



Microsoft Ignite 2025

Annoucements





Thank you Sponsors



Gold



RECAST SOFTWARE

Silver



Secure At Work

Technical Partners



Book of news

The screenshot shows the Microsoft Book of News website. At the top, there's a navigation bar with the Microsoft logo, a search bar, and a cart icon. Below the navigation is a dark purple header with a lightbulb icon and binary code. On the right side of the header are buttons for 'Table of Contents', 'Download Visual Assets', and language selection ('English'). The main content area features a dark background with three people: a man in a beanie, a woman in a striped shirt, and a woman in a dark sweater looking at a smartphone. A 'Journalist' dropdown menu is open above them. A text overlay says, 'These summaries were generated with the help of AI and may be incorrect. Please refer to the original BoN item for full details.' A 'Scroll to read' button is visible at the bottom left. The bottom portion of the page has a white background with the text 'MICROSOFT IGNITE BOOK OF NEWS November 18 - 21, 2025' and the title 'Microsoft Ignite 2025 Book of News' at the very bottom.

MICROSOFT IGNITE

BOOK OF NEWS

November 18 - 21, 2025

[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.

The screenshot shows the Microsoft Copilot Studio interface. At the top, there's a search bar with the placeholder "Describe your agent to create it" and three buttons: "Helpdesk", "Expense tracking", and "HR and benefits". Below the search bar, there's a text input field with the placeholder "Use everyday words to describe what your agent should do". A note below the input says "Features labeled as 'preview' are subject to supplemental terms. [See terms](#)".

The main area is titled "Explore agents" and contains a grid of six cards:

- Website Q&A** (Agent template): Instantly answer user questions using the content of your website or other knowledge.
- Voice** (Agent template): An agent with voice capabilities.
- Safe Travels** (Agent template): Provides answers to common travel questions and related health and safety guidelines.
- Benefits** (Agent template): Benefits Agent provides personalized information on various benefits offered by the employer that are tailored to employee's unique circumstances.
- IT Helpdesk** (Agent template): Empowers employees to resolve issues and effortlessly create/view support tickets.
- Financial Insights** (Agent template): Help financial services professionals get quick and concise info from their org's financial documents and other available resources.

Below the agent cards, there's a section titled "Learning resources" with several cards:

- Free Copilot Studio Workshop**
- Getting started with Copilot Studio**
- Quick start: Create and deploy an agent**
- Documentation**
- Security and Governance**
- Responsible AI FAQs**
- Quick start: Use Generative AI in an agent**
- Support community**
- Coming soon: See release plans**
- What's new: See release notes**
- Agent Message Consumption Estimator**



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.

Home > Endpoint security | Conditional access > Conditional Access | Policies >

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
[Learn more ↗](#)

Name *

Example: 'Device compliance app policy'

Assignments

Users, agents or workload identities ⓘ

Specific agents (Preview) included

✖ "Select agents" must be configured

Target resources ⓘ

No target resources selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

Block access

Block access

Grant ⓘ

Block access

Grant ⓘ

Control access based on who the policy will apply to, such as users and groups, agents, workload identities, directory roles, or external guests.
[Learn more ↗](#)

What does this policy apply to?

Agents (Preview) ▾

Include Exclude

None

All agent identities (Preview) ⓘ

Select agents

Select agents acting as users ⓘ

None

Select agent identities based on attributes ⓘ

None

Select individual agent identities

None



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)

[Enable Dark mode](#)

- Home
- Copilot
- Agents
- Users
- Devices
- Teams & groups
- Marketplace
- Billing
- Setup

- Customize navigation
- Show all

Baseline security mode

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](#)[Report settings](#)

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.

Settings > Endpoints

Endpoints

General

Advanced features

Licenses

Email notifications

Auto remediation

Permissions

Roles

Device groups

Rules

Alert suppression

Indicators

Custom Data Collection

AMSI - Collect All

Edit Delete

AMSI - Collect All

General information

Create rule

Define rule scope

Review and finish

Define rule scope

You can set the custom collection rule to collect data from specific device groups only.

Custom collection only applies to Windows devices.

Select devices to collect data from *

All applicable client devices

Devices with specific tags

FileCreation ... Enabled DeviceFileEvents FileCr...

ImageLoad Enabled DeviceImageLo... Image...

ProcessCreat... Enabled DeviceProcessE... Proce...

Organization

Created on

9 Dec 2025 21:10:56

Last updated

9 Dec 2025 21:27:41



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.

The screenshot displays the Microsoft Sentinel platform interface. On the left, a sidebar shows navigation options like Home, Dashboards, and Incidents. The main area is titled "Incidents > Malicious AWS federated sign-in using a compromised Entra ID account (attack disruption)". A sub-tile for "ID 140020: Malicious AWS federated sign-in using a compromised Entra ID account (attack..." is shown, indicating it's a high-severity (red) active incident last updated on Aug 20, 2025 at 6:26:12 PM. It includes tabs for Attack story, Alerts (5), Activities (8), Assets (3), Evidence (2), Similar incident, and Summary. The "Attack story" tab is selected, showing a timeline of events:

- Aug 20, 2025 12:10:02 PM | Active Email messages removed after delivery by JonathanW to 'Zava Bonus'
- Aug 20, 2025 6:15:07 PM | Active Possible compromised user account sign-in by Jonathan Wolcott (IP: 218.107.132.66)
- Aug 20, 2025 6:22:32 PM | Active Malicious AWS federated sign-in with compromised Entra ID account by JonathanW (IP: 218.107.132.66)
- Aug 20, 2025 6:26:12 PM | Active Malicious AWS IAM user backdoor account (IP: db_backup_job)

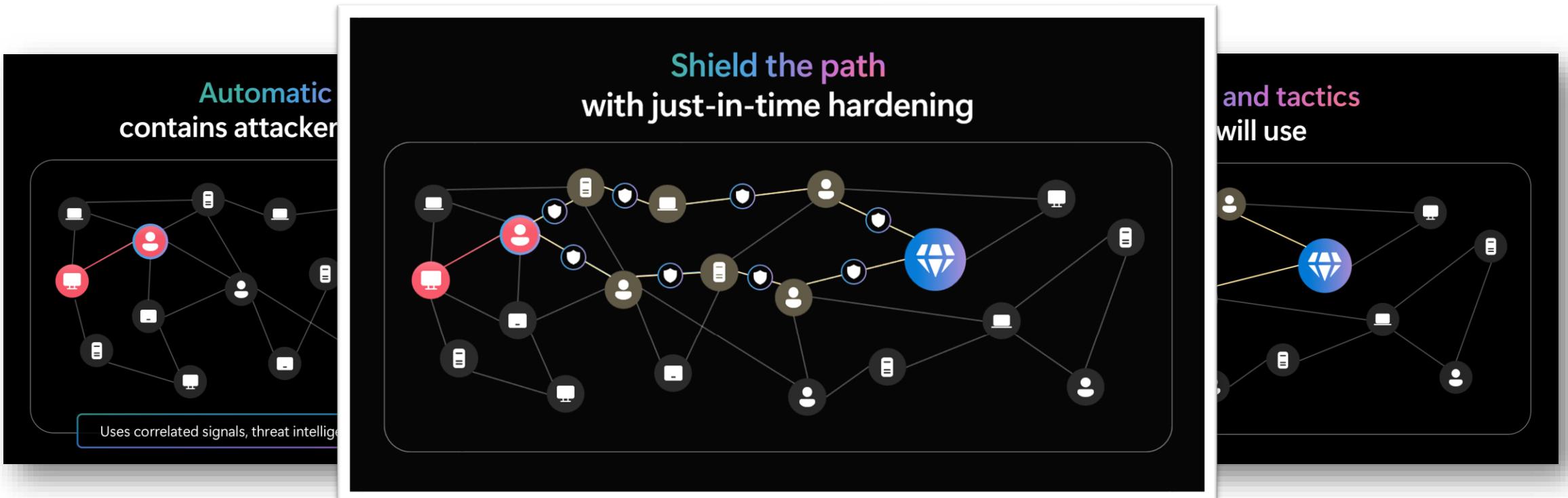
Below the timeline is an "Incident graph" showing relationships between entities. Entities include "Zava Bonus" (Email icon), "JonathanW@zava.com" (User icon), "Jonathan Wolcott" (User icon labeled "Disabled"), "AWSAdminRole" (Role icon labeled "Session revoked"), and "db_backup_job" (Job icon labeled "Disabled"). Associations show links between these entities, such as "Email messages removed after delivery" and "Malicious AWS federated sign-in".

On the right, there are two panels: "Tasks" and "Summary". The "Tasks" panel shows a list of tasks with 0 completed. The "Summary" panel contains an "Incident summary" section with details about the attack and its prevention, and an "Attack Disruption" section indicating an automated response took place.



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**

The screenshot displays the Microsoft Defender portal interface, specifically the 'Defender for Cloud' section. On the left, a sidebar menu lists various security features: Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, and Cloud security. The 'Cloud security' option is currently selected, showing an 'Overview' section with a progress bar at 50% and a '7 critical recommendations' link. The main content area is titled 'Defender for Cloud' and describes it as 'Protects your cloud-native workloads from code to runtime.' It shows a 'Cloud secure score (preview)' of 100%, a 'Security posture' of 'Cloud secure score (preview) Moderate', and a 'Threat detection' section with 'Security alerts'. Below these are tabs for 'Cloud Inventory' (selected), 'All Assets', 'VMs', 'Data', 'Containers', 'AI', 'API', 'DevOps', 'Identity', and 'Serverless'. The 'Cloud Inventory' tab shows a total of 529 assets, with 8 critical assets. A chart indicates 'Defender coverage' status: Covered (green), Partially Covered (orange), and Not Covered (grey). A table below lists assets with columns for Name, Asset type, Asset label, Environment, Criticality level, Defender coverage, Recommendations, and Alerts. Examples include 'dfc-lab-20-contextual-security-mys3bucket-rby0m8ng...', 'e0980d89-1d0c-42da-baad-c51270cce4d3', and 'kv-wus-fabrikam'.



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.

The screenshot displays the Microsoft Threat Hunting Agent interface, which integrates advanced hunting, security copilot, and results visualization.

Advanced hunting: On the left, a sidebar lists various log sources under "Schema". The main area shows a query editor with the following code:

```
71 ) on UserPrincipalName
72 | project
73     TimeGenerated,
74     Id,
75     Description,
76     Score
```

Below the query editor, the "Results" tab is selected, showing a summary by Copilot. Observations include:

- High-score anomalies (0.7) concentrated on August 1st; sporadic anomalies scored low.
- Logon originated from Burien, United States, using IP 107.189.30.22.
- Anomalies include uncommon actions, apps, and resources accessed.

A line chart titled "Results visualization" shows event counts over time, with a sharp spike on August 1st.

Security Copilot: On the right, the "Selected workspace: Zava" section displays:

- Detected behaviors included:**
 - Action uncommonly performed by the user
 - App uncommonly used by the user
 - Resource uncommonly accessed
 - Uncommon high volume of actions
 - Country uncommonly connected from
- Insights:** The IP address 107.189.30.22 was used in anomalous sign-ins associated with a public DNS service.
- Recommended actions:** "Disable user 'cloud_sync_user'".
- Threat Hunting Agent:** A button to "Apply in Take Actions wizard".



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.

The screenshot shows the Microsoft Defender portal interface. On the left is a navigation sidebar with sections like Investigation & response, Threat intelligence (selected), Assets, Microsoft Sentinel, Identities, and Endpoints. The main area is titled "Threat analytics". It features a "Executive summary by Threat Intelligence Briefing Agent" card with stats: Active (388), Actor (267), Core threat (13), Technique (44), Tool (126), and Vulnerability (161). Below this are sections for "Latest threats" and "High-impact threats", each with a grid of threat profiles. At the bottom is a search bar and filter options. To the right, a modal window titled "TI Briefing: Oct 30, 2025 10:02 AM" displays the "Executive Summary" for Storm-2581, detailing its operations and impact across various sectors. The modal also includes a "Manage agent" button and a note about AI-generated content.



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.

The screenshot displays the Microsoft Defender Zava interface. At the top, it shows an incident titled "ID 140020: Malicious AWS federated sign-in using a compromised Entra ID account (attack disruption)". The left sidebar contains navigation icons and a search bar. The main area features an "Incident graph" showing connections between entities: "Zava Bonus", "JonathanW@zava.com", "Jonathan Wolcott", "db.backup.job", "AWSAdministratorRole", and "218.107.132.66". Below the graph, the "Alerts" section lists several incidents, including "Suspicious Connected Apps Reconnaissance Activity" and "Malicious AWS federated sign-in with compromised Entra ID account". A detailed "Alert description" for the reconnaissance activity is shown, stating: "Unusual enumeration or metadata access activity targeting federated or OAuth-connected applications has been detected. Such activity may indicate an attacker attempting to discover integrated services or identity trust relationships—such as AWS, Salesforce, or Google—that rely on the organization's identity provider." The "Recommended actions" section provides links for further investigation. On the right side, there are sections for "Suspicious Connected Apps Reconnaissance Activity", "Alert State", "Classification", "Alert Details", and "Generated on".



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.

The screenshot shows the Microsoft Sentinel interface with a central modal dialog titled "Let's set up your new SIEM". The dialog contains two main options: "Migrate from your current SIEM" and "Start from scratch (Coming soon)". The "Migrate from your current SIEM" option includes a sub-instruction: "Upload configuration data from your current SIEM to identify the connectors and detections you need." Below the dialog, the main workspace shows a summary of "SIEM setup (22)" items, with 57 Active, 15 Completed, and 0 In progress items. A progress bar indicates the status of the migration process. The sidebar on the left lists various navigation options like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Endpoints, Email & collaboration, Cases, Reports, Learning hub, Trials, More resources, System, and Customize navigation.



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.

The screenshot shows the Microsoft Sentinel interface. On the left, there's a navigation bar with 'Microsoft Defender' at the top, followed by 'Exposure management', 'Investigation & response', and 'Threat intelligence'. The main area is titled 'Tables' with a sub-section 'Manage DeviceProcessEvents'. It shows 'Number of tables 15' and 'Analytics tier 6'. A message box says: 'After Microsoft Sentinel data lake is set up, data added to this table will also be stored in the data lake. To access data archived prior to the setup, use search and restore. Learn more about data retention.' Below this, a large callout box says 'Keep the right data ready' with the sub-instruction 'Use new storage and retention options to stay compliant and ensure data is accessible.' and a 'Manage tables' button. At the bottom, there's a list of data sources: 'Endpoints', 'Email & collaboration', 'Cloud apps', 'Cloud security', 'DeviceLogonEvents' (Data lake), 'DeviceImageLoadEvents' (Analytics), 'DeviceEvents' (Data lake), 'DeviceFileCertificateInfo' (Data lake), and 'DeviceTvmSoftwareVulnerabilities' (Analytics). There are 'Save' and 'Cancel' buttons at the bottom right.

Your Sentinel data lake is ready

It's time to connect all your security data and explore new, powerful capabilities. As your data grows, we'll build graphs that enable visual investigations and smarter AI agents.

Keep the right data ready

Use new storage and retention options to stay compliant and ensure data is accessible.

Manage tables

Endpoints
Email & collaboration
Cloud apps
Cloud security
DeviceLogonEvents Data lake
DeviceImageLoadEvents Analytics
DeviceEvents Data lake
DeviceFileCertificateInfo Data lake
DeviceTvmSoftwareVulnerabilities Analytics

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.

The screenshot shows the Microsoft Intune admin center interface. On the left, there's a navigation sidebar with links like Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main area is titled "Tenant admin | Admin tasks (preview)" and displays a list of tasks. The tasks are listed in a table with columns for Task, Source, and Status. Some tasks shown include "This is a lovely script", "MAA for Scripts", "DCL-VM01", "cmd.exe", "Update Adobe Acrobat Reader Dc", "Update Citrix Workspace", and "Update Chrome". The status column includes icons for Multi admin approval, Endpoint privilege management approval, Defender security task, and various status indicators like Needs Attention, Compliant, Active, and Pending.

Task	Source	Status
This is a lovely script	Multi admin approval	Needs Attention
MAA for Scripts	Multi admin approval	Compliant
DCL-VM01	Multi admin approval	Needs Attention
cmd.exe	Endpoint privilege management approval	Expired
Update Adobe Acrobat Reader Dc	Defender security task	Active
Update Citrix Workspace	Defender security task	Active
Update Chrome	Defender security task	Pending



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.

The screenshot shows the Microsoft Intune admin center dashboard. On the left, there's a sidebar with navigation links: Home, Dashboard, All services, Explorer, Devices, Apps, Endpoint security, Agents, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. A 'Hide text labels' button is visible above the sidebar. The main area has a dark background with a central banner for 'Daalmans Consulting B.V.' It displays a warning about updating firewall configurations. Below the banner, the text 'Securely manage devices, access, and apps with Intune' is shown, along with a subtext: 'Maximize productivity and simplify administration without compromising endpoint management and security.' To the right, there's a 'Status' section with four items: 'Devices not in compliance' (7), 'Configuration policies with errors or conflict' (10), 'Client app install failures' (7), and 'Connector errors' (1). The status for 'Service health' is listed as 'Healthy' and 'Account status' as 'Active'. On the far right, there are sections for 'Spotlight' (with a preview of 'The unified s... Help, Endpoint AI-powered more.'), 'Explore' (with a preview of 'Explore'), and a 'The unified s... Help, Endpoint AI-powered more.' icon.

Status	Value	Status	
Devices not in compliance	7	Connector errors	1
Configuration policies with errors or conflict	10	Service health	Healthy
Client app install failures	7	Account status	Active



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.

Microsoft Intune admin center

Home > Create a deployment

Basics Deployment schedule Scope tags Review + create

Name: Customer-Svc-Win32-update-v2
Description: Contoso Retail Store Customer service Win32 app refresh v2. Ops approved safe-controlled 3 ring retail-store rollout plan.
Platform: Managed devices (Windows 10 and later)

Excluded groups: Retail-LT-mgrs (Not applicable), Corp-IT-DogFood-Devices (None), Retail-StoreLab-Devices (None), Retail-Insider-Devices (None), North-Region-BackOffice (None), South-Region-FrontOffice (None)

Deployment schedule:

- Ring 0 - Canary: Start: 11/17/25 at 00:00:00am
- Ring 1 - Low-Impact Regions: Start date: 11/25/25 at 00:00:00am

Previous Create



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

A screenshot of the Microsoft Intune Admin Center interface. The main title is "Devices | Windows recovery". Below it, there are several sections: "Overview" (with tabs for "Recovery devices", "Remediation scripts", "Bare metal recovery", and "Configuration"), "Windows recovery" (described as "Manage Windows recovery and remediation policies and settings"), "Recovery device status" (Current: 100, Recent recovery mode: 1), and "Remediation action status" (Successful: 100, Pending: 0, Failed: 100, Not started: 100). There are also "Monitoring reports" (Connection Quality Report) and "Resource performance" sections.

More information: [Windows Recovery and Remediation for Quick Machine Recovery](#)

Simulated experience. Actual product performance may vary.



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.

The screenshot shows the Microsoft Intune admin center interface. The left sidebar has a 'Endpoint security' section with 'Endpoint Privilege Management' selected. The main content area is titled 'Endpoint security | Endpoint Privilege Management'. It features a '48-hour snapshot' section with statistics: '365 users have only unmanaged elevations' and '1637 users have both managed and unmanaged elevations'. Below this is a 'Files to watch' section with tables for 'Frequently unmanaged elevations' and 'Frequently approved by support'.

File	Elevations
cmd.exe	11410
control.exe	11891
powershell.exe	7895

File	Elevations
cmd.exe	11410
control.exe	11891
powershell.exe	7895



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**.

Microsoft Intune admin center

Home > Devices | Windows > Windows | Configuration >

Create profile

Windows 10 and later - Settings catalog

Basics Configuration settings Scope tags Assignments Review + create

Maintenance Windows

Maintenance Windows

Update Action

Start Date

Start Time

Duration

Repeat Schedule

Enabled

Not configured

Download, install and restart

Install and restart

Restart

Not configured

Simulated ex...

Back Next



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





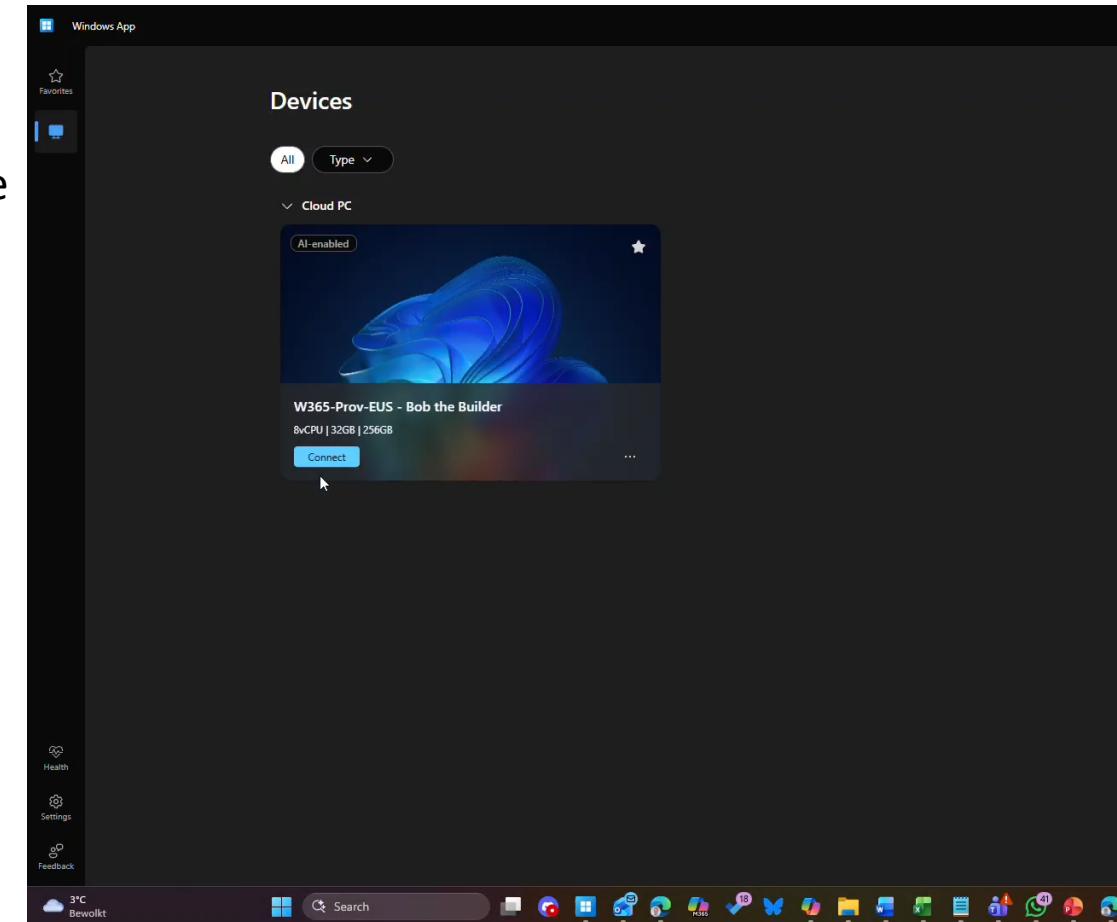
Windows 365

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

18 M365 40 P

14:57 23-11-2025

The screenshot shows the Windows App interface with a dark theme. At the top, there's a navigation bar with icons for back, forward, home, and search, along with a URL bar showing the address https://windows.cloud.microsoft/#/devices. Below the navigation bar is a header with the title "Windows App" and a user profile icon. On the left side, there's a sidebar with sections for "Favorites" and "Devices". The main area is titled "Devices" and contains a list of devices. The first item in the list is a card for a "Cloud PC" named "W365-Provisioning - Peter Daalmans". The card features a blue background with abstract white shapes, a star icon in the top right corner, and the device details: "8vCPU | 32GB | 512GB". It includes a "Connect" button and a dropdown menu icon. At the bottom of the screen, there's a taskbar with various pinned icons, including the Start button, File Explorer, and several Microsoft Office applications. The system tray at the bottom right shows the date and time (14:57, 23-11-2025) and weather information (3°C, Bewolkt).

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. (Verified ID)

Conditional Access Optimization Agent

Analyze my tenant Remove agent Chat with agent Give Microsoft feedback

Overview Activities Suggestions Settings

Agent summary
From Oct 24, 2025 to Nov 23, 2025

In the past 30 days, 0 suggestions have been applied to protect 0 users and 0 applications. Conditional Access Optimization Agent has analyzed a total of 0 new users and 8 new applications.

Unprotected users discovered 31 Unprotected apps discovered 1,080 Sign-ins protected 0 Security compute units used 0.00

Agent is active
Agent finished analyzing your tenant on July 4, 2025 at 11:14 AM.
[View agent's full activity](#)

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.

No agent suggestions yet
To see suggestions, the agent will need to complete a run.
This should take a few minutes.

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

Recent activity



Synced Passkeys

Entra ID

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

Edit passkey profile

Certain combinations of these settings could target passkeys that may not exist. This can prevent your users from registering and signing in with a passkey.

[View compatibility documentation](#)

Name *

Default passkey profile

Enforce attestation ⓘ

Target types *

Device-bound, Synced (preview)

Device-bound

Synced (preview)



**Microsoft
Entra ID**



Conditional Access for Agents





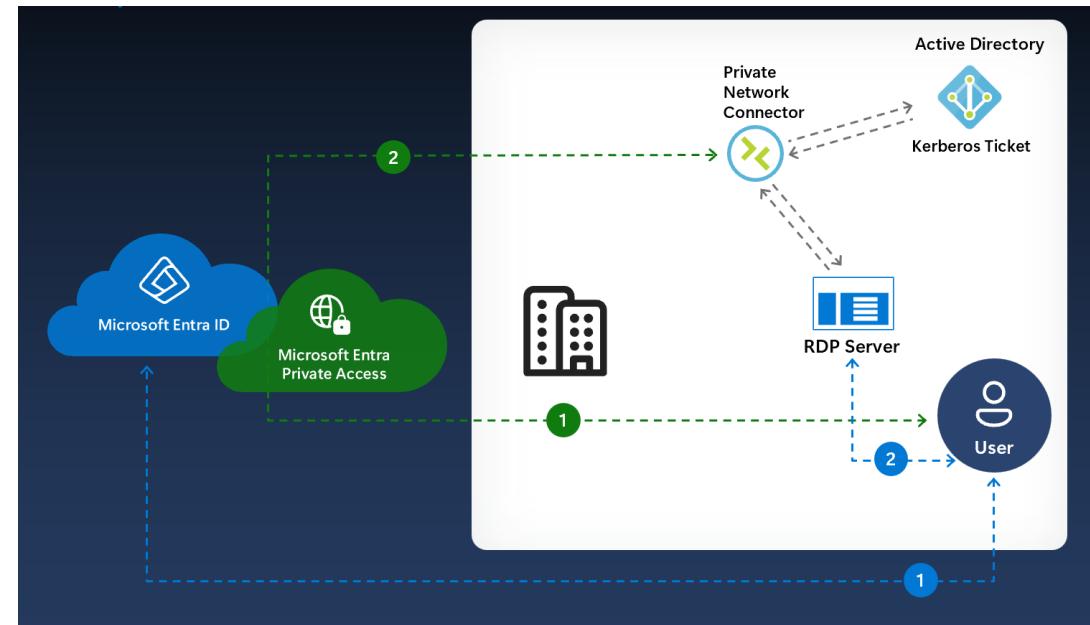
Global Secure Access

- **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
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

