Workplace Ninja

User Group Finland

Empowering Intune Admins with Microsoft Security Copilot

Panu Saukko
ProTrainIT Oy

THANKS FOR THE SPONSORS!

PATCH MY PC

PLENTICS

twoday

Microsoft

DELL

Workplace Ninja User Group Finland

intel

Panu Saukko
ProTrainIT Oy

MVP – Microsoft Intune &
Microsoft Security Copilot

Panu Saukko | LinkedIn
Panu.Saukko@protrainit.fi

Workplace Ninja User Group Finland

UTAH JAZZ

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

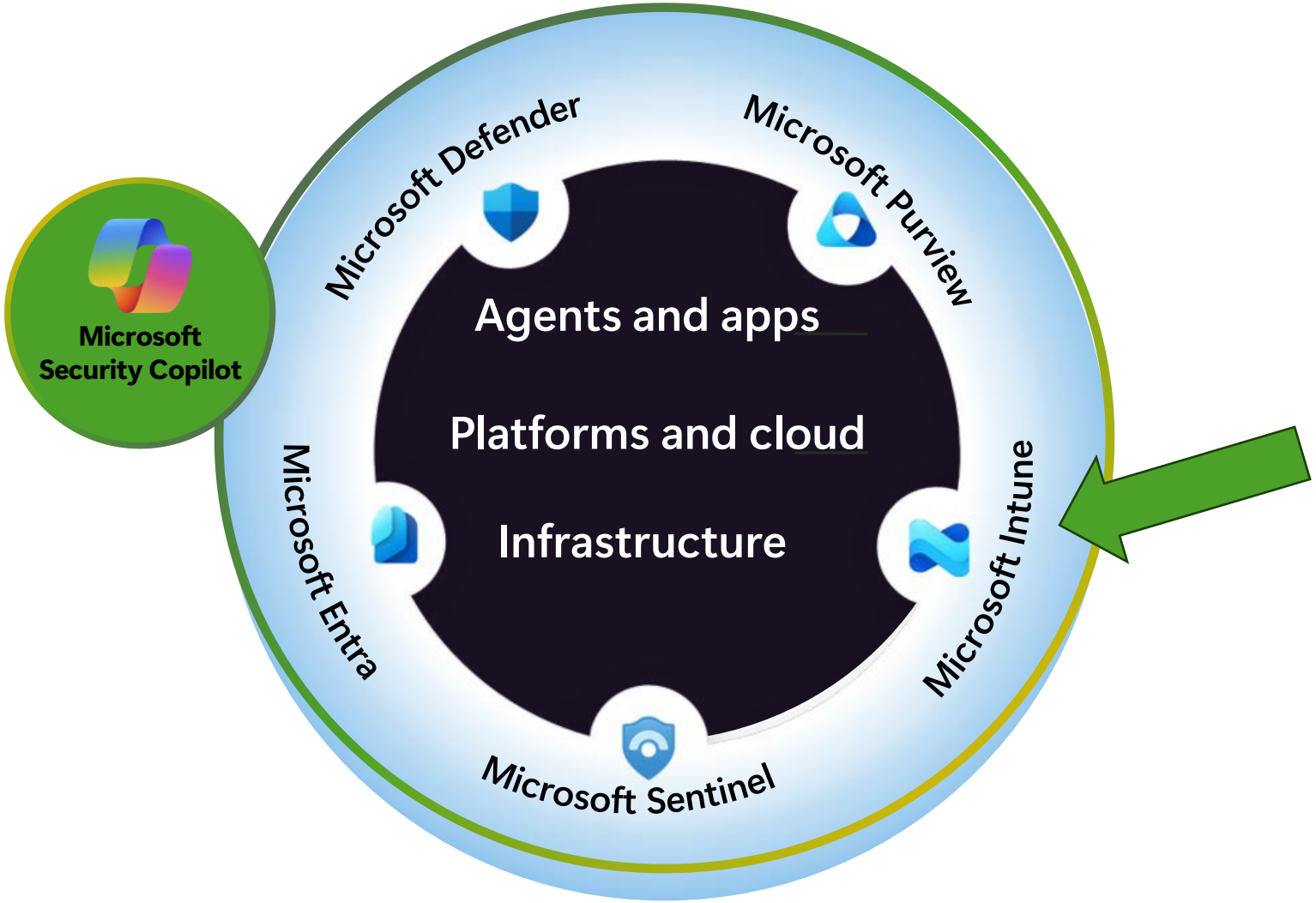
Rita Mae Brown (1983)

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

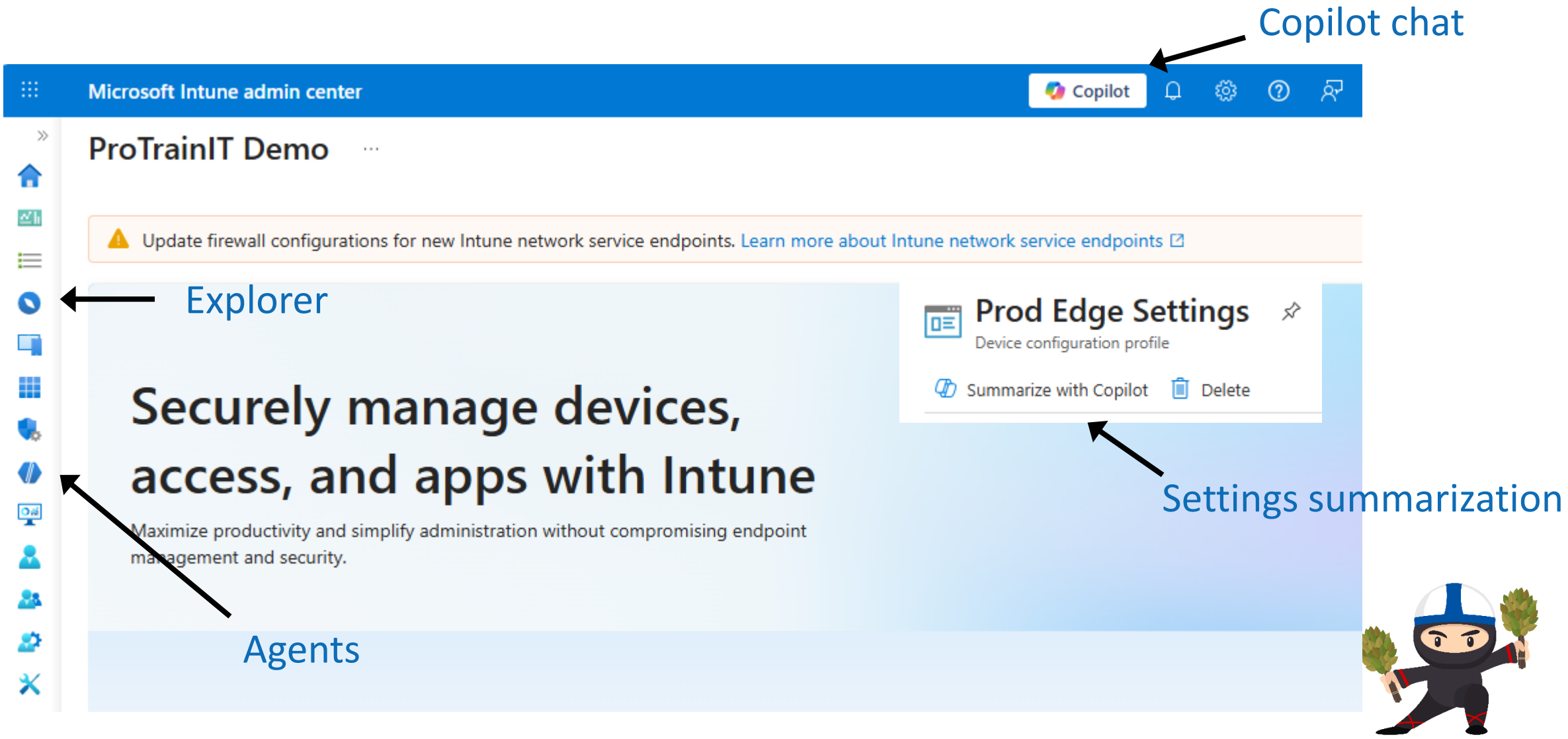
Assistive

Expert assistance
embedded across Intune
to guide daily operations

Agentic

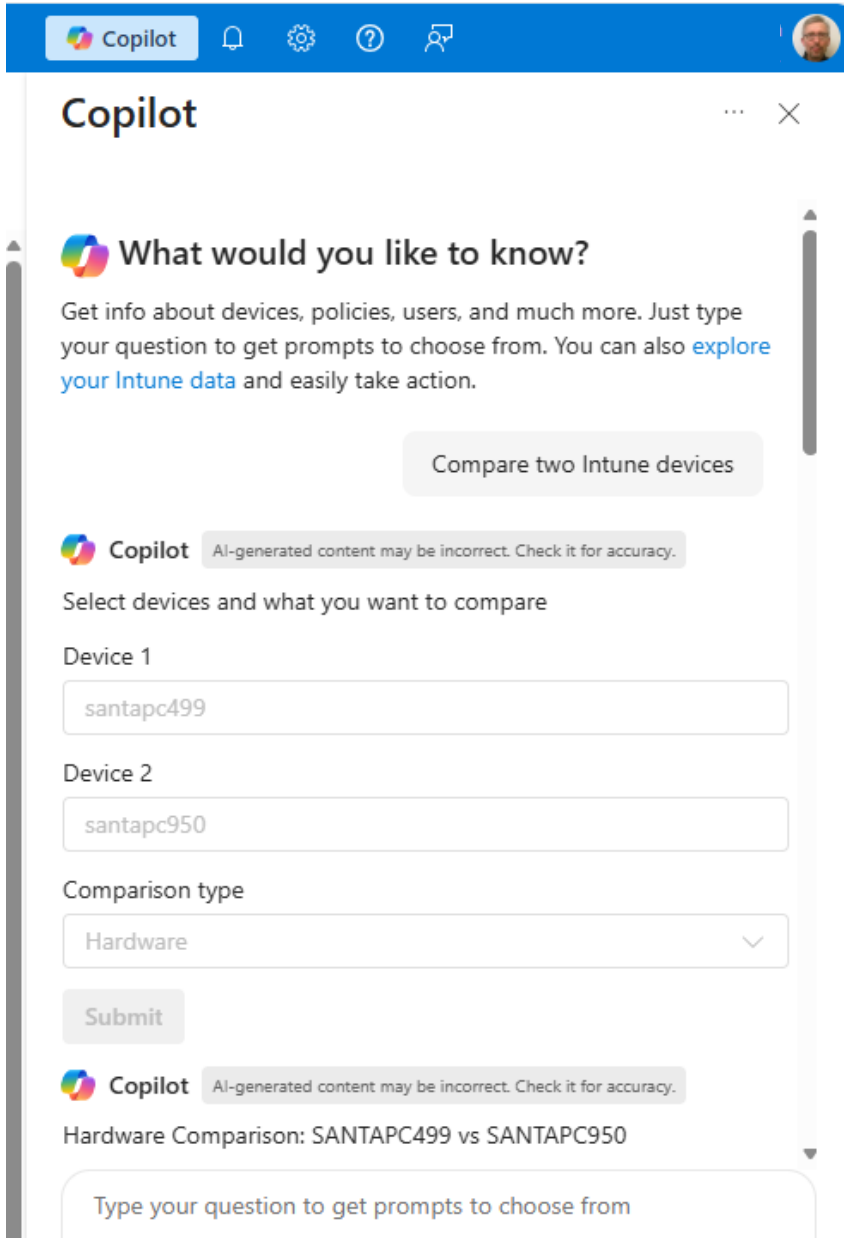
Endpoint task automation at scale

Copilot tools within Intune console



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



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

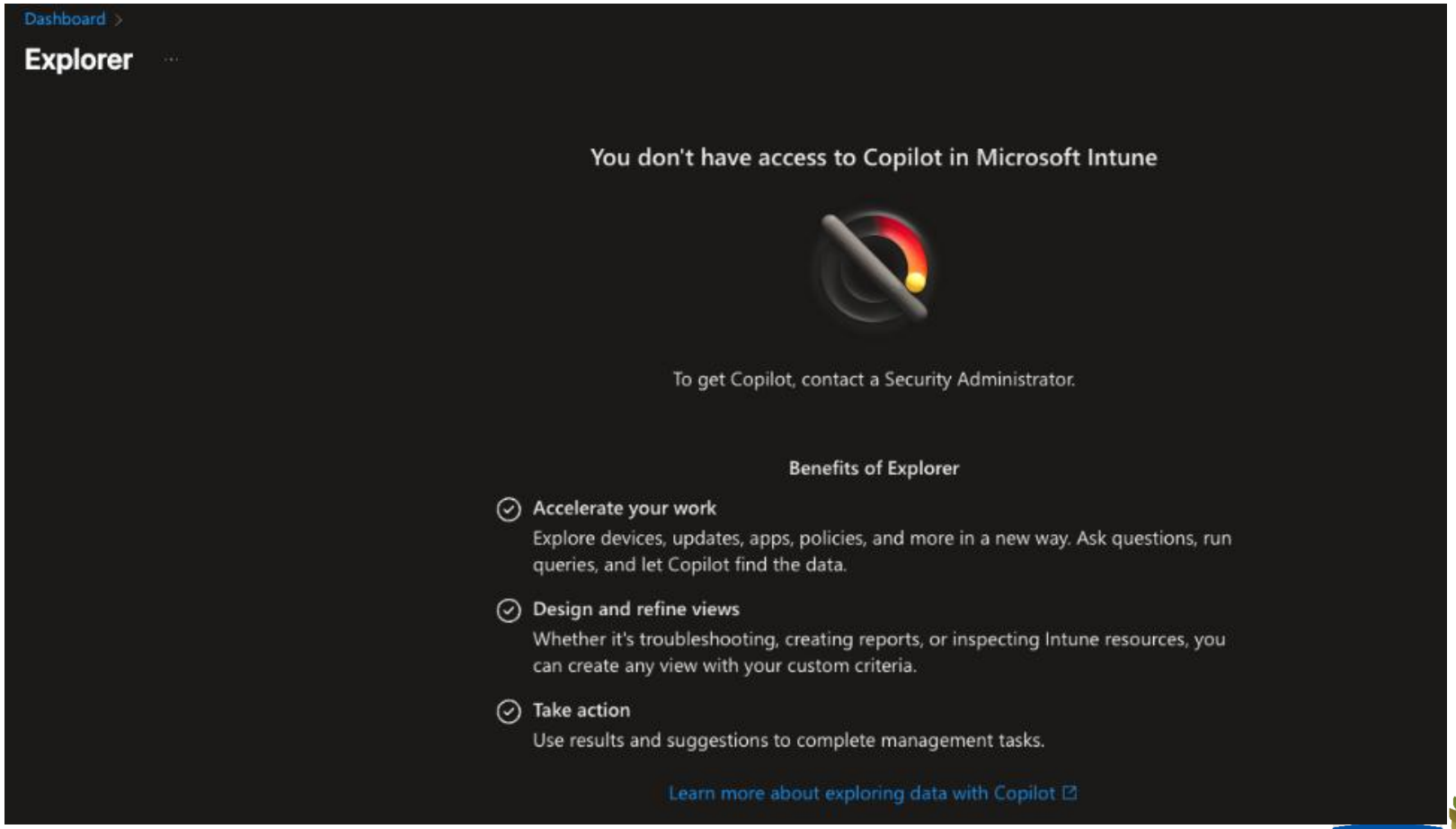
Apps
Get Managed App Type applications

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

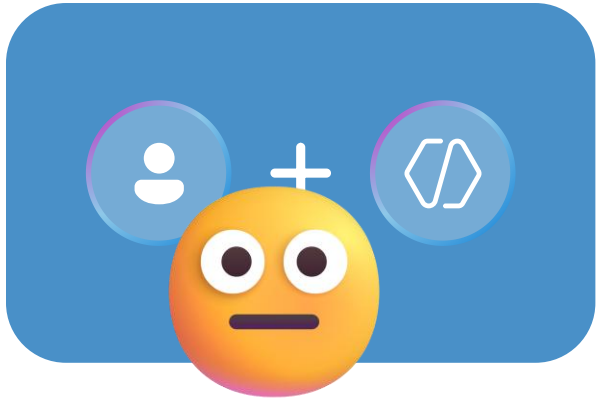
Controlled agency to act with knowledge and permission

Navigates complexity to deliver tangible outcomes

Known context | Admin authority | Outcome driven

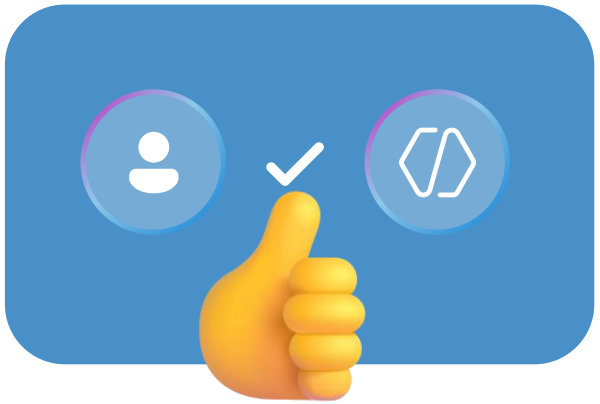
Agentic remediation types

Guided



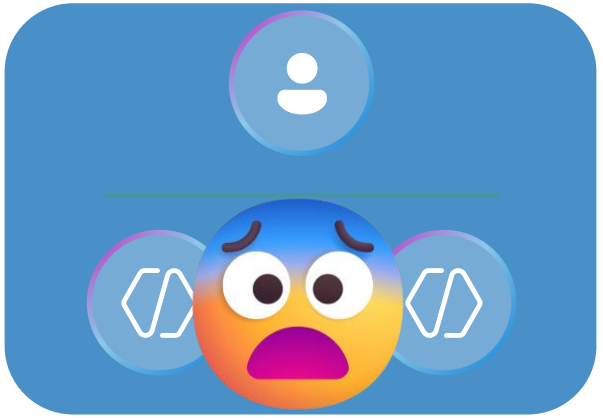
Admin remediation

Assisted



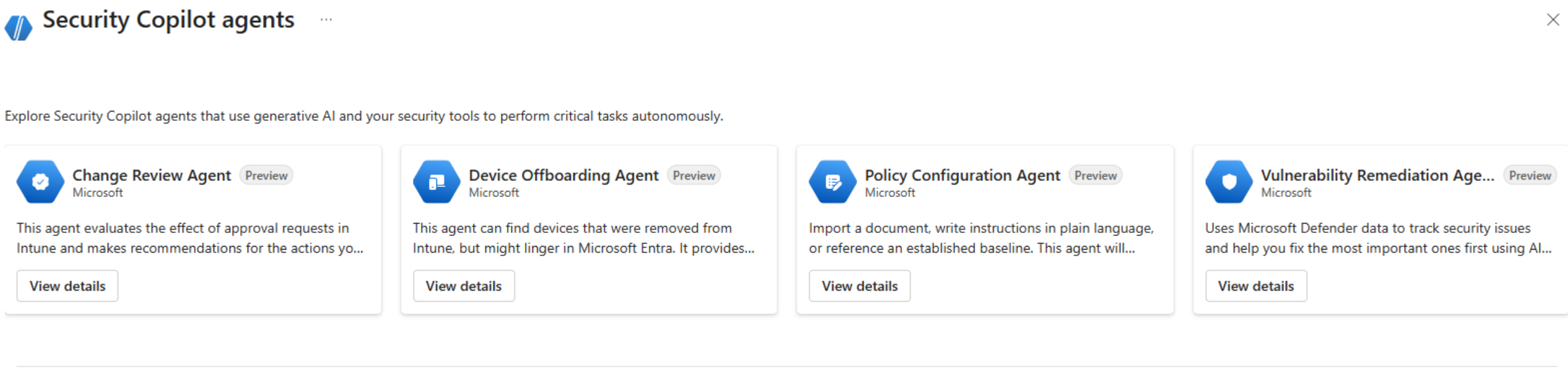
Admin approved automation

Autonomous



Automatous remediation

Security Copilot Agents



More agents coming!

You can create your own agents.
No coding required!

Vulnerability Remediation Agent

Deploy

Admin runs the agent, wanting to remediate new vulnerabilities

Discover

The agent analyzes vulnerability data from Microsoft Defender Vulnerability Management (MDVM) to help IT pros discover the vulnerabilities in their environment

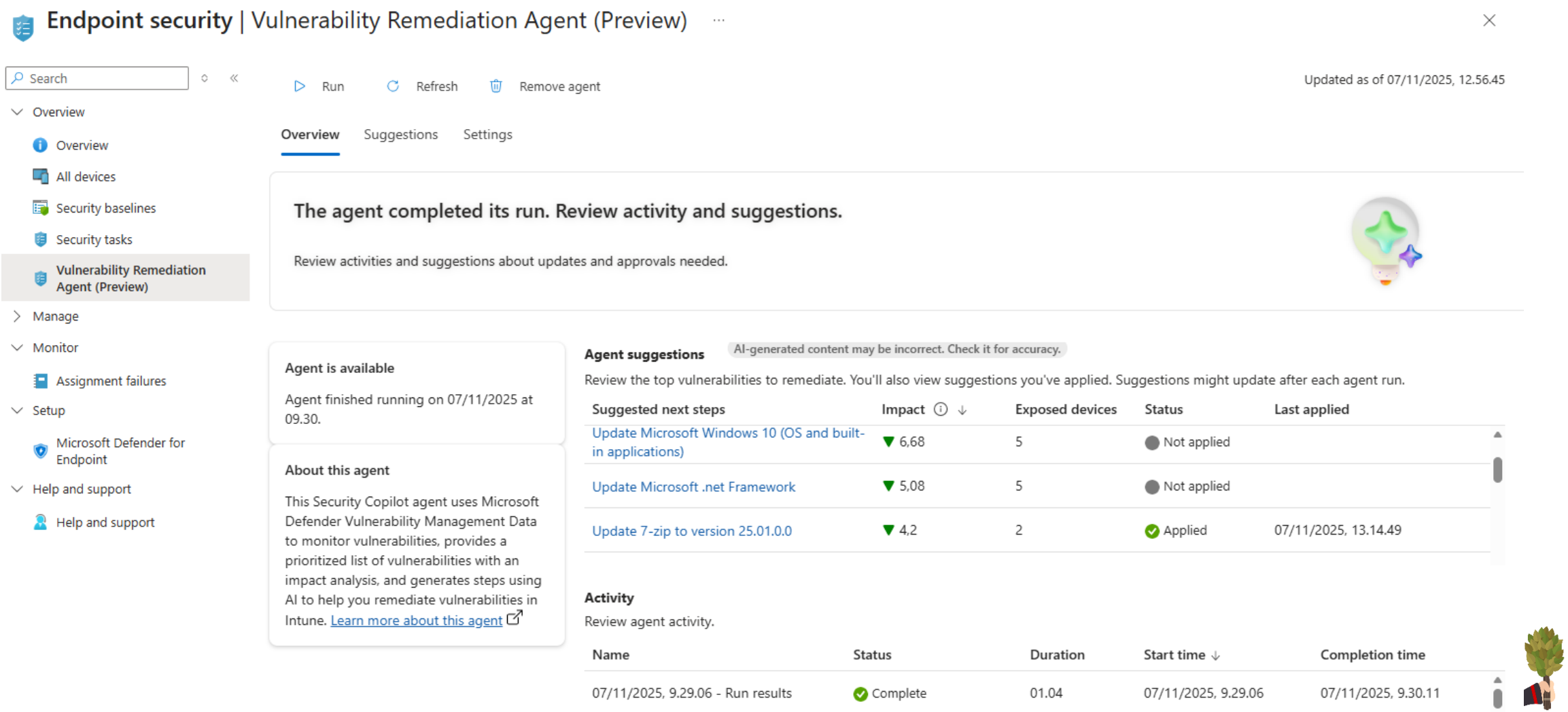
Assess

The agent prioritizes the remediation of high impact vulnerabilities by leveraging MDVM and Copilot for an impact analysis, providing explanations for its recommendations in clear, natural language & offering full transparency in its decision making

Remediate

The agent provides a step-by-step remediation guide, equipping admins with both the critical insights needed to assess high-impact vulnerabilities and the actionable steps to take in Intune to resolve them

Vulnerability Remediation Agent



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	New	Review suggestion
Review policy Disable legacy authentication with no break glass accounts	Suggested policy review	11/7/25, 12:04:24 PM	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	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	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	Not applied	Review suggestion

Policy Configuration Agent

Translate requirements into policies

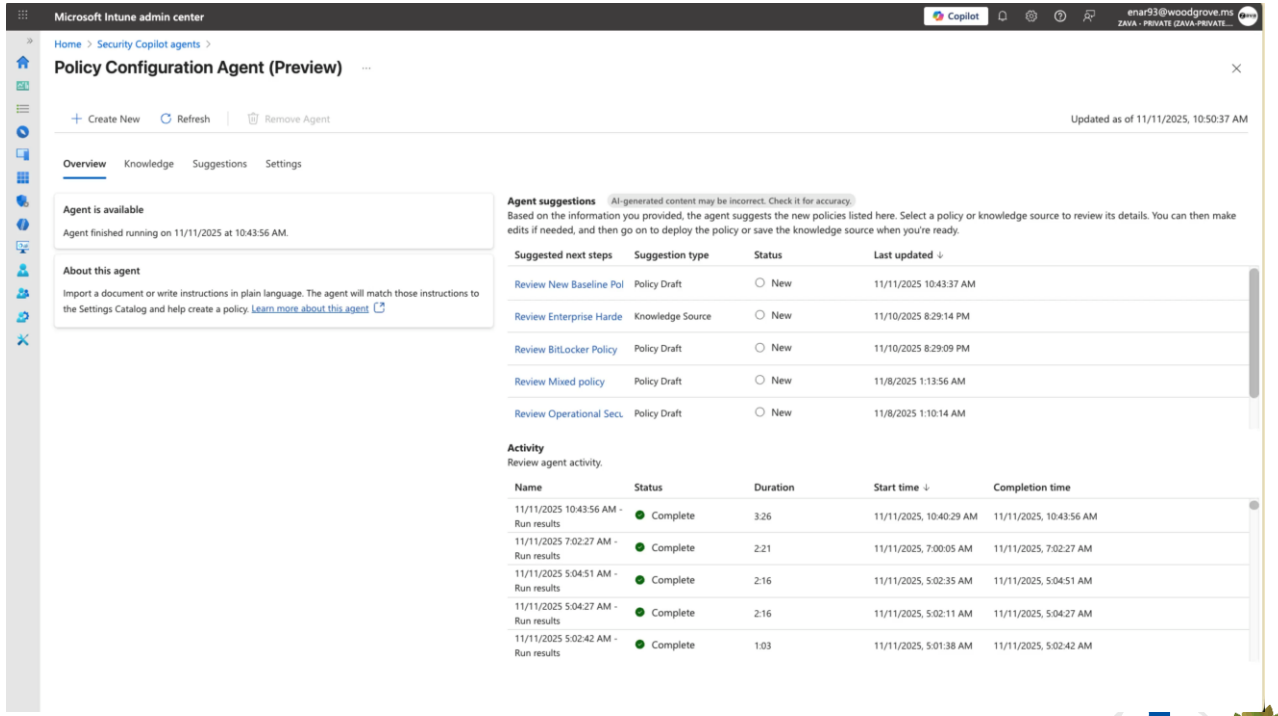
- Converts complex or ambiguous compliance standards into actionable Intune policy settings automatically.

Help ensure compliance at scale

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

Reduce manual mapping

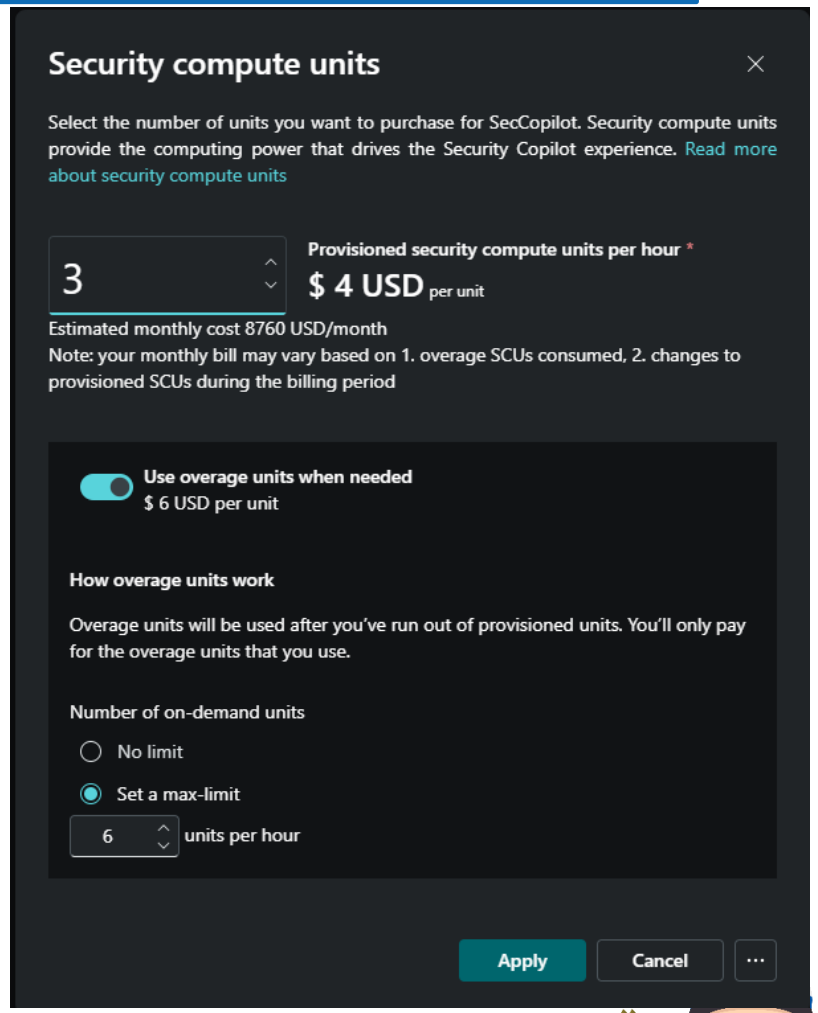
- Eliminates time-consuming interpretation of documents like CIS or STIG, accelerating policy deployment.



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**



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-	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!

PATCH MY PC

PLENTICS

twoday

Microsoft

DELL

Workplace Ninja
User Group Finland

intel

Thank you!