



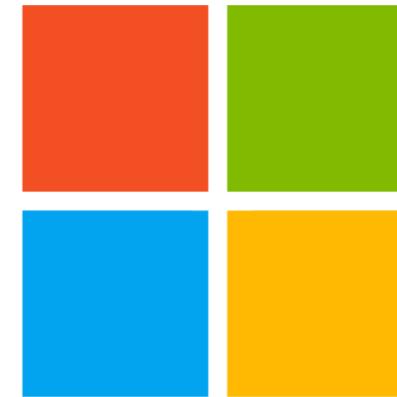
# Workplace Ninja

## User Group Finland

Empowering Intune Admins  
with Microsoft Security Copilot

Panu Saukko  
ProTrainIT Oy

# THANKS FOR THE SPONSORS!



**twoday**





Panu Saukko  
ProTrainIT Oy

MVP – Microsoft Intune &  
Microsoft Security Copilot

Panu Saukko | LinkedIn  
[Panu.Saukko@protrainit.fi](mailto:Panu.Saukko@protrainit.fi)



‘Insanity is doing the same thing over and over again and expecting different results.’

Rita Mae Brown (1983)

That was before cloud services & AI



# Agenda

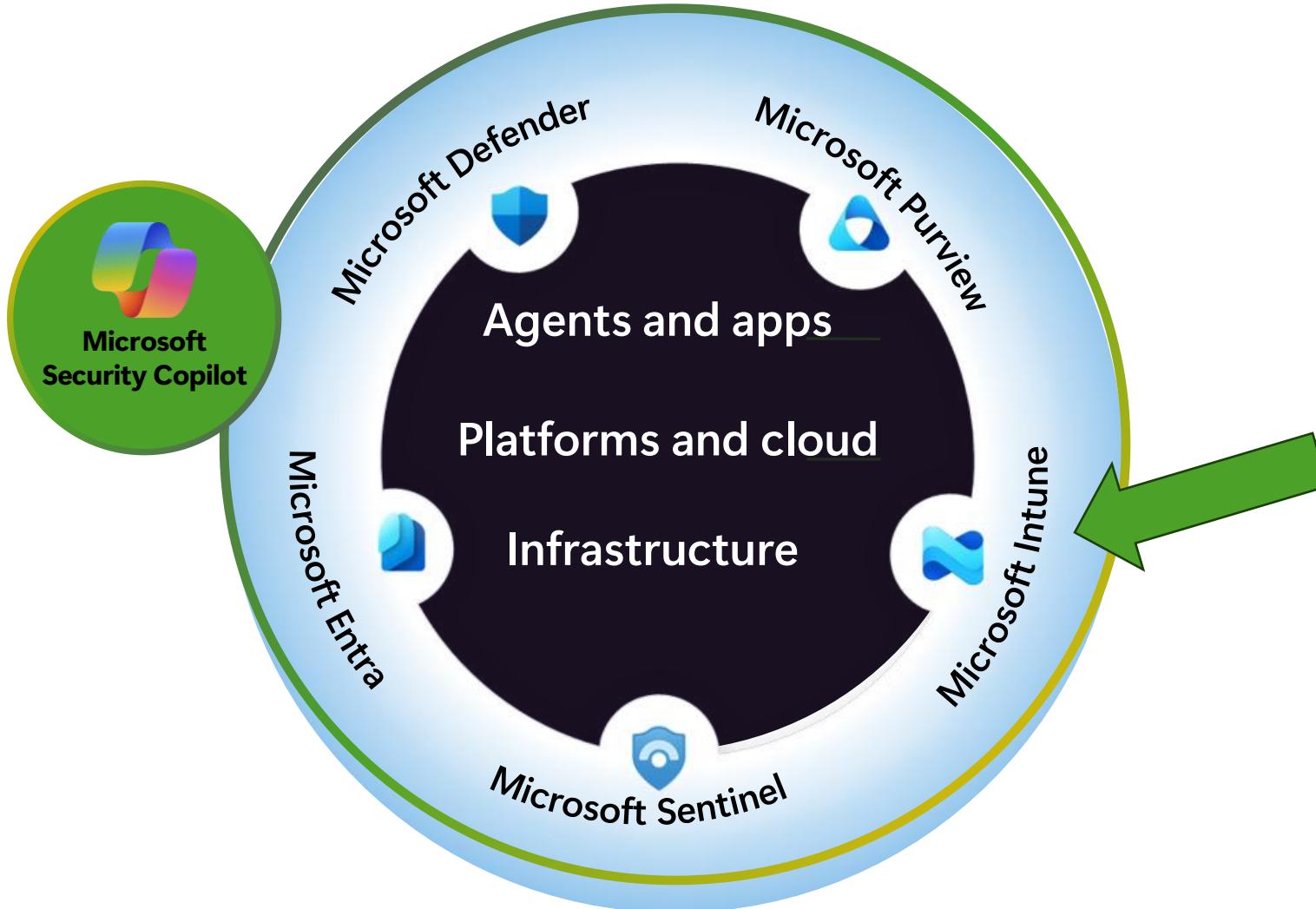
---

- Introduction to Microsoft Security Copilot
- Feature for endpoint admins
- Using Explorer
- Different agents
- Security Compute Units (SCU)



# Security Copilot

---



# Microsoft's responsible AI principles

---

1. Your data is your data
2. Your data is not used to train the foundation AI models
3. Your data is protected



# Security Copilot for Intune admins

---

**Assistive**

Expert assistance  
embedded across Intune  
to guide daily operations



**Agentic**

Endpoint task  
automation at scale



# Copilot tools within Intune console

The screenshot shows the Microsoft Intune admin center interface. At the top, there's a blue header bar with the title "Microsoft Intune admin center". On the right side of the header are several icons: a "Copilot" icon with a colorful circular logo, a bell, a gear, a question mark, and a magnifying glass. An arrow points from the text "Copilot chat" to the "Copilot" icon. On the left, there's a vertical sidebar with various icons and a main content area titled "ProTrainIT Demo". The main content area features a large callout: "Securely manage devices, access, and apps with Intune" with the subtext "Maximize productivity and simplify administration without compromising endpoint management and security." Below this is another callout: "Agents". On the right, there's a card for a "Device configuration profile" named "Prod Edge Settings" with options to "Summarize with Copilot" and "Delete". An arrow points from the text "Settings summarization" to the "Summarize with Copilot" button. In the bottom right corner, there's a cartoon illustration of a ninja holding two swords.

Copilot chat

Microsoft Intune admin center

ProTrainIT Demo

Copilot

Explorer

Prod Edge Settings

Device configuration profile

Summarize with Copilot

Delete

Settings summarization

Agents

# Chat with Copilot

- Across every blade and workflow
- Windows 365, Surface Management Portal
  - Also Entra portal
- Troubleshooting, policy management
- Always ready
- Chat history
- Ever present – in context
- Open prompt vs built-in examples

The screenshot shows the Microsoft Copilot interface. At the top, there's a blue header bar with the Copilot logo, a notification bell, settings, help, and search icons, and a user profile picture. Below the header, the title "Copilot" is displayed. A main query area asks "What would you like to know?" It explains that users can type a question to get prompts, explore Intune data, or take action. A "Compare two Intune devices" button is visible. The main content area starts with a "Copilot" section stating "AI-generated content may be incorrect. Check it for accuracy." It asks to select devices and what to compare. Two input fields are shown: "Device 1" containing "santapc499" and "Device 2" containing "santapc950". A dropdown menu for "Comparison type" is set to "Hardware". A "Submit" button is present. Below this, another "Copilot" section provides a "Hardware Comparison" between "SANTAPC499" and "SANTAPC950". A text input field at the bottom encourages users to "Type your question to get prompts to choose from".

# Natural language to KQL

Single and multi device query to get more info from one or multiple devices

Single and multi device query are part of Advanced analytics from Intune suite

Properties

Search

query microsoft 365 app configuration from the registry

Run Cancel

```
1 // Generated by Copilot. AI-generated content may be incorrect.  
2 // Your request: query microsoft 365 app configuration from the registry  
3 // KQL Description: This query retrieves all registry values under the Microsoft 365 ClickToRun configuration  
4 WindowsRegistry('HKLM:\SOFTWARE\Microsoft\Office\ClickToRun\Configuration')  
5
```

Very useful with limited KQL skills

näytä 5 konetta isoimmalla kovalevyllä. Näytä koneen nimi ja levyn koko gikoina

Run Cancel

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

```
2 // Your request: näytä 5 konetta isoimmalla kovalevyllä. Näytä koneen nimi ja levyn koko gikoina  
3 // KQL Description: This query finds each device's largest physical disk from the DiskDrive table, converts its size to GB, and orders the results by disk size in descending order, then takes the top 5.  
4 DiskDrive  
5 | summarize LargestDiskBytes = max(SizeBytes) by Device.DeviceName  
6 | project DeviceName = Device.DeviceName, DiskSizeGB = LargestDiskBytes/1024/1024/1024  
7 | order by DiskSizeGB desc  
8 | take 5
```



# Demo: Basic Copilot features



# Explorer

## Collection of queries against Intune data

Explore data in your tenant based on device, app, and management properties. [Learn more about exploring data, including what's coming soon](#)

Query your data

Start typing to search your Intune data, or see below for examples

Updates frequently!



Find the Intune data you're looking for

Search your tenant for info about devices, users, apps, compliance, or updates. Copilot can also help you understand what kind of questions you can ask and how to ask them.

Show examples for: All categories

Is this AI?

Devices

Get devices where encryption method type is [Encryption Method](#) and encryption is [True False](#)

Autopilot

Get all devices whose Windows Autopilot device preparation deployment lasted longer than [Number Of Minutes](#) minutes in last [Number Of Days](#) days

Advanced Analytics

Get devices that have high CPU usage with spike percentage greater than [Cpu Spike Percentage Threshold](#)

Apps

Get all managed app install results for user [/User](#)

Devices

Get [Platform](#) devices that are [Ownership](#) owned and have a compliance grace period ending before [Date](#)

Device Configuration

Get device configuration policies that are not of the type [Device Configuration Policy Type Name](#)

Devices

Get [Platform](#) devices that are enrolled by [/User](#) and [Ownership](#) owned

Device Configuration

Get policies that have settings configured where the setting name contains [Setting Name](#)

Apps

Get [Managed App Type](#) applications

All categories

Advanced Analytics

App Configuration

App Protection

Apps

Autopilot

Compliance

Device Configuration

Device Updates

Devices

Endpoint Privilege Management

All categories



# Explorer prerequisites

SCUs must be configured,  
even though they are not  
(yet) used

Dashboard >  
**Explorer** ...

You don't have access to Copilot in Microsoft Intune



To get Copilot, contact a Security Administrator.

Benefits of Explorer

- 🕒 Accelerate your work  
Explore devices, updates, apps, policies, and more in a new way. Ask questions, run queries, and let Copilot find the data.
- 🕒 Design and refine views  
Whether it's troubleshooting, creating reports, or inspecting Intune resources, you can create any view with your custom criteria.
- 🕒 Take action  
Use results and suggestions to complete management tasks.

[Learn more about exploring data with Copilot](#)

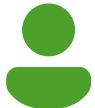


# Demo: Explorer



# Agentic AI

Operates in the context of your organization



Informed by your procedures, jobs to be done, priorities



Controlled agency to act with knowledge and permission



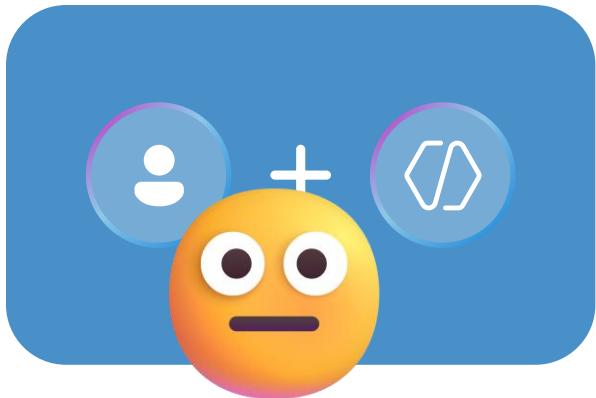
Navigates complexity to deliver tangible outcomes



Known context | Admin authority | Outcome driven

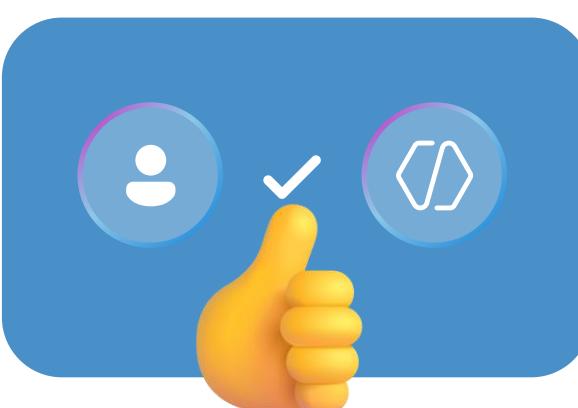
# Agentic remediation types

Guided



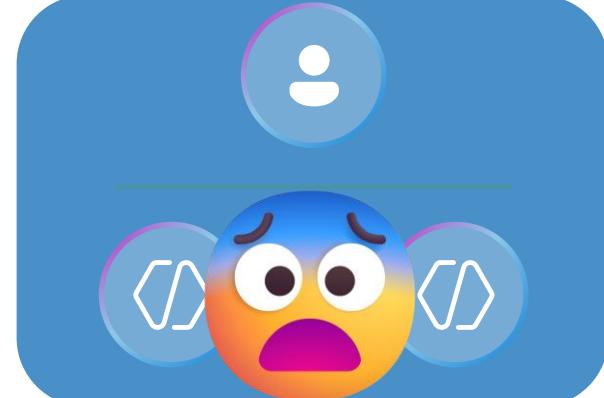
Admin remediation

Assisted



Admin approved  
automation

Autonomous



Automatous  
remediation



# Security Copilot Agents

## Security Copilot agents

X

Explore Security Copilot agents that use generative AI and your security tools to perform critical tasks autonomously.

### Change Review Agent Preview

Microsoft  
This agent evaluates the effect of approval requests in Intune and makes recommendations for the actions yo...

[View details](#)

### Device Offboarding Agent Preview

Microsoft  
This agent can find devices that were removed from Intune, but might linger in Microsoft Entra. It provides...

[View details](#)

### Policy Configuration Agent Preview

Microsoft  
Import a document, write instructions in plain language, or reference an established baseline. This agent will...

[View details](#)

### Vulnerability Remediation Age... Preview

Microsoft  
Uses Microsoft Defender data to track security issues and help you fix the most important ones first using AI...

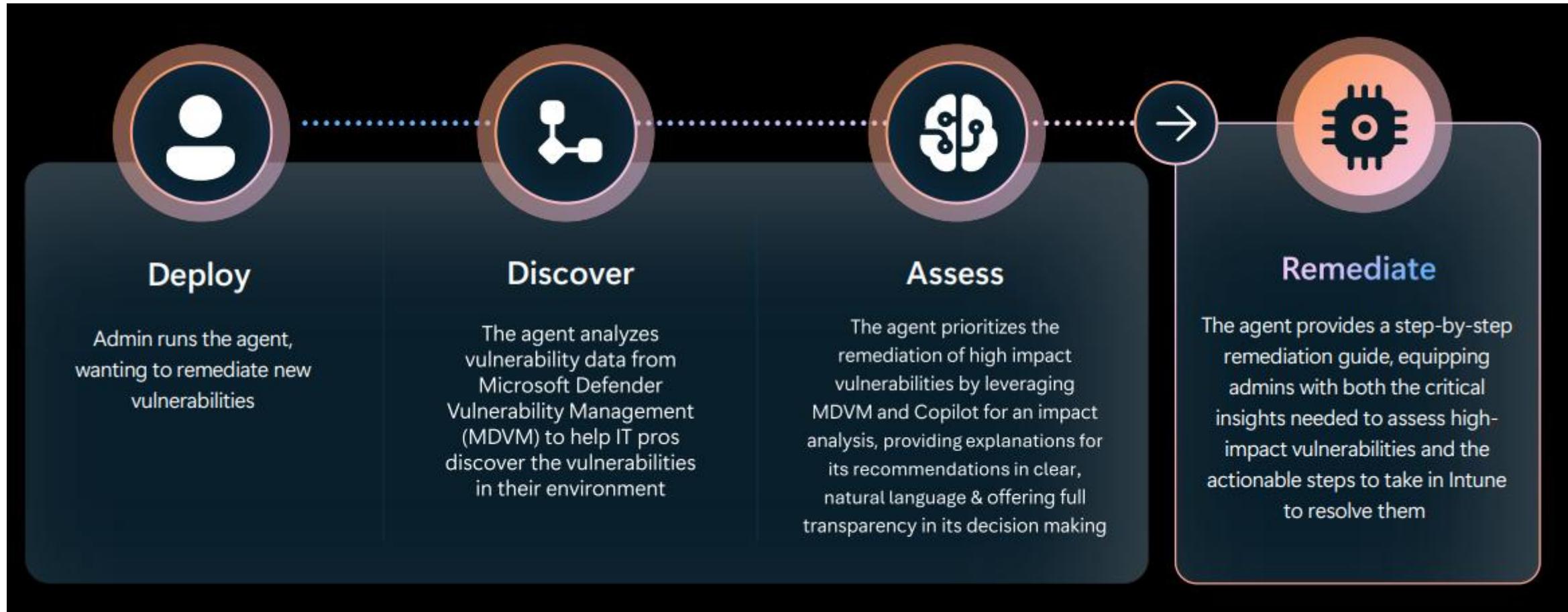
[View details](#)

More agents coming!

You can create your own agents.  
No coding required!



# Vulnerability Remediation Agent



# Vulnerability Remediation Agent

Endpoint security | Vulnerability Remediation Agent (Preview) ⋮ X

Search Run Refresh Remove agent Updated as of 07/11/2025, 12.56.45

Overview All devices Security baselines Security tasks Vulnerability Remediation Agent (Preview)

Overview Suggestions Settings

The agent completed its run. Review activity and suggestions.

Review activities and suggestions about updates and approvals needed.

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

Agent finished running on 07/11/2025 at 09:30.

About this agent This Security Copilot agent uses Microsoft Defender Vulnerability Management Data to monitor vulnerabilities, provides a prioritized list of vulnerabilities with an impact analysis, and generates steps using AI to help you remediate vulnerabilities in Intune. [Learn more about this agent](#)

**Agent suggestions** Review the top vulnerabilities to remediate. You'll also view suggestions you've applied. Suggestions might update after each agent run.

Suggested next steps	Impact ⓘ ↓	Exposed devices	Status	Last applied
Update Microsoft Windows 10 (OS and built-in applications)	▼ 6,68	5	● Not applied	
Update Microsoft .net Framework	▼ 5,08	5	● Not applied	
Update 7-zip to version 25.01.0.0	▼ 4,2	2	✓ Applied	07/11/2025, 13.14.49

**Activity** Review agent activity.

Name	Status	Duration	Start time ↓	Completion time
07/11/2025, 9.29.06 - Run results	✓ Complete	01.04	07/11/2025, 9.29.06	07/11/2025, 9.30.11
06/11/2025, 9.29.07 - Run results	✓ Complete	01.08	06/11/2025, 9.29.07	06/11/2025, 9.30.16
05/11/2025, 9.29.07 - Run results	✓ Complete	01.04	05/11/2025, 9.29.07	05/11/2025, 9.30.12

# Conditional Access Optimization Agent

Conditional Access Optimization Agent ... >

Analyze my tenant | Remove agent | Chat with agent | Give Microsoft feedback

Overview Activities Suggestions Settings

## Agent summary

From Oct 8, 2025 to Nov 7, 2025

In the past 30 days, **3 suggestions have been applied to protect 30 users and 777 applications.** Conditional Access Optimization Agent has analyzed a total of 0 new users and 11 new applications.

Unprotected users discovered ⓘ Unprotected apps discovered ⓘ Sign-ins protected ⓘ Security compute units used ⓘ

30	777	0	0.56
----	-----	---	------

### Agent is active

Agent finished analyzing your tenant on November 7, 2025 at 12:05 PM.  
[View agent's full activity](#)

Agent will scan users, apps and policies on November 8, 2025 at 12:32 PM

### About this agent

The agent scans all new users and apps added in the last 24 hours to assess their applicability to Conditional Access policies enforcing multifactor authentication, device compliance, and blocking legacy authentication and device code flow. It reviews existing enabled policies to suggest

### 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 report-only mode.

[View all](#)

Suggested next steps	Actions taken by agent	Time generated ↓	Status	
Review policy MFA for all high risk users with no break glass accounts	Suggested policy review	11/7/25, 12:04:24 PM	<input type="radio"/> New	<a href="#">Review suggestion</a>
Review policy Disable legacy authentication with no break glass accounts	Suggested policy review	11/7/25, 12:04:24 PM	<input type="radio"/> New	<a href="#">Review suggestion</a>
Turn on new policy to enforce device compliance for Linux users (1 group)	Suggested policy update	10/23/25, 1:27:27 PM	<input checked="" type="radio"/> Applied	<a href="#">View policy</a>
Turn on policy Require password change for high-risk users with phased rollout	Suggested phased rollout	10/21/25, 1:04:38 PM	<input type="radio"/> Not applied	<a href="#">Review suggestion</a>
Turn on new policy to enforce device compliance for Windows users (4 groups)	Created new report-only policy	10/20/25, 1:04:34 PM	<input type="radio"/> Not applied	<a href="#">Review suggestion</a>



# Policy Configuration Agent

## Translate requirements into policies

- Converts complex or ambiguous compliance standards into actionable Intune policy settings automatically.

## Help ensure compliance at scale

- Audits devices against organizational and industry benchmarks, reducing manual checks and gaps.

## Reduce manual mapping

- Eliminates time-consuming interpretation of documents like CIS or STIG, accelerating policy deployment.

The screenshot shows the Microsoft Intune admin center interface for the Policy Configuration Agent (Preview). The top navigation bar includes 'Copilot', 'Home', 'Security Copilot agents', and 'Policy Configuration Agent (Preview)'. The main content area has tabs for 'Overview', 'Knowledge', 'Suggestions', and 'Settings'. The 'Overview' tab is selected, showing that the agent is available and finished running on 11/11/2025 at 10:43:56 AM. The 'Agent suggestions' section lists five suggested steps: 'Review New Baseline Pol.', 'Review Enterprise Harde', 'Review BitLocker Policy', 'Review Mixed policy', and 'Review Operational Sec.'. The 'Activity' section lists six completed runs from 11/11/2025, showing start and completion times and durations.

Name	Status	Duration	Start time ↓	Completion time
11/11/2025 10:43:56 AM - Run results	Complete	3:26	11/11/2025, 10:40:29 AM	11/11/2025, 10:43:56 AM
11/11/2025 7:02:27 AM - Run results	Complete	2:21	11/11/2025, 7:00:05 AM	11/11/2025, 7:02:27 AM
11/11/2025 5:04:51 AM - Run results	Complete	2:16	11/11/2025, 5:02:35 AM	11/11/2025, 5:04:51 AM
11/11/2025 5:04:27 AM - Run results	Complete	2:16	11/11/2025, 5:02:11 AM	11/11/2025, 5:04:27 AM
11/11/2025 5:02:42 AM - Run results	Complete	1:03	11/11/2025, 5:01:38 AM	11/11/2025, 5:02:42 AM



# Demo: Security Copilot Agents



# Secure Compute Units (SCU)

- Engine behind all Security Copilot operations
  - Need to have “enough” SCUs
  - Should be called SCU hours
    - One query can last a few seconds, but it takes e.g. 0,7 SCU hours
    - If capacity runs out, need to wait for the next hour
  - Three types of SCUs
    - Provisioned: charged 24/7
      - Even if nobody is using SCUs
    - Overage: charged only when needed
    - Included with M365 E5 licenses
      - 40 SCU hours/100 M365 E5/month

## Security compute units

Select the number of units you want to purchase for SecCopilot. Security compute units provide the computing power that drives the Security Copilot experience. [Read more about security compute units](#)

**Provisioned security compute units per hour \***

**3** ^ ^ **\$ 4 USD** per unit

Estimated monthly cost 8760 USD/month

Note: your monthly bill may vary based on 1. overage SCUs consumed, 2. changes to provisioned SCUs during the billing period

**Use overage units when needed**

**\$ 6 USD per unit**

**How overage units work**

Overage units will be used after you've run out of provisioned units. You'll only pay for the overage units that you use.

**Number of on-demand units**

No limit

Set a max-limit

**6** ^ ^ units per hour

**Apply** **Cancel** **...**



# SCU usage monitoring

3a004a9da09f	c72d9424- bc52-4ed3- 91a8- 05ffb752a6d8	Oct 29, 05:31 PM	9.3	PS Panu Saukko	User prompt	Manual	Copilot in Microsoft Entra	Query Microsoft Graph data
c72d9424- bc52-4ed3- 91a8- 05ffb752a6d8	Oct 29, 05:31 PM	0.9	PS Panu Saukko	User prompt	Manual	Copilot in Microsoft Entra	Query Microsoft Graph data	
c72d9424- bc52-4ed3- 91a8- 05ffb752a6d8	Oct 29, 05:27 PM	0.7	PS Panu Saukko	User prompt	Manual	Copilot in Microsoft Entra	Query Microsoft Graph data	
c72d9424- bc52-4ed3- 91a8- 05ffb752a6d8	Oct 29, 05:25 PM	0.7	PS Panu Saukko	User prompt	Manual	Copilot in Microsoft Entra	Query Microsoft Graph data	
c72d9424- bc52-4ed3- 91a8- 05ffb752a6d8	Oct 29, 05:25 PM	0.7	PS Panu Saukko	User prompt	Manual	Copilot in Microsoft Entra	Query Microsoft Graph data	
c72d9424- bc52-4ed3- 91a8- 05ffb752a6d8	Oct 29, 05:22 PM	0.9	PS Panu Saukko	User prompt	Manual	Copilot in Microsoft Entra	Query Microsoft Graph data	
c72d9424- bc52-4ed3- 91a8- 05ffb752a6d8	Oct 29, 05:21 PM	0.6	PS Panu Saukko	User prompt	Manual	Copilot in Microsoft Entra	Query Microsoft Graph data	
c72d9424- bc52-4ed3- 91a8- 05ffb752a6d8	Oct 29, 05:20 PM	1.2	PS Panu Saukko	User prompt	Manual	Copilot in Microsoft Entra	Query Microsoft Graph data	
c72d9424- bc52-4ed3- 91a8- 05ffb752a6d8	Oct 29, 05:14 PM	1	PS Panu Saukko	User prompt	Manual	Copilot in Microsoft Entra	Query Microsoft Graph data	
c72d9424- bc52-4ed3- 91a8- 05ffb752a6d8	Oct 29, 05:13 PM	0.6	PS Panu Saukko	User prompt	Manual	Copilot in Microsoft Entra	Query Microsoft Graph data	

Some observations:

1. Agents consume very little SCUs
2. The more exact prompt  
→ the less SCUs used
3. Open prompting use the most SCUs
4. 10 sec prompt can take >1 SCU/hours
5. Explorer doesn't consume SCUs (yet?)



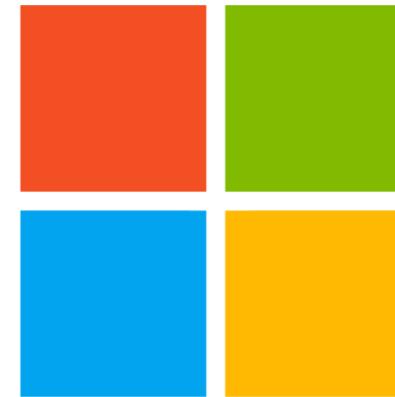
# Summary

---

- Microsoft is investing heavily to improve Security Copilot functionality
  - The journey has just started
- Security Copilot is now more affordable to use
  - SCU hours with M365 E5 licenses
  - Overage SCU hours
- Are you ready for agents? 😊



# THANK YOU ALL AND A SPECIAL THANKS TO OUR SPONSORS!



**twoday**



# Thank you!

