



Workplace Ninja

User Group Finland

Empowering Intune Admins
with Microsoft Security Copilot

Panu Saukko
ProTrainIT Oy

THANKS FOR THE SPONSORS!



Workplace Ninja
User Group Finland



Microsoft





Panu Saukko
ProTrainIT Oy

MVP – Microsoft Intune &
Microsoft Security Copilot

Panu Saukko | LinkedIn
Panu.Saukko@protrainit.fi



Workplace Ninja
User Group Finland



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

Rita Mae Brown (1983)

That was before cloud services & AI

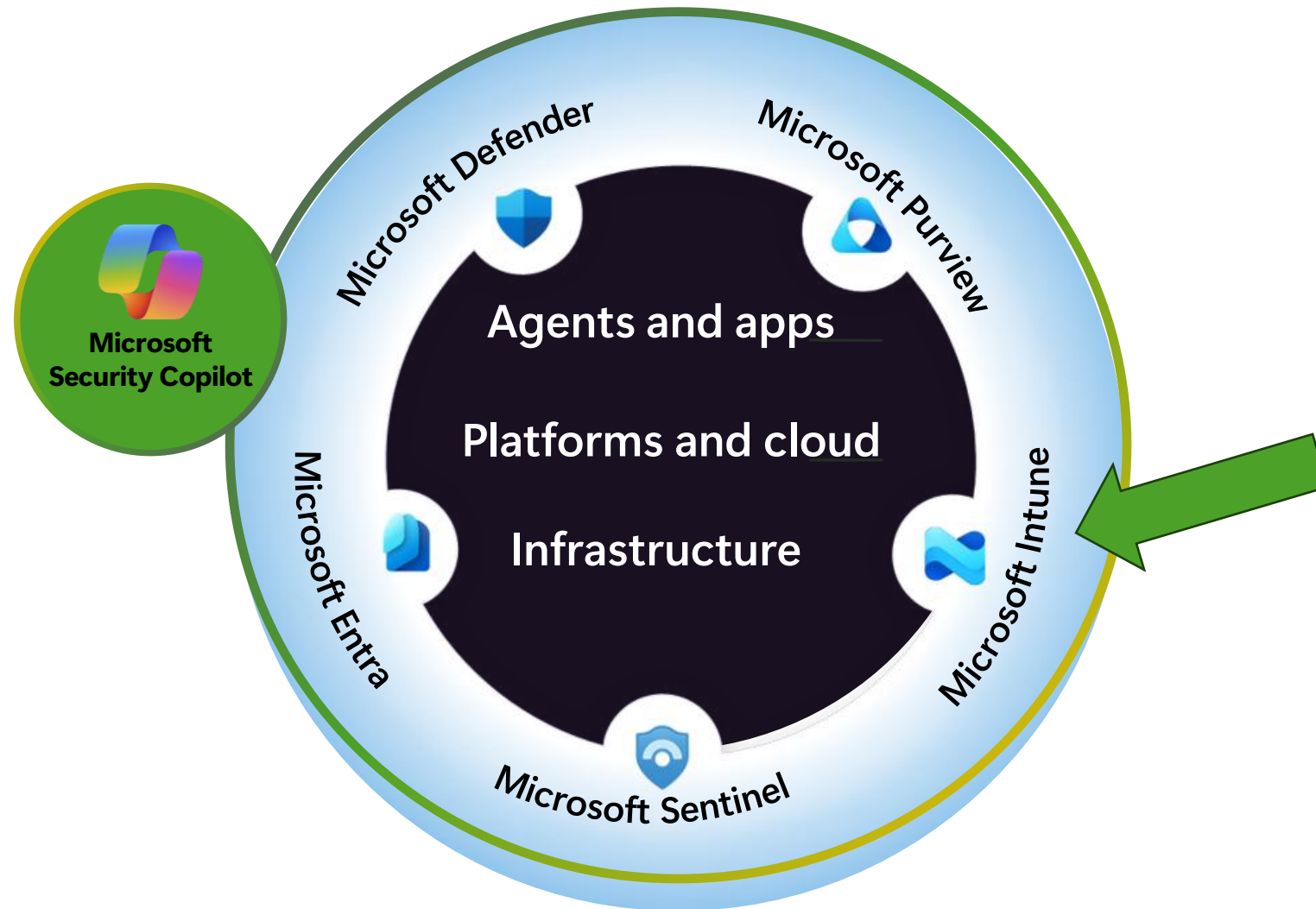


Agenda

- 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 displays the Microsoft Intune admin center interface. At the top, the header bar includes the 'Microsoft Intune admin center' title and a 'Copilot' button. An arrow labeled 'Copilot chat' points to this button. Below the header, a navigation pane on the left contains icons for various Intune features. An arrow labeled 'Explorer' points to the 'Explorer' icon, and another arrow labeled 'Agents' points to the 'Agents' icon. The main content area features a large blue card titled 'Securely manage devices, access, and apps with Intune' with the subtitle 'Maximize productivity and simplify administration without compromising endpoint management and security.' To the right of this card, a 'Prod Edge Settings' card is shown, labeled 'Device configuration profile'. This card has two buttons: 'Summarize with Copilot' and 'Delete'. An arrow labeled 'Settings summarization' points to the 'Summarize with Copilot' button. In the bottom right corner, there is a cartoon illustration of a ninja holding two green plants.

Microsoft Intune admin center

Copilot

ProTrainIT Demo

Update firewall configurations for new Intune network service endpoints. [Learn more about Intune network service endpoints](#)

Explorer

Securely manage devices, access, and apps with Intune

Maximize productivity and simplify administration without compromising endpoint management and security.

Agents

Prod Edge Settings

Device configuration profile

Summarize with Copilot Delete

Settings summarization

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 displays the Microsoft Copilot chat interface. At the top is a blue header bar with the Copilot logo, a bell icon, a gear icon, a question mark icon, and a user profile picture. Below the header, the chat area has a title bar with 'Copilot' and a close button. The main content area starts with a prompt: 'What would you like to know?' followed by a description: 'Get info about devices, policies, users, and much more. Just type your question to get prompts to choose from. You can also [explore your Intune data](#) and easily take action.' Below this is a button labeled 'Compare two Intune devices'. The next section shows the Copilot logo and a warning: 'AI-generated content may be incorrect. Check it for accuracy.' This is followed by the instruction 'Select devices and what you want to compare'. There are three input fields: 'Device 1' with the value 'santapc499', 'Device 2' with the value 'santapc950', and 'Comparison type' with a dropdown menu showing 'Hardware'. A 'Submit' button is below these fields. The final section shows the Copilot logo and another warning: 'AI-generated content may be incorrect. Check it for accuracy.' This is followed by the text 'Hardware Comparison: SANTAPC499 vs SANTAPC950'. At the bottom is a text input field with the placeholder 'Type your question to get prompts to choose from'.

Copilot

What would you like to know?

Get info about devices, policies, users, and much more. Just type your question to get prompts to choose from. You can also [explore your Intune data](#) and easily take action.

Compare two Intune devices

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

Select devices and what you want to compare

Device 1

santapc499

Device 2

santapc950

Comparison type

Hardware

Submit

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

Hardware Comparison: SANTAPC499 vs SANTAPC950

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

▼ BiosInfo

▼ Certificate

▼ Cpu

 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



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



▶ Run ✕ Cancel

```
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
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.

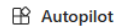
Show examples for:

All categories



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

Is this AI?

All categories

Advanced Analytics

App Configuration

App Protection

Apps

Autopilot

Compliance

Device Configuration

Device Updates

Devices

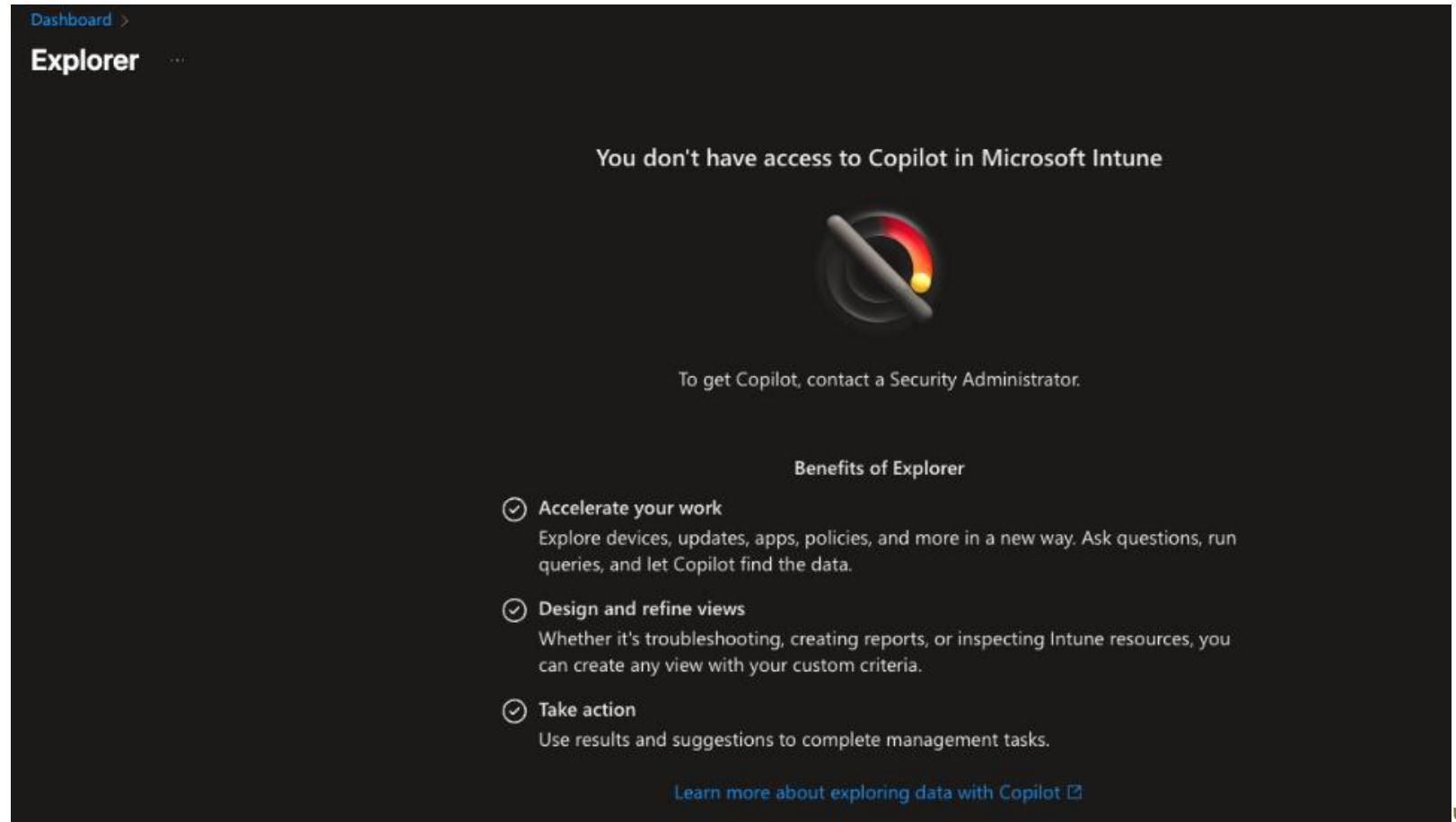
Endpoint Privilege Management

All categories



Explorer prerequisites

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



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



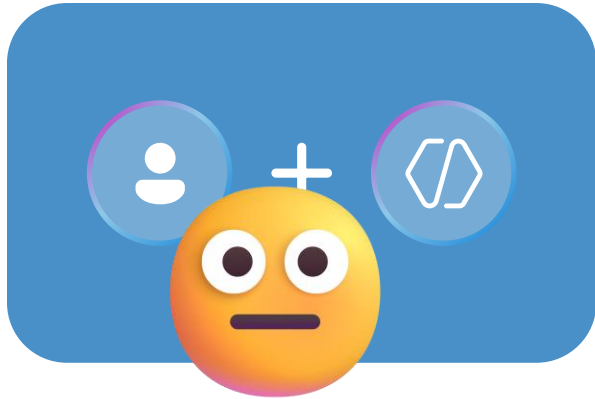
Navigates
complexity to
deliver tangible
outcomes

Known context | Admin authority | Outcome driven



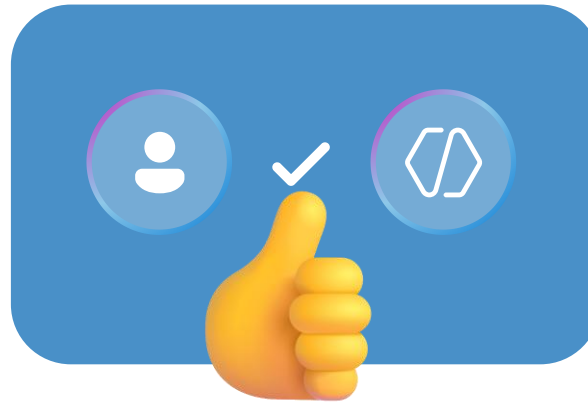
Agentic remediation types

Guided



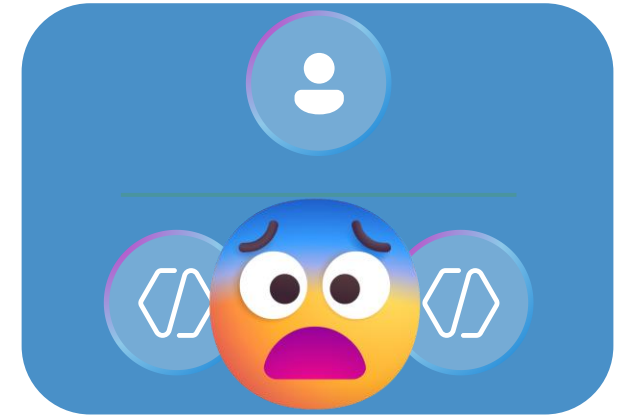
Admin remediation

Assisted



Admin approved
automation

Autonomous



Automatous
remediation



Security Copilot Agents

Security Copilot agents ...



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...

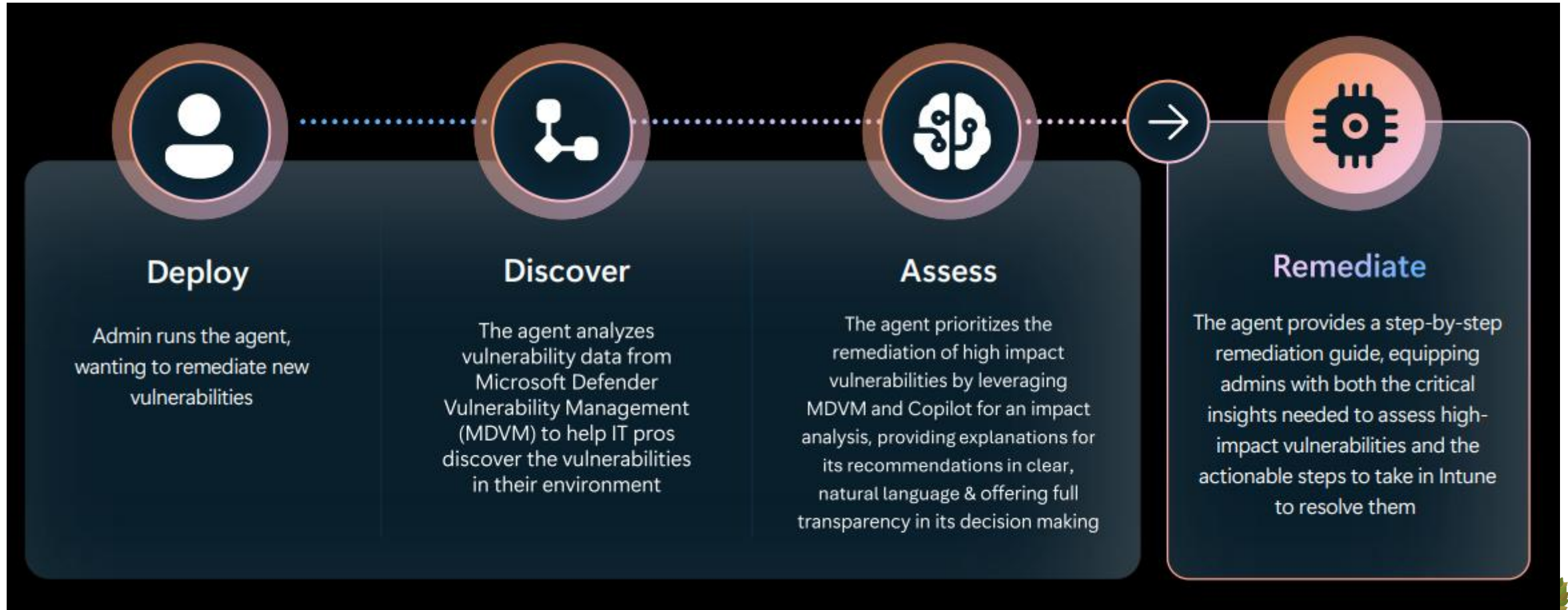
[View details](#)

More agents coming!

You can create your own agents.
No coding required!



Vulnerability Remediation Agent



Vulnerability Remediation Agent

Endpoint security | Vulnerability Remediation Agent (Preview) ...

Search

Run Refresh Remove agent

Updated as of 07/11/2025, 12.56.45

Overview

Overview

All devices

Security baselines

Security tasks

Vulnerability Remediation Agent (Preview)

Manage

Monitor

Assignment failures

Setup

Microsoft Defender for Endpoint

Help and support

Help and support

The agent completed its run. Review activity and suggestions.

Review activities and suggestions about updates and approvals needed.

Agent is available

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

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

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 ⓘ

30

Unprotected apps discovered ⓘ

777

Sign-ins protected ⓘ

0

Security compute units used ⓘ

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 all](#)

View the agent's suggestions about policy updates and new policies that were created in report-only mode.

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	Review suggestion
Review policy Disable legacy authentication with no break glass accounts	Suggested policy review	11/7/25, 12:04:24 PM	<input type="radio"/> New	Review suggestion
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	View policy
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	Review suggestion
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	Review suggestion



Policy Configuration Agent

Translate requirements into policies

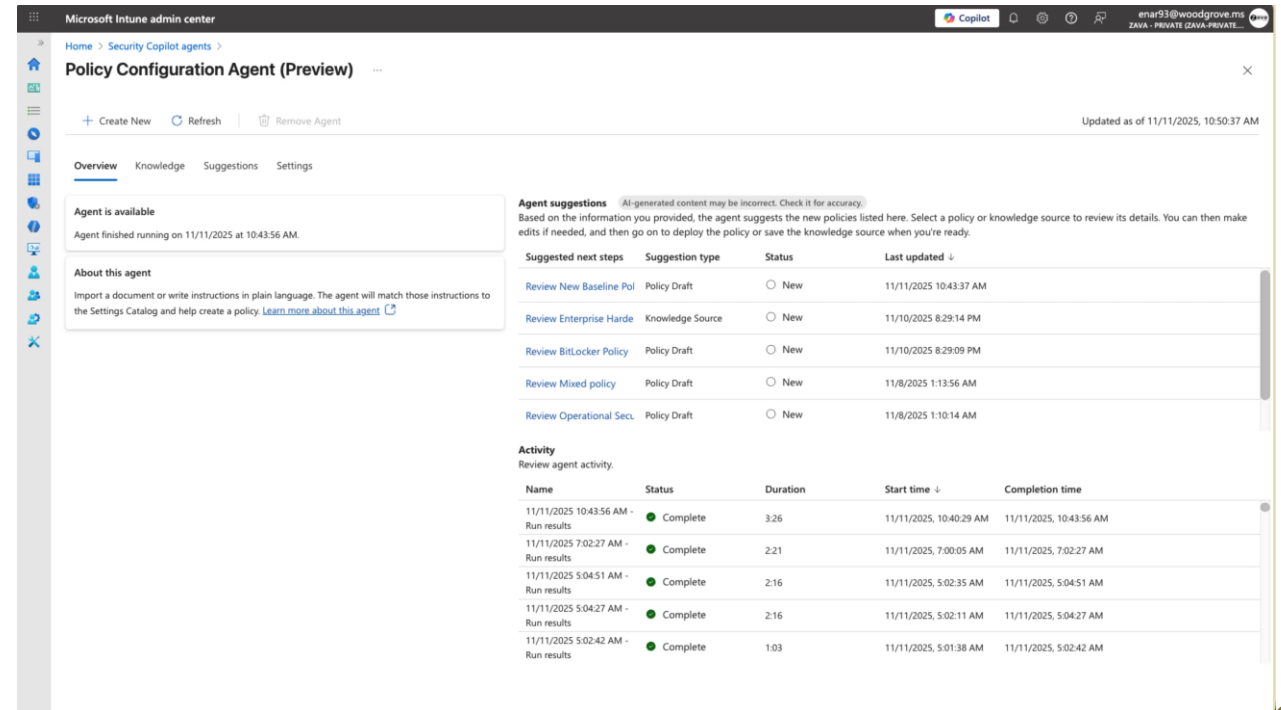
- Converts complex or ambiguous compliance standards into actionable Intune policy settings automatically.

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 displays the Microsoft Intune admin center interface for the Policy Configuration Agent (Preview). The page is titled "Policy Configuration Agent (Preview)" and includes a sidebar with navigation options: Home, Security Copilot agents, and a list of agents. The main content area is divided into several sections:

- Overview:** Shows the agent's status as "Agent is available" and "Agent finished running on 11/11/2025 at 10:43:56 AM".
- Knowledge:** Provides instructions on how to import a document or write instructions in plain language for the agent to match.
- Suggestions:** Lists suggested next steps for policy configuration, including "Review New Baseline Pol", "Review Enterprise Harde", "Review BitLocker Policy", "Review Mixed policy", and "Review Operational Sec".
- Activity:** A table showing the agent's activity history, including the name of the run, its status (Complete), duration, start time, and completion time.

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](#)

3

Provisioned security compute units per hour *
\$ 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

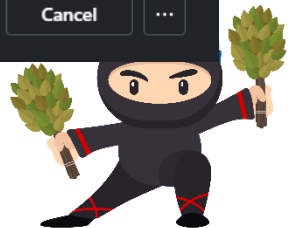
☒ Set a max-limit

6 units per hour

Apply

Cancel

...



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



Workplace Ninja
User Group Finland



Microsoft



Thank you!

