Microsoft Ignite 2025

Annoucements

Thank you Sponsors

Gold

liquidware

2Pint

PINK

RECAST SOFTWARE

Silver

PATCH MY PC

Technical Partners

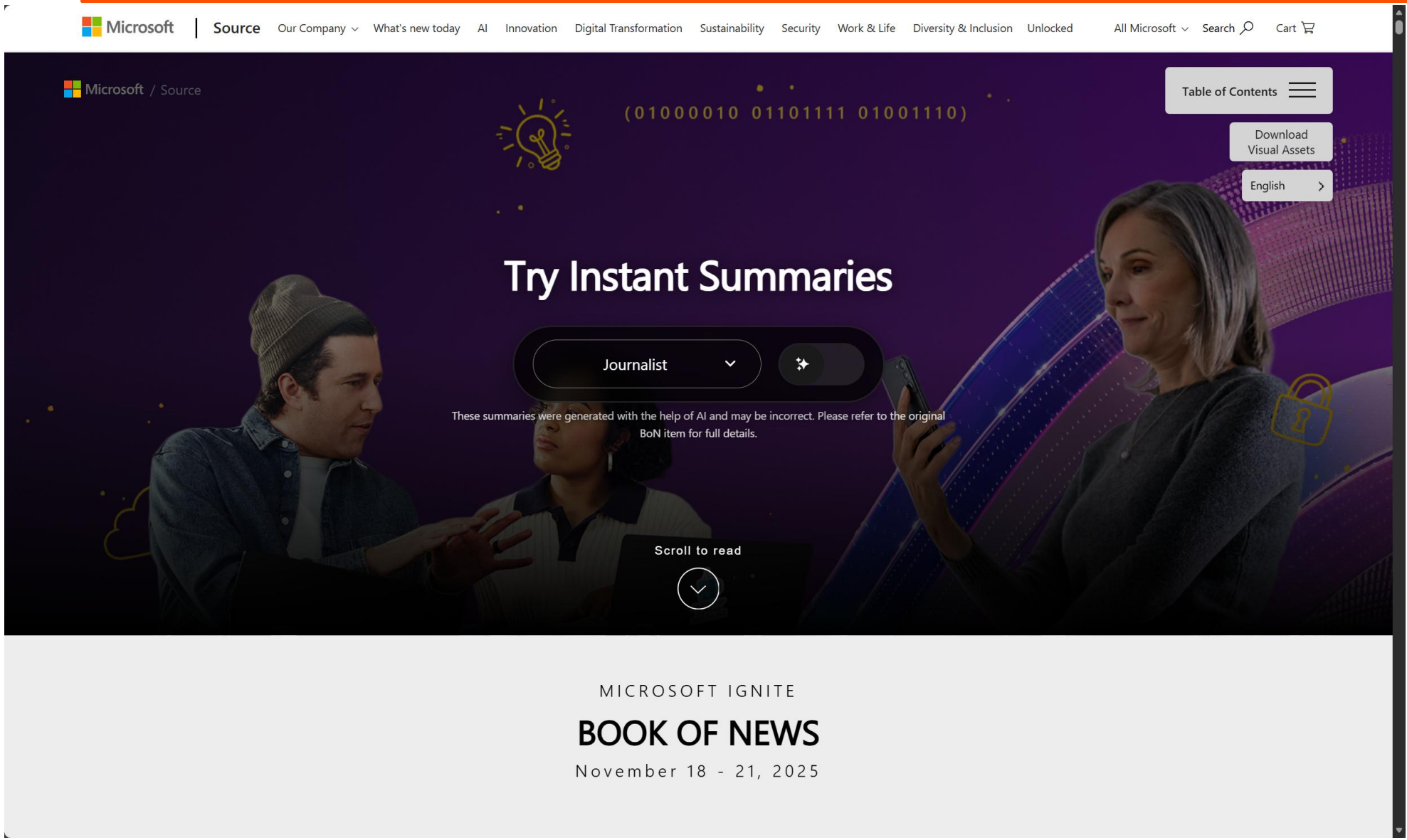
CONSULTEQ

PROXSYS

Daalmans consulting

Secure At Work

Book of news

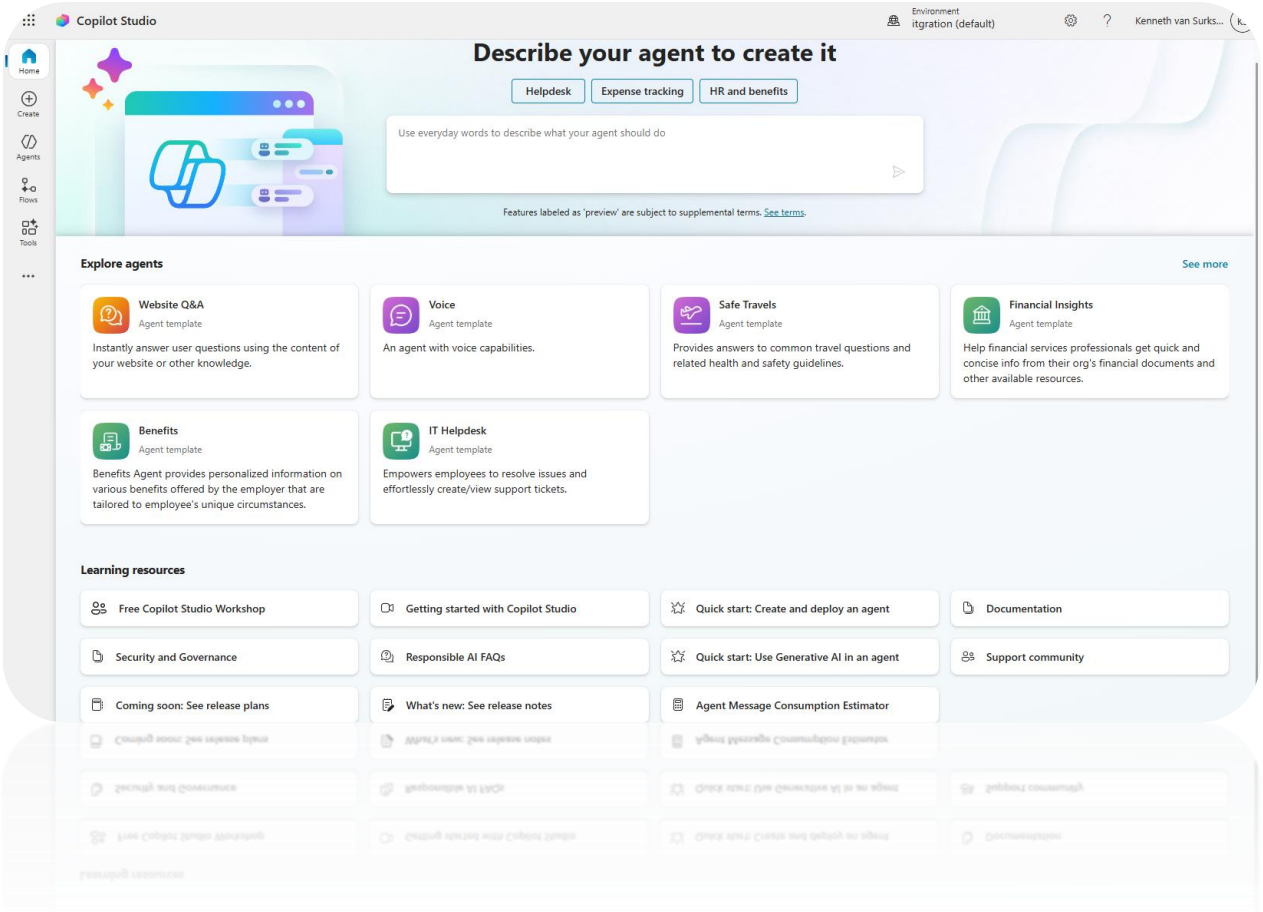


[Microsoft Ignite 2025 Book of News]

AI Agents

AI Agents

- Microsoft Agent 365: Control plane for managing AI agents similar as users at scale.
- New Agents: Sales Development, Workforce Insights, People, Learning.
- Copilot Enhancements: Agent Mode in Word, Excel, PowerPoint.
- Copilot Studio Updates: Agent evaluations, monitoring, Entra Agent ID.
- Foundry IQ & Fabric IQ: Unified context layer for advanced reasoning.



Autonomous agents

- **Sales Development Agent** – Supports sales teams by researching prospects, qualifying leads, and automating outreach.
- **Workforce Insights Agent** – Helps HR/leadership with org analytics, workforce insights, and structural visibility.
- **People Agent** – Helps employees find the right colleagues, skills, and expertise across the organization.
- **Learning Agent** – Delivers personalized micro-learning and role-specific training for employees.

- **Teams Admin Agent** – Assists IT admins with provisioning, monitoring, and Teams governance tasks.
- **SharePoint Admin Agent** – Detects oversharing, ownerless sites, permission sprawl; supports compliance/governance.

Agent Mode in Word, Excel, PowerPoint

- Agent Mode is a new Copilot mode inside Word, Excel, and PowerPoint that turns Copilot into an active, multi-step agent rather than a simple prompt responder.
- It analyzes your file, creates a plan, and executes steps directly in the document/spreadsheet/presentation.
  - In Word: drafts, rewrites, restructures, formats, and iterates with you.
  - In Excel: builds formulas, analyses, charts, data models, and fixes issues automatically.
  - In PowerPoint: creates/updates slides, designs layouts, reorganizes content, and adapts to the target audience.It’s interactive — you see the steps, approve, adjust, or rerun.

- Rollout: Word is GA; Excel/PowerPoint are in preview and expanding through 2026.

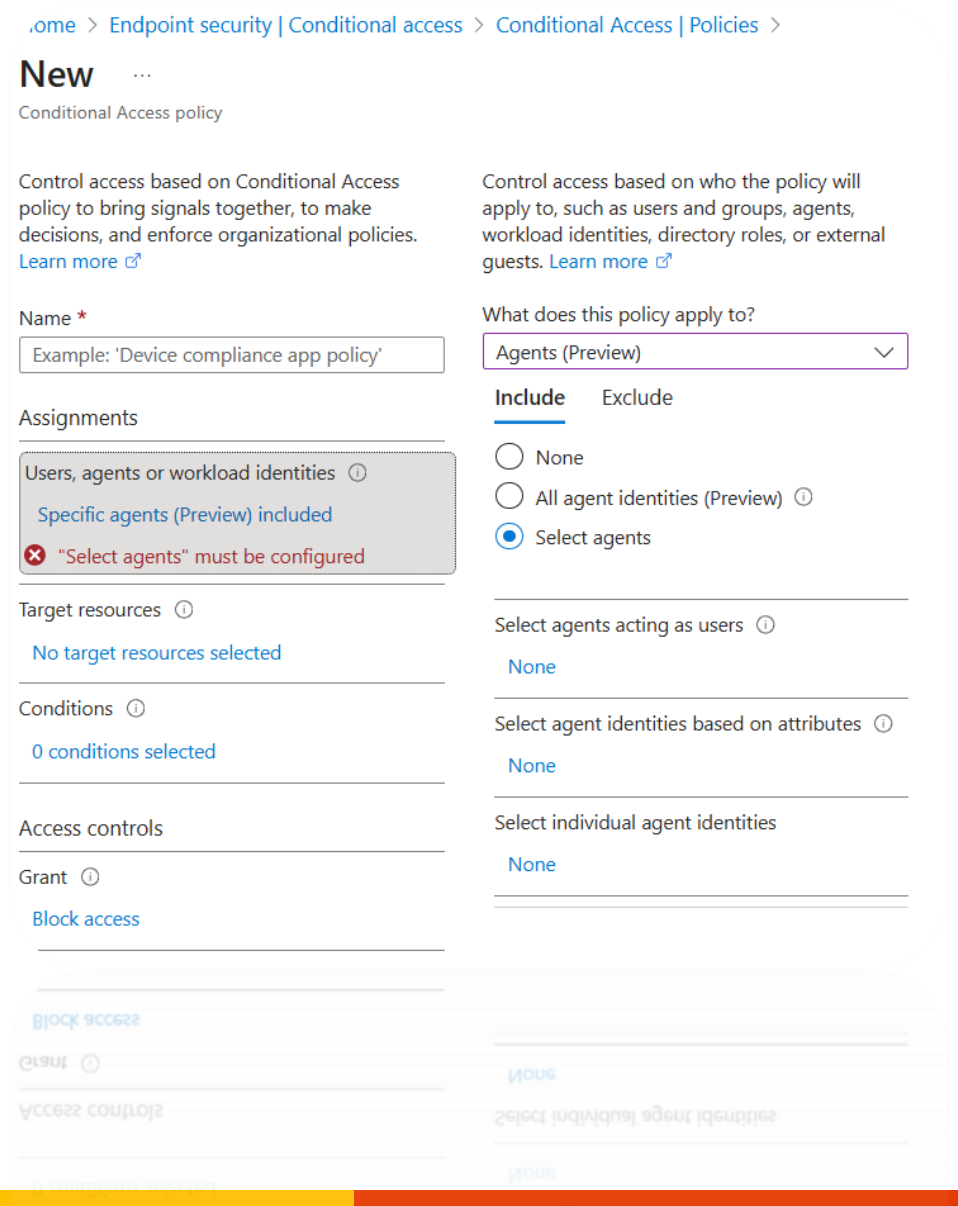
Copilot Studio

- **New models:** Support for GPT-4.1 + GPT-5 family (Chat, Auto, Reasoning).
- **Computer-use automation:** Agents can control apps/websites via mouse/keyboard for GUI-based workflows.
- **Multi-agent orchestration:** Coordinate multiple agents across complex tasks + improved evaluation & analytics.
- **Better grounding:** Stronger context from org data (SharePoint, Work IQ, Foundry IQ, Fabric IQ).
- **Low-code creation:** Natural-language app and workflow builder for non-dev users.
- **Enterprise governance:** Integrated with Agent 365 for permissions, identity, lifecycle & compliance management.

Microsoft Agent 365

Core capabilities:

- Registry of agents (including “shadow agents”)
- Access control (risk-based conditional access)
- Visualization of data flows
- Interoperability with productivity apps and data sources
- Built-in security via tools like Microsoft Defender, Microsoft Entra, and Microsoft Purview.



Model Context Protocol (MCP)

- **Native MCP support on Windows (preview):** Windows now supports MCP natively, enabling agents to use built-in connectors (e.g. File Explorer, System Settings) for file operations and device configuration.
- **Unified MCP tool catalog for enterprises:** Developers get a managed catalog of MCP servers/tools (public & private), simplifying discovery, governance, and reuse of connectors across apps and agents.
- **MCP extended to business applications:** Enhanced MCP servers for Dynamics 365 (ERP, Dataverse, Sales, Customer Service) and Power Platform — enabling agents to interact with ERP / CRM data and business-workflows securely.
- **Integration with automation platforms:** Azure Logic Apps (via “Agent Loop”) now supports MCP — letting agents call external tools/services through a standardized interface, enabling robust automation across systems.
- **Cross-tool & cross-app agent collaboration in Microsoft Teams:** Agents in Teams channels can now interact with third-party apps and other agents via MCP — enabling workflows like pulling tasks from tools (e.g. Jira, Asana) and scheduling follow-up right from Teams.

Security

Security

- 400 Security Compute Units (SCU) each month for every 1000 paid user license Microsoft 365 E5, up to 10.000 SCU per month at no additional costs
- Microsoft Baseline Security Mode - Ignite’25 Spotlight: Announcing Microsoft Baseline security mode | Microsoft Community Hub

- Defender Innovations: Integration with GitHub Advanced Security.
- Unified posture management and threat protection for AI agents.
- Security Copilot: 12 new agents for SOC, identity, and data security.
- Microsoft Purview: Expanded DSPM and agent observability.
- Security Dashboard for AI: Unified view of AI risk posture.
- Microsoft Defender Experts Suite (CY26)

Home
Copilot
Agents
Users
Devices
Teams & groups
Marketplace
Billing
Setup
Customize navigation
Show all

Enable Dark mode

Baseline security mode

Report settings

Manage these policies to reduce your attack surface and harden your Microsoft 365 organization from malicious attacks. Each policy is recommended to reach the minimum security benchmark.

Learn about baseline security mode and why it's important

Progress to meet standard 94%

Your progress ▼Standard benchmark You have applied 17 out of 18 recommendations

Recommended setting automation

Microsoft recommended setting adjustments as of Tue Nov 11 2025

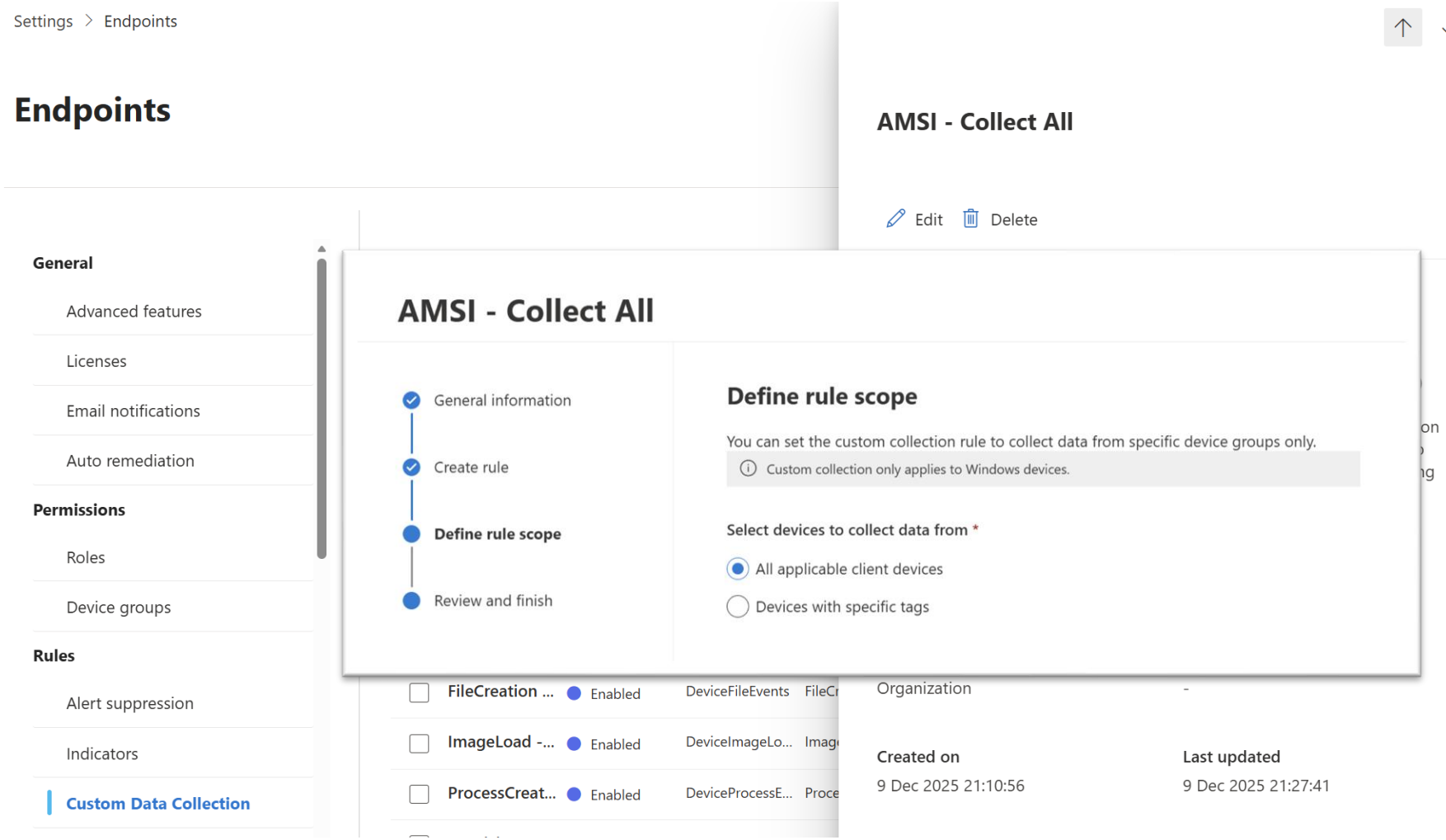
Filters: Category: all | Workload: all | Status: all | Reset all filters

Setting recommendation	Status	Service
Authentication (12)		
Require phishing-resistant authentication for admins	In review	Entra ID
Block legacy authentication	Meets standard	Entra ID
Block new password credentials in apps	Meets standard	Entra ID
Turn on restricted management user consent settings	Meets standard	Entra ID
Block access to Exchange Web Services	Meets standard	Exchange
Block basic authentication prompts	Meets standard	Microsoft 365 apps
Block files from opening with insecure protocols	Meets standard	Microsoft 365 apps
Block files from opening with FPRPC protocol	Meets standard	Microsoft 365 apps
Block legacy browser authentication connections to SharePoint	Meets standard	SharePoint
Block IDCRL protocol connections to SharePoint	Meets standard	SharePoint

Custom Data Collection

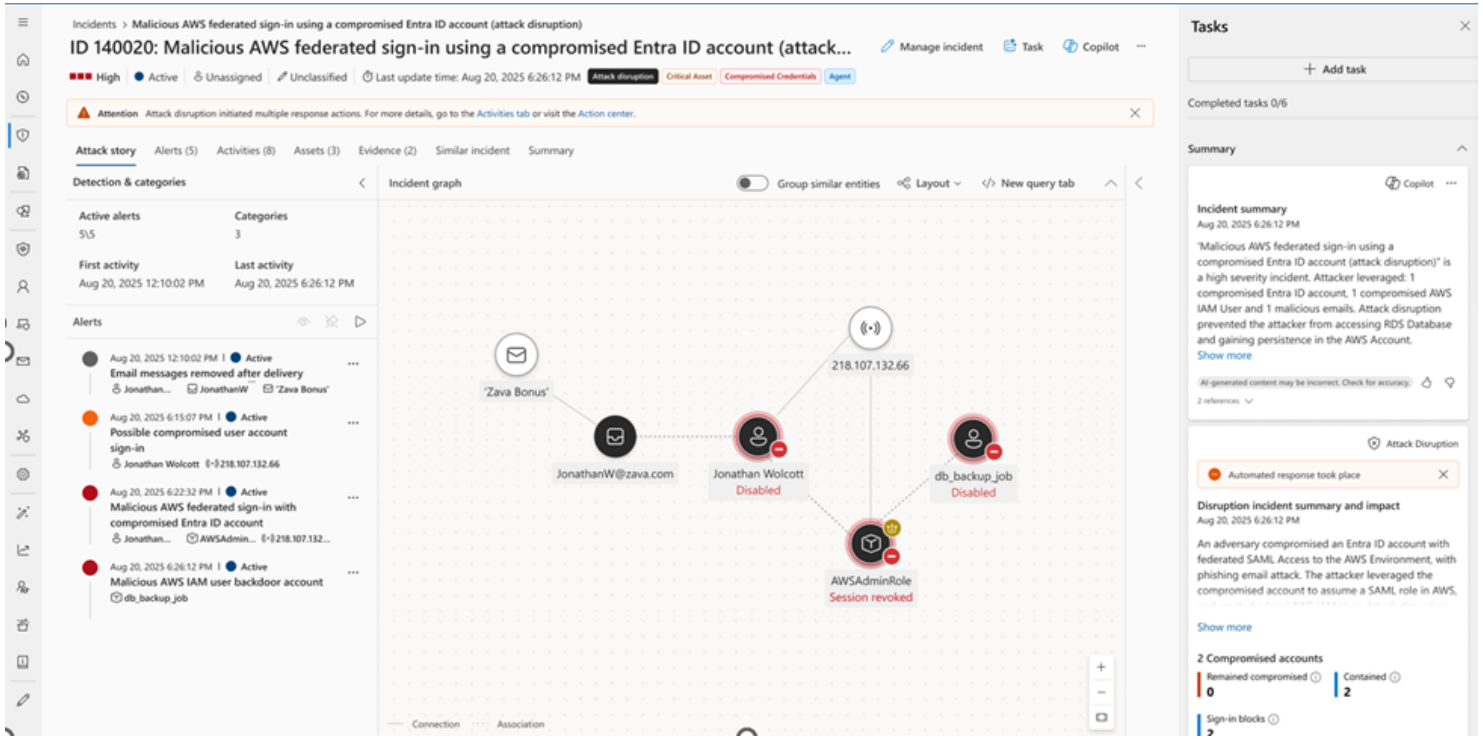
Custom data collection (Preview) enables organizations to expand and customize telemetry collection beyond default configurations to support specialized threat hunting and security monitoring needs.

This feature allows security teams to define specific collection rules with tailored filters for event properties such as folder paths, process names, and network connections.



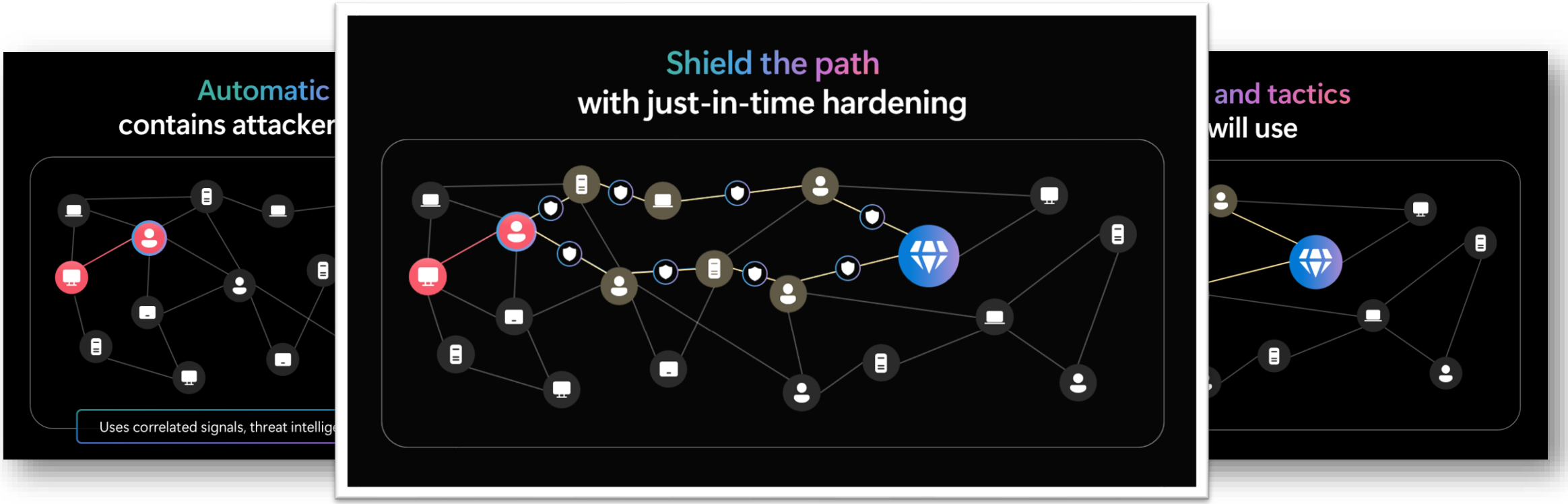
Proactive Response: Automatic attack disruption on AWS, Proofpoint & Okta

Automatic attack disruption is now extending beyond XDR, incorporating data from AWS, Proofpoint and Okta when brought in through Sentinel. By leveraging millions of signals from Microsoft Threat Intelligence, this feature uses AI to detect sophisticated threats like phishing, business email compromise, and identity compromise across federated accounts and cloud boundaries.



Predictive Shielding

Predictive shielding: Defender is the first security solution to not only respond instantly during an attack but also jump ahead of attackers, predicting and preventing the next move before it happens with just-in-time hardening controls that block specific attacker techniques to protect critical assets.

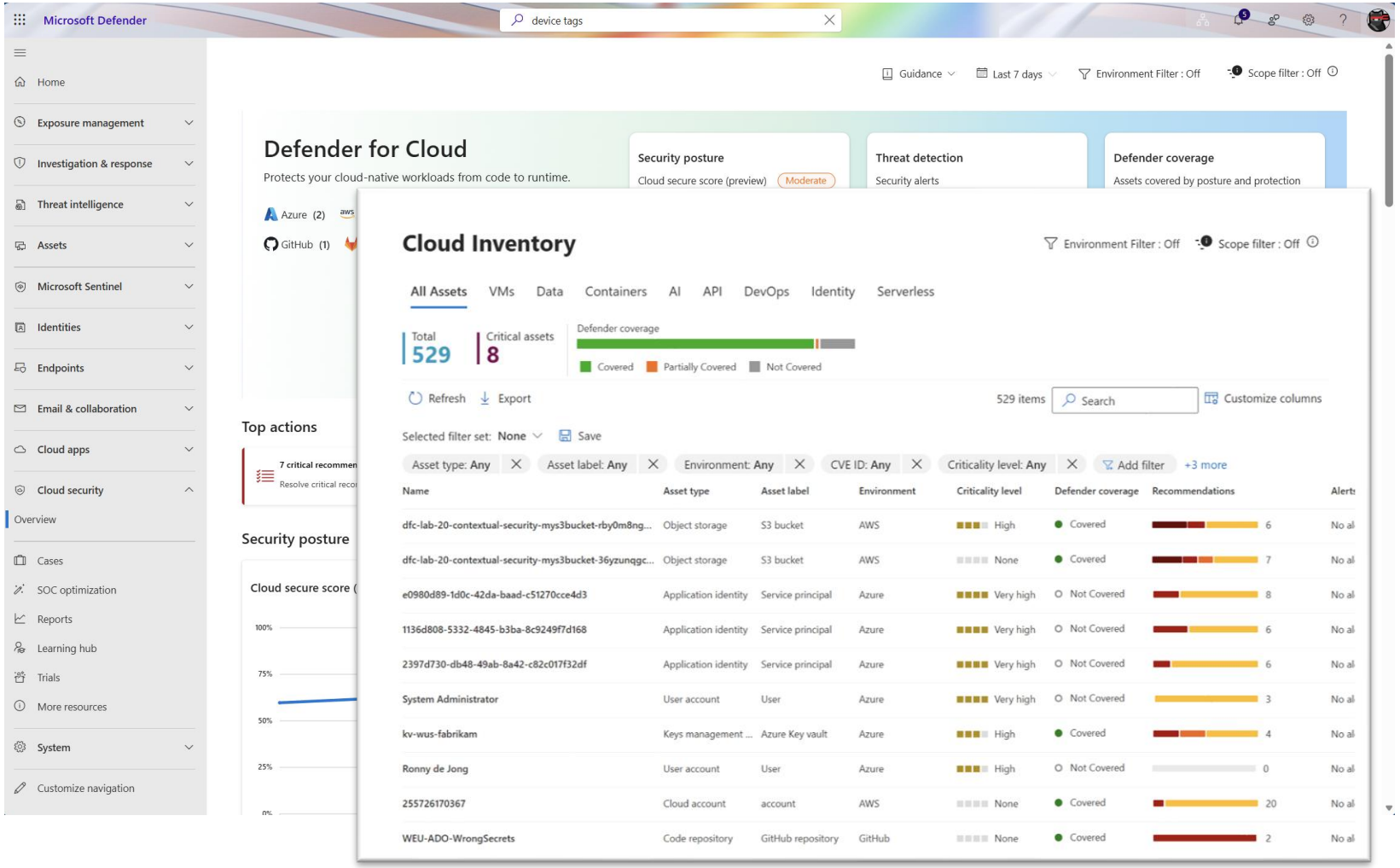


Unified Security Posture Management

MDC integrated into the Defender portal for security personas. This native integration will eliminate silos so security teams can see and act on threats across all environments from one place.

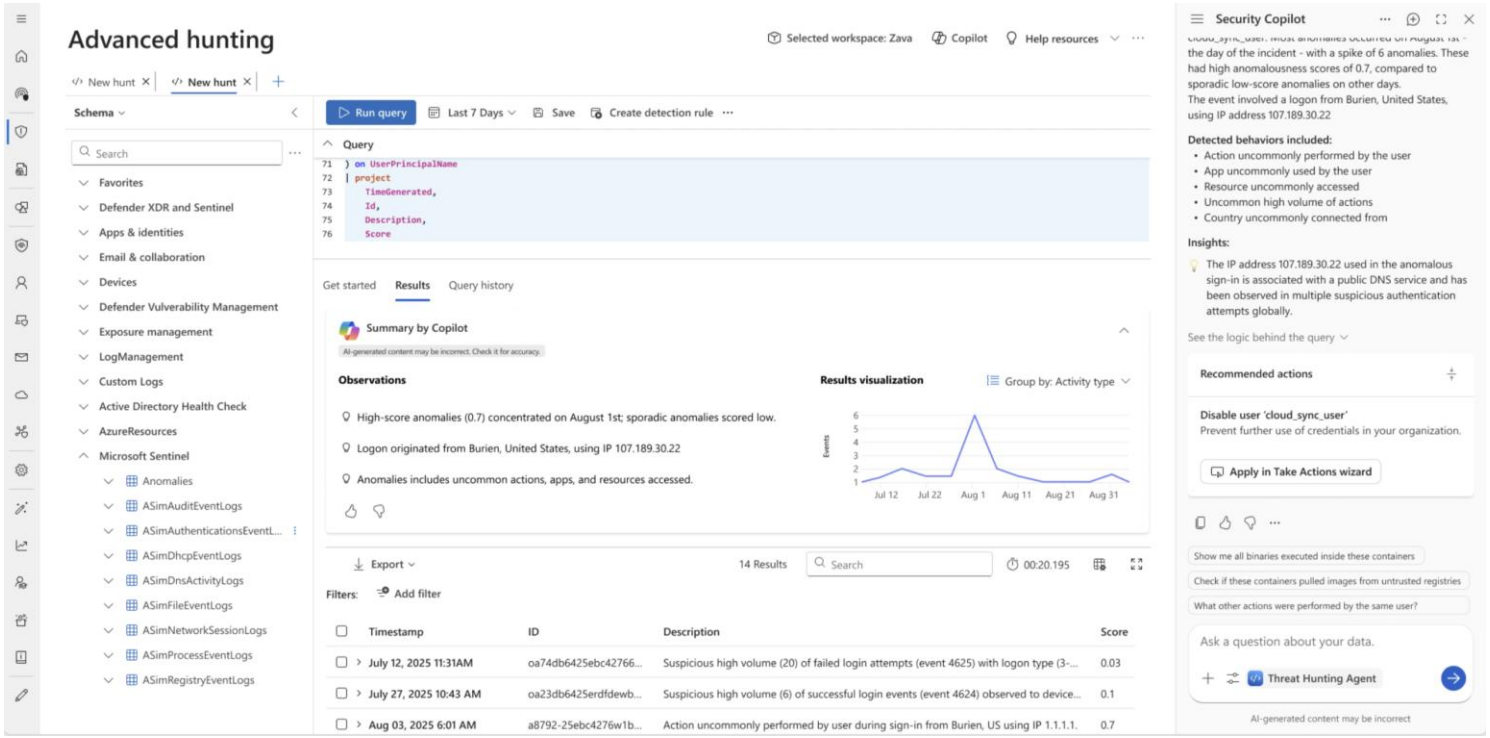
This integration will offer:

- **Cloud security dashboard**
- **Unified cloud posture capabilities**
- **Centralized asset inventory**



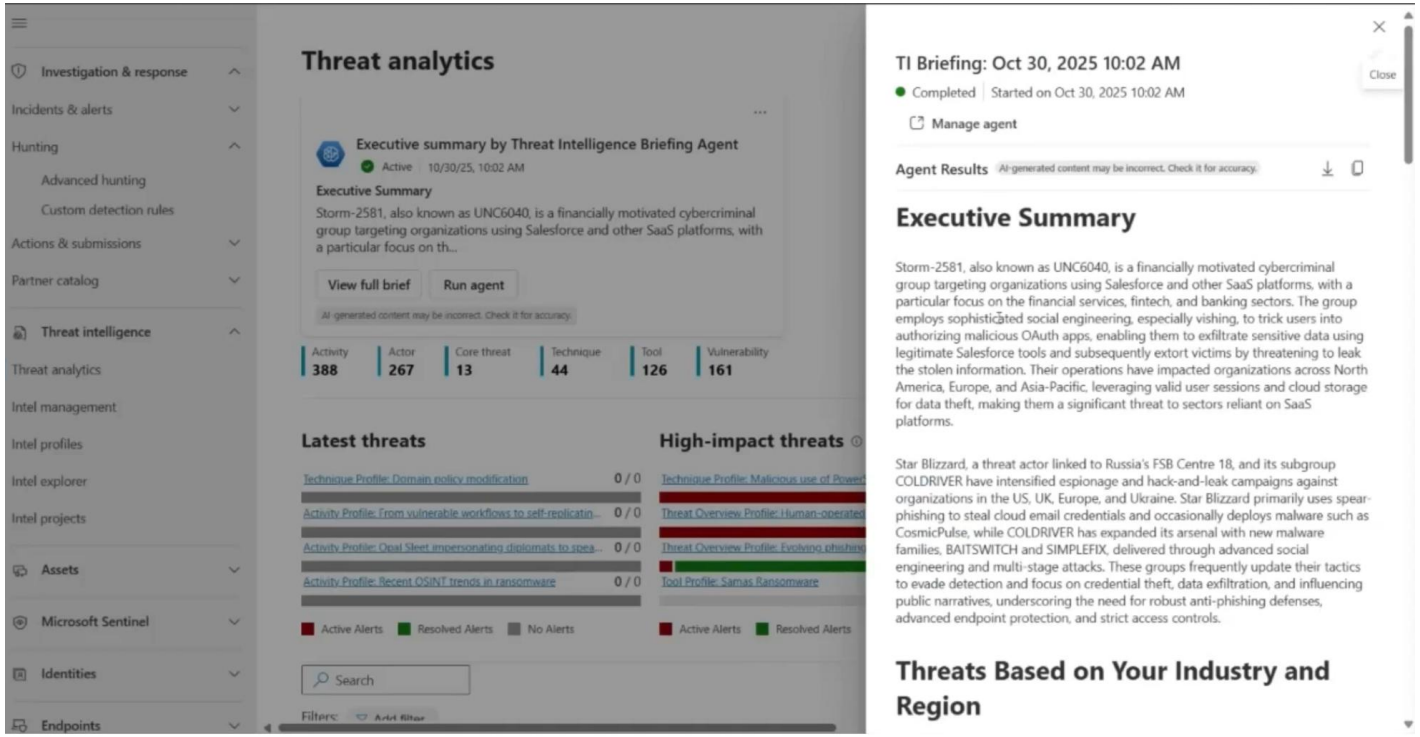
AI-Assisted SOC: Threat Hunting Agent

The **Threat Hunting Agent** transforms threat hunting by allowing analysts to conduct end-to-end investigations using natural language. It provides direct answers, guides users through investigative steps, and surfaces actionable insights. This agent-driven experience helps analysts of all skill levels hunt faster, more accurately, and with rich security context.



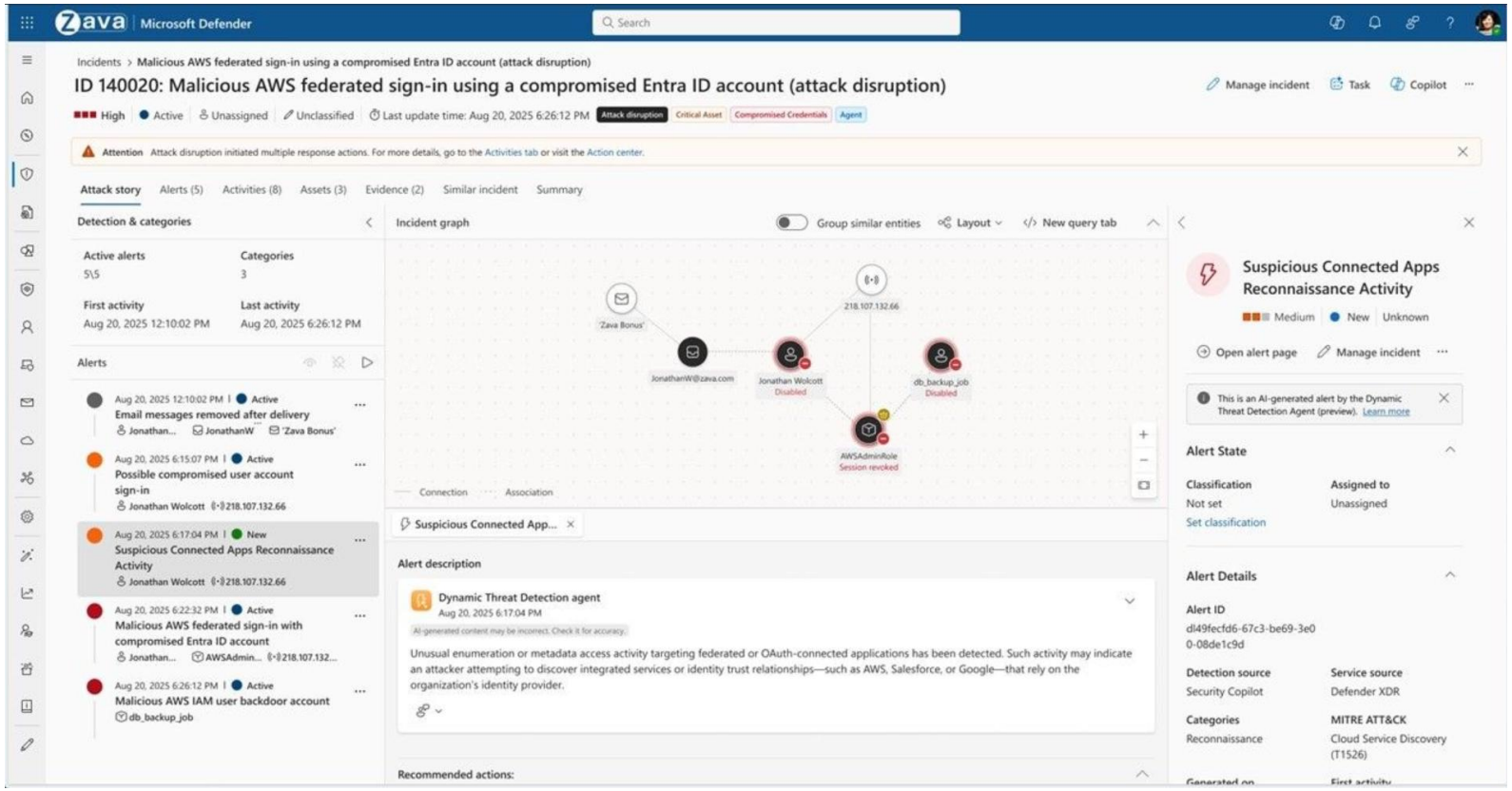
AI-Assisted SOC: Threat Intelligence Briefing Agent

- The **Threat Intelligence Briefing Agent** is now seamlessly integrated into the Microsoft Defender portal. In just a few minutes, the agent generates tailored threat briefings that synthesize the latest insights from Microsoft Threat Intelligence and hundreds of global sources, directly contextualized to an organization's unique environment.



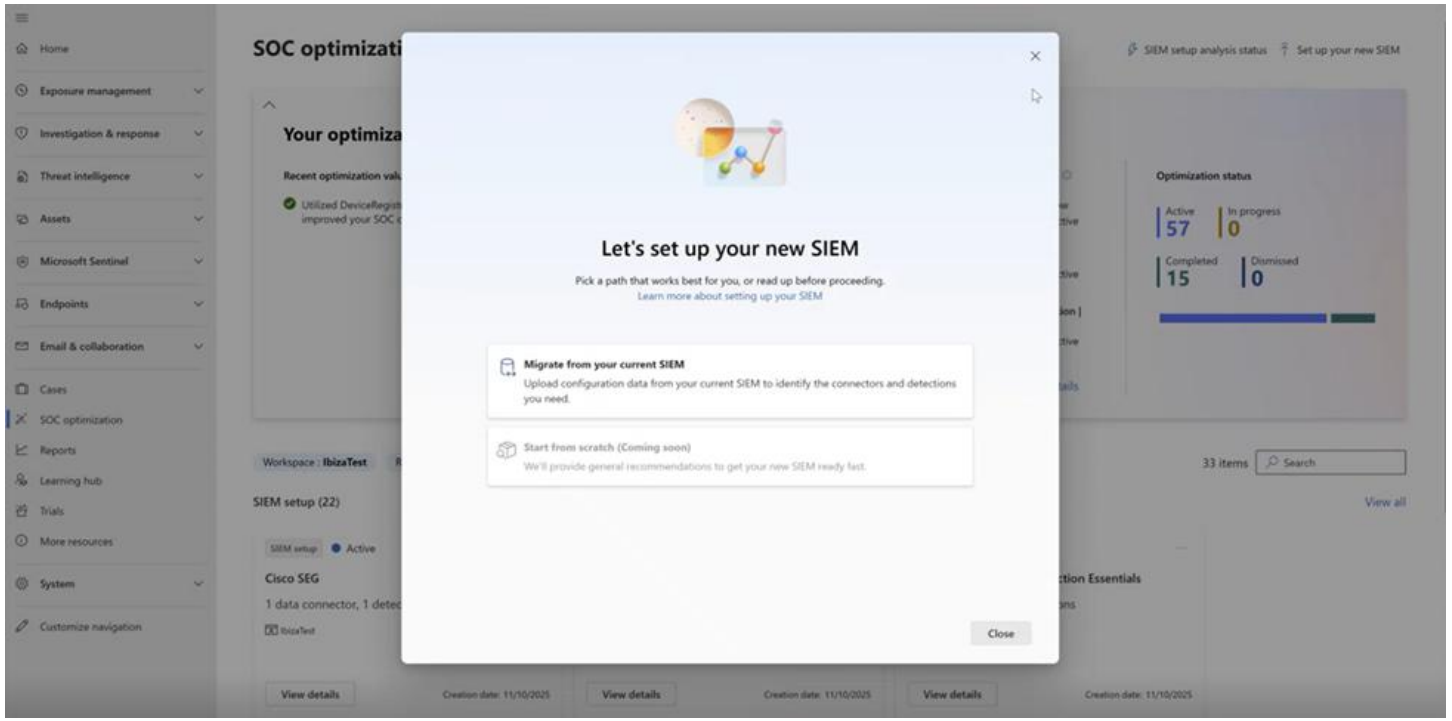
AI-Assisted SOC: Dynamic Threat Detection Agent

- The **Dynamic Threat Detection Agent** proactively hunts for false negatives and blind spots that traditional alerting might miss.
- When a critical incident happens, Copilot automatically hunts to uncover undetected threats—like unusual residual activity around a sensitive identity.
- This agent turns ‘probably fine’ into proven secure—finding and fixing false negatives to keep organizations safer.



Accelerated Onboarding: AI powered SIEM migration tool

We’re excited to announce the new enhanced SIEM migration experience for Microsoft Sentinel—designed to simplify and accelerate migrations from Splunk and QRadar. SIEM migrations are complex and resource-intensive, often taking months. While many solutions simply convert queries into proprietary syntax, Microsoft takes a different approach—driving true SOC transformation with advanced correlation and insights that go beyond syntax conversion. This ensures a fully integrated, future-ready SOC aligned with modern security needs—not just translated legacy queries.

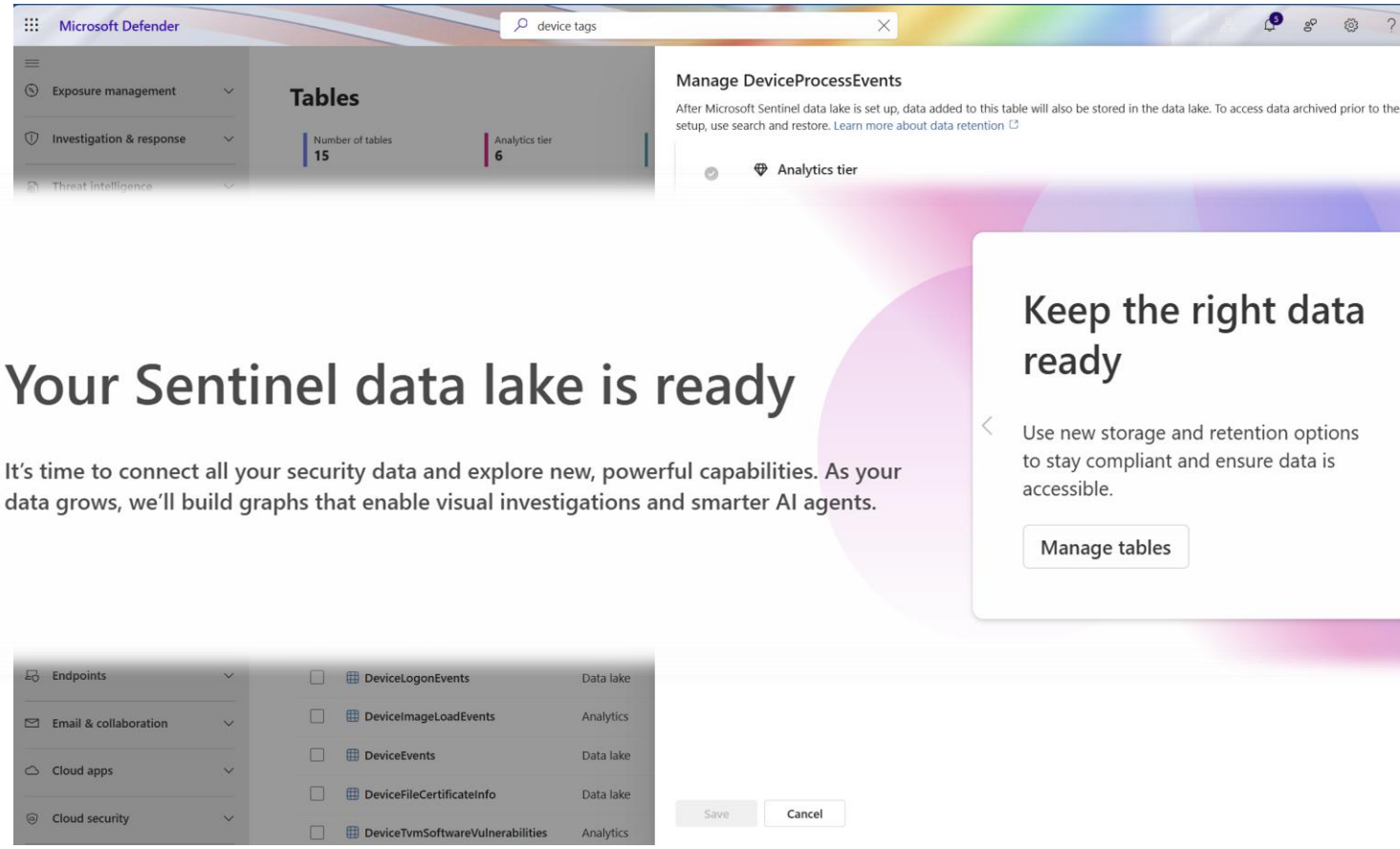


Sentinel Data Lake

- Microsoft Defender for Endpoint (MDE) directly into the Sentinel data lake
- Expansion to MDO and MDA is coming in early December.

The result: improved visibility, historical analysis, lower total cost of ownership, and powerful capabilities for modern security operations.

- Plus, you can also ingest Entra, Syslog, CEF, and CommonSecurityLog data directly into the data lake for even broader and cost-efficient coverage.



Endpoints

Microsoft Intune

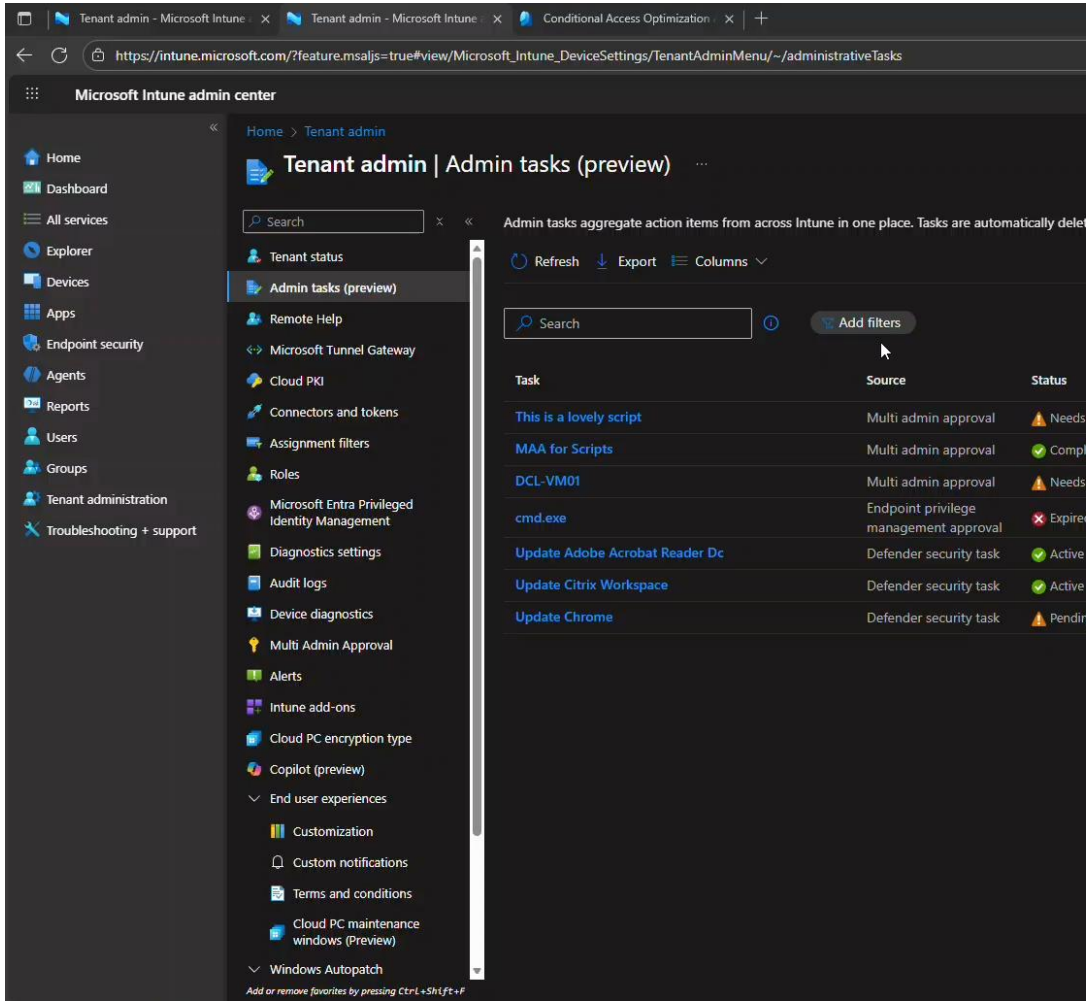
- **AI-powered Intune agents (via Security Copilot):**
  - Change Review Agent, Policy Configuration Agent, Device Offboarding Agent.
- **Copilot integrated in Intune:** natural-language queries across Autopilot, apps, EPM, analytics.
- **Safer admin operations:** new *Admin Tasks* hub + multi-admin approvals.
- **Risk-reduced rollouts:** phased *Deployments* for apps/updates (rings).
- **Improved fleet resilience:** remote WinRE management + backup/restore of user settings & Store apps.
- **More flexible app delivery:** expanded script-based Win32 deployment + managed installer enhancements.
- **Stronger privilege controls:** EPM improvements incl. shared device elevations & readiness dashboard.
- **Better update control:** maintenance windows for cloud-managed devices (2026 preview).

Agents for Microsoft Intune

- **Change Review Agent**
- Analyzes proposed Intune changes (scripts, policy updates, app rollouts) before deployment.
- Flags risky settings, conflicts with existing policies, and potential compliance impact.
- Helps avoid “fat-finger” outages and misconfigurations at scale.

- **Policy Configuration Agent**
- Admin describes intent in natural language (e.g. *“Require BitLocker with X, Y, Z”*).
- Generates recommended Intune policies + highlights gaps vs best practices.
- Reduces time from “requirement” to “deployable configuration”.

- **Device Offboarding Agent**
- Identifies stale, non-compliant, or inactive devices in the estate.
- Proposes actions such as retire, wipe, or remove from scope.
- Shrinks attack surface by cleaning up “ghost” endpoints.



Copilot Integrated in Intune

Natural-language queries across Intune
•Ask questions like *“Show devices failing EPM elevation”* or *“Why is Autopilot slow for Ring 2?”*.
•Copilot interprets intent and retrieves the right data from Intune, Autopilot, EPM, analytics, and app management.

Operational troubleshooting assistant
•Explains policy conflicts, deployment failures, or configuration drifts in plain language.
•Suggests next steps or remediation actions (e.g., “these apps conflict with your assignment filters”).

Data-driven insights for admins
•Identifies trends across devices, apps, and configurations.
•Surfaces anomalies like unusual failure spikes, misconfigured baselines, or patterns in compliance failures.

Accelerates admin workflows
•Reduces time spent searching logs and consoles.
•Gives frontline IT staff faster answers with less context switching.

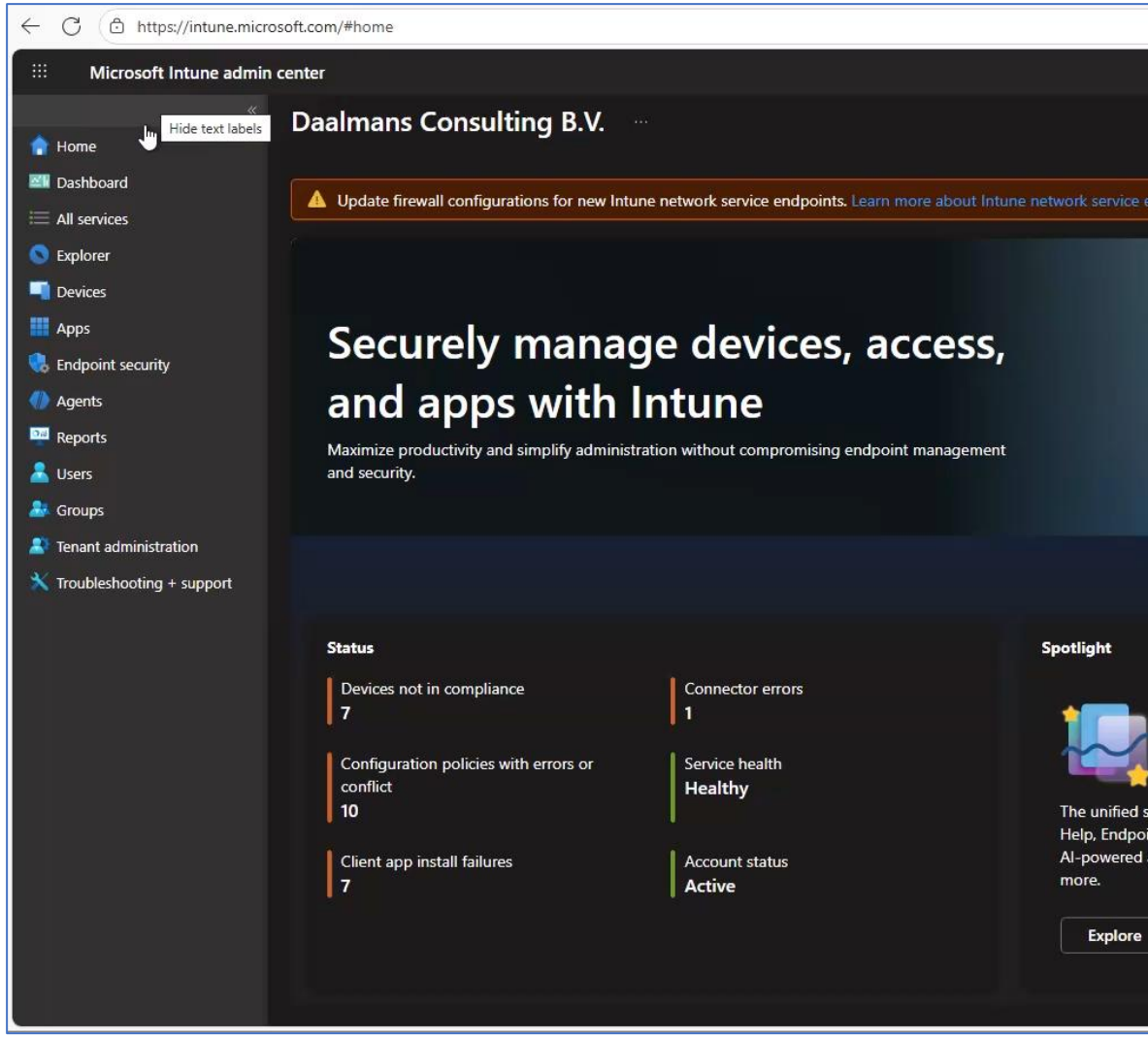
Safer Admin Operations in Intune

New *Admin Tasks* hub
•Single place for reviewing and approving sensitive operations.
•Consolidates tasks from Autopilot, EPM, policy changes, and (soon) AI-powered agents.

Built-in multi-admin approvals
•Critical changes (e.g., wiping devices, major policy updates, privilege elevations) can require a second approver.
•Reduces insider risk and accidental large-scale misconfigurations.

Stronger oversight for escalated tasks
•Tracks who requested, who approved, and when tasks were completed.
•Provides auditable history aligned with compliance requirements.

Future-ready for agent-driven workflows
•AI agents (Change Review, Policy Configuration, Device Offboarding) will also route tasks here.
•Ensures human validation stays in the loop for impactful operations.



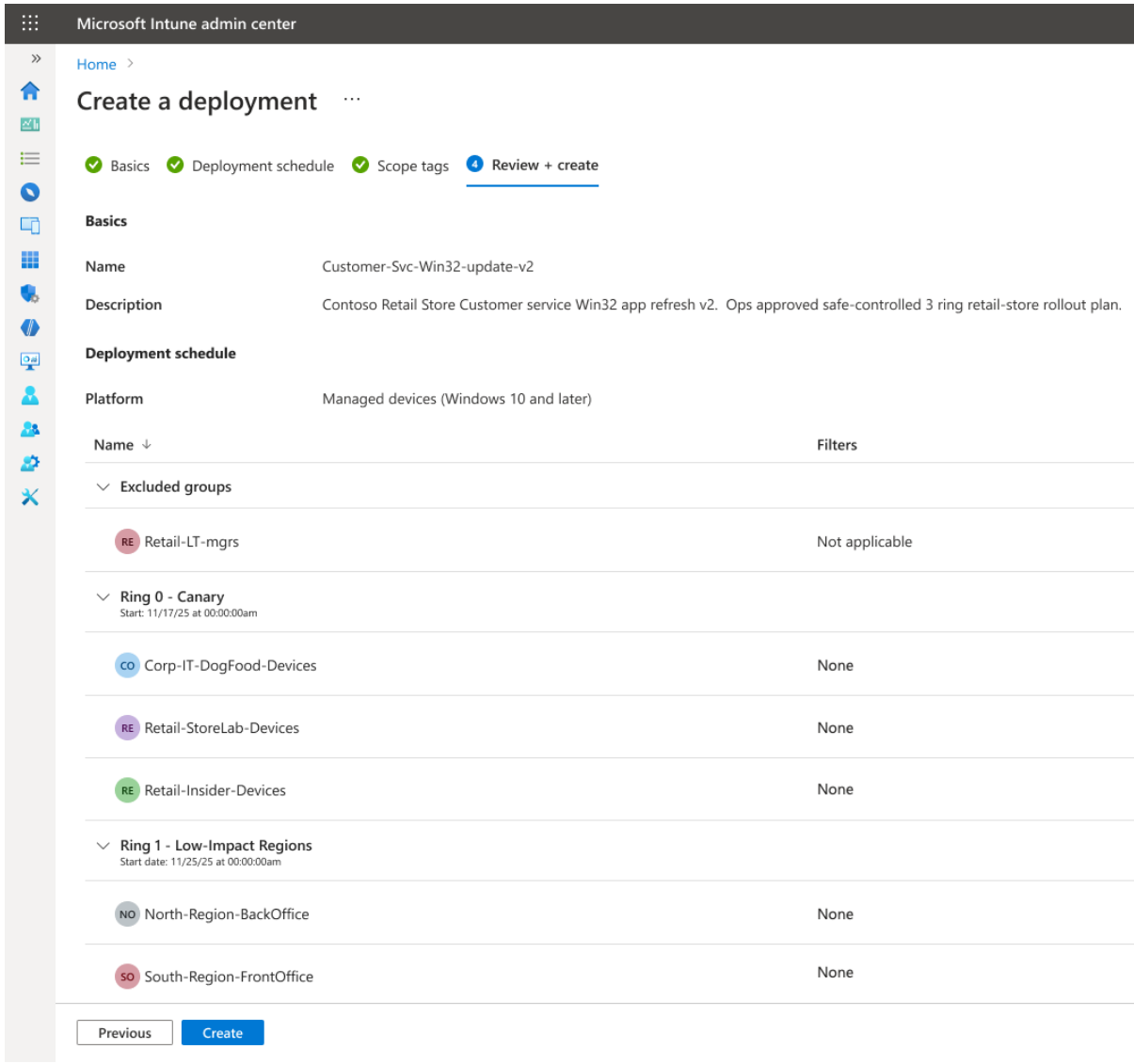
Risk-Reduced Rollouts with Phased Deployments

New *Deployments* model in Intune
•Supports ring-based, staged rollouts for apps, updates, and configurations.
•Replaces “all-at-once” assignments with controlled, multi-phase delivery.

Automatic health gating
•Intune can pause or slow down rollout if failures exceed thresholds.
•Prevents widespread outage when a bad app version or policy hits production.

Flexible ring design
•Define pilot, early adopters, broad deployment, and final rings.
•Each ring can have different schedules, controls, and rollback strategies.

Consistent admin experience
•Uniform deployment pipeline across Win32 apps, Store apps, and eventually more configuration types.
•Reduces fragmented management patterns.

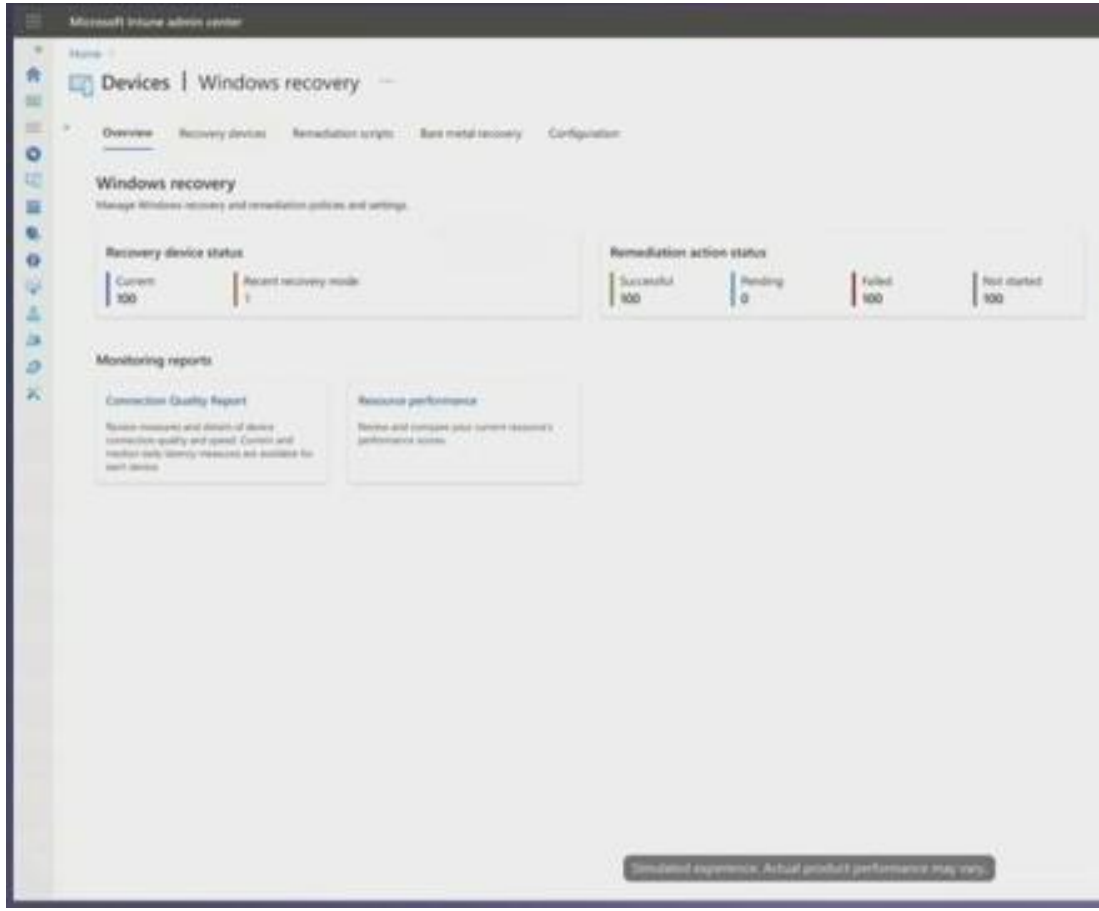


Windows Recovery and Remediation

- Remote Windows Recovery allows an admin to remotely initiate a **Windows repair, reset, or full recovery** on an enrolled and compliant Windows device.

- Cloud-powered OS repair/reset for Windows 11 devices
- Initiate recovery remotely via Intune — no physical access needed
- Supports repair, reset, or full recovery using cloud sources
- Works even when local recovery image is missing/corrupted
- Reduces need for USB sticks, on-site visits, or manual rebuilds
- Ideal for remote/hybrid workers and MSP scale-out scenarios
- Integrates with Autopatch, Autopilot, and Intune device management
- Provides IT with a last-resort, low-touch remediation option for broken devices

More information: Windows Recovery and Remediation for Quick Machine Recovery



More Flexible App Delivery in Intune

Enhanced script-based Win32 app deployment
•Admins can use more flexible installer scripts for complex or custom enterprise applications.
•Supports advanced logic, pre-checks, dependency validation, and conditional flows.

Enterprise App Catalog improvements
•Streamlined packaging and publishing experience for internal line-of-business apps.
•Better version management and simplified updating.

Managed Installer enhancements
•Improved compatibility with script-based apps and custom installers.
•Paves the way for better endpoint protection and trust-based execution via Defender Application Control (WDAC).

Better handling of non-standard installers
•Supports scenarios where EXE installers, custom bootstrap scripts, or multi-file app bundles are required.
•Reduces the need for workaround packaging tools.

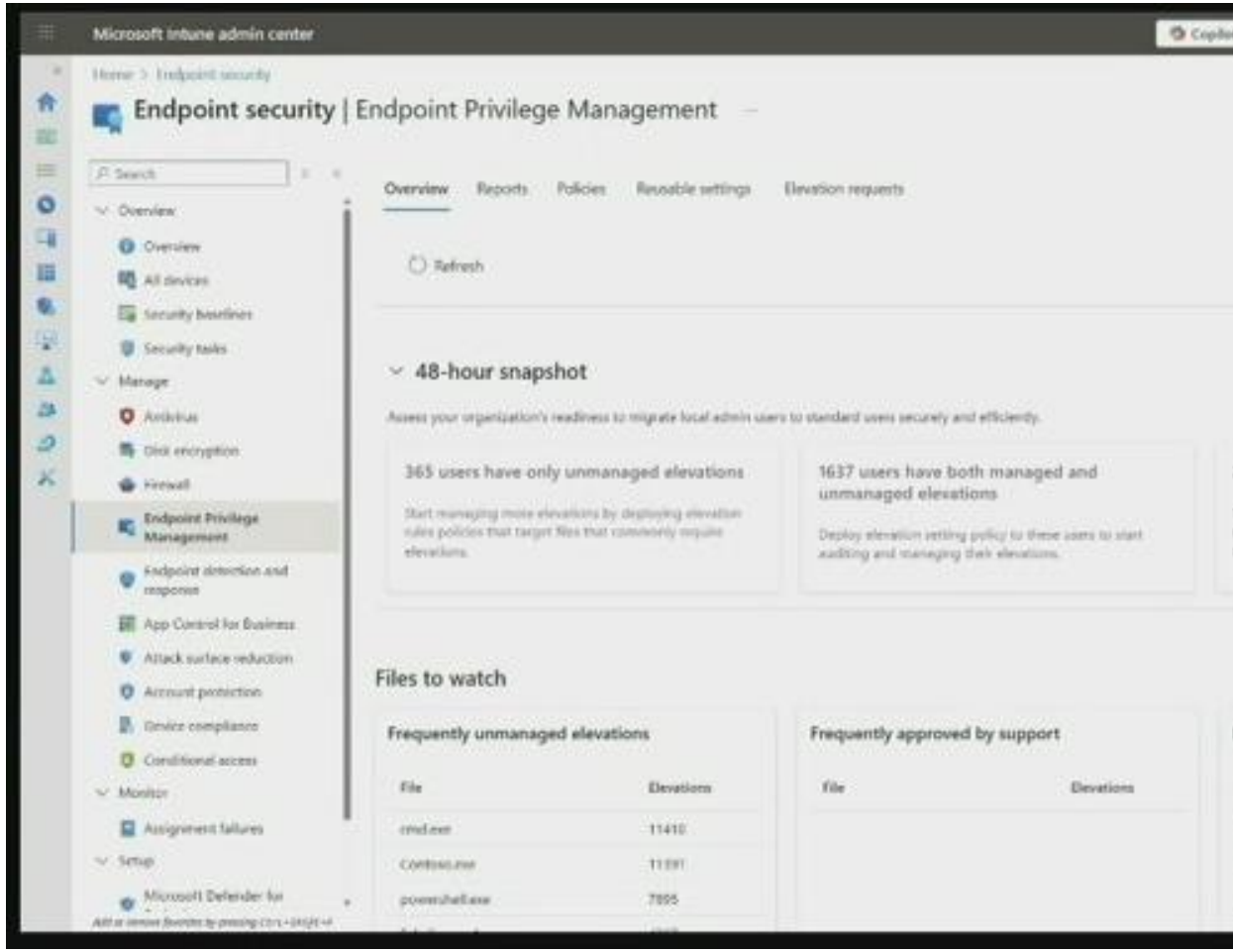
Stronger Privilege Controls with EPM Enhancements

Elevation for non-primary users on shared devices
•EPM now supports elevations even when the user is not the device's primary enrolled user.
•Critical for frontline/shift workers, labs, and shared workstation environments.

New EPM readiness dashboard
•Centralized view of devices eligible for elevation.
•Highlights misconfigurations, enrollment gaps, and policy readiness issues.

Expanded elevation rule types
•Upcoming support for **network configuration elevation rules** (preview 2026).
•Allows controlled access to advanced network settings without giving full admin rights.

Better audit and compliance insights
•Richer logging of elevation attempts, approvals, and denials.
•Enables organizations to validate adherence to least-privilege baselines.



Better Update Control with Maintenance Windows

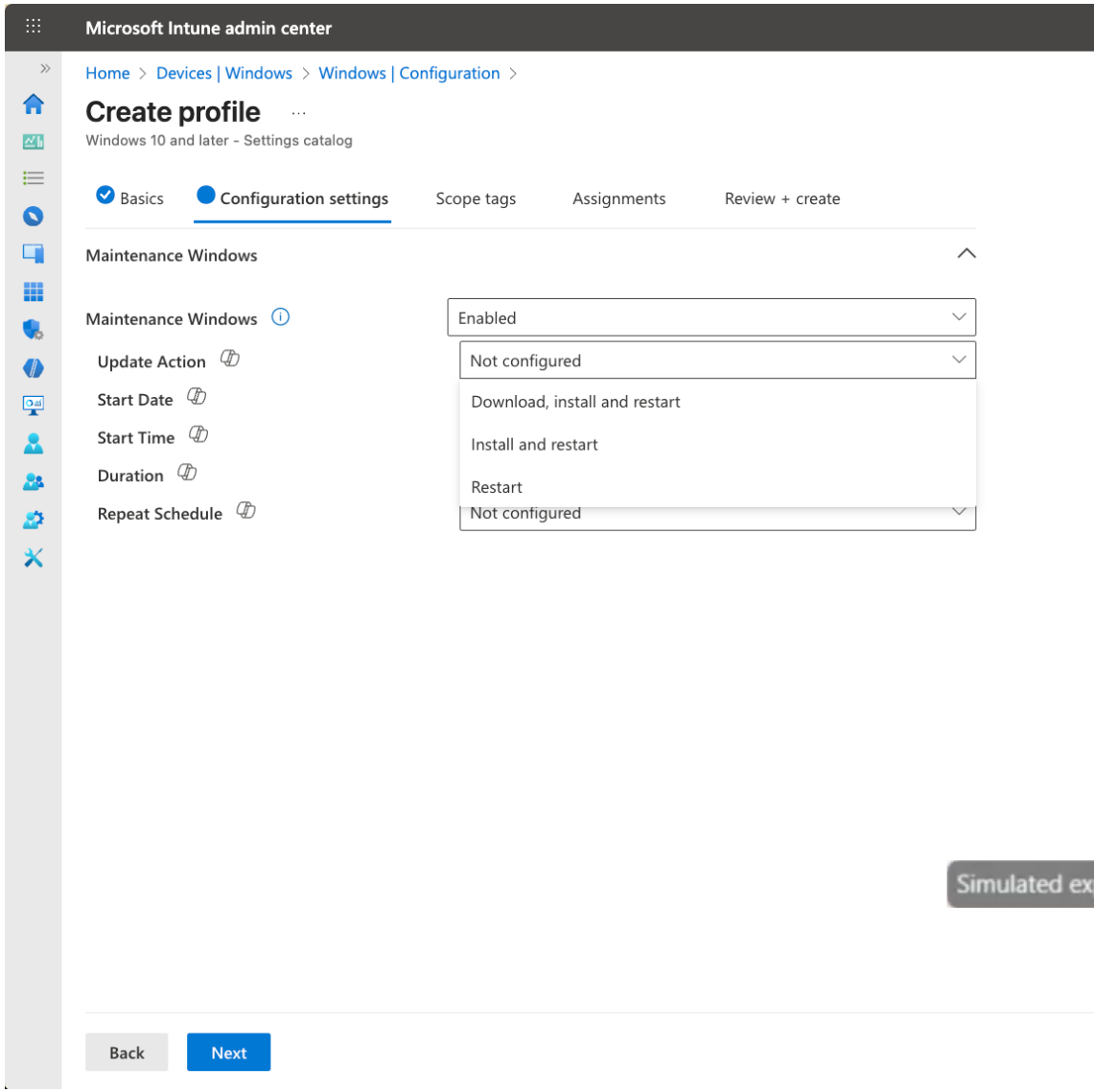
Configurable maintenance windows
•Define allowed time slots when updates can install and reboot.
•Reduces unexpected downtime and minimizes workflow interruptions.

Applies to cloud-managed Windows devices
•Ideal for frontline workers, shift-based environments, and devices with strict availability requirements.
•Ensures updates happen at the right time without manual intervention.

Supports phased rollout strategies
•Combine with new Intune *Deployments* to control both *when* and *who* receives updates.
•Enables precise change-management workflows.

Better compliance outcomes
•Devices update more consistently, improving patch currency and reducing exposure windows.
•Less reliance on users to keep devices online at the right moments.

Preview timeline
•Feature expected to enter preview in **H1 2026**.



Windows enhancements

- Sysmon functionality in Windows (coming soon)
- Hardware accelerated BitLocker
- Zero Trust DNS
- Passkey sync
- Wi-Fi 7 support for Enterprises (WPA3)
- Passkey manager integration with (Microsoft Password Manager, 1Password and Bitwarden

Sysinternals/
Sysmon

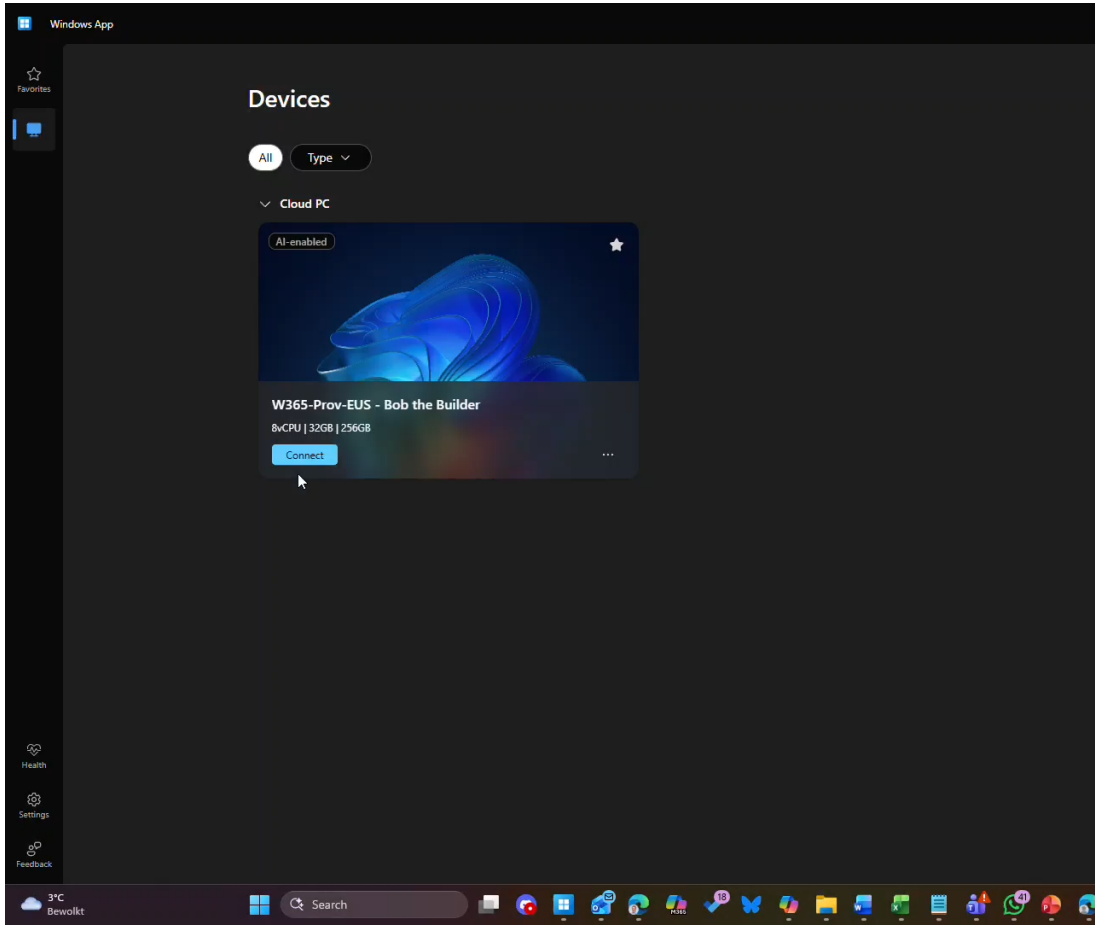
Windows 365

Windows 365 and AI

- Windows 365: AI-enabled Cloud PCs and Windows 365 Link device updates.

Windows 365 enhancements

- Support for external identities
- Windows 365 Reserve
- Windows 365 Cloud Apps
- User Experience Sync (UES) now generally available
- Windows Cloud Keyboard Input Protection now in preview



Windows App

https://windows.cloud.microsoft/#/devices

Windows App

Favorites

Devices

All

Type

A-Z

Cloud PC

W365-Provisioning - Peter Daalmans

8vCPU | 32GB | 512GB

Connect

Feedback

Download

3°C
Bewolkt

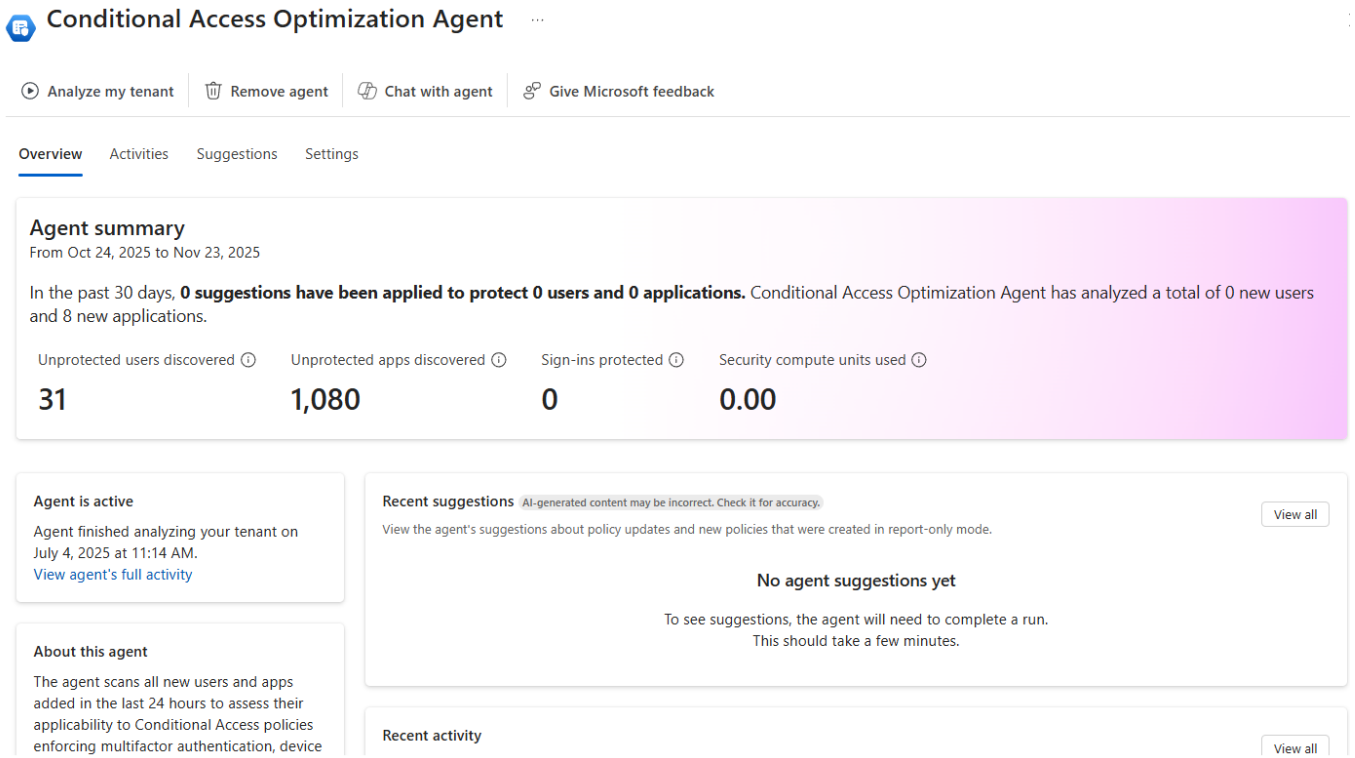
Search

14:57
23-11-2025

Identity

Identity

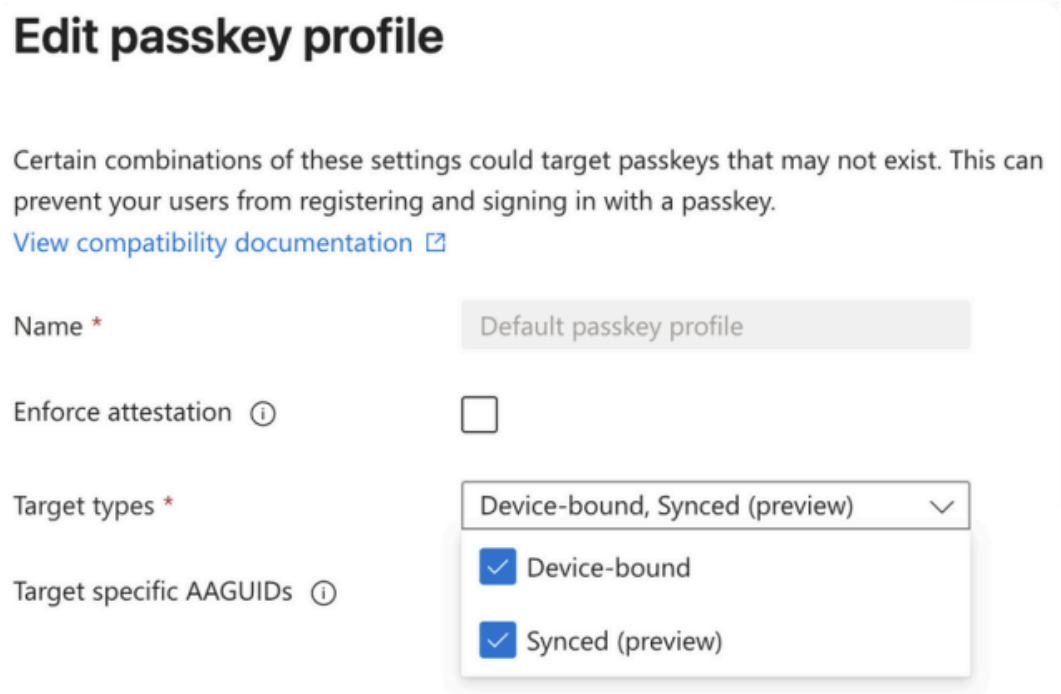
- Microsoft Entra: Entra Agent ID for secure AI agent identity management.
- New AI-powered agents for conditional access and identity risk.
  - Conditional Access Optimization Agent
  - Access Review Agent
  - Risk Management Agent (coming soon)
  - Application Lifecycle Management Agent (coming soon)
- Expanded passwordless authentication and secure self-service recovery. (Verfified ID)



Synced Passkeys

Entra ID

- Support for synced passkeys from Apple, Google and other third-party providers, and passkey profiles for easier management.

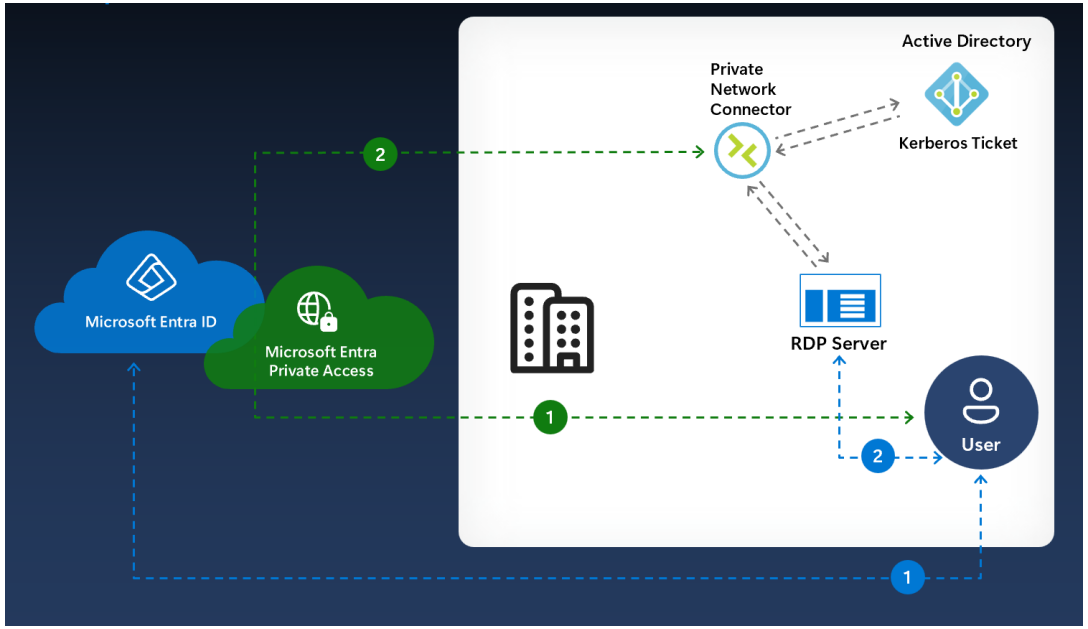


Microsoft Entra ID

Conditional Access for Agents

Global Secure Access

- **Private Access**
  - Assign traffic profile to remote network (Updated)
  - Create remote networks (Updated)
  - Manage remote networks (Updated)
  - Enable Intelligent Local Access



- **Internet Access**
  - Real-time protection against prompt injection attacks across all generative AI apps — sanctioned, unsanctioned or custom.
  - Expanded visibility into network traffic to uncover unsanctioned AI usage, including custom apps.
  - Integration of network file filtering with Microsoft Purview to discover and block sensitive content in files sent to generative AI and software-as-a-service (SaaS) apps.

MCP Server for Enterprise (Preview)

- https://mcp.svc.cloud.microsoft/enterprise

Licenses

License Changes

New capabilities coming in 2026	Business Basic	Business Standard	Business Premium	Office 365 E1	Office 365 E3	Microsoft 365 E3	Microsoft 365 E5
	Lightweight web and mobile apps to kickstart your business.	Powerful web, mobile, and desktop apps to run your business.	Everything your business needs to be more productive and secure.	Lightweight web and mobile apps, and basic security.	Powerful productivity apps, basic security, and identity management capabilities.	Powerful Productivity apps with enhanced security and compliance capabilities.	Best-in-class AI-powered productivity apps with advanced security, compliance, analytics, and AI readiness capabilities.
Copilot Chat enhancements	●	●	●	●	●	●	●
Security, management, and analytics for Copilot Chat	●	●	●	●	●	●	●
URL checks in Outlook and Office apps (web and mobile)	●	●		●			
+50 GB email storage	●	●	●				
Microsoft Defender For Office P1					●	●	
Microsoft Intune Remote Help						●	●
Microsoft Intune Advanced Analytics						●	●
Microsoft Intune P2						●	●
Intune Endpoint Privilege Management							●
Intune Enterprise Application Management							●
Microsoft Cloud PKI							●
Microsoft Security Copilot							●

Thank You