Security Conversations that Matter:
Microsoft Intune integrated endpoint security and Copilot in Intune

Eugenie Burrage, Director – Product Marketing
Catarina Rodrigues, Product Manager

Eugenie Burrage
Redmond, WA, USA

Director – Intune Product Marketing

Intune Business Group - Product Strategy

Microsoft Intune Blog | Microsoft Community Hub

https://www.linkedin.com/in/eugeniedaoust

Music, mountains and the cabin on the lake

Catarina Rodrigues
Spain

Product Manager – Intune
Customer Experience

Copilot in Intune . FLW – Android/iOS

From the frontlines: Delivering critical early responder device management | Microsoft Community Hub

https://www.linkedin.com/in/catarinarodrigues3

Surf, ski, travel

Endpoint Management Is Security-Critical

The endpoint is now the security control plane

Endpoint management has moved from basic hygiene to the **control plane where security intent succeeds or fails**.

AI, agents, and Shadow AI push risk to the edge, where enforcement actually happens.

92%

of breaches now target unmanaged endpoints[1]

1. Microsoft Digital Defense Report 2024

80%

Of leaders cite leakage of sensitive data as a main concern of AI use[2]

2: Microsoft Security Whitepaper,

What “Good” Looks Like (Operationally)

Fewer risks • fewer fixes • fewer surprises

This is not about *adding more controls*. It is about **predictable, explainable outcomes at scale**

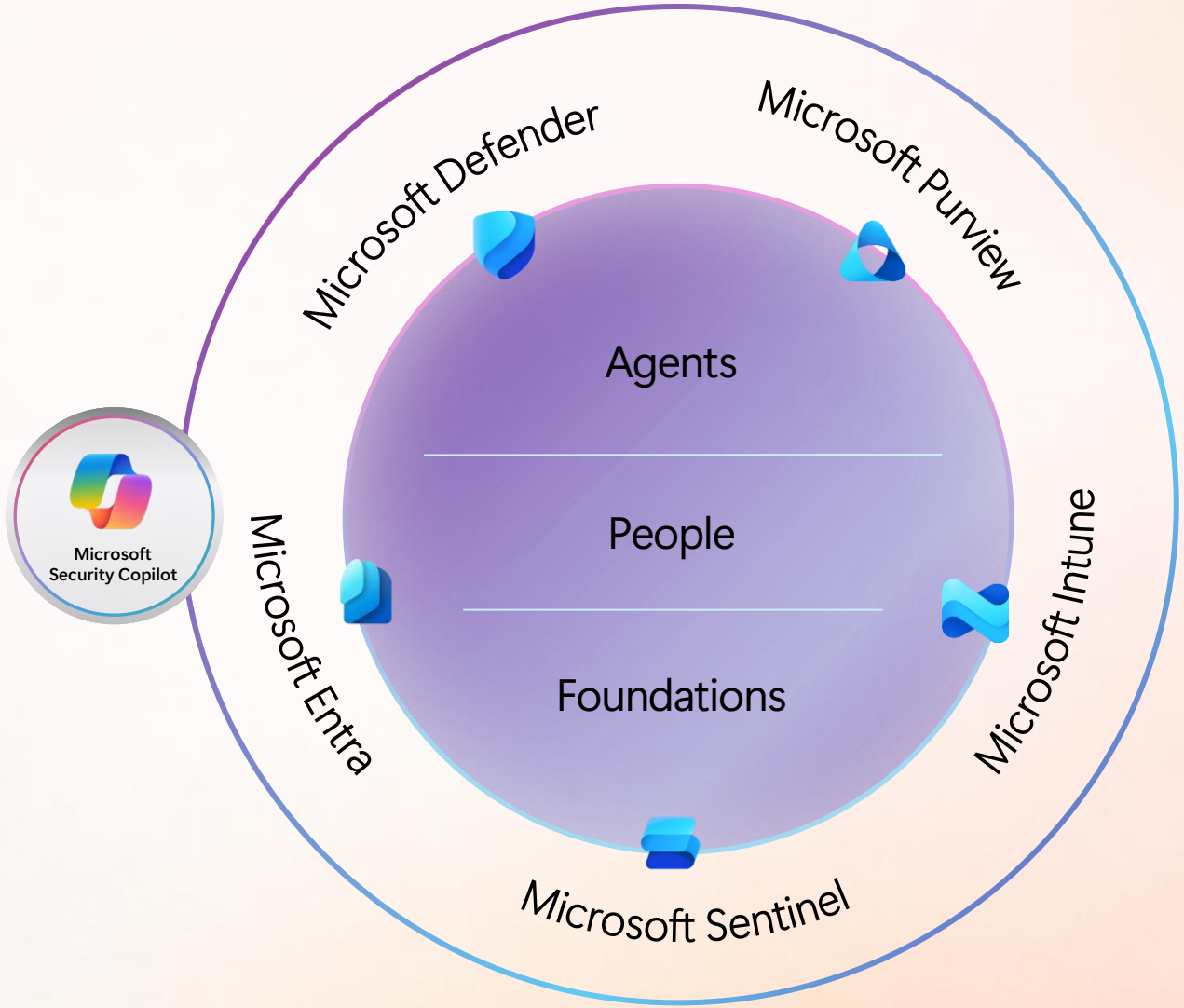
Secure by Design

Secure by Default

Secure Operations

Secure Future Initiative

Microsoft end-to-end security platform



Threat intelligence
100 trillion daily signals [1]

1.5 million customers[2]
Supported through services
Professional | Managed | Technical support

1 Based on Microsoft internal data. Accurate as of July 2025
2 3Microsoft FY25 Fourth Quarter Earnings Conference Call, Jonathan Neilson, Satya Nadella, Amy Hood. July 30, 2025

Eliminate the Top Sources of Risk

Focus on what's repeatable and preventable

Most endpoint risk comes from a small set of known failure modes.

Unknown risks

Lagging compliance and drift

Expanding attack surface

Agenda

Security conversations that matter

- Know your risks
- Reduce the attack surface
- Secure user experiences

Know Your Risks

Compliance is not a checkbox

Compliance as a Live Security Signal

Compliance is not a checkbox.
It is a signal that drives security outcomes.

1. **Explain every decision**
   IT can trace why access was allowed or blocked, eliminating guesswork and escalation.

2. **See risk in one place**
   Compliance context is unified in one place, so there is no portal hopping to piece together device posture.

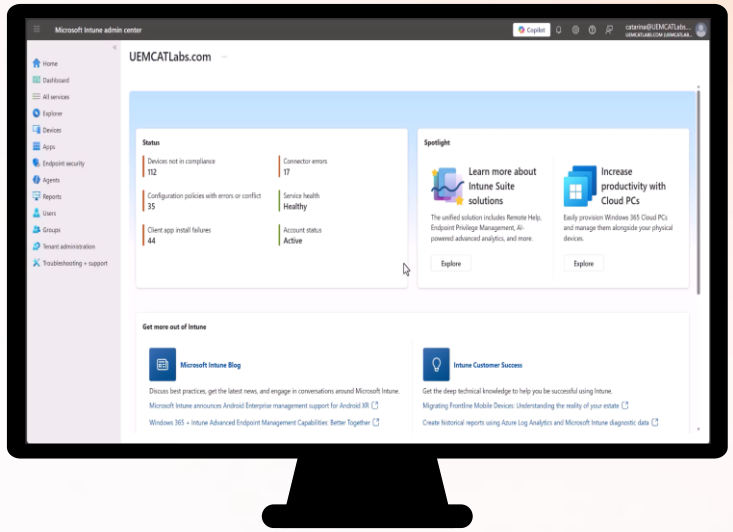
3. **Evaluate continuously**
   Frequent evaluation catches configuration drift at the point of action, not after the fact.

Up next: See Copilot surface device risk and compliance context ▶

Device compliance and risk

Copilot in Intune

Turn signals into explainable device risk.



Prevent Fixes Before They're Needed

Misconfiguration causes more damage than missing tools.

Today

- ✕ **Reactive cleanup**
  Fix misconfigurations after they cause incidents
- ✕ **Tribal knowledge**
  Policy intent lives in someone's head, not in a reviewable system

With Copilot in Intune

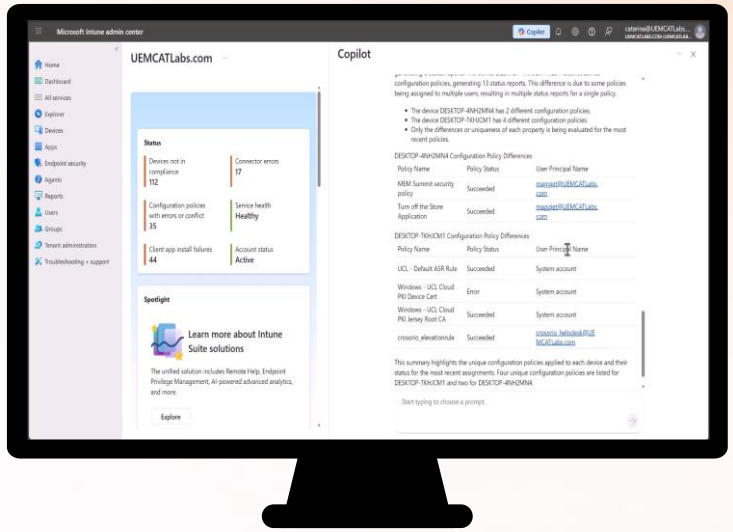
- ✓ **Guided configuration**
  Ask Copilot about policy intent, settings, and get proactive recommendations
- ✓ **Policy Configuration Agent**
  Reviews settings against frameworks like STIG at scale, making policy intent auditable and repeatable

Up next: See Copilot in Intune help you explore policy and settings ▶

Prevent misconfigurations

Copilot in Intune

From reactive cleanup to guided configuration



Compliance as a Security Foundation

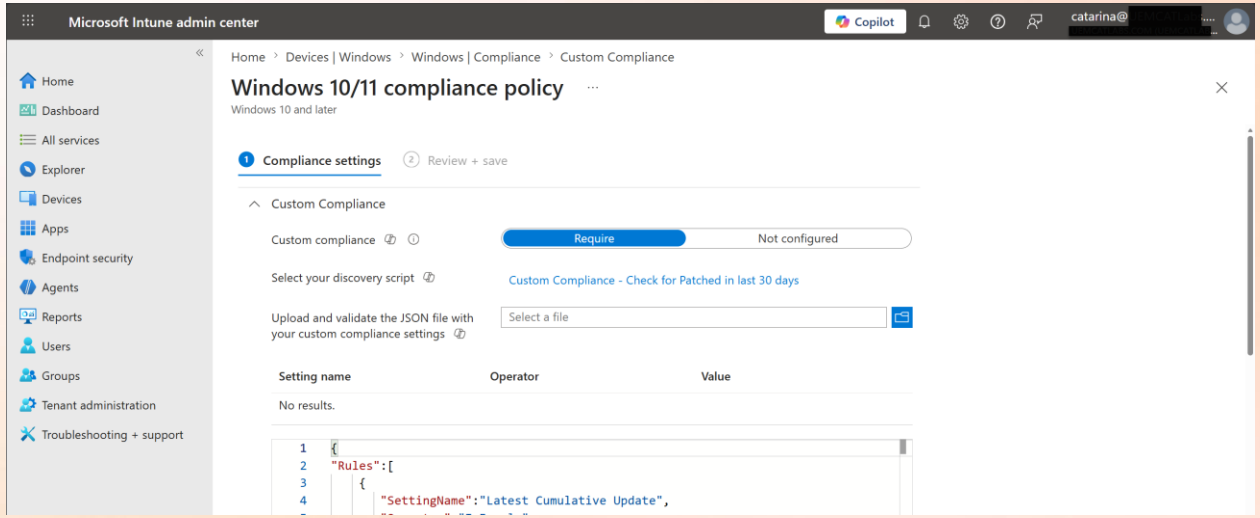
Why compliance matters

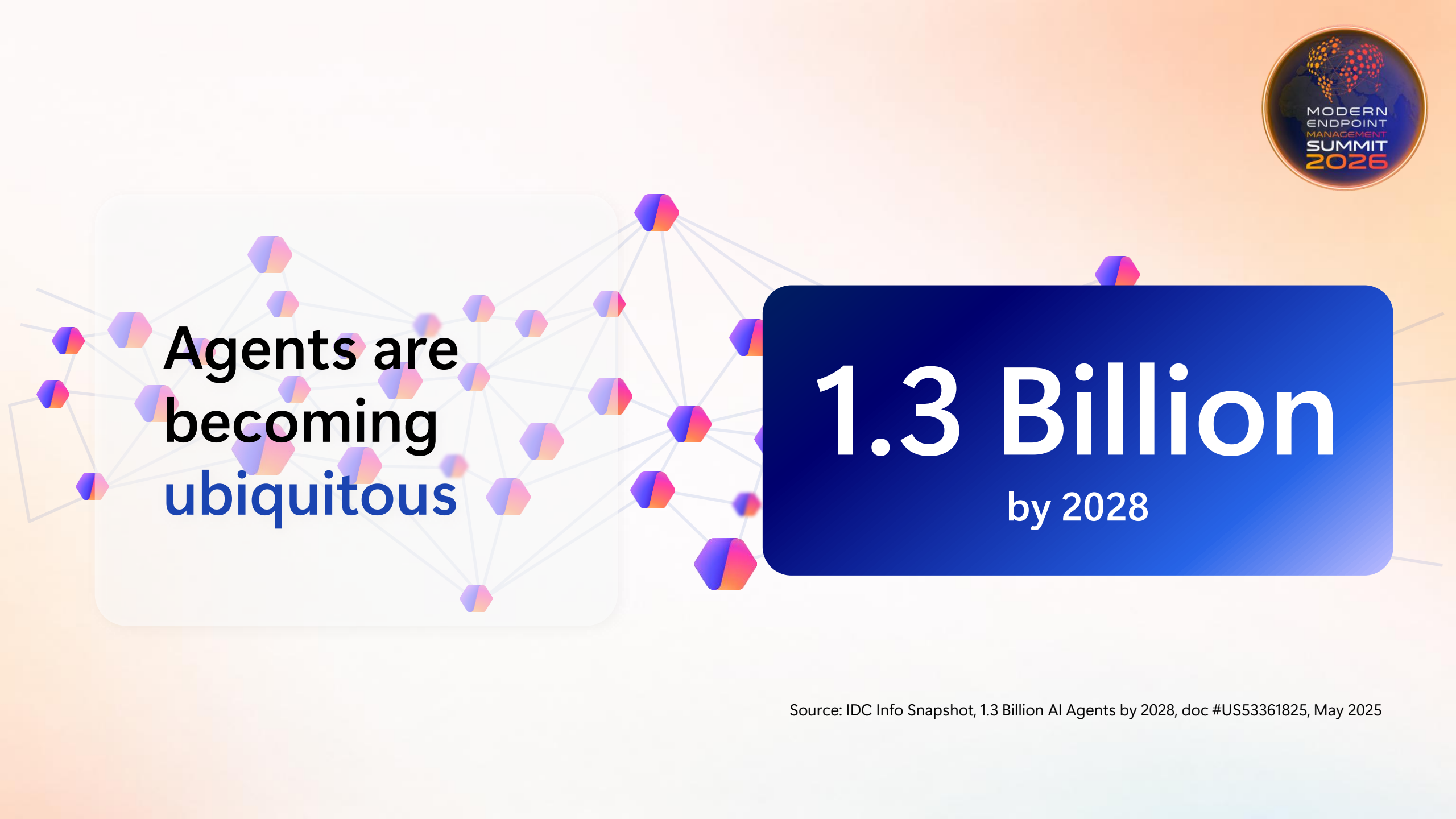
- Compliance validates that **security policies are enforced**, not just defined
- Non-compliant devices are the **most common entry point** for lateral movement and data exfiltration
- Continuous compliance evaluation provides **trust signals** that underpin Zero Trust access decisions

Custom compliance encodes your organization's real risk

- IT can encode **organization-specific risk** into enforceable compliance signals
- Custom compliance is a **Conditional Access signal,** driving real access decisions, not just audit reports

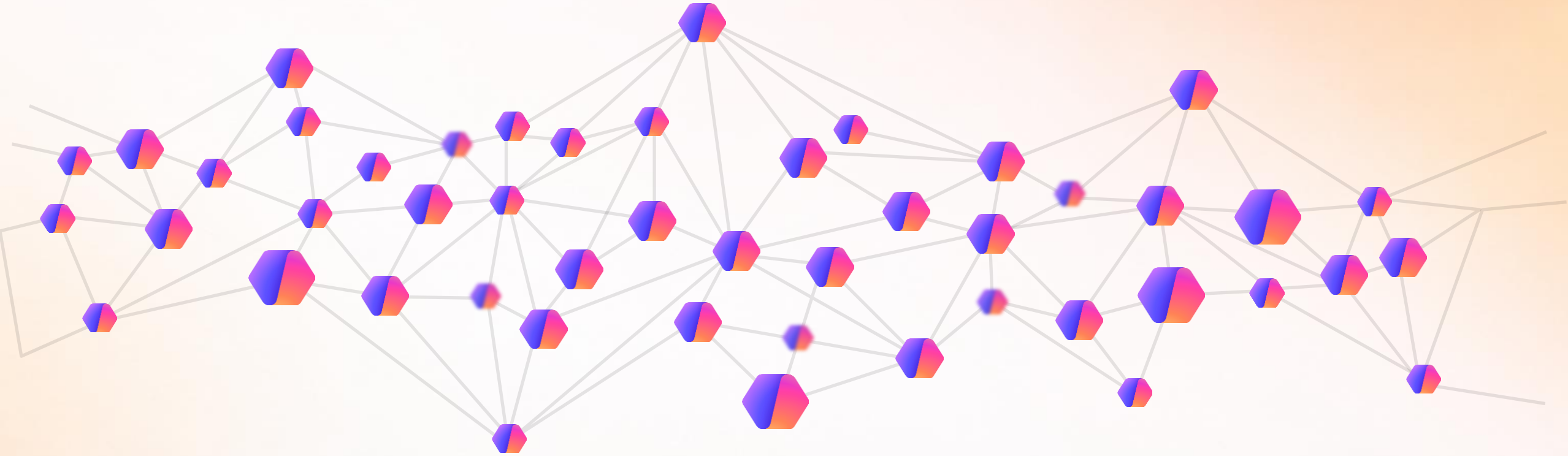
Available today on Windows; coming soon to macOS





Source: IDC Info Snapshot, 1.3 Billion AI Agents by 2028, doc #US53361825, May 2025

Is your organization ready?



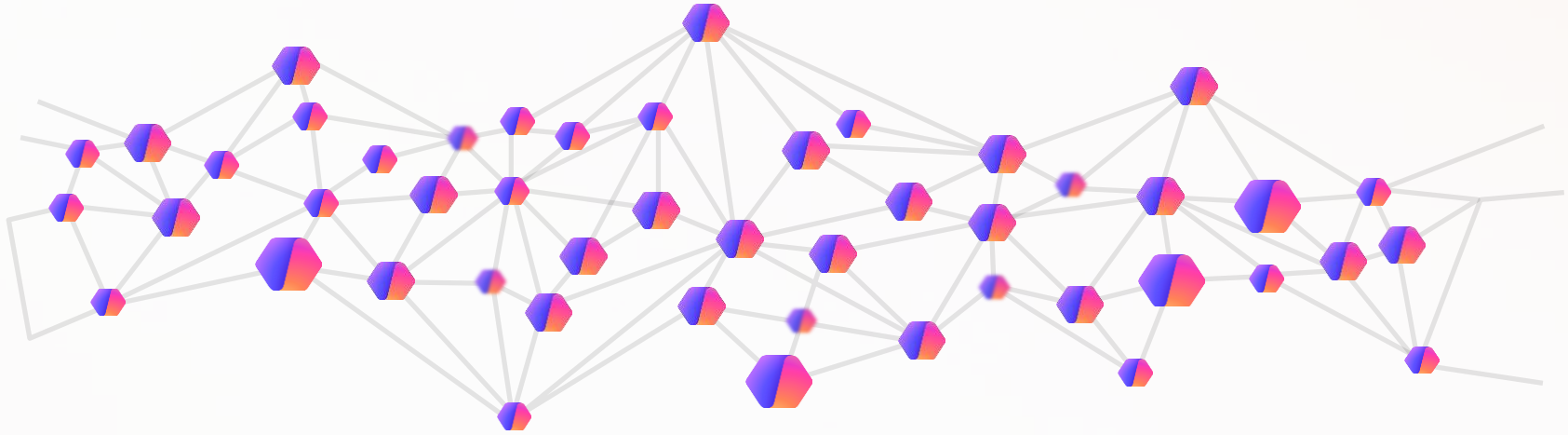
Can we track and monitor all agents? Do we know what agents are doing?

Do we have proper guardrails for agents and people that interact with them?

Are agents protected? Do they have the right access? Can they leak sensitive data?

Microsoft Agent 365

The control plane for agents



Observe

Govern

Secure

Microsoft Agent 365

The control plane for agents

Observe

Monitor and manage agents in real time

- **Registry**: Register and track every agent
- **Mapping**: Visualize agent usage and behavior
- **Analytics**: Measure agent adoption, performance, and ROI
- **Role-specific oversight**: Extend agent visibility to security and business leaders

Govern

Establish guardrails for agents and users

- **Onboarding**: Bring agents under control from day one
- **Integration management**: Control what agents can access and do
- **Lifecycle management**: Automate agent lifecycle policies
- **Audit and logging**: Strengthen traceability and be audit ready
- **Data compliance**: Meet AI regulations and policies

Secure

Protect agents comprehensively

- **Access control**: Protect agent identities and access
- **Data security**: Prevent oversharing and data leaks
- **Threat protection**: Defend against threats and vulnerabilities

Comprehensive security for agents

The best way to manage agents is to extend infrastructure you use for managing users.

Microsoft 365 Admin Center

Centralized hub to manage users, apps, and settings securely across your Microsoft 365 environment.

Microsoft Defender

Extend comprehensive security posture and advanced threat protection to agents.

Microsoft Entra

Protect agent identities and secure their access to apps and resources.

Microsoft Purview

Manage, protect and govern data that agents use and create across your entire organization.

Microsoft Intune

Configure agent access from only compliant devices and manage policies to protect agent browser interactions.

Extend Zero Trust boundaries to agents

Agent 365 - the control plane for agents

Observe

Monitor and manage agents in real time

- App inventory
- Device inventory
- MDQ
- Explore with Copilot

Govern

Establish guardrails for agents and users

- App Control for Business
- CSPs
- Firewall rules

Secure

Protect agents comprehensively

- Require device compliance for Conditional Access
- Endpoint Privilege Management
- Security baselines

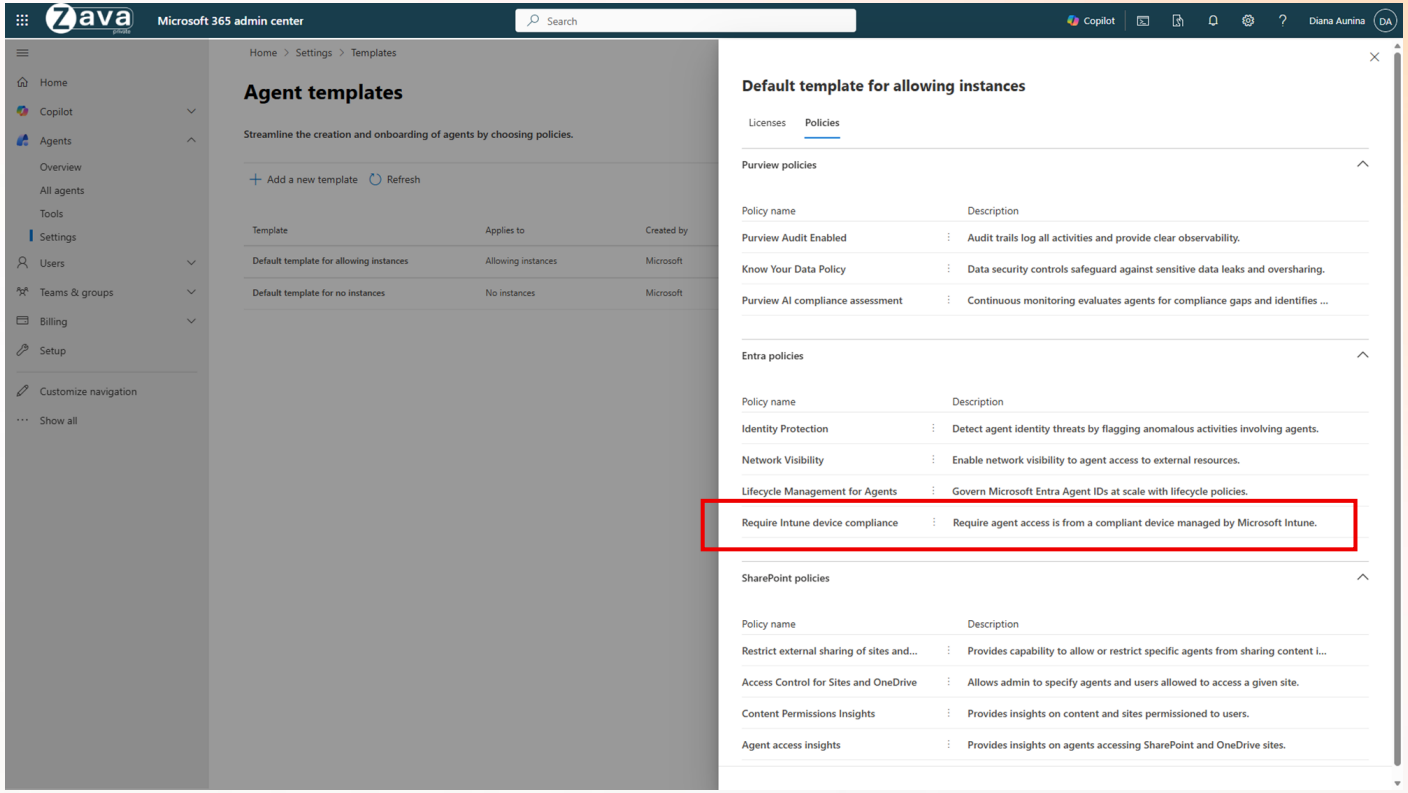
Intune tools to extend boundaries so agents inherit the same access controls as users.

Device-based Conditional Access for agents

Extend device-based Conditional Access from users to agents acting on behalf of users.

Require that agents, acting on behalf of users, only access resources from compliant devices.

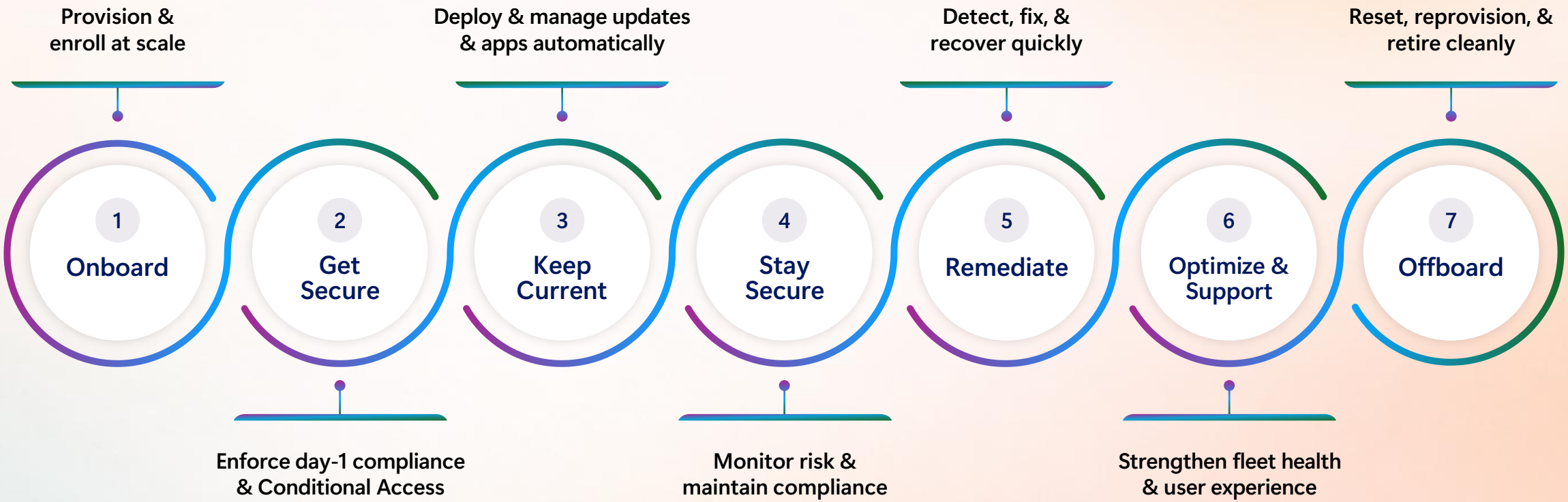
Generally available May 2026



Supported agent types/platforms during preview is subject to change

Reduce the attack surface

Intune helps IT meet enterprise needs at every stage of the device lifecycle



Get secure: Security update status dashboard

Visibility

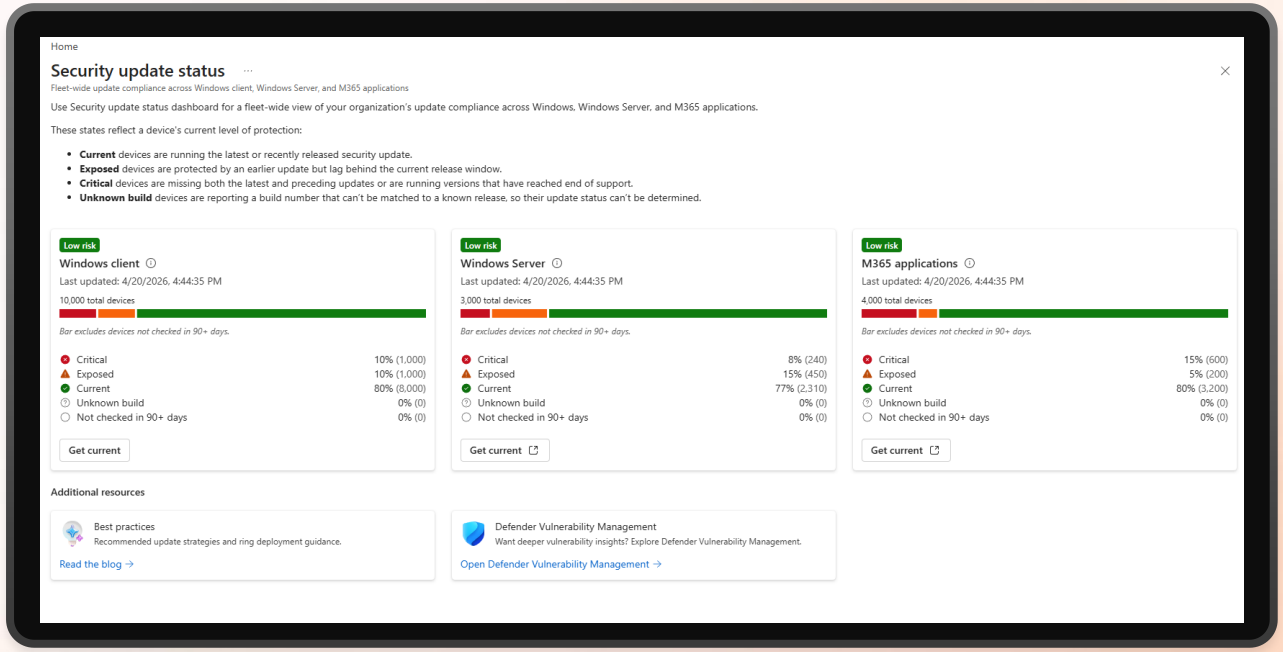
See which devices are current, which are falling behind, and where remediation gaps exist

Data

Prioritize action, track progress across deployment rings, and demonstrate compliance posture

Insights

Know where exposure is critical and needs immediate attention



NEW

Endpoint security: your attack surface reduction toolkit

- **Security update status dashboard –** new!
- **Antivirus policies** – real-time Defender AV protection
- **Attack Surface Reduction rules** – pre-execution exploit blocking
- **Firewall & network protection** – traffic control and threat isolation
- **Endpoint Detection & Response** – threat visibility and auto-remediation
- **Account protection & device compliance** – identity and posture enforcement

But what happens when these settings drift or conflict across multiple configuration sources?

Controlled Configuration: one source of truth

Eliminating configuration drift with a single authoritative policy source

The problem: Multiple configuration sources (GPO, ConfigMgr, scripts) create policy conflicts and unpredictable device state.

The answer: Secure Controlled Configuration (SCC) enforces Intune-delivered Defender settings only; all other sources are ignored.

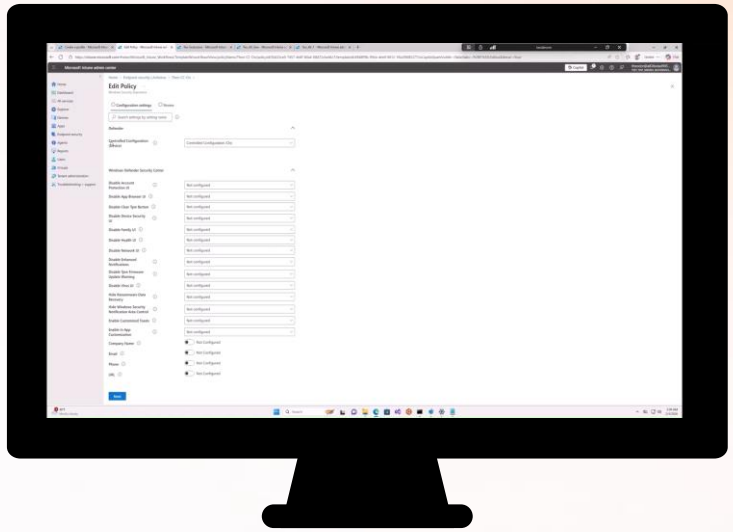
- Extends Tamper Protection with admin-defined guarantees
- Covers AV and EDR today; ASR, firewall, and more coming
- Supports Intune MDM and MDE Attach

Up next: See a walkthrough of enabling Controlled Configuration ▶

Control how security configurations apply

Controlled Configuration

One Source of Truth



COMING SOON

Reduce the attack surface

Unpatched applications remain one of the largest recurring exposure vectors

Today we're focused on building the foundation

Enterprise App Catalog

Prioritized set of pre-packaged apps

Cloud-native app management integrated into Microsoft Intune

Access to a rich app catalog with 1000+ pre-vetted apps

A guided upgrade experience

Support for managed apps

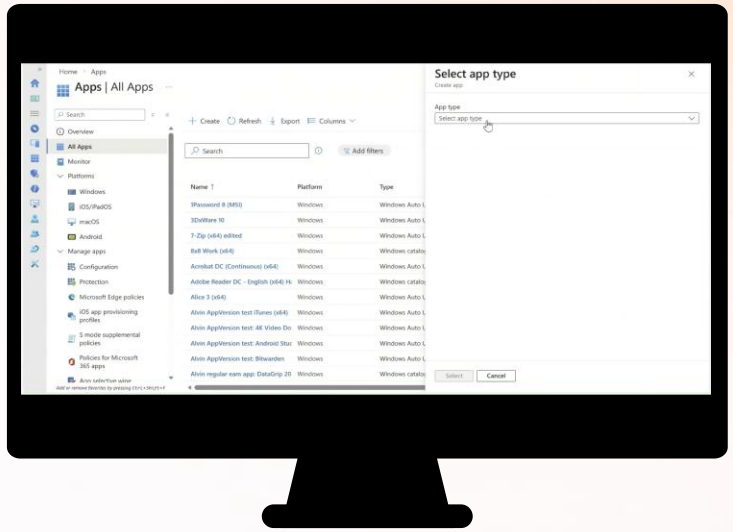
Seamless deployment, updates, and configuration

Reduces IT overhead and improves security

Automatically patch your most common apps

Enterprise App Management

Reduce exploit windows and remove user dependency.



COMING SOON

Shape user experience with security

Security should adapt to how people work **without lowering the bar**.

Meeting end-users where they are

Every organization enforces its own Zero Trust boundary on a single device

- A consultant with three clients, has per-client app protection on one device
- Doctor rotating hospitals, facility-specific protection applied at sign-in
- Merger scenario, side-by-side access to both companies under separate policies

THE CONSULTANT

MON – TUE	WED – THU	FRIDAY
Main Company Primary employer	Company A Client project	Company B Advisory role

THE DOCTOR

MON – TUE	WEDNESDAY	THU – FRI
Hospital Alpha Cardiology consults	Hospital Beta Surgery department	Hospital Gamma & University Emergency / Faculty

App Protection Policies

How app-level policies strengthen your security posture

Why App Protection Matter for Security

APP secure corporate data at the app level with no MDM required, personal data untouched.

- **Stops data leaks at the source,** blocking copy/paste, sharing, and save-as to unmanaged apps
- **Threat-aware access control,** integrating with Defender and MTD to block compromised devices in real time
- **Tiered protection -** basic, enhanced, and high levels matched to data sensitivity and risk
- **Enforces Conditional Access,** by guaranteeing only APP-protected apps can reach corporate resources

Data Protection

Encrypts corporate data, controls copy/paste and save-as between managed and unmanaged apps, and enables selective wipe

Access Requirements

Enforces PIN, biometrics, or credentials for app access with configurable inactivity timers

Conditional Launch

Validates device health, OS version, app version, and threat level before granting access to corporate data

Separate Corporate and Personal

Separates corporate and personal data within the same app so policies apply only to work accounts

Securely access data from several organizations

Multiple Managed Accounts for Teams iOS

Secure multiple corporate identities without data leakage or user friction.

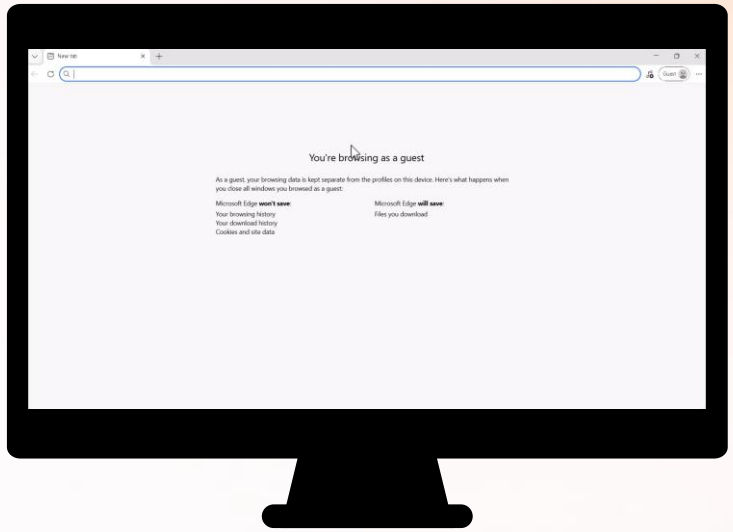
MODERN ENDPOINT MANAGEMENT SUMMIT 2026

COMING SOON

Intune app protections for unmanaged Windows devices

Edge MAM

Protect corporate data for contractors without managing their full devices.



Day-to-Day Impact for IT Teams

Fewer escalations
Policy intent matches device reality, so tickets drop and engineers stop chasing drift.

Faster answers
Copilot explains compliance and risk in plain language—no portal-hopping during incidents.

Less audit anxiety
Policy rationale is visible, explainable, and defensible at scale.

Higher confidence in enforcement
Defender signals flow through Intune to the device—automatically.

Microsoft Intune

Why This Matters for Zero Trust and AI Readiness

- **AI multiplies the cost of every misconfiguration.** Blast radius scales with automation—one bad policy now reaches further, faster.
- **Zero Trust depends on endpoints you can actually trust.** Compliant, current, and enforced—verified in real time, not assumed.
- **Predictable enforcement is the foundation for safe AI adoption.** If the endpoint isn't reliable, the AI controls layered on top aren't either.

SPOTLIGHT

Agent 365

Same Zero Trust boundary for agents.

- Users accessing Agent 365 — gated by device compliance.
- Agents acting on behalf of users — governed by the same CA policies.
- Intune supplies the compliance signal; Entra enforces in real time.

Secure Endpoints Without Burning Out IT

- **Predictable.** Policy intent becomes device reality—every time.
- **Understandable.** Risk, compliance, and enforcement explained in plain language.
- **Sustainable.** Operations your team can actually run—every day, at scale, without burnout.

Better security outcomes come from operations that are predictable, understandable, and sustainable.

Call to action. Released April 22

- **Read the blog:** Ales Holecek, Chief Architect and Corporate Vice President Microsoft Security. aka.ms/PrioritizingDefense
- **Take action** guide: Microsoft - Secure now
- **Learn** from Intune: aka.ms/PrioritizingDefenseIntuneBlog

Steps Microsoft is taking to help customers in response to an AI-accelerated threat landscape.

Thank you!