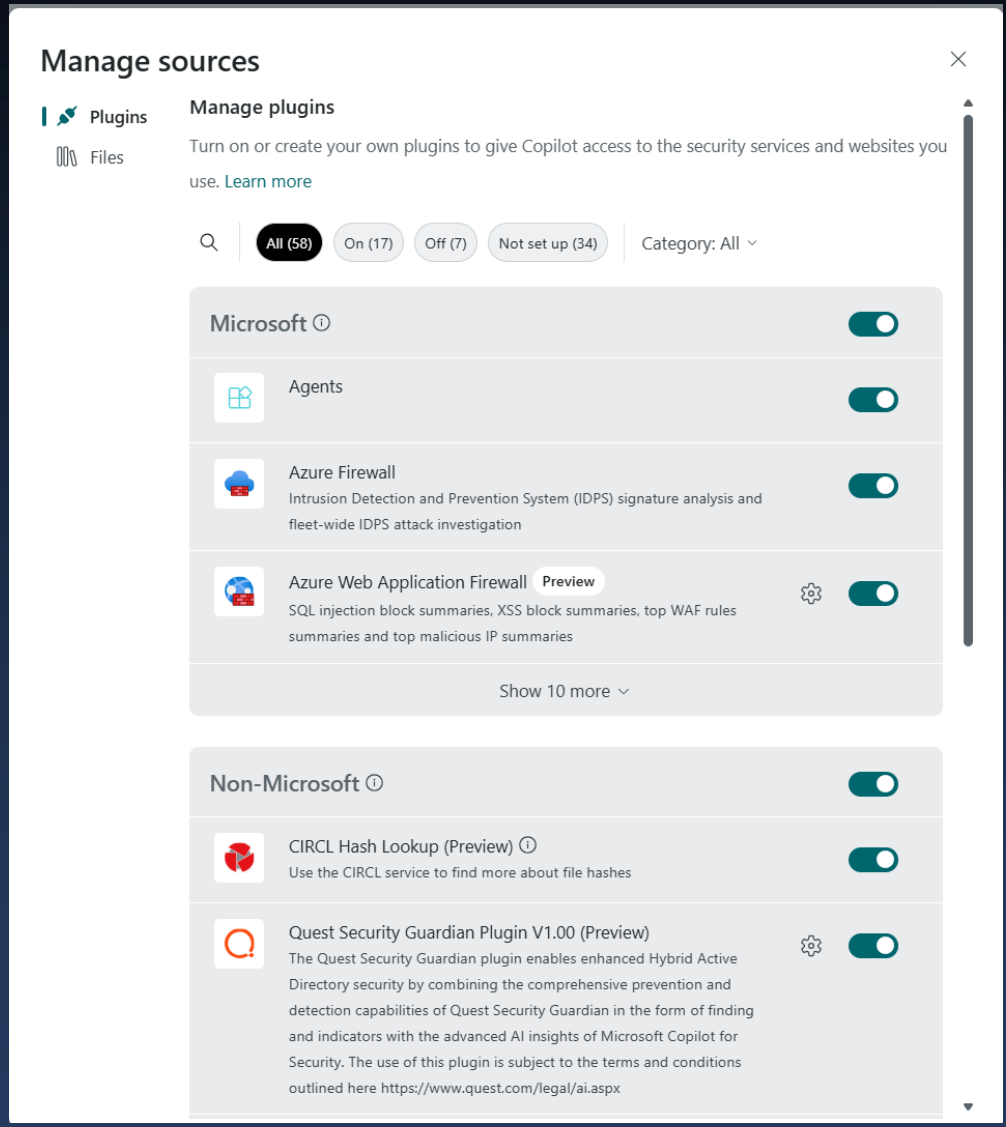
Plugins

Pre-built

Pre-built plugins from 1st & 3rd Party applications & services. Invoke skills within plugins using natural-language prompts or direct skill invocation. Enable Plugins for all users or just you; Admins have the control!

Custom

You can build your own plugins (API, GPT, KQL) to enrich your investigations.



Custom plugin examples

API plugins

- Additional threat intelligence sources
- Device IoT systems
- Perimeter defense systems

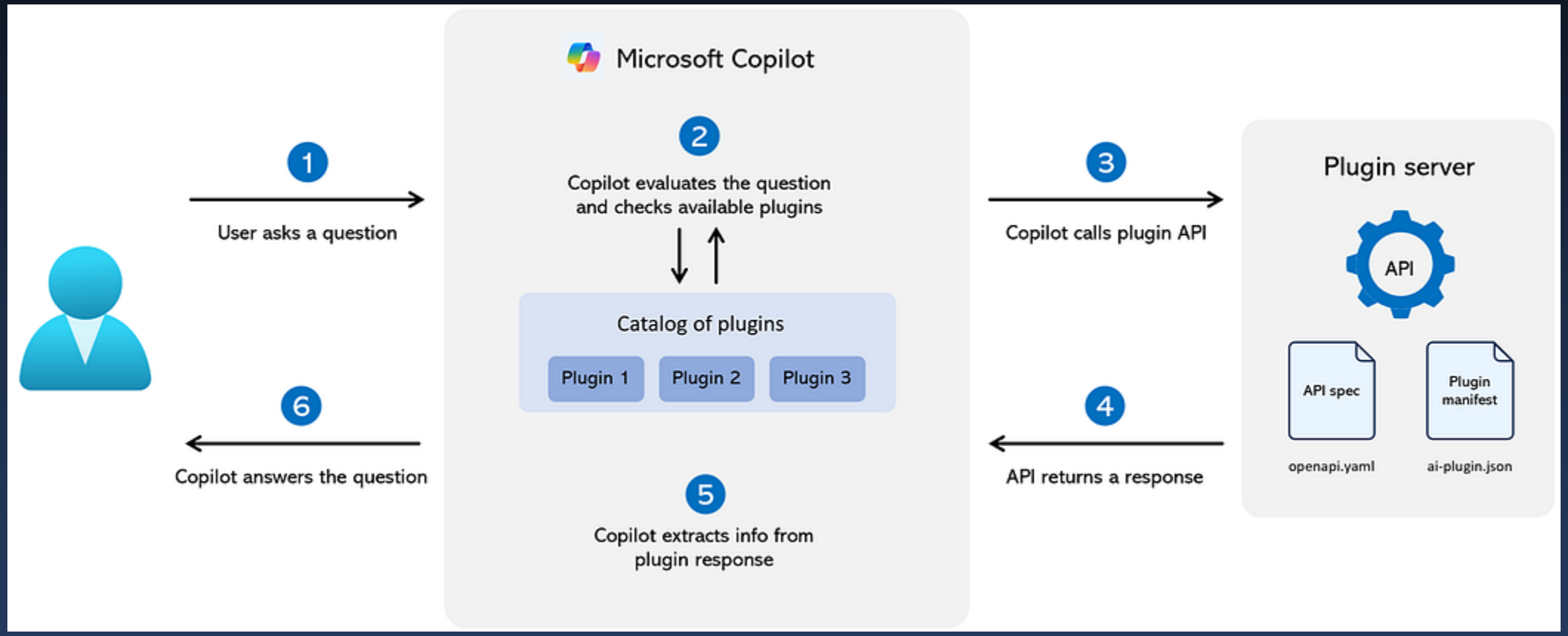
KQL plugins

- Query a KQL database
- Log analytics workspaces
- Defender XDR Advanced Hunting

GPT plugins

- Summarize sessions in specific formats
- Define reporting structure
- Reformat specific subtext

How to interact with Security Copilot



A plugin consists of two main components

OpenAPI Specification

This component describes how the API of the plugin works. It defines the endpoints, request and response formats, authentication mechanisms, and any other relevant details about the plugin's API.

```yaml
openapi: 3.0.0
info:
    title: Microsoft Graph API Plugin to access data from Entra ID and Conditional Access Policies
    description: Specification to retrieve information from the Graph API for Conditional Access P
    version: "1.0"
servers:
    - url: https://graph.microsoft.com/v1.0
paths:
    /identity/conditionalAccess/policies:
        get:
            operationId: ListCAPolicies
            summary: List all Entra ID Conditional Access Policies.
            responses:
                200:
                  description: Successful retrieval.
                401:
                  description: Unsuccessful authentication.
```

Plugin Manifest

The plugin manifest file is used to explain to Copilot how to use the plugin. The manifest file helps Copilot understand how to integrate and interact with the plugin.

```yaml
Descriptor:
  Name: Conditional Access - Graph API Plugin
  DisplayName: Conditional Access - Graph API Plugin
  Description: Retrieves information from Microsoft Graph API with the current user permissions.
  Authorization:
    Type: AADDelegated
    EntraScopes: https://graph.microsoft.com/.default
SkillGroups:
  - Format: API
    Settings:
      OpenApiSpecUrl: https://raw.githubusercontent.com/rdejong1979/security-copilot-plugins/refs/
```

KQL Type Plugin

Help the orchestrator to select this plugin with good description and example prompts

```
Descriptor:
  Description: >
    Identity Security skills to query Identity events for detection and forensics hunting across User Risk Assessment,
    Sign-in Monitoring, Admin Activity Monitoring, Application Usage Monitoring, Privileged Identity Management, Access Review

SkillGroups:
  - Format: KQL
    Skills:
      - Name: IdentityGetUserRiskAssesment
        DisplayName: Get User Risk Assessment
        Description: >
          Fetches the user risk levels based on their activities. This could include sign-in attempts from unfamiliar locations,
          repeated failed sign-in attempts, or other suspicious behavior.
        ExamplePrompt:
          - "Get all risky users"
          - "Fetch risky users"
          - "Run users risk assessment"
          - "List all risky users"
        Settings:
          Target: Defender //
          Template: |-
            // Query to fetch user risk events with sign-in details
            let RiskyEvents = AADUserRiskEvents
            | where TimeGenerated > ago(1d)
            | project UserPrincipalName, RiskLevel, RiskEventType, TimeGenerated;
            let SignInAttempts = SigninLogs
            | where TimeGenerated > ago(1d)  // Same time filter
            | summarize AttemptCount = count(), FailedAttempts = sumif(1, ResultType != 0) by UserPrincipalName, Location = tostring(LocationDetails), IPAddress, TimeGenerated;
            RiskyEvents
            | join kind=inner (SignInAttempts) on UserPrincipalName
            | where RiskLevel != "None"  // Filter out non-risky users
            | project UserPrincipalName, RiskLevel, RiskEventType, AttemptCount, FailedAttempts
            | order by RiskLevel desc, TimeGenerated desc
            | take 1000
```

Target can be:

- Sentinel
- Defender
- Log analytics
- ADX

Query input

Return only the fields you need

API Type Plugin

```yaml
openapi: 3.0.1
info:
  title: Microsoft Graph API - List Conditional Access Policies
  description: Retrieve a list of conditional access policy objects.
  version: 1.0.0
servers:
  - url: https://graph.microsoft.com/v1.0
paths:
  /identity/conditionalAccess/policies:
    get:
      summary: List conditional access policies
      description: Retrieve a list of conditional access policy objects.
      operationId: listConditionalAccessPolicies
      parameters:
        - name: $skip
          in: query
          description: Skip the first n results.
          required: false
          schema:
            type: integer
        - name: $top
          in: query
          description: Show only the first n results.
          required: false
          schema:
            type: integer
        - name: $count
          in: query
          description: Include count of items.
          required: false
          schema:
            type: boolean
        - name: $filter
          in: query
          description: Filter items by property values.
          required: false
          schema:
            type: string
        - name: $orderby
          in: query
          description: Order items by property values.
          required: false
```

In the **info object** is like a summary of key details about the API.
It usually includes things like the title, a brief description, the version number, and links to stuff like licenses and terms of service.
The only things that are required in there are the title and version

In the servers object, we can list one or more main paths used in requests to the API.
This section is in array format, so each path needs to be specified separately, unlike the values in the info section.
The basepath is the part of the web address that comes before the specific endpoint. The only required property is the url

The Paths object
The paths object can be seen as a roadmap for the endpoints available within the API.
It provided details on how to access the endpoints and what actions you can perform.
Each endpoint is represented by a unique path within the paths object
To break this section a bit more down into digestible chunks, I will describe the most important parts.

- path
- HTTP methods
- operation object ...

Operation Object
For each HTTP method specified, there must be an associated operation object containing additional information about the operation.
Examples of these operation objects are parameters, request body, responses, etc.

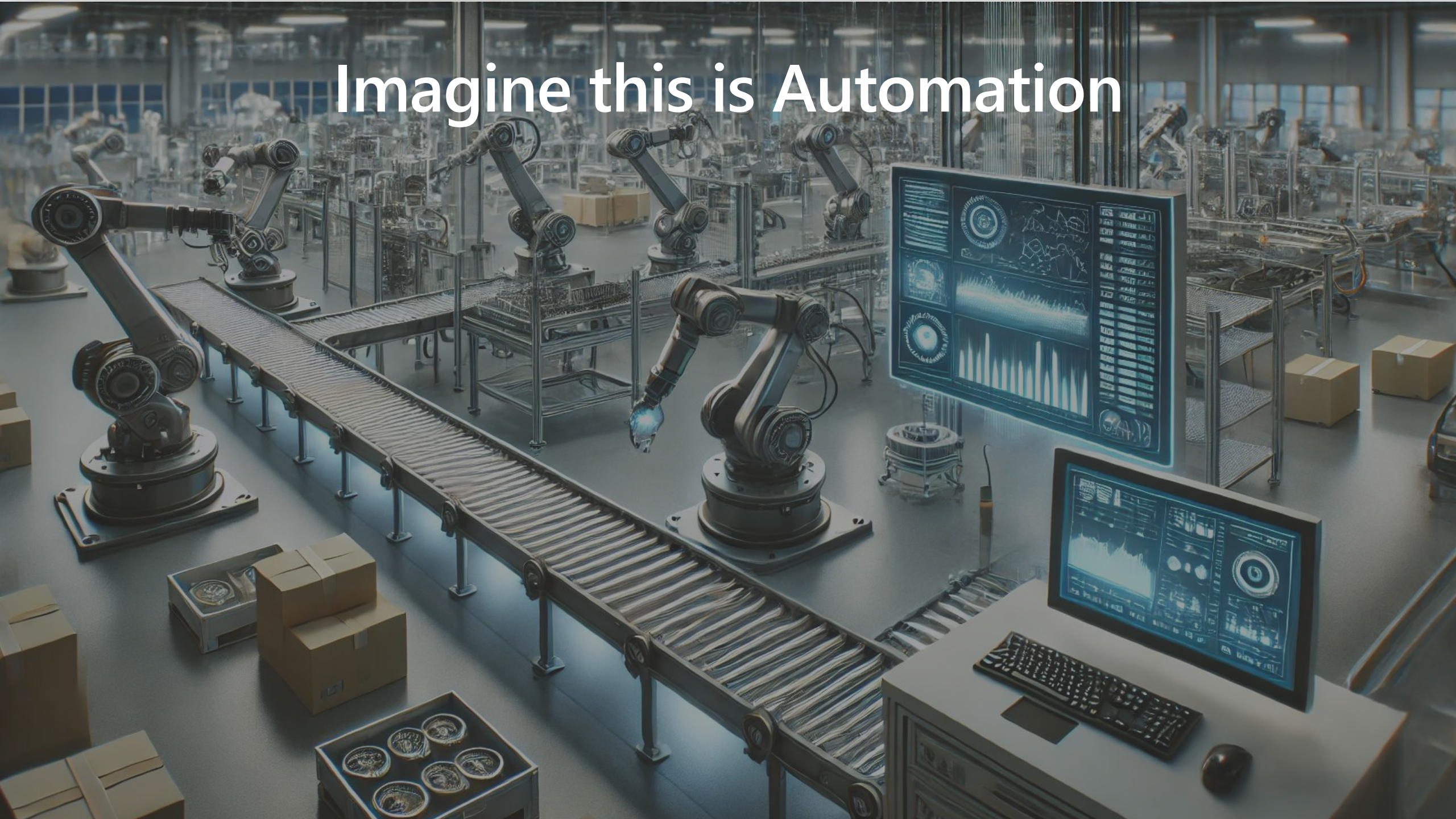
The only required values are summary and the operation object responses
The summary field provides a brief, human-readable description of the endpoint.

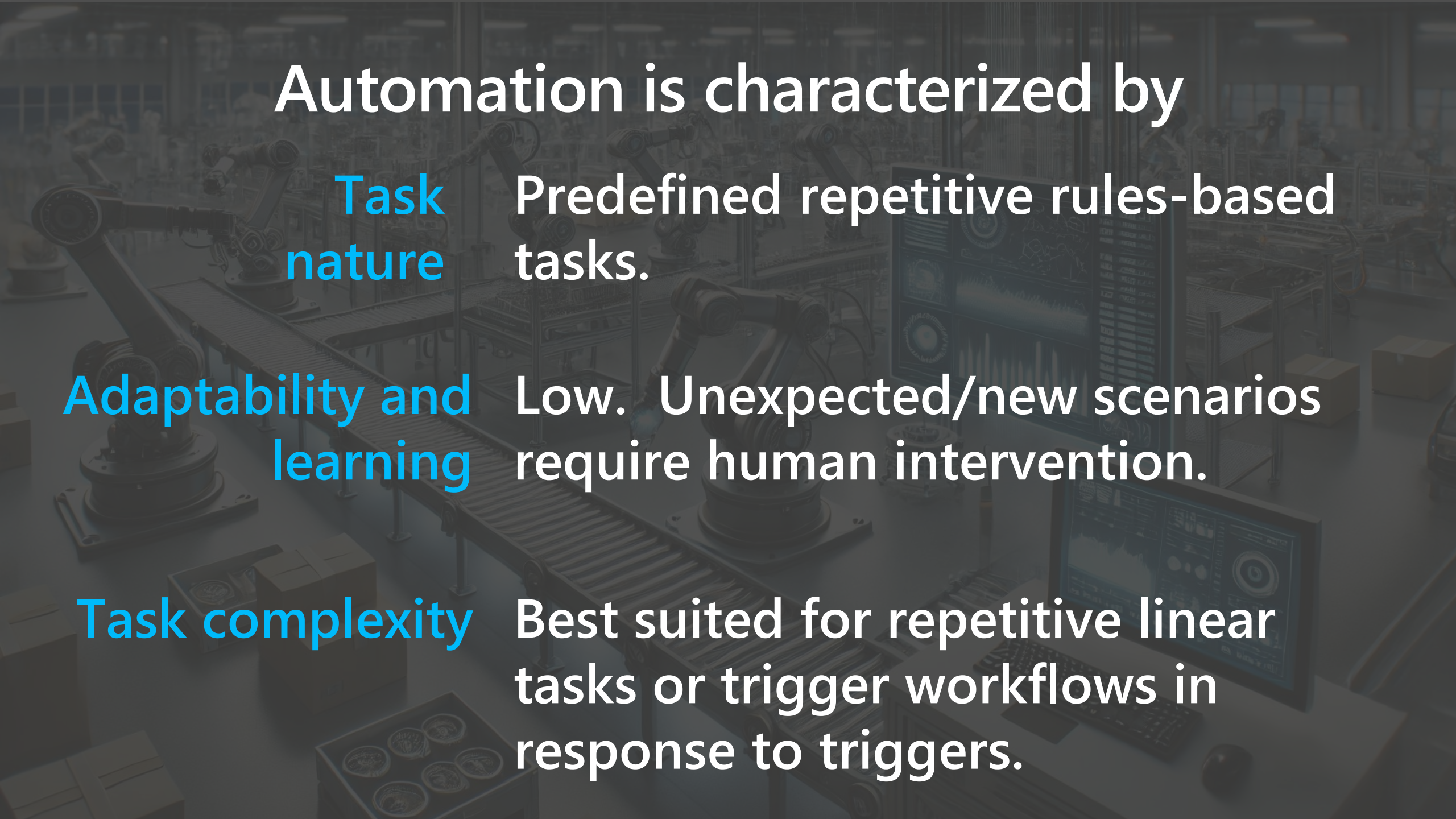
In the responses section, we define the possible responses that the API can return when that endpoint is accessed. It contains the HTTP status codes and their corresponding descriptions.
Optionally, the responses section includes details about the response payload, like the format and schema definition.

Parameter Object
You don't have to use the parameter object, but it's handy when making a plugin for Copilot(s).
If you include the parameter object in the path item, the parameters will affect all actions on that path.
Alternatively, you can place parameters in the operations object, where they'll only affect that specific action.

Depending on the API, the parameters can reside in different locations, indicated by the in field.

Imagine this is Automation





Automation is characterized by

Task nature	Predefined repetitive rules-based tasks.
Adaptability and learning	Low. Unexpected/new scenarios require human intervention.
Task complexity	Best suited for repetitive linear tasks or trigger workflows in response to triggers.

Demo #2

Automation & extend Security Copilot with Microsoft Entra

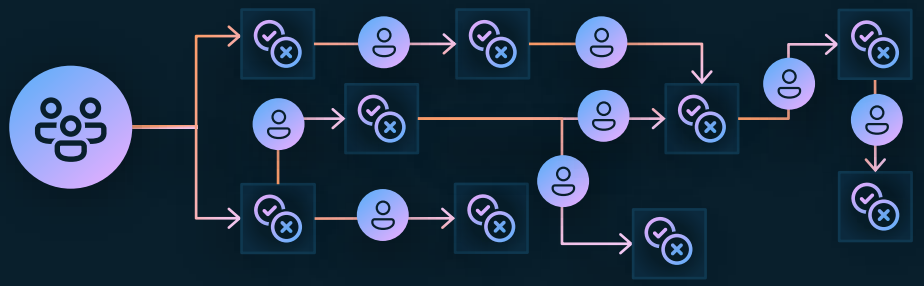
Then this is an agent

An agent Is different

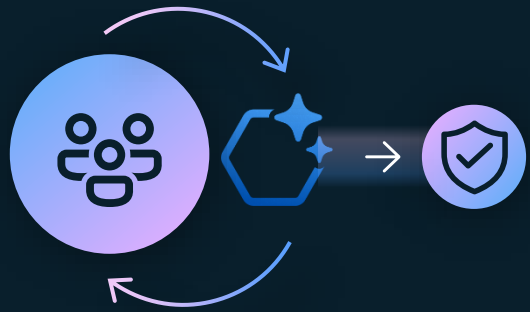
Task nature	Simulates intelligent behavior to create and plan dynamic workflows.
Adaptability and learning	High. Agents learn, analyze patterns, and adapt using reinforcement learning.
Task complexity	Well-suited for complex, non-linear tasks requiring decision making.

Agents go further than traditional automation

Traditional automation



Agentic AI



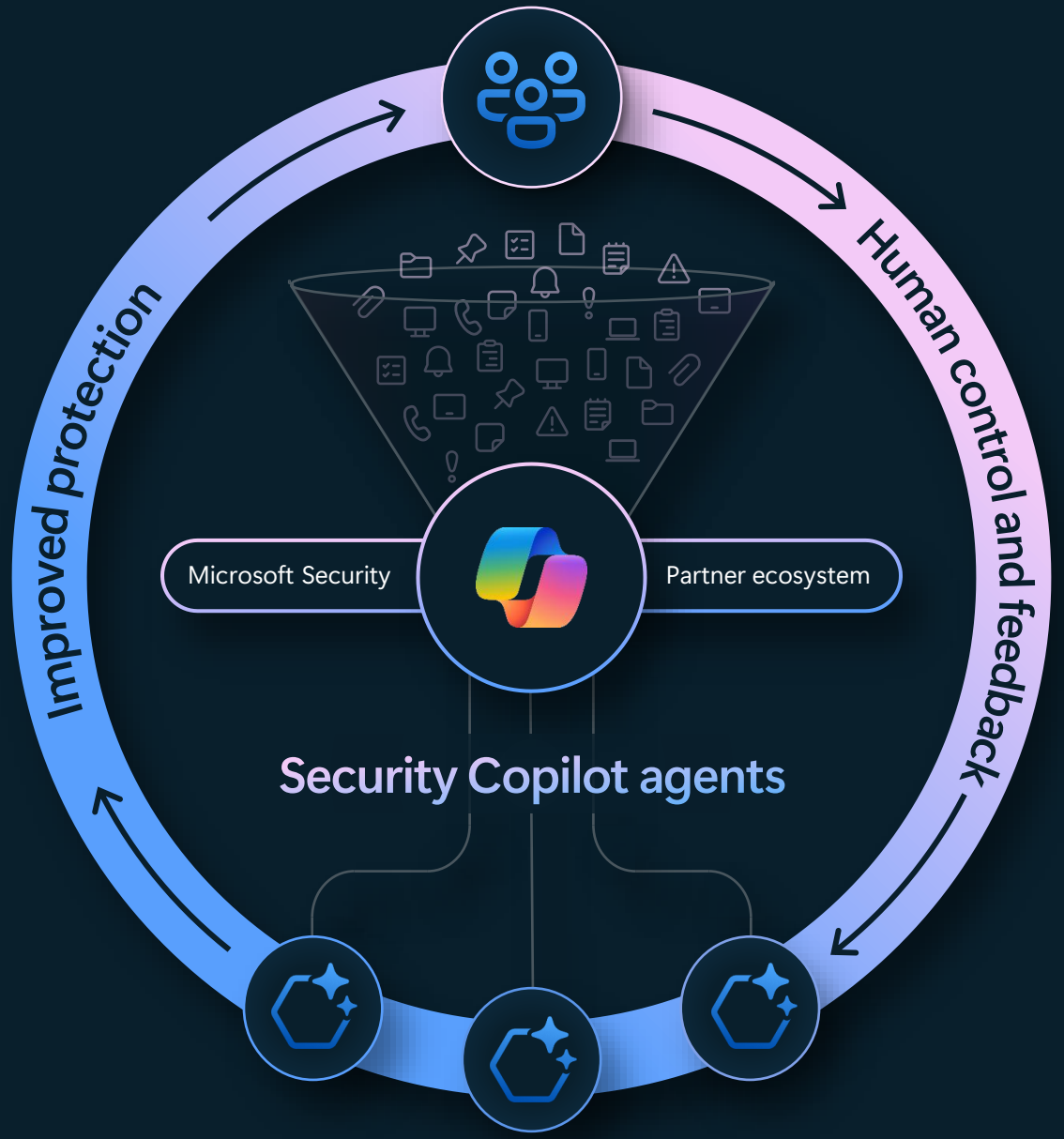
Rigid	Adaptive
Static	Dynamic
Manual updates	Continuous learning
Pre-defined	Context-aware

Smarter defense with Security Copilot agents

Seamlessly integrated with Microsoft Security solutions and partner ecosystem, **Microsoft Security Copilot agents** enhance security and IT operations with autonomous and adaptive automation.

Purpose-built for security, agents:

- **continuously learn** from feedback
- **dynamically reason and adapt** with your team fully in-control
- **operate securely** within Microsoft's Zero-Trust framework



Conditional Access Optimization Agent in Microsoft Entra

Quickly identify security gaps

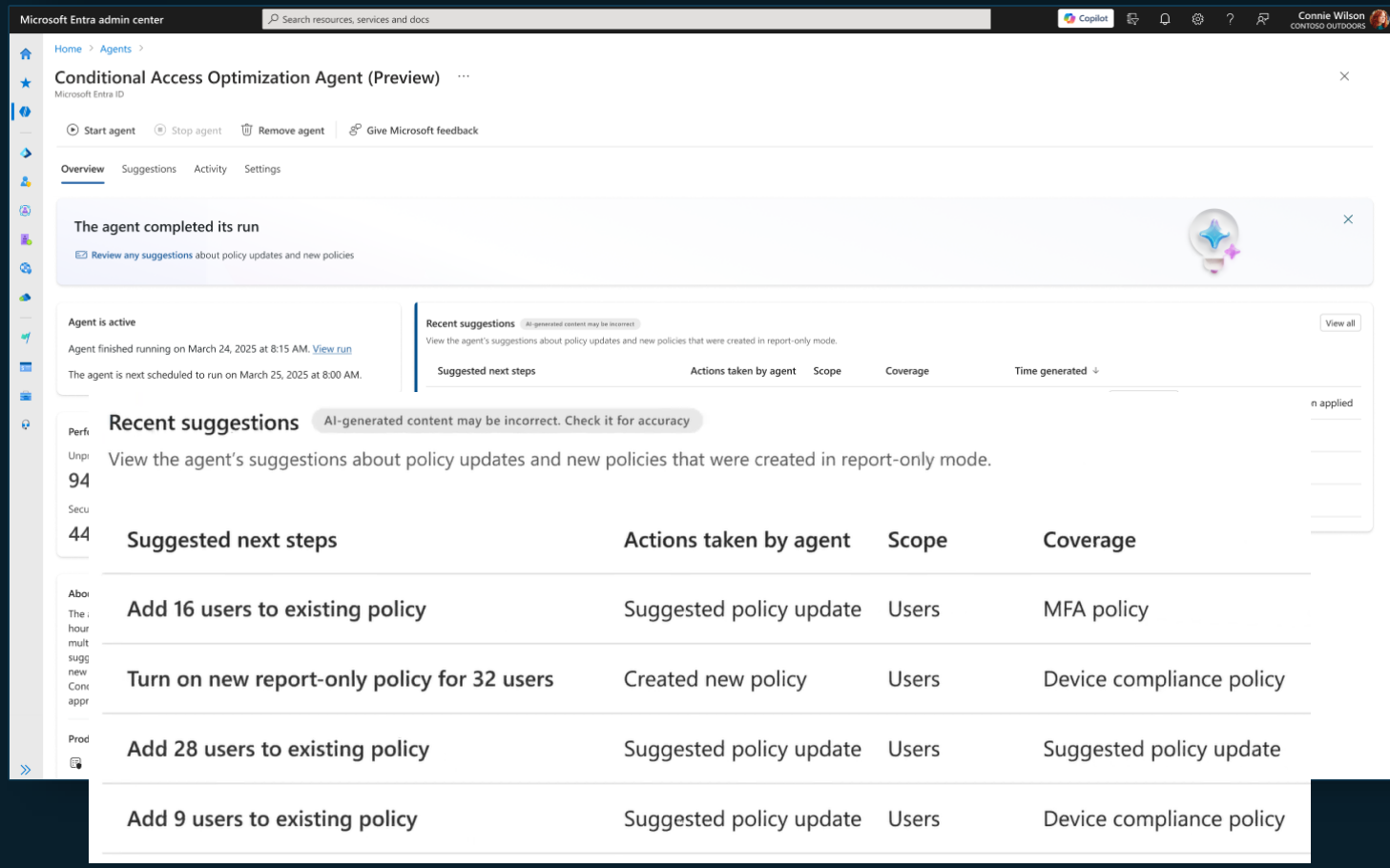
The agent continuously monitors for new users and apps to detect misalignments with Conditional Access policies, reducing unnoticed vulnerabilities.

One-click fixes

Get actionable recommendations with easy one-click remediation, streamlining CA policy updates and enhancing security with minimal effort.

Secure access as conditions change

The agent continually responds to changes in the environment, enhancing protection and reducing manual audits.



Demo #3

Conditional Access Optimization Agent in Microsoft Entra

Microsoft Entra

https://entra.microsoft.com

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

Connie Wilson
CONTOSO OUTDOORS

Microsoft Entra | Home

- Home
- Agents
- Favorites
- Entra ID
- ID Protection
- ID governance
- Verified ID
- Global Secure Access
- Permissions Management
- What's new
- Billing
- Diagnose & solve problems
- New support request

Security Copilot agents are here

Discover a whole new way to automate security with AI.

Go to agents

Contoso Outdoors

Tenant ID 485739sjdije03-8jh8-323o4578...

Primary domain contosooutdoors.ms

67,876 View users

56,745 View devices

7,046 View groups

32,423 View apps

Connie Wilson

23904732-238u43u2r32u-32iu4434

View user profile

My Entra role assignments

125 role assignments

Active role assignments

Eligible role assignments

View my roles

55 users at high risk

Number of risky users with risk level "high".

Learn more

5% in the last 30 days

View high risk users

Shortcuts

Add | Sign-ins | Audit logs | Authentication methods | Blocked users | Domain names | Unused service principals | Named locations | Cross-Tenant Access Policies | Tenant restrictions | Risky sign-ins | Risk policies

Get the most out of your licenses and subscriptions

Licenses

Entra P2

Workload ID

Subscriptions

2

View license usage

Deployment suggestions

Microsoft suggests that you deploy these features to improve your security posture

Tasks	Time	Progress
Set up risk-based Conditional Access policies	5 minutes	Not started
Get started with passwordless authentication	8 minutes	Not started
Create an access package for guest users	1 minute	Not started

Tenant status

Identity Secure Score

65.15%

View recommendations

Microsoft Entra Connect

Enabled

View Entra Connect

ditional Access Optimization Preview
nt
soft
ailable

ls new users and apps in your tenant
e they're covered by policies.

Conditional Access Optimization Agent (Preview)

The agent will scan all newly created users and apps from the last 24 hours and determine if they are in scope of at least one policy with multifactor authentication (MFA) or device compliance controls. It will suggest policy changes based on Zero Trust best practices and create new policies in report-only mode. It won't add new users to existing Conditional Access policies or turn on new policies without your approval. Learn more about this agent

Trigger

The agent will run once every 24 hours. You will also be able to run the agent manually at any time.

Permissions

- ✓ Read access for users, devices, and applications
- ✓ Read and write access for groups and Conditional Access policies

Identity

The agent will run using your identity. Agent authentication will expire according to your policies and need to be renewed. Learn more about agent authentication

Products

Conditional Access

Plugins

Microsoft Entra

Role-based access

Conditional Access Administrators, Security Administrators, Global Administrators. Learn more about who can use the agent

Once started, the agent will run in your tenant. You can remove the agent or customize the agent output.

Cancel

Start agent

Generating suggestions for gaps identified ...

Stop the agent if you want to stop this run.

Agent is running

Generating suggestions for gaps identified ...

- ✓ Identified gaps based on data analysis
- ✓ Cross-referenced new users with existing policies to determine if new users are included or excluded
- ✓ Scanned your tenant's Conditional Access policies for policies enforcing multifactor authentication access control
- ✓ Scanned your tenant's audit log to identify new users added in the last 24 hours

Recent suggestions

AI-generated content may be incorrect. Check it for accuracy

View the agent's suggestions about policy updates and new policies tha

Performance highlights

Unprotected users discovered

Sign-ins protected

The agent completed its run

Review any suggestions about policy updates and new policies

Agent is active

Agent finished running on March 18, 2025 at 9:07 AM. View run

The agent is next scheduled to run on March 19, 2025 at 9:00 AM.

Performance highlights

Unprotected users discovered

63

Sign-ins protected

0

About this agent

The agent will scan all newly created users and apps from the last 24 hours and determine if they are in scope of at least one policy with

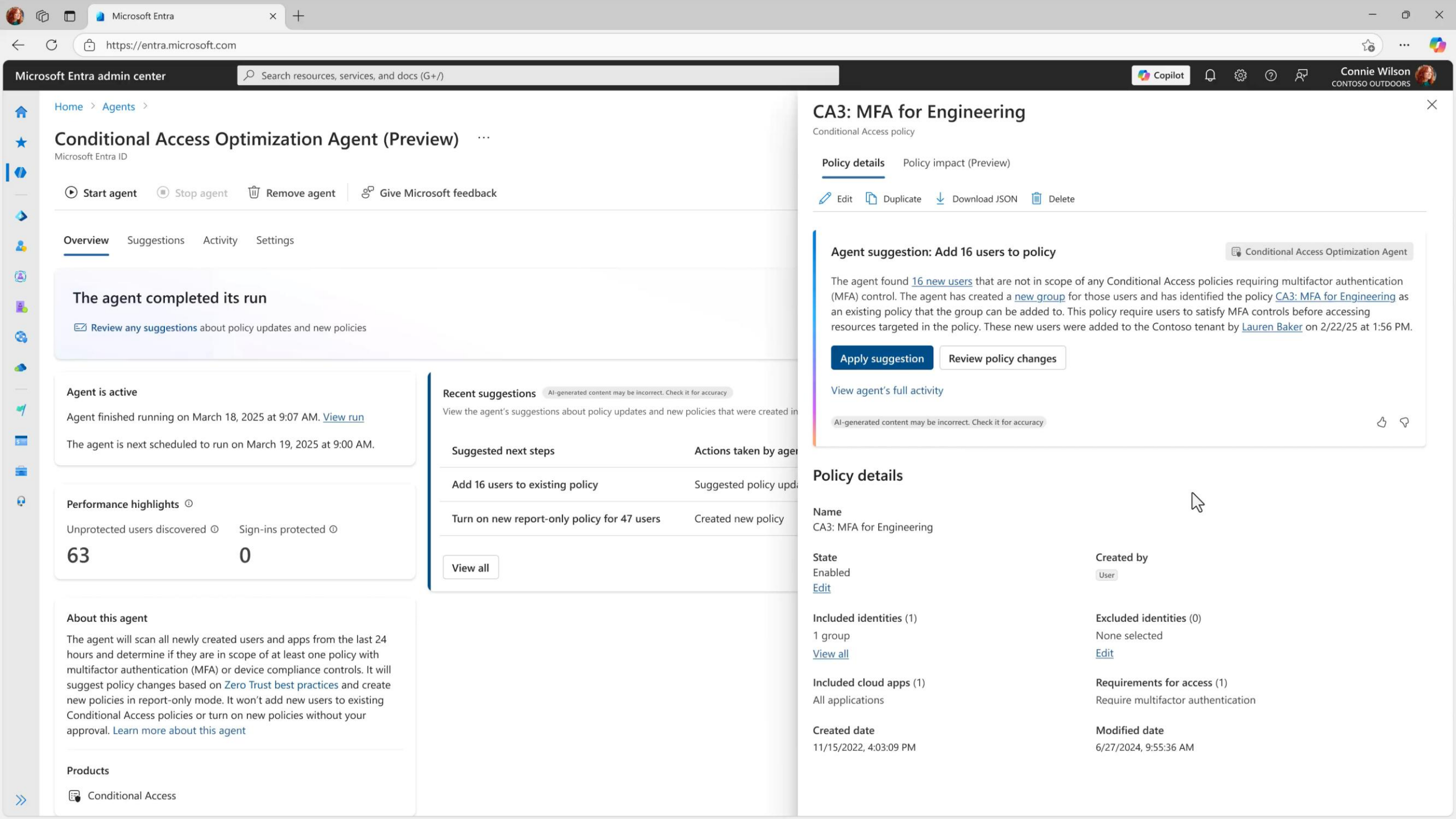
Recent suggestions

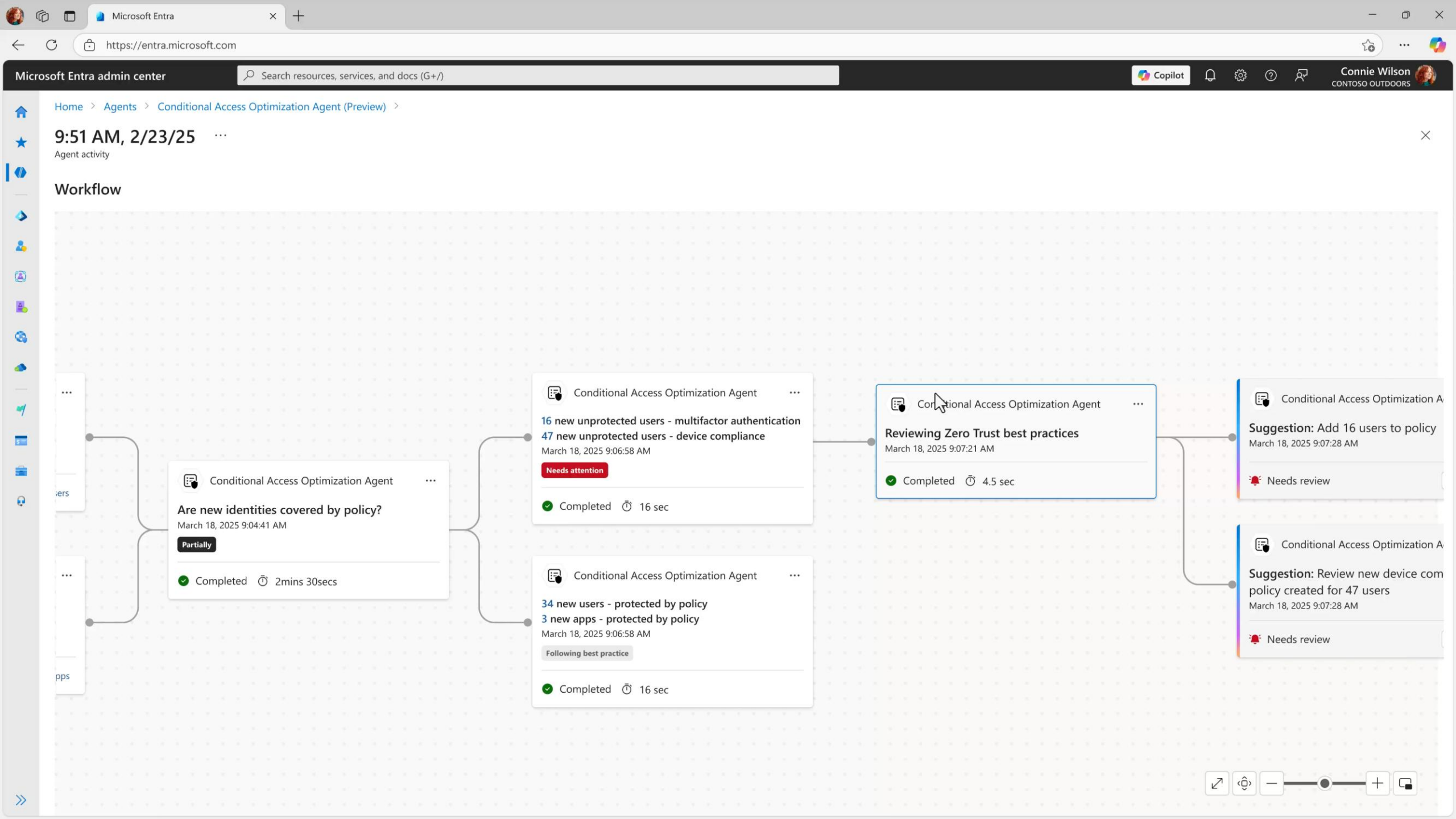
AI-generated content may be incorrect. Check it for accuracy

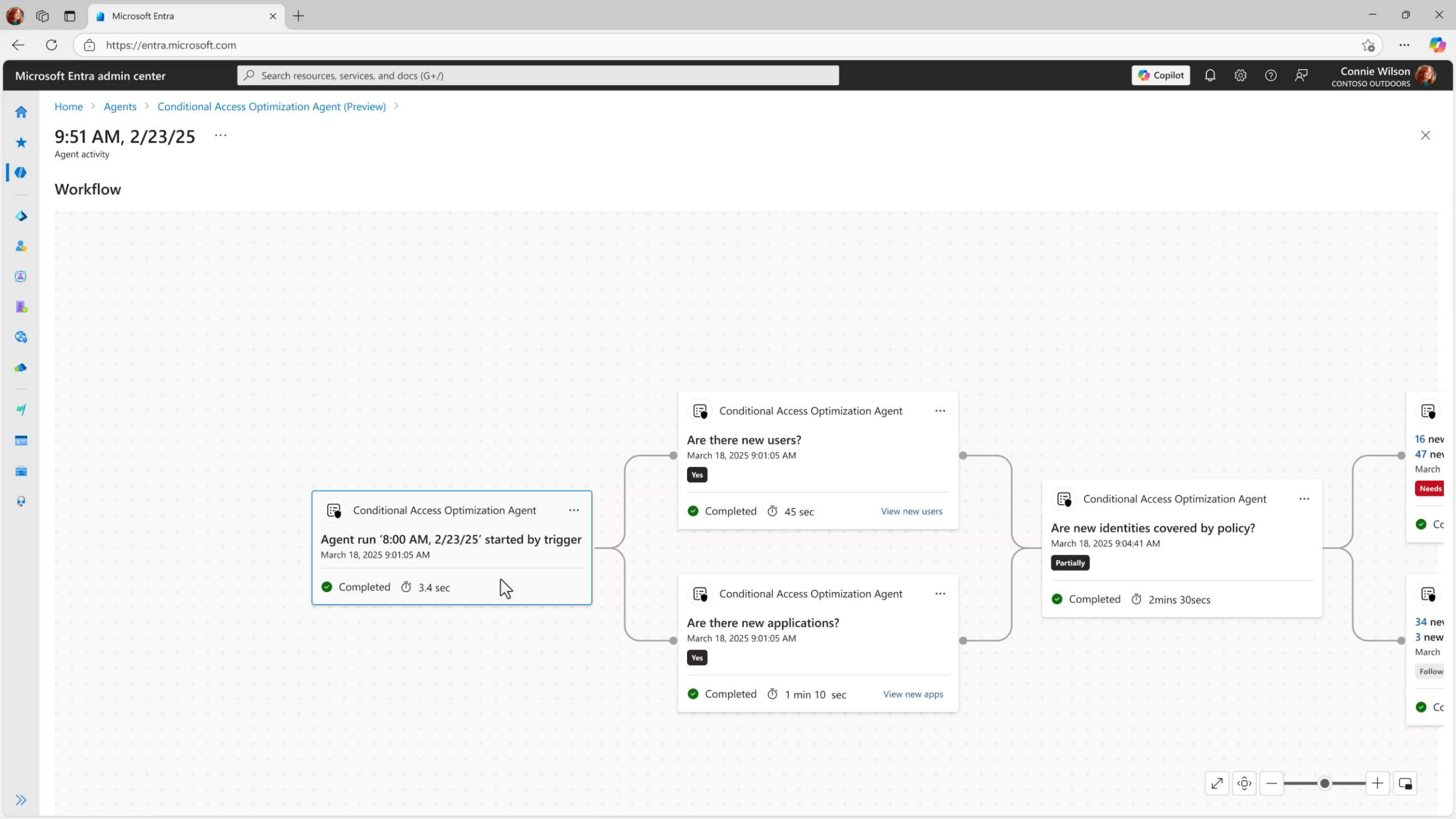
View the agent's suggestions about policy updates and new policies tha

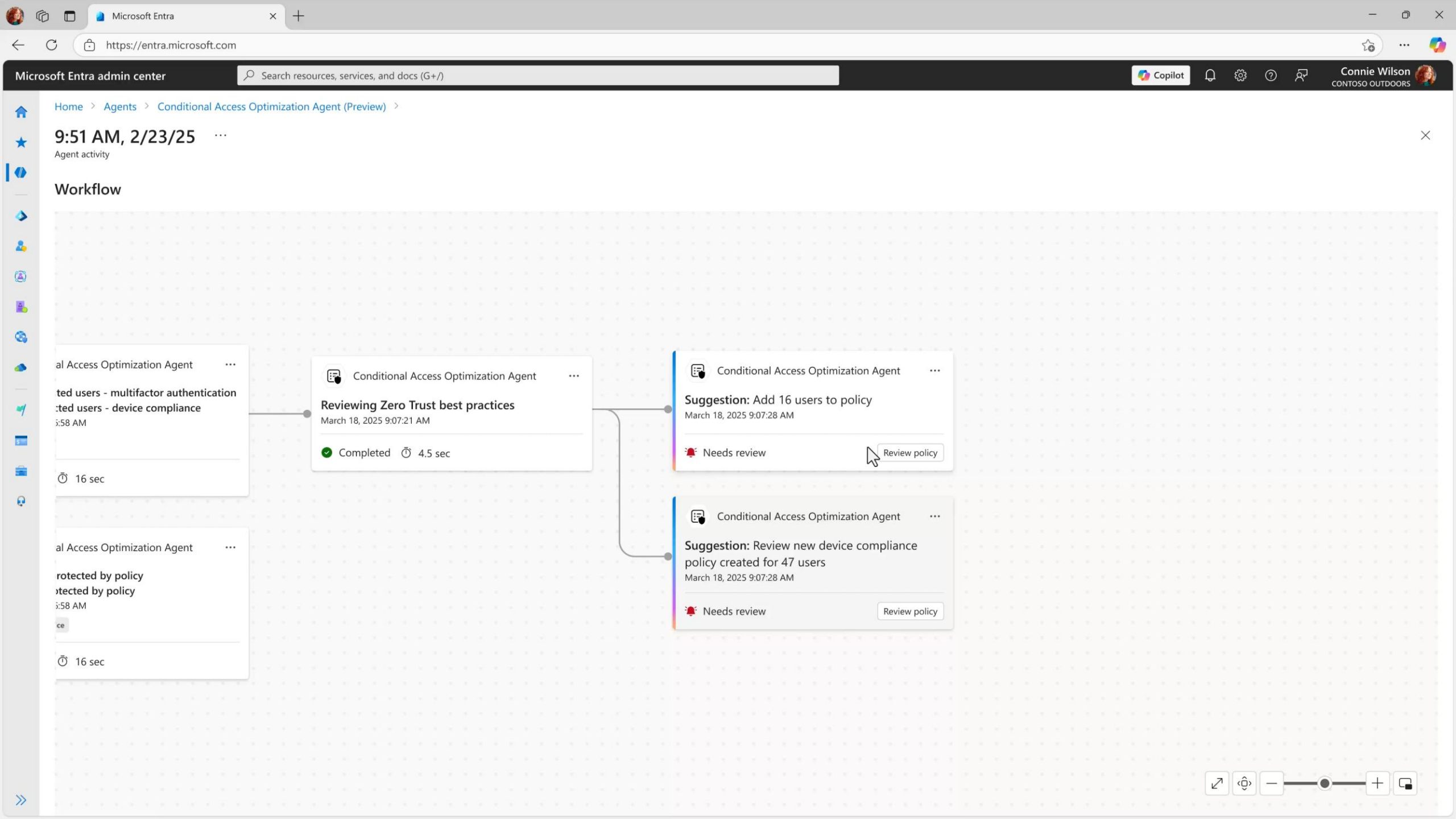
Suggested next steps	Actions
Add 16 users to existing policy	Sugges
Turn on new report-only policy for 47 users	Created

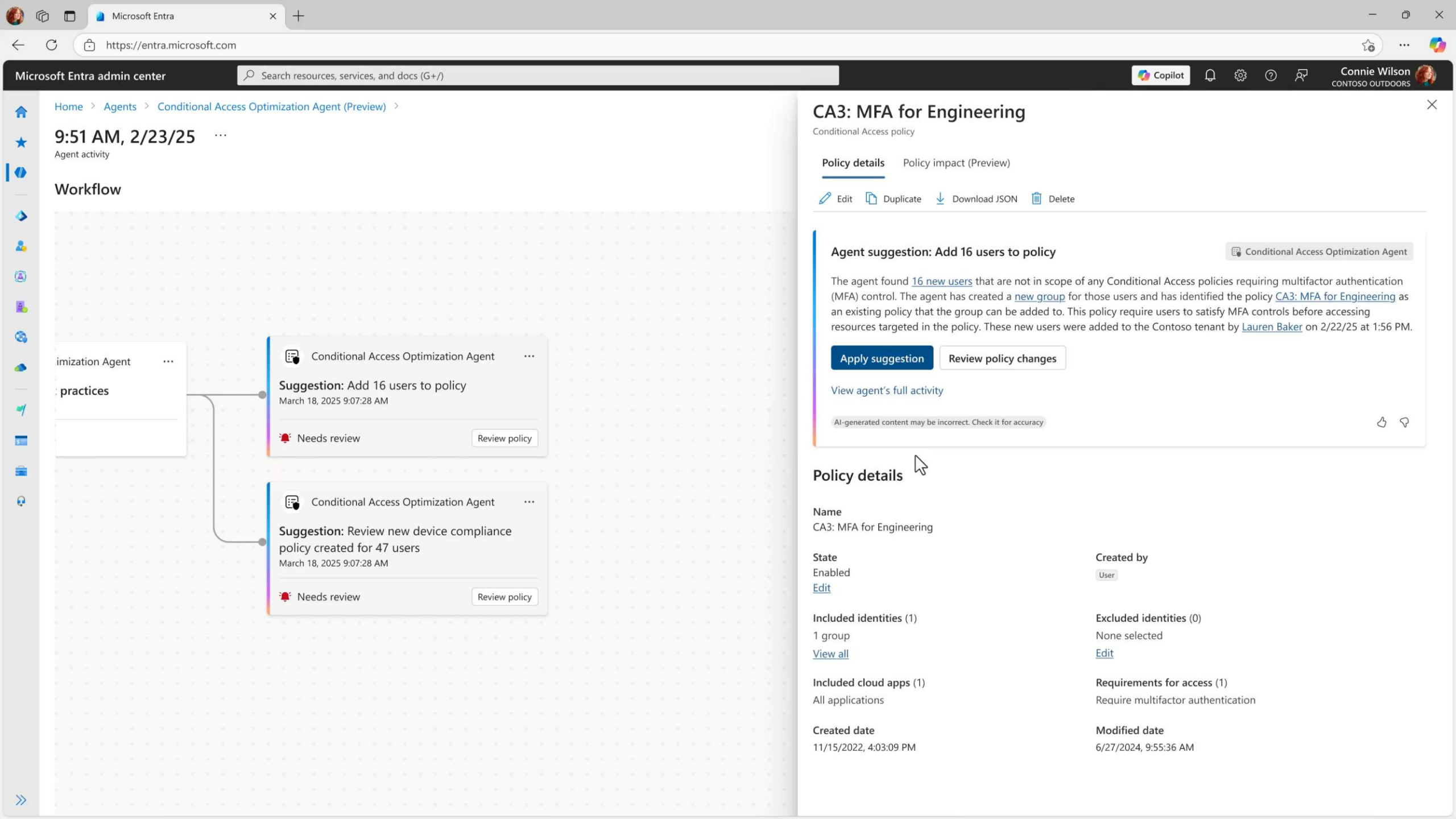
View all

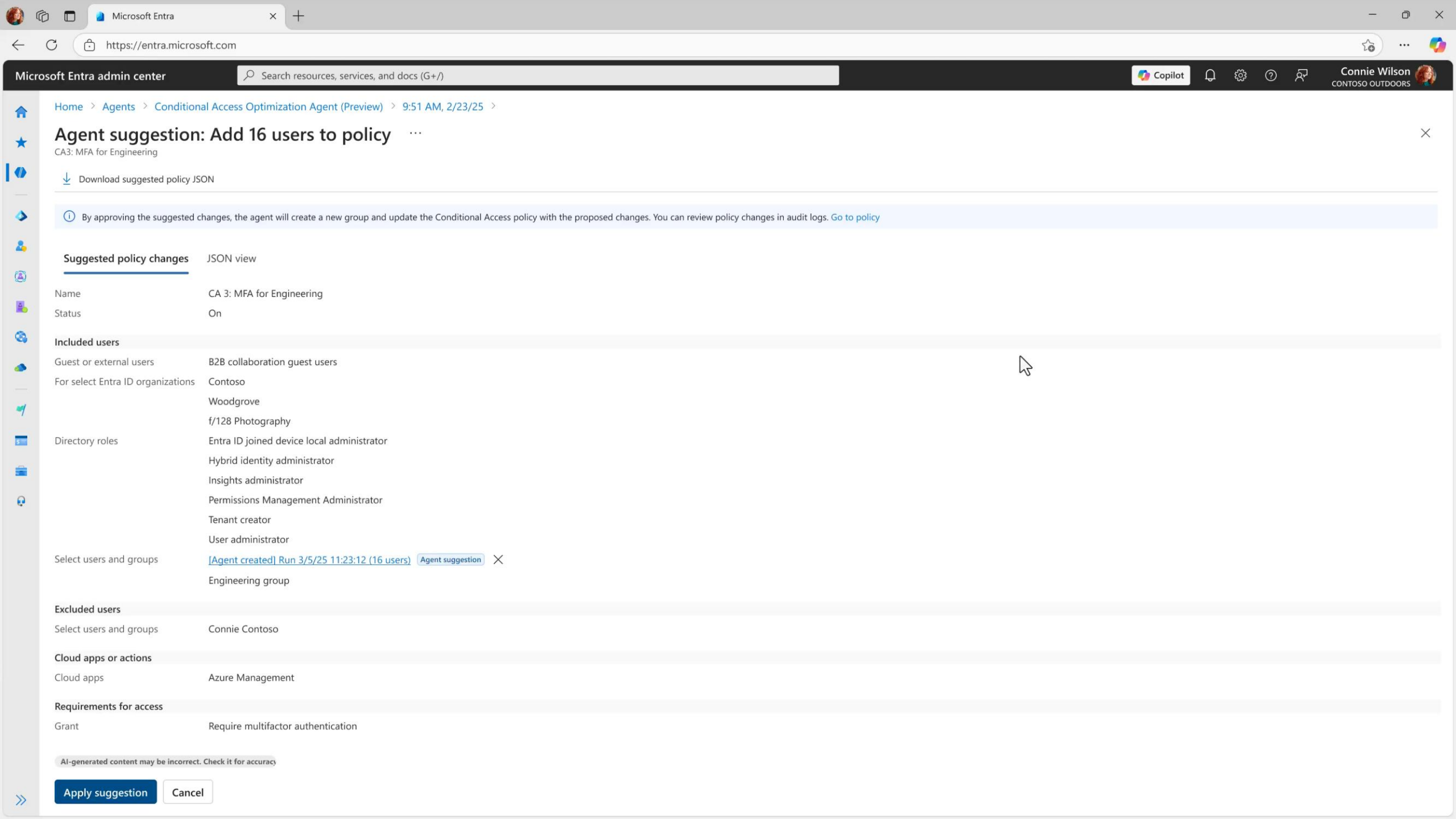

Microsoft Entra
https://entra.microsoft.com
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Connie Wilson
CONTOSO OUTDOORS
Home > Agents >
Conditional Access Optimization Agent (Preview)
Microsoft Entra ID
Start agent
Stop agent
Remove agent
Give Microsoft feedback
Overview
Suggestions
Activity
Settings
The agent completed its run
Review any suggestions about policy updates and new policies
Agent is active
Agent finished running on March 18, 2025 at 9:07 AM. View run
The agent is next scheduled to run on March 19, 2025 at 9:00 AM.
Performance highlights
Unprotected users discovered
63
Sign-ins protected
0
Recent suggestions
AI-generated content may be incorrect. Check it for accuracy
View the agent's suggestions about policy updates and new policies that were created in
Suggested next steps
Actions taken by ager
Add 16 users to existing policy
Suggested policy upd
Turn on new report-only policy for 47 users
Created new policy
View all
About this agent
The agent will scan all newly created users and apps from the last 24 hours and determine if they are in scope of at least one policy with multifactor authentication (MFA) or device compliance controls. It will suggest policy changes based on Zero Trust best practices and create new policies in report-only mode. It won't add new users to existing Conditional Access policies or turn on new policies without your approval. Learn more about this agent
Products
Conditional Access
CA3: MFA for Engineering
Conditional Access policy
Policy details
Policy impact (Preview)
Edit
Duplicate
Download JSON
Delete
Agent suggestion: Add 16 users to policy
Conditional Access Optimization Agent
The agent found 16 new users that are not in scope of any Conditional Access policies requiring multifactor authentication (MFA) control. The agent has created a new group for those users and has identified the policy CA3: MFA for Engineering as an existing policy that the group can be added to. This policy require users to satisfy MFA controls before accessing resources targeted in the policy. These new users were added to the Contoso tenant by Lauren Baker on 2/22/25 at 1:56 PM.
Apply suggestion
Review policy changes
View agent's full activity
AI-generated content may be incorrect. Check it for accuracy
Policy details
Name
CA3: MFA for Engineering
State
Enabled
Edit
Created by
User
Included identities (1)
1 group
View all
Excluded identities (0)
None selected
Edit
Included cloud apps (1)
All applications
Requirements for access (1)
Require multifactor authentication
Created date
11/15/2022, 4:03:09 PM
Modified date
6/27/2024, 9:55:36 AM


Microsoft Entra
https://entra.microsoft.com
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Connie Wilson
CONTOSO OUTDOORS
Home
Agents
Conditional Access Optimization Agent (Preview)
9:51 AM, 2/23/25
Agent activity
Workflow
Conditional Access Optimization Agent
Are new identities covered by policy?
March 18, 2025 9:04:41 AM
Partially
Completed
2mins 30secs
Conditional Access Optimization Agent
16 new unprotected users - multifactor authentication
47 new unprotected users - device compliance
March 18, 2025 9:06:58 AM
Needs attention
Completed
16 sec
Conditional Access Optimization Agent
34 new users - protected by policy
3 new apps - protected by policy
March 18, 2025 9:06:58 AM
Following best practice
Completed
16 sec
Conditional Access Optimization Agent
Reviewing Zero Trust best practices
March 18, 2025 9:07:21 AM
Completed
4.5 sec
Conditional Access Optimization A
Suggestion: Add 16 users to policy
March 18, 2025 9:07:28 AM
Needs review
Conditional Access Optimization A
Suggestion: Review new device com
policy created for 47 users
March 18, 2025 9:07:28 AM
Needs review


Microsoft Entra
https://entra.microsoft.com
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Connie Wilson
CONTOSO OUTDOORS
Home
Agents
Conditional Access Optimization Agent (Preview)
9:51 AM, 2/23/25
Agent activity
Workflow
Conditional Access Optimization Agent
Agent run '8:00 AM, 2/23/25' started by trigger
March 18, 2025 9:01:05 AM
Completed
3.4 sec
Conditional Access Optimization Agent
Are there new users?
March 18, 2025 9:01:05 AM
Yes
Completed
45 sec
View new users
Conditional Access Optimization Agent
Are there new applications?
March 18, 2025 9:01:05 AM
Yes
Completed
1 min 10 sec
View new apps
Conditional Access Optimization Agent
Are new identities covered by policy?
March 18, 2025 9:04:41 AM
Partially
Completed
2mins 30secs
16 nev
47 nev
March
Needs
Cc
34 nev
3 new
March
Follow
Cc


Microsoft Entra
https://entra.microsoft.com
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Connie Wilson
CONTOSO OUTDOORS
Home
Agents
Conditional Access Optimization Agent (Preview)
9:51 AM, 2/23/25
Agent activity
Workflow
al Access Optimization Agent
ted users - multifactor authentication
:ted users - device compliance
:58 AM
16 sec
al Access Optimization Agent
rotected by policy
tected by policy
:58 AM
ce
16 sec
Conditional Access Optimization Agent
Reviewing Zero Trust best practices
March 18, 2025 9:07:21 AM
Completed
4.5 sec
Conditional Access Optimization Agent
Suggestion: Add 16 users to policy
March 18, 2025 9:07:28 AM
Needs review
Review policy
Conditional Access Optimization Agent
Suggestion: Review new device compliance policy created for 47 users
March 18, 2025 9:07:28 AM
Needs review
Review policy


Microsoft Entra
https://entra.microsoft.com
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Connie Wilson
CONTOSO OUTDOORS
Home > Agents > Conditional Access Optimization Agent (Preview) >
9:51 AM, 2/23/25
Agent activity
Workflow
imization Agent
practices
Conditional Access Optimization Agent
Suggestion: Add 16 users to policy
March 18, 2025 9:07:28 AM
Needs review
Review policy
Conditional Access Optimization Agent
Suggestion: Review new device compliance policy created for 47 users
March 18, 2025 9:07:28 AM
Needs review
Review policy
CA3: MFA for Engineering
Conditional Access policy
Policy details
Policy impact (Preview)
Edit
Duplicate
Download JSON
Delete
Agent suggestion: Add 16 users to policy
Conditional Access Optimization Agent
The agent found 16 new users that are not in scope of any Conditional Access policies requiring multifactor authentication (MFA) control. The agent has created a new group for those users and has identified the policy CA3: MFA for Engineering as an existing policy that the group can be added to. This policy require users to satisfy MFA controls before accessing resources targeted in the policy. These new users were added to the Contoso tenant by Lauren Baker on 2/22/25 at 1:56 PM.
Apply suggestion
Review policy changes
View agent's full activity
AI-generated content may be incorrect. Check it for accuracy
Policy details
Name
CA3: MFA for Engineering
State
Enabled
Edit
Created by
User
Included identities (1)
1 group
View all
Excluded identities (0)
None selected
Edit
Included cloud apps (1)
All applications
Requirements for access (1)
Require multifactor authentication
Created date
11/15/2022, 4:03:09 PM
Modified date
6/27/2024, 9:55:36 AM


Microsoft Entra
https://entra.microsoft.com
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Connie Wilson
CONTOSO OUTDOORS
Home > Agents > Conditional Access Optimization Agent (Preview) > 9:51 AM, 2/23/25 >
Agent suggestion: Add 16 users to policy
CA3: MFA for Engineering
Download suggested policy JSON
By approving the suggested changes, the agent will create a new group and update the Conditional Access policy with the proposed changes. You can review policy changes in audit logs. Go to policy
Suggested policy changes
JSON view
Name
CA 3: MFA for Engineering
Status
On
Included users
Guest or external users
B2B collaboration guest users
For select Entra ID organizations
Contoso
Woodgrove
f/128 Photography
Directory roles
Entra ID joined device local administrator
Hybrid identity administrator
Insights administrator
Permissions Management Administrator
Tenant creator
User administrator
Select users and groups
[Agent created] Run 3/5/25 11:23:12 (16 users)
Agent suggestion
Engineering group
Excluded users
Select users and groups
Connie Contoso
Cloud apps or actions
Cloud apps
Azure Management
Requirements for access
Grant
Require multifactor authentication
AI-generated content may be incorrect. Check it for accuracy
Apply suggestion
Cancel

Directory roles	Entra ID joined device local administrator
	Hybrid identity administrator
	Insights administrator
	Permissions Management Administrator
	Tenant creator
	User administrator
Select users and groups	[Agent created] Run 3/5/25 11:23:12 (16 users) Agent suggestion
	Engineering group

Excluded users

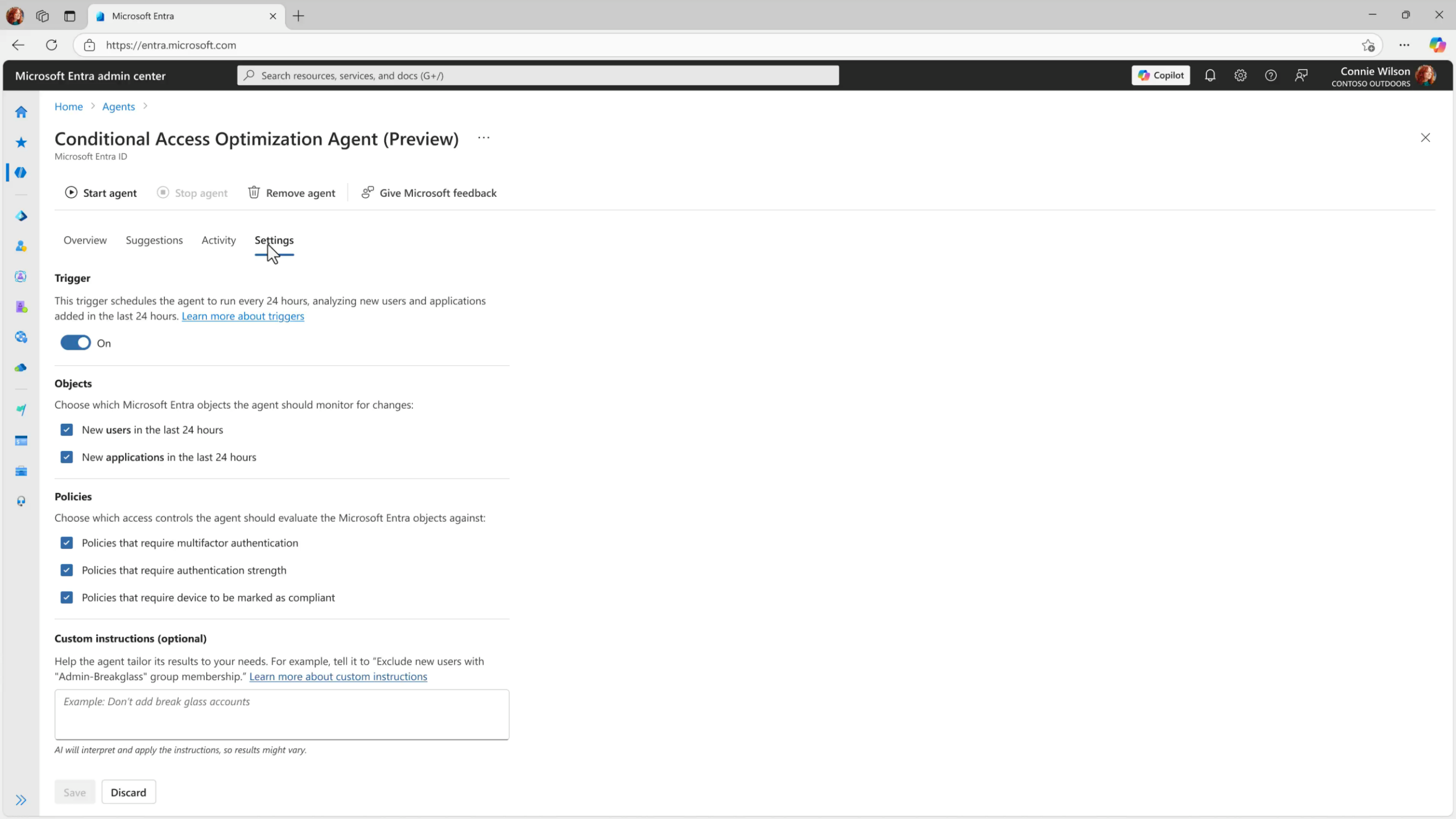
Select users and groups	Connie Contoso

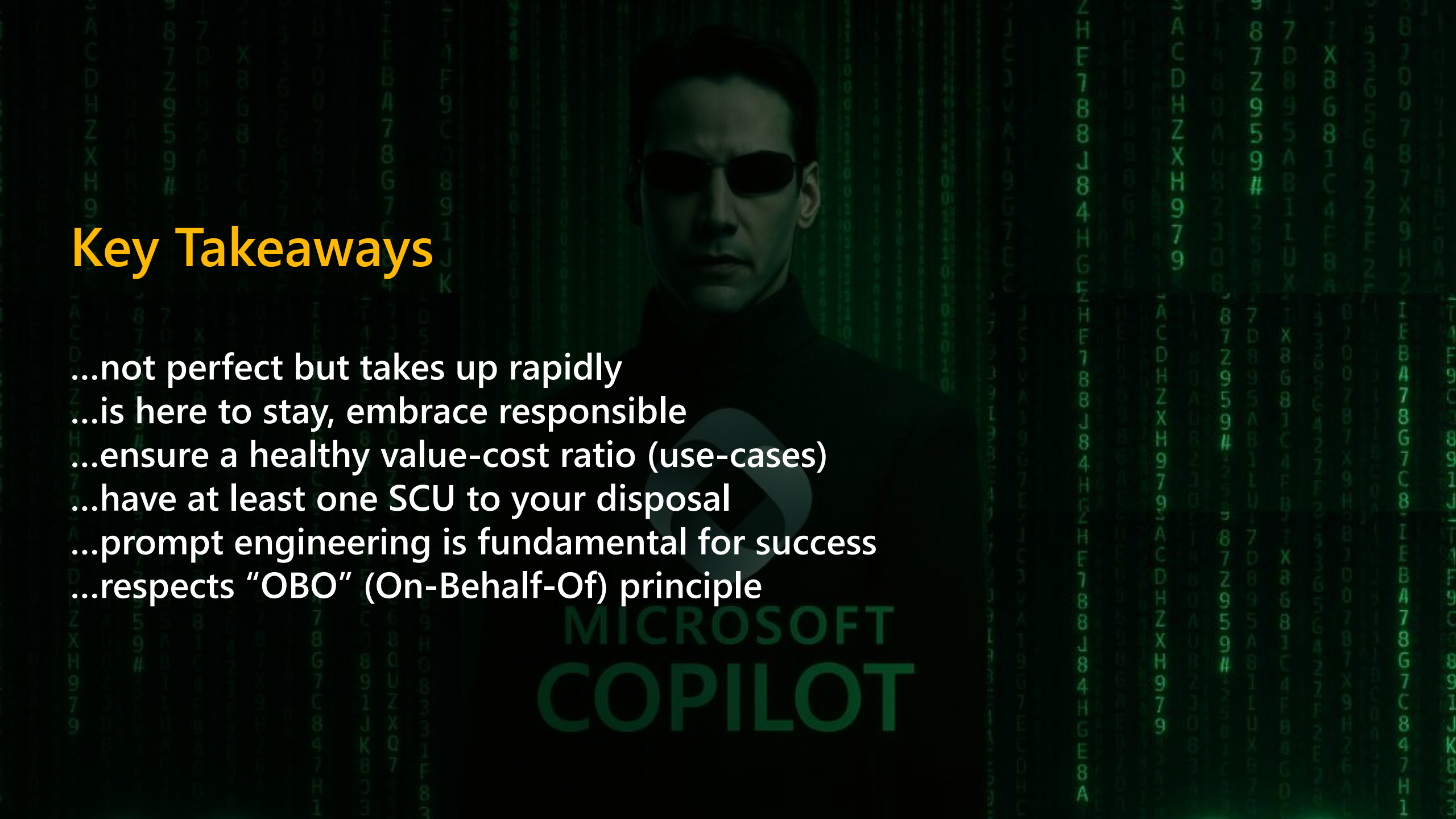
Cloud apps or actions

Cloud apps	Azure Management

Requirements for access

Grant	Require multifactor authentication


Microsoft Entra
https://entra.microsoft.com
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Connie Wilson
CONTOSO OUTDOORS
Home
Agents
Conditional Access Optimization Agent (Preview)
Microsoft Entra ID
Start agent
Stop agent
Remove agent
Give Microsoft feedback
Overview
Suggestions
Activity
Settings
Trigger
This trigger schedules the agent to run every 24 hours, analyzing new users and applications added in the last 24 hours. Learn more about triggers
On
Objects
Choose which Microsoft Entra objects the agent should monitor for changes:
New users in the last 24 hours
New applications in the last 24 hours
Policies
Choose which access controls the agent should evaluate the Microsoft Entra objects against:
Policies that require multifactor authentication
Policies that require authentication strength
Policies that require device to be marked as compliant
Custom instructions (optional)
Help the agent tailor its results to your needs. For example, tell it to "Exclude new users with "Admin-Breakglass" group membership." Learn more about custom instructions
Example: Don't add break glass accounts
AI will interpret and apply the instructions, so results might vary.
Save
Discard



Key Takeaways

…not perfect but takes up rapidly
…is here to stay, embrace responsible
…ensure a healthy value-cost ratio (use-cases)
…have at least one SCU to your disposal
…prompt engineering is fundamental for success
…respects “OBO” (On-Behalf-Of) principle

Useful resources

https://github.com/Azure/Security-Copilot
https://github.com/JanVidarElven/copilot-for-security-plugins
https://rogierdijkman.medium.com/part-1-develop-a-basic-security-copilot-plugin-bb2d317f76ef
https://learn.microsoft.com/en-us/copilot/security/prompting-security-copilot