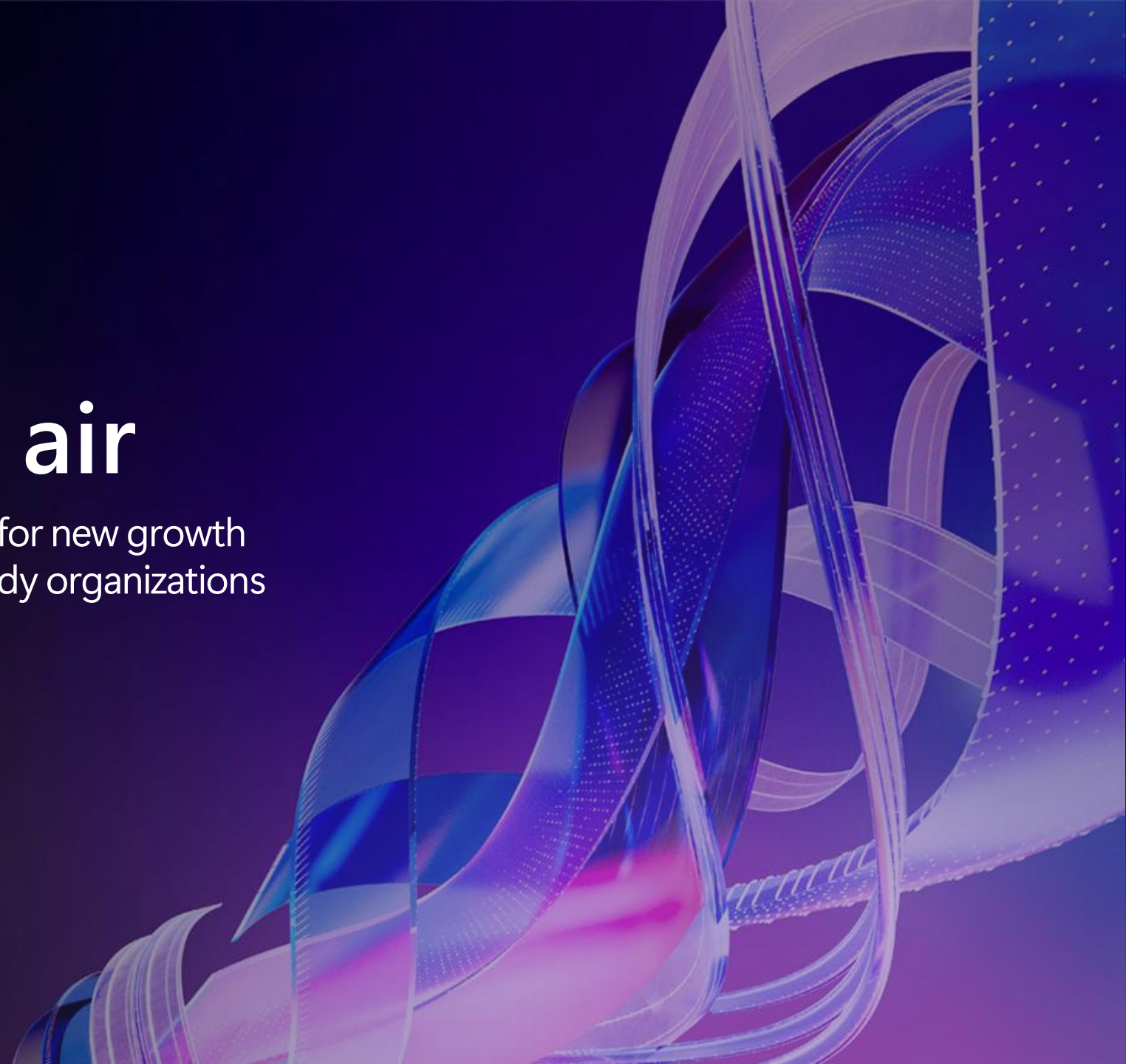
Microsoft

Spring is in the air

Rooting strongly in Zero Trust to prepare for new growth with cloud-connected, secure, and AI-ready organizations



Sangeetha Visweswaran, Intune Engineering VP
Lior Bela, Intune Business Director

Your Speakers

Lior Bela

Intune Business Director

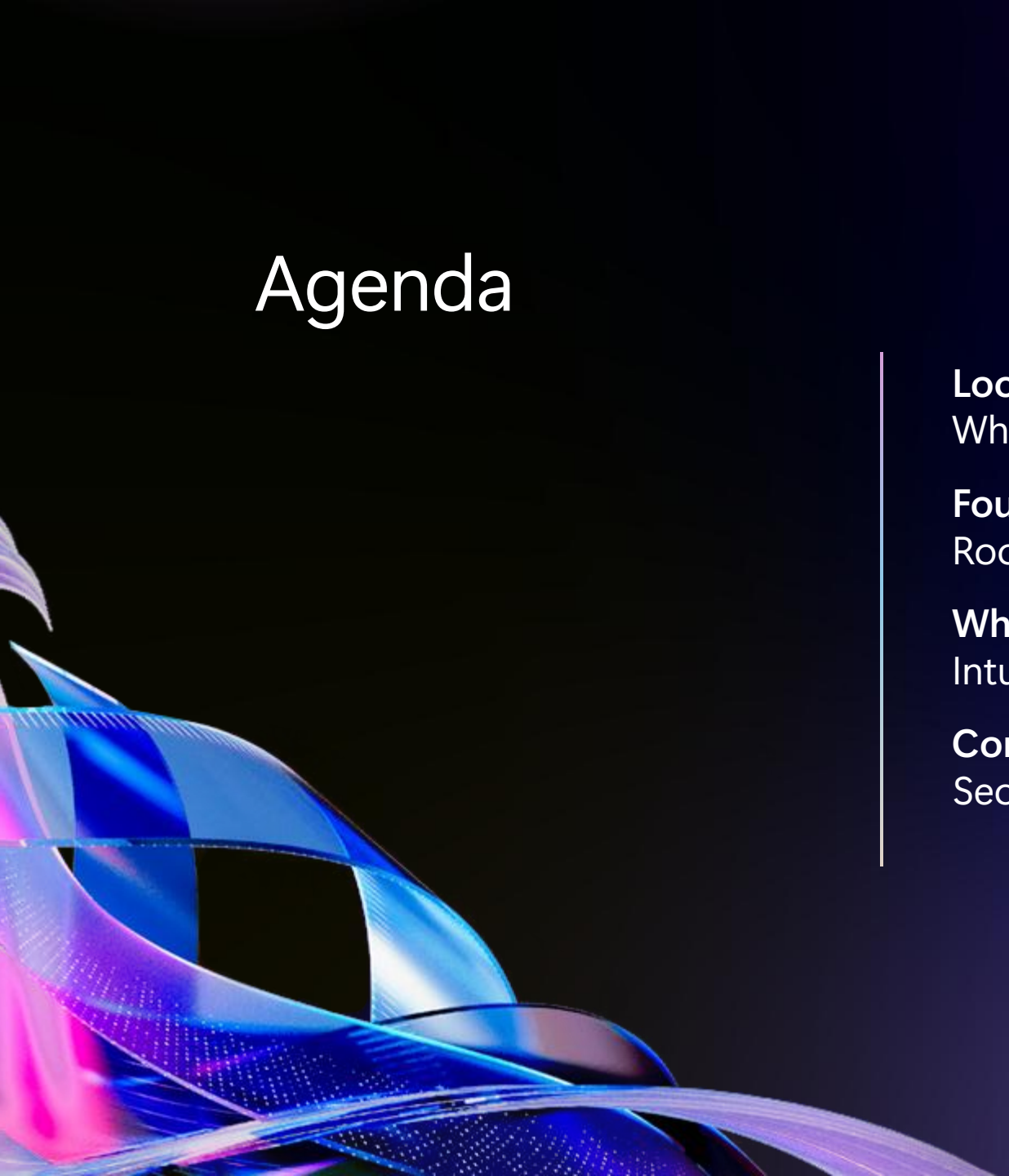
- Likes to talk anything technology
- If he could snap his fingers and master a skill: removing bureaucracy
- Daydreams about: Time with the family

Sangeetha Visweswaran

Intune VP of Engineering

- Likes to listen to people
- If she could snap her fingers and master a skill: would deliver jokes with perfect timing
- Daydreams about: Travelling to destinations on Bing wallpaper

Agenda



Lookback:
What we announced in the last year

Foundations:
Rooting in Zero Trust

What's new:
Intune's investments

Connecting the dots:
Security and AI


Most
Secure
Standing

Stay standing if you or your organization

Enforce MFA for all admin/privileged roles

Enforce conditional access policies for devices and identities

Have deployed a custom agent to secure your posture

End Game

AI is already in your workplace

Enterprise ChatGPT use grew 8× in one year.[1]

AI gives every worker 40–60 minutes back each day.[2]

AI-skill job postings are up 70%+ year-over-year.[3]

1., 2.: Source: Chatterji, A., Cunningham, T., Deming, D., Hitzig, Z., Ong, C., Shan, C., & Wadman, K. (2025). *How People Use ChatGPT*. OpenAI / National Bureau of Economic Research (NBER Working Paper No. 34255). Cited in Microsoft New Future of Work Report 2025.

3. Source: LinkedIn Economic Graph Team. (2025). Global AI Talent and Skills Trends Report. LinkedIn Corporation. Cited in Microsoft New Future of Work Report 2025

The AI mindset shift

Human world	AI world
User signs in occasionally	Agents act continuously
Access is session-based	Access is task-based
Changes are intentional	Changes are autonomous
Identity = person	Identity = workload

Zero Trust is how we make AI usable at enterprise scale

You no longer trust who signed in

You must trust:

- the device
- the workload
- the policy state
- the risk posture
- the change intent
- the agent identity at execution time

Three years of keynotes

2024

Cloud Native + Intune Suite

2025

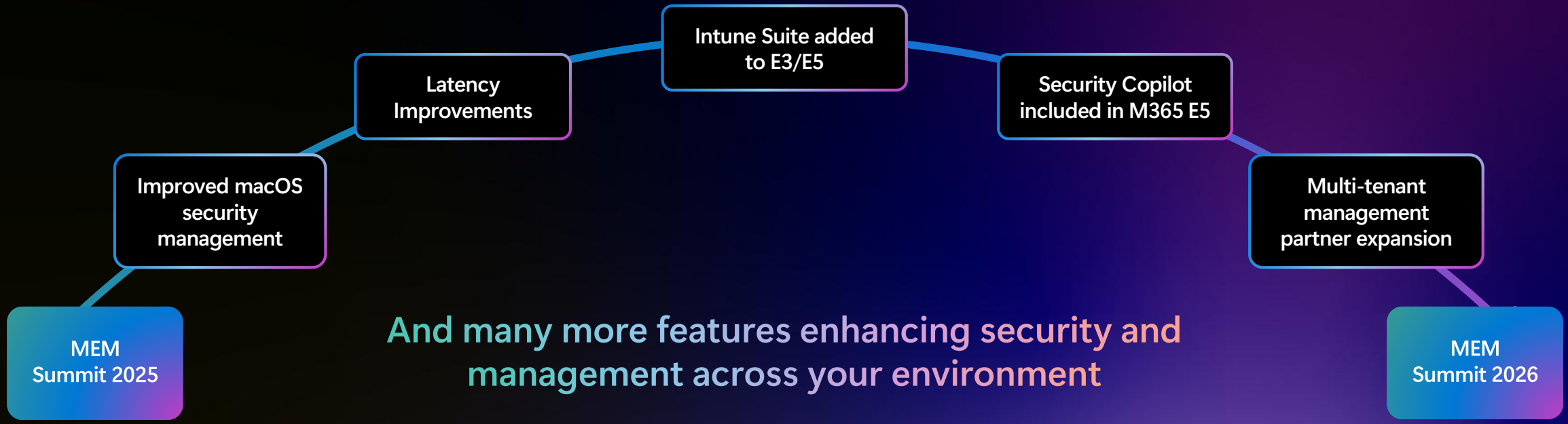
Preparing for the AI Era

2026

Strengthen your security foundations, then enable enterprise AI

The question is not whether you are ready.
The question is whether you built the foundation.

A year of growth



And many more features enhancing security and management across your environment

April 2025

April 2026

The Cloud Native piece of the puzzle

Conditional Access Policies

Microsoft Entra

Microsoft Intune

Application migration partners

Rimo3

robopack
empowered by SOFTWARE CENTRAL

aka.ms/IntuneAppMigration

Intune for MSPs multi-tenant management partners

AvePoint

cipp

inforcer

nerdio

SOFTWARE CENTRAL_TENANTMGR

aka.ms/IntuneForMSPs

Verify explicitly

- Conditional Access
- Hardware backed attestation
- Require multifactor authentication
- Device compliance policies
- Cloud PKI
- Remote Help
- Windows Autopilot
- Windows Hello for Business
- MFA
- Security baselines
- Biometric logins

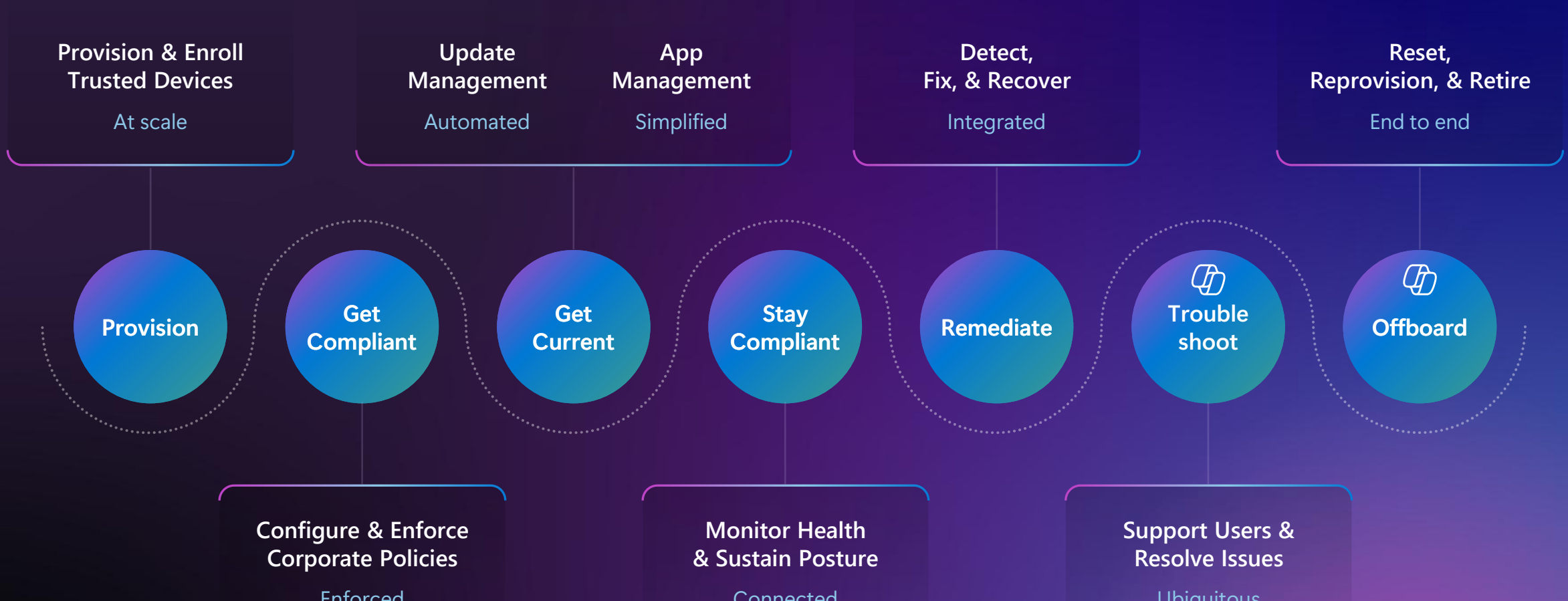
- Endpoint Privilege Management
- Tunnel for MAM
- Cloud Local Admin Password Solution
- Role-based access control
- Multi-admin approval
- Scope tags
- Local account management for macOS

Least privilege access

- Enterprise Application Management
- Advanced Endpoint Analytics
- Require encryption
- OS patching
- Mobile Threat Defense

Assume breach

Delivering Zero Trust value across the lifecycle



Latency improvements

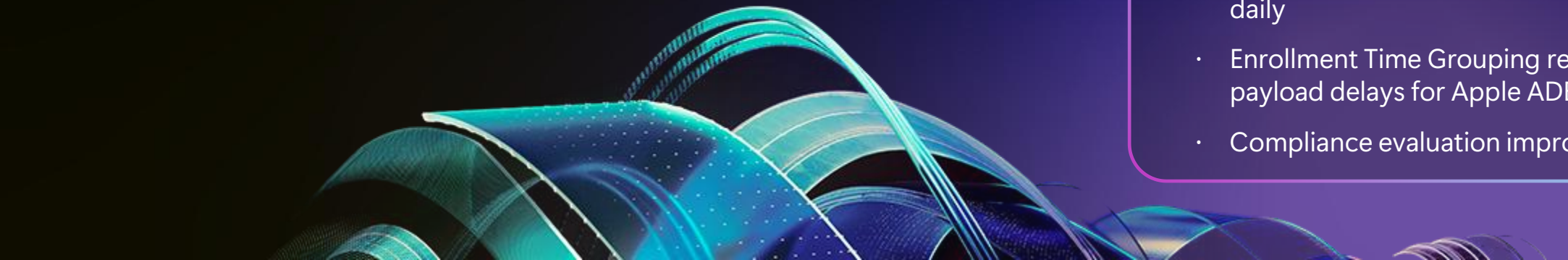
Important check-ins happen fast with an intelligent, priority-aware system

This feature is a work-in-progress

95%

p50 notification latency with pending changes happen on first attempt

- Fine grained check-in prioritization with shorter retry times
- ‘Fast lane’ coming to all payloads and gateways
- Priority lane for small changes (p99 <5min)
- Modernizing push notifications for Windows devices
- Improved data freshness (from hours to minutes in certain reports)
- Faster inventory, now multiple updates daily
- Enrollment Time Grouping reduces payload delays for Apple ADE enrollments
- Compliance evaluation improvements

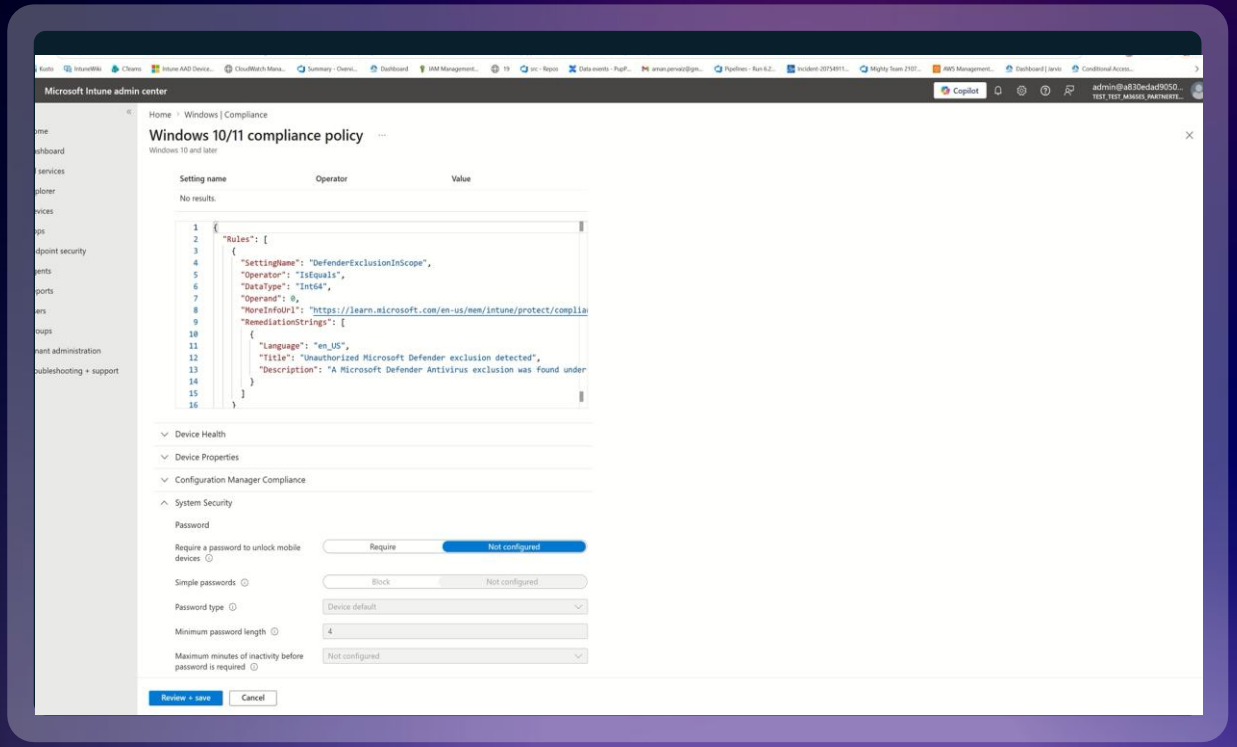


Latency: Client-driven compliance evaluation

This feature is a work-in-progress

MDM settings drift detection

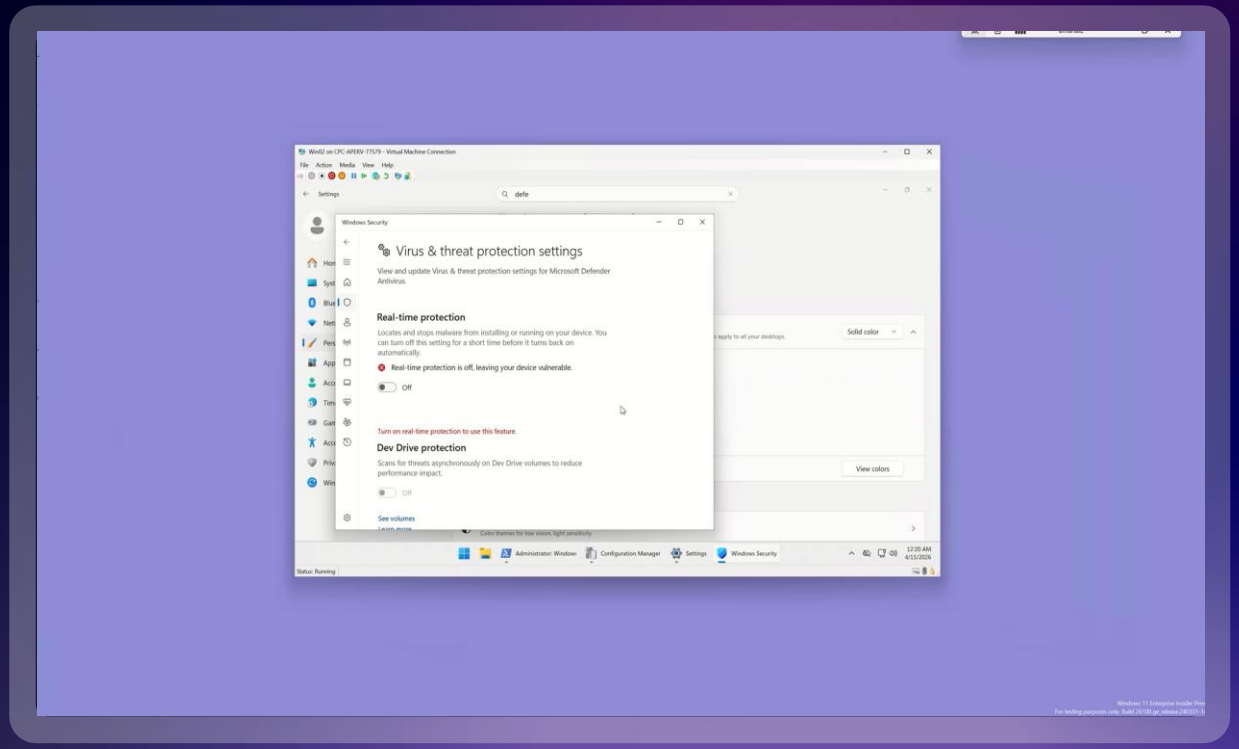
When the device detects a settings change locally, it can immediately start compliance evaluation without waiting for the next scheduled sync.



Latency: Client-driven compliance evaluation

Device settings drift detection

The detection works in reverse – when a change is made on device to restore compliance, Intune is notified and access is granted



Latency: The Sync Button

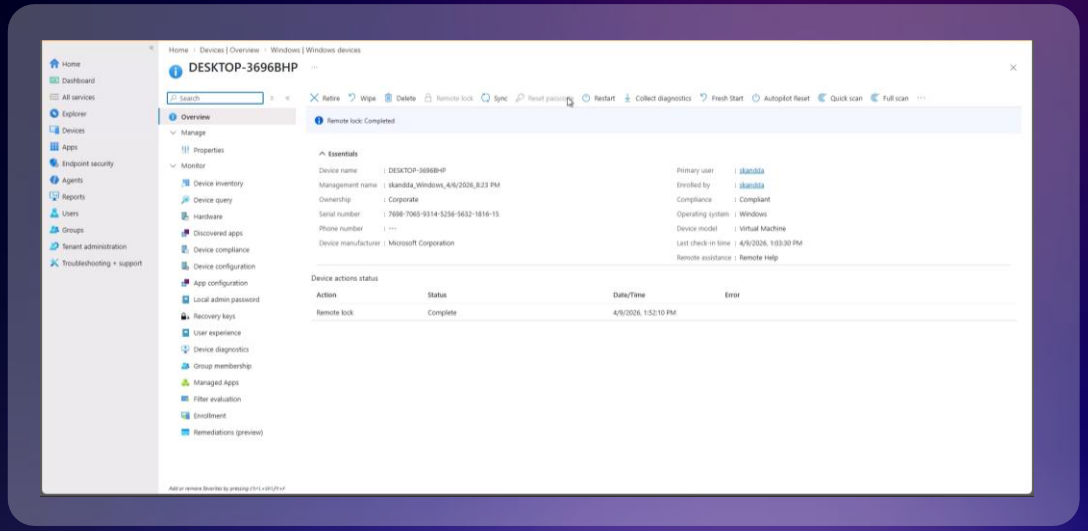
This feature is a work-in-progress

Consistency

- MDM channel check in
- IME channel check in

Transparency

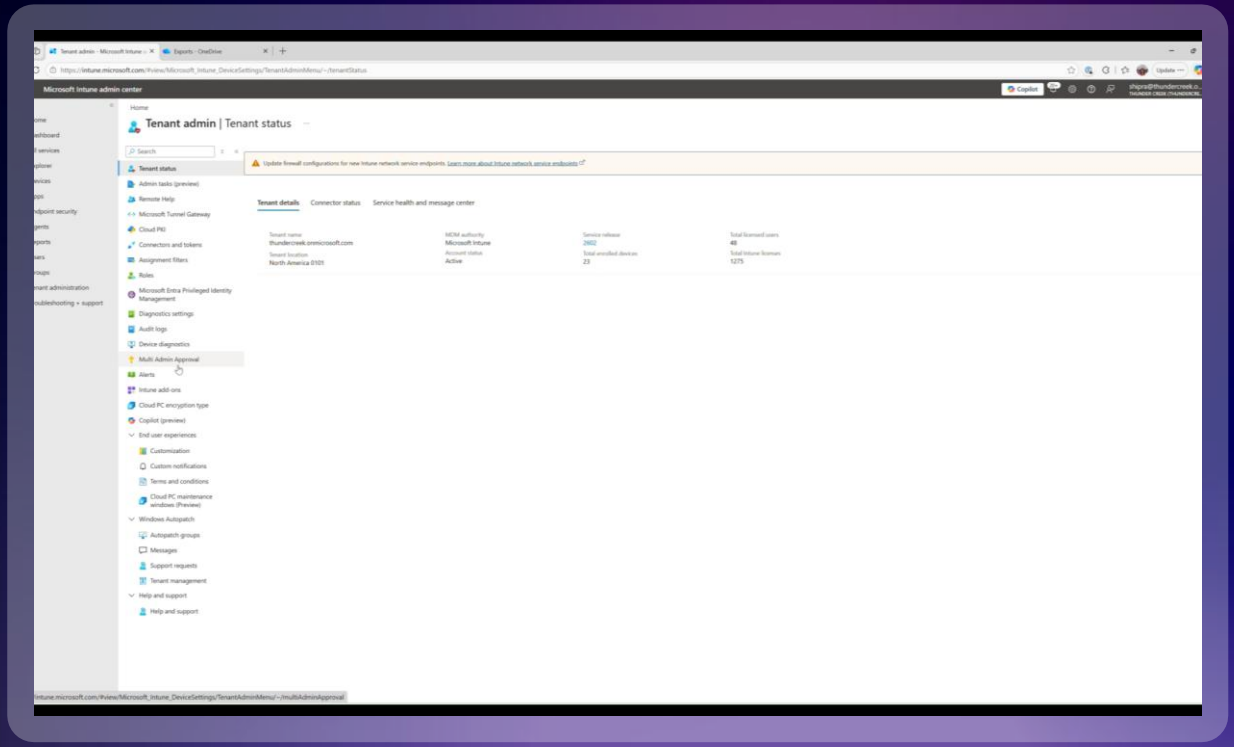
- View a clear transcript of
- What actions were taken,
- What changed, and
- Where things are at right now



Multi-admin approval + Admin Tasks

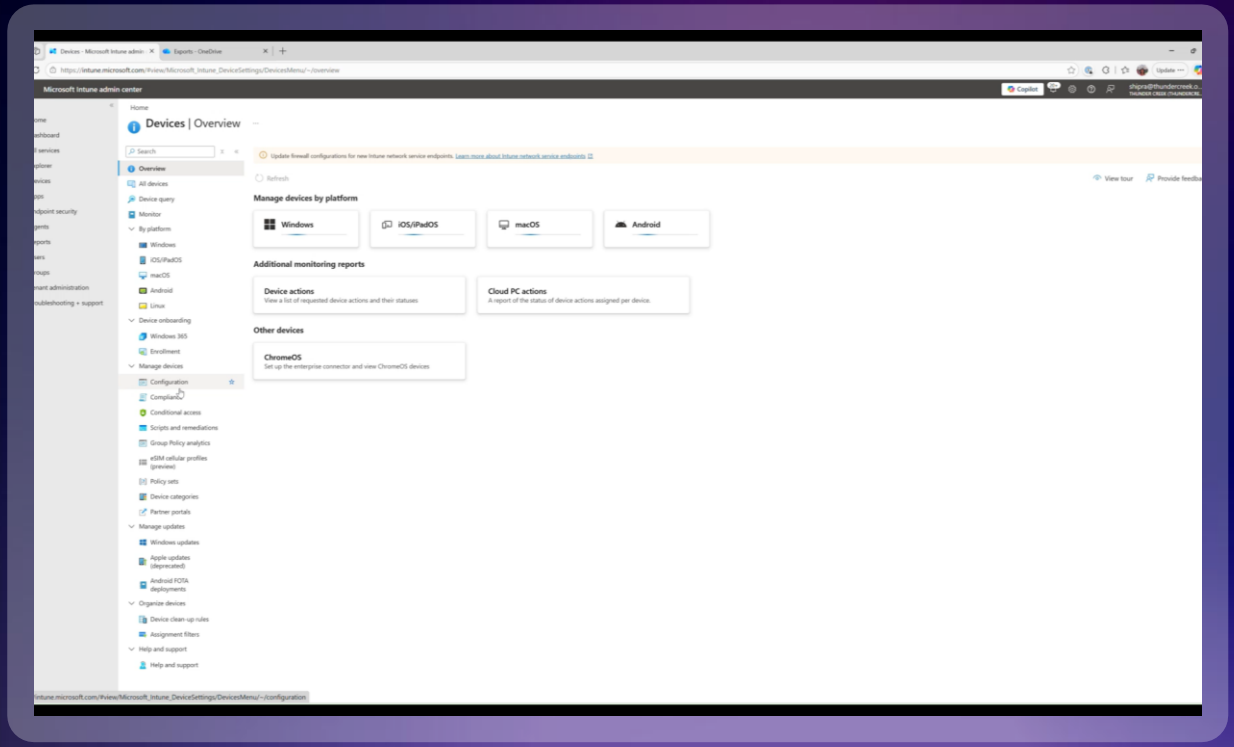
Script access policy creation

- Prevent unauthorized or unintended changes
- Requestor and approver notes
- Audit trail



Multi-admin approval + Admin Tasks

Creating a script



Deployment plans

What this enables

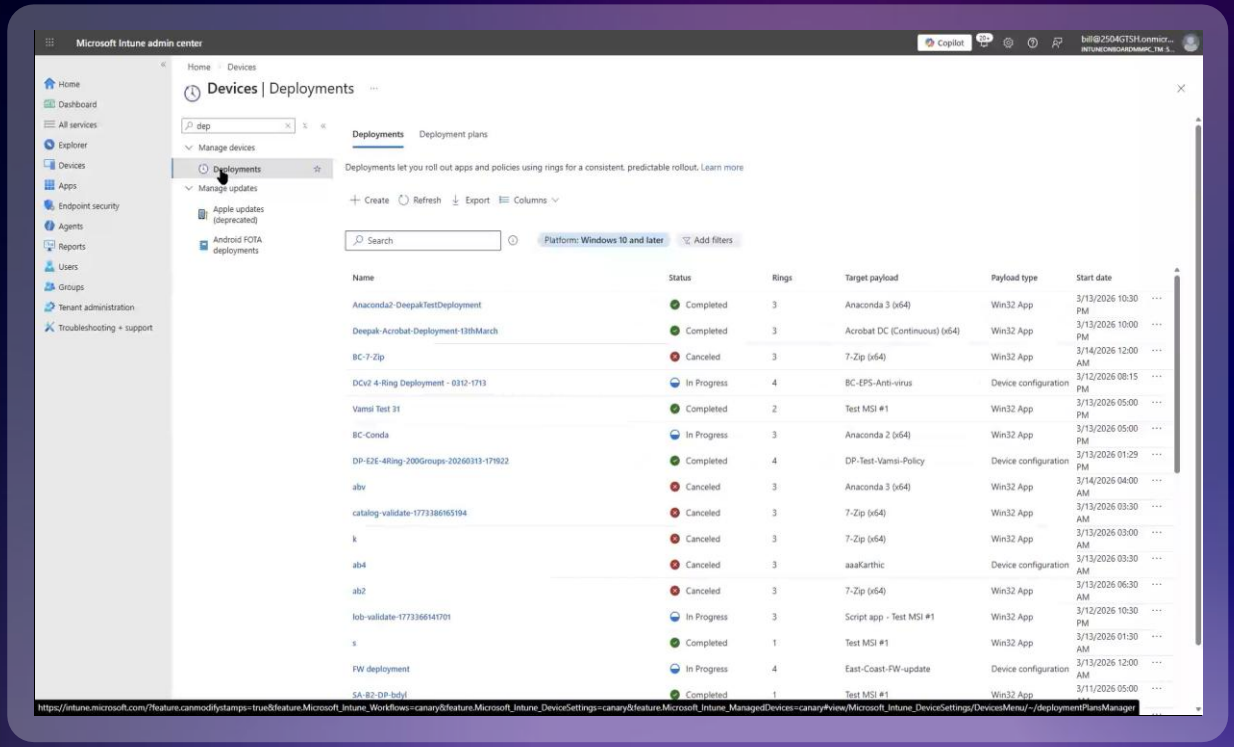
Admins can now create a gradual, controlled rollout of any Intune payload

Standardized approach

Create standardized deployment plans that bring predictability and consistency to how changes reach devices

Works across payload types

Apps, device configuration policies, and more - providing the foundation for future agentic rollouts—critical for scaling new AI-powered features and applications



Expanded hardware-backed attestation

We have existing solutions for

- ✓ Windows
- ✓ Samsung Knox
- ✓ iOS

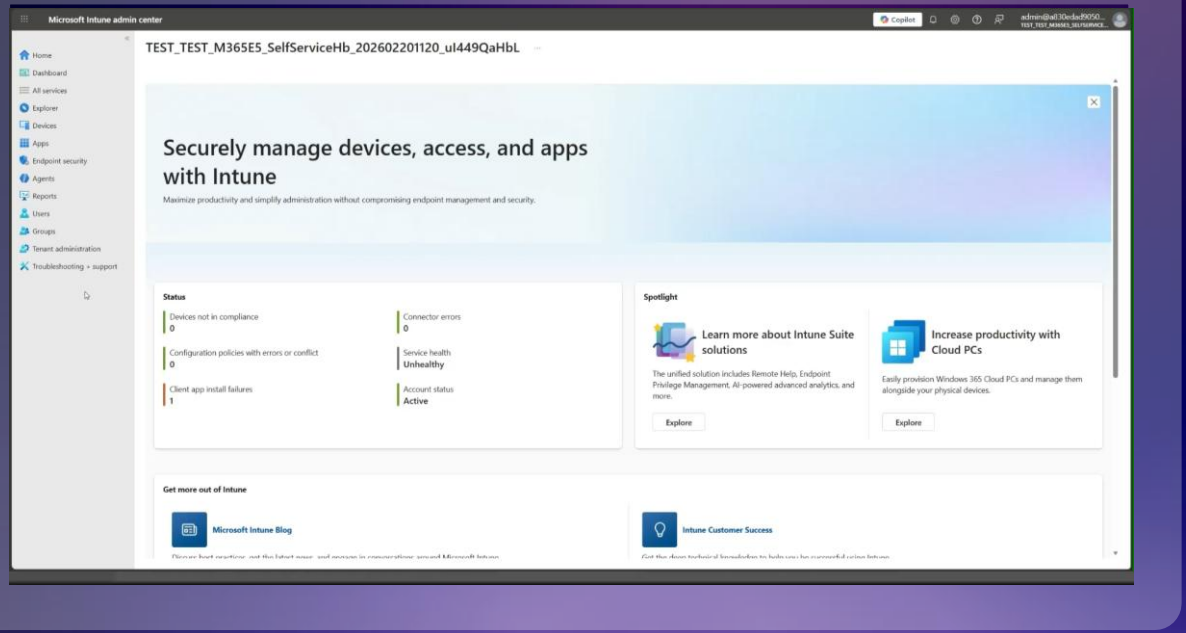
And now Android

Introducing Attestation Verification Key:
Cryptographic proof of device integrity

- ✓ Zero Trust enforcement without user friction
- ✓ Hardware-level root/emulator detection
- ✓ Better Conditional Access decisions

Deeper Application inventory

- Intune’s enhanced application inventory improves visibility, risk detection, and response speed across managed endpoints.
- Deeper inventory shifts app management from reactive cleanup to proactive risk reduction.
- Security and IT gain a shared, authoritative view of the app estate, reducing blind spots and operational friction.



Intune Suite Value in E3 and E5

Learn more at our AMA immediately after this at 9:50

Advanced Analytics

E3 E5

Proactively address endpoint issues with device queries and holistic visibility, uncover anomalies and unreported performance issues, and troubleshoot and remediate with granular insights to enhance end-user experience.

Remote Help

E3 E5

Empower the helpdesk with an easy-to-use experience that uses Zero Trust based protection, including conditional access policies, device compliance checks, and multifactor authentication.

Advanced mobility solutions

E3 E5

Empower your workforce to remain connected on personal mobile devices to on-premises resources, update firmware over the air and manage specialty devices.

Enterprise Application Management

E5

Reduce time and effort for IT administrators to package apps and track updates while streamlining fix deployments to keep apps up to date and secure.

Endpoint Privilege Management

E5

Allow standard users to perform tasks normally reserved for an administrator on cloud-native endpoints. Set policies for automatic, user-confirmed, and support-approved elevation scenarios.

Microsoft Cloud PKI

E5

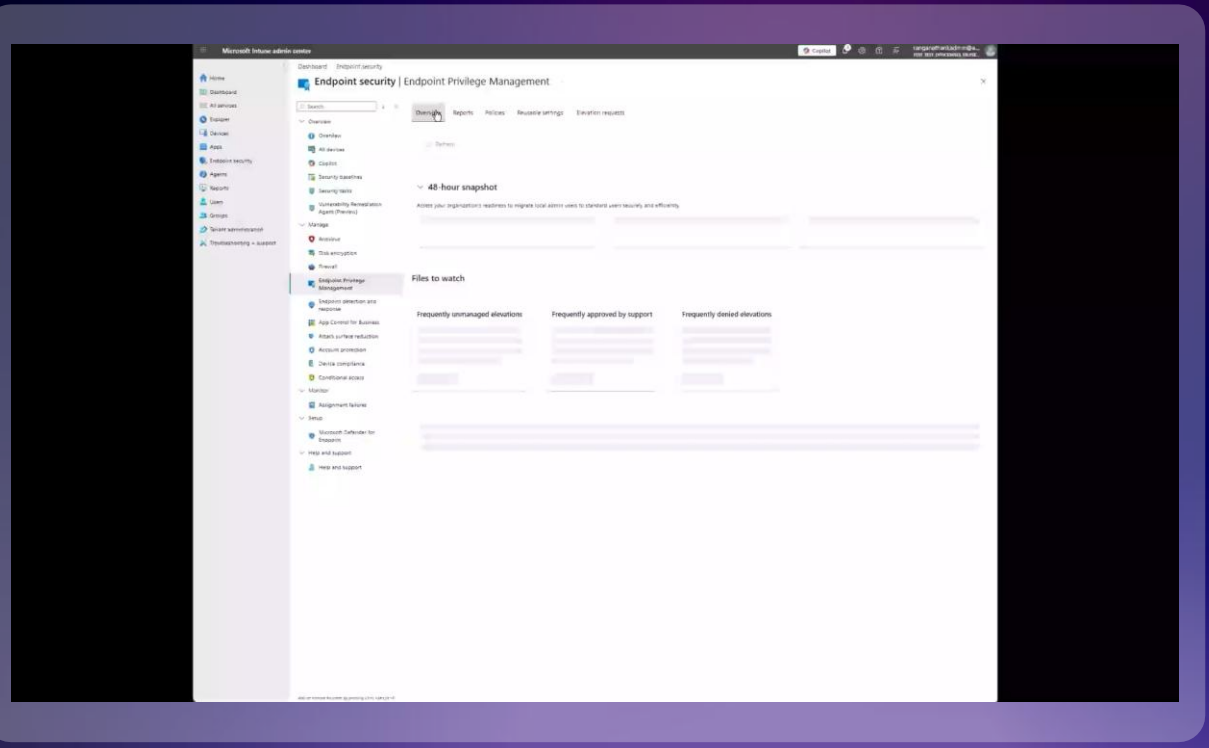
Create, revoke, and manage certificates in the cloud, removing the cost and complexity associated with on-premise PKI infrastructure. Improve security with certificate-based authentication.

Endpoint Privilege Management (EPM)

Capabilities expanded

Dashboard

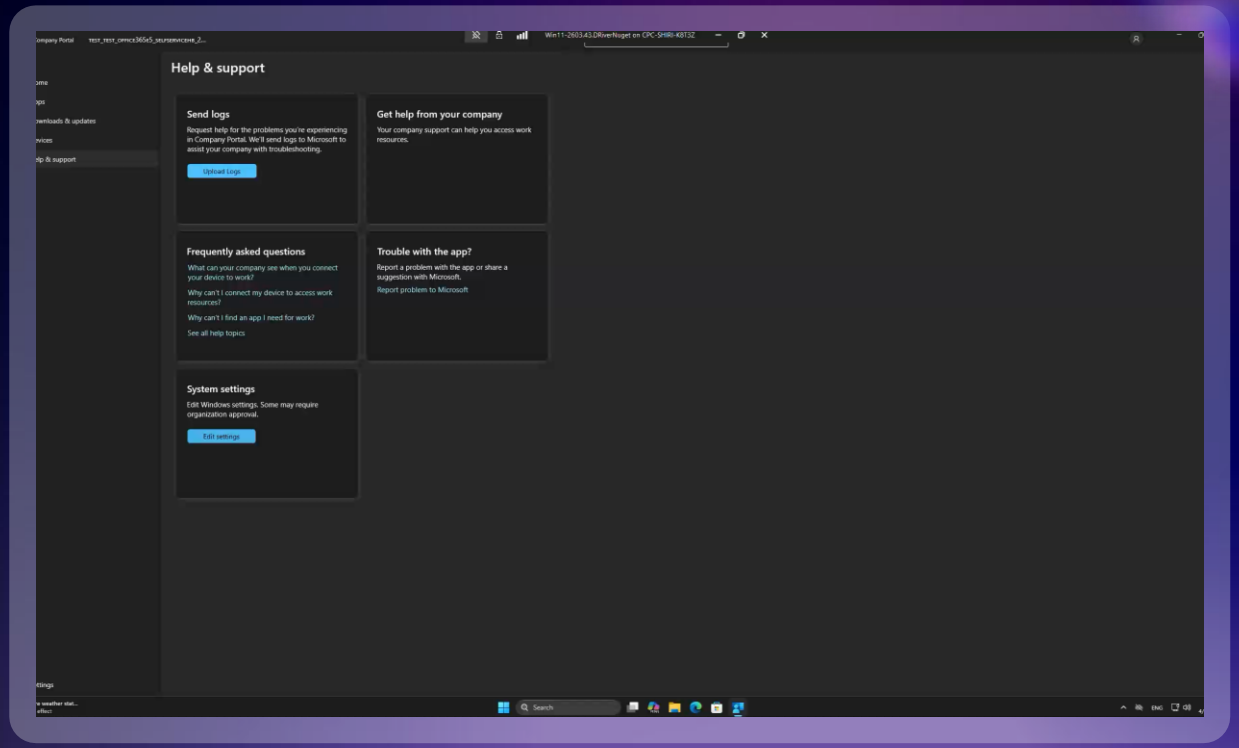
- Standard user readiness
- Top approval requests
- Elevation trends



Endpoint Privilege Management (EPM)

Capabilities expanded

System setting network configuration support



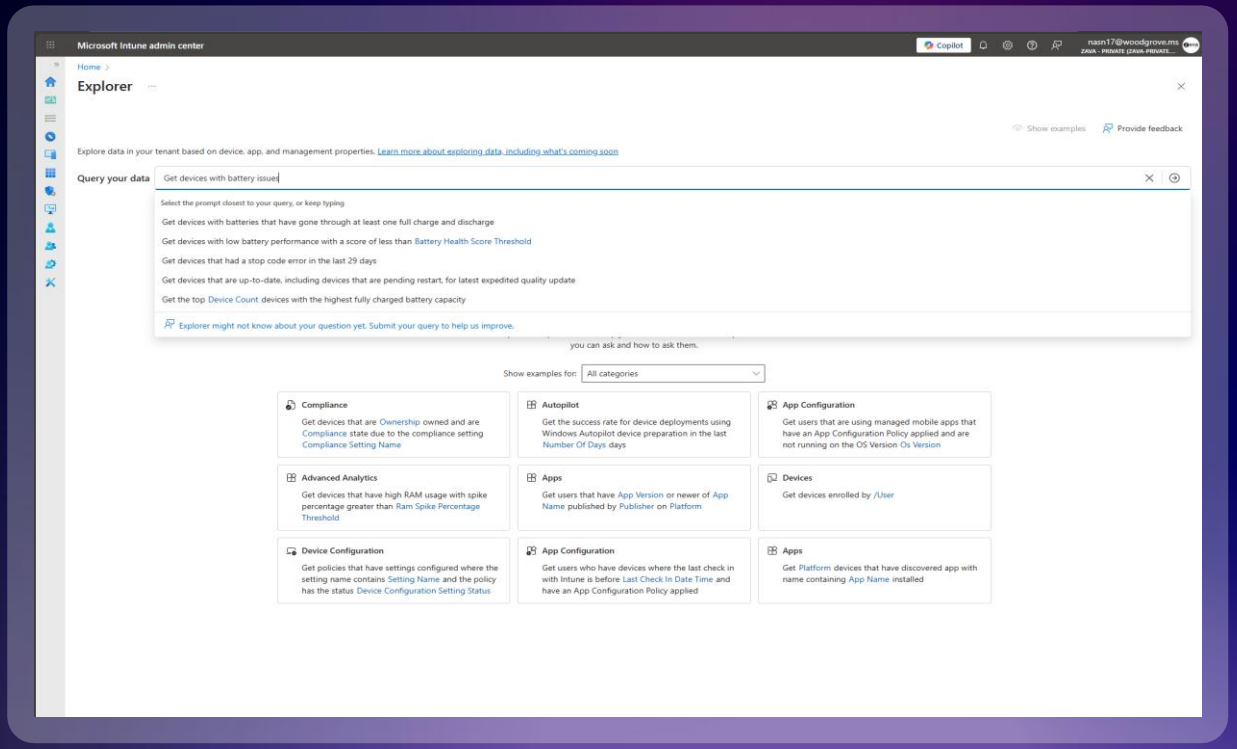
Explore Intune data with Copilot

An enhanced experience is in development

Adding to the prompt library

Making the experience more consistent

Redesigning the user interface



Contextual | Ambient | Always learning

Practical approaches to strengthen protections

- Start with least privilege
- Embrace phishing resistant auth & privileged access hygiene
- Enable Multi Admin Approval in Intune

Minimum Viable Trust Fabric for Enterprise AI

1	**Enable Conditional Access**	Every device, every identity, every access request evaluated
2	**Enforce Compliance Policies**	Non-compliant devices blocked at the network edge
3	**Deploy MDE EDR**	Microsoft Defender for Endpoint, Endpoint detection and response integrated natively with Intune
4	**Activate Endpoint Privilege Mgmt**	Remove standing admin rights across your fleet
5	**Enable Security Copilot Agents**	Let AI defend your AI environment — policy, change review, remediation
6	**Register AI Agents in Entra**	Every agent needs a verified, managed identity
7	**Audit Regularly**	Advanced Analytics and Compliance Reports — your continuous feedback loop

Agentic AI

Change Review skills

Analyzes requested changes

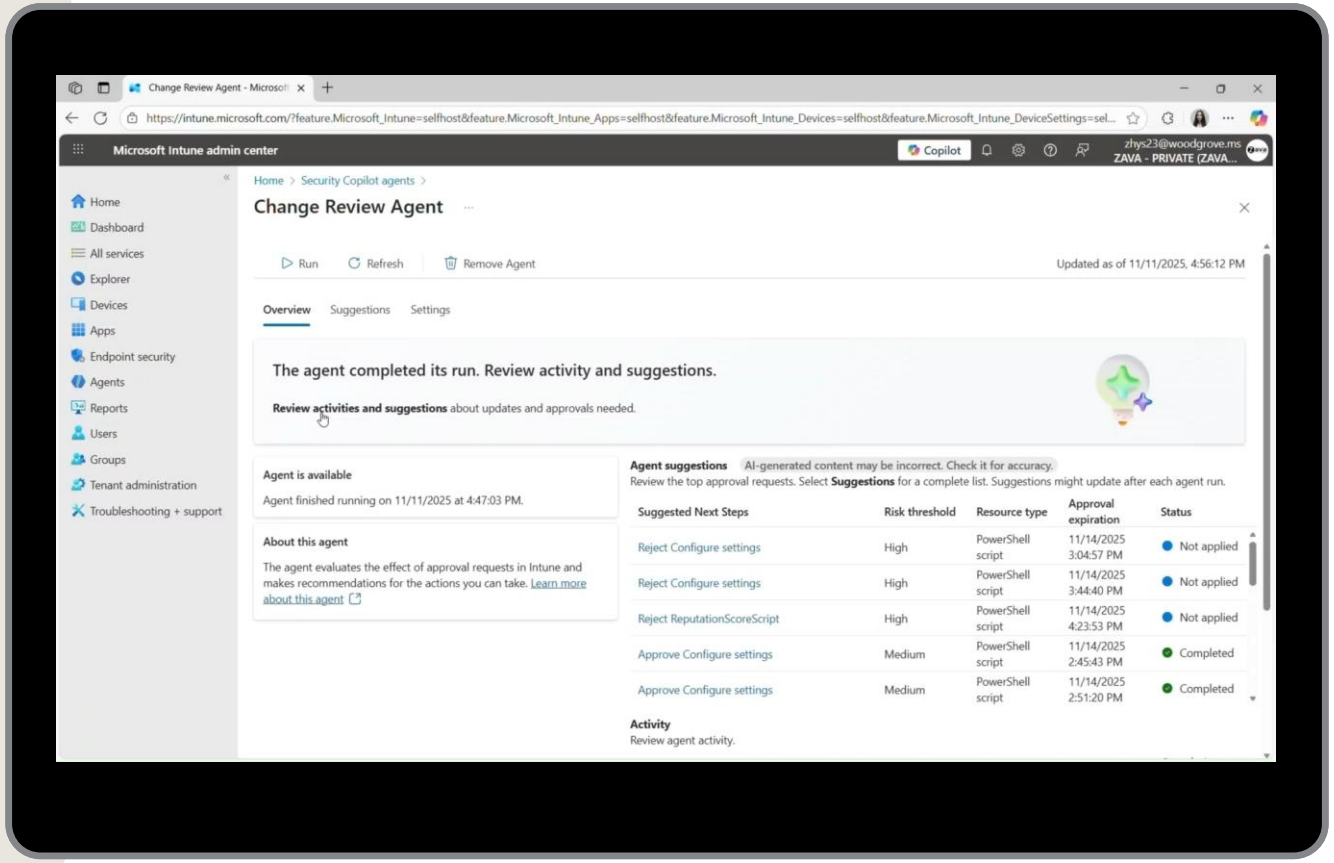
Uses advanced AI to analyze each change in context, checking for risks.

Gain deep understanding

Provides detailed insights on the impact the change would have on the environment.

Make informed decisions

Makes clear recommendations, so you can move forward with confidence.



Preview

Vulnerability Remediation Agent

Preview

Continuously detect evolving threats

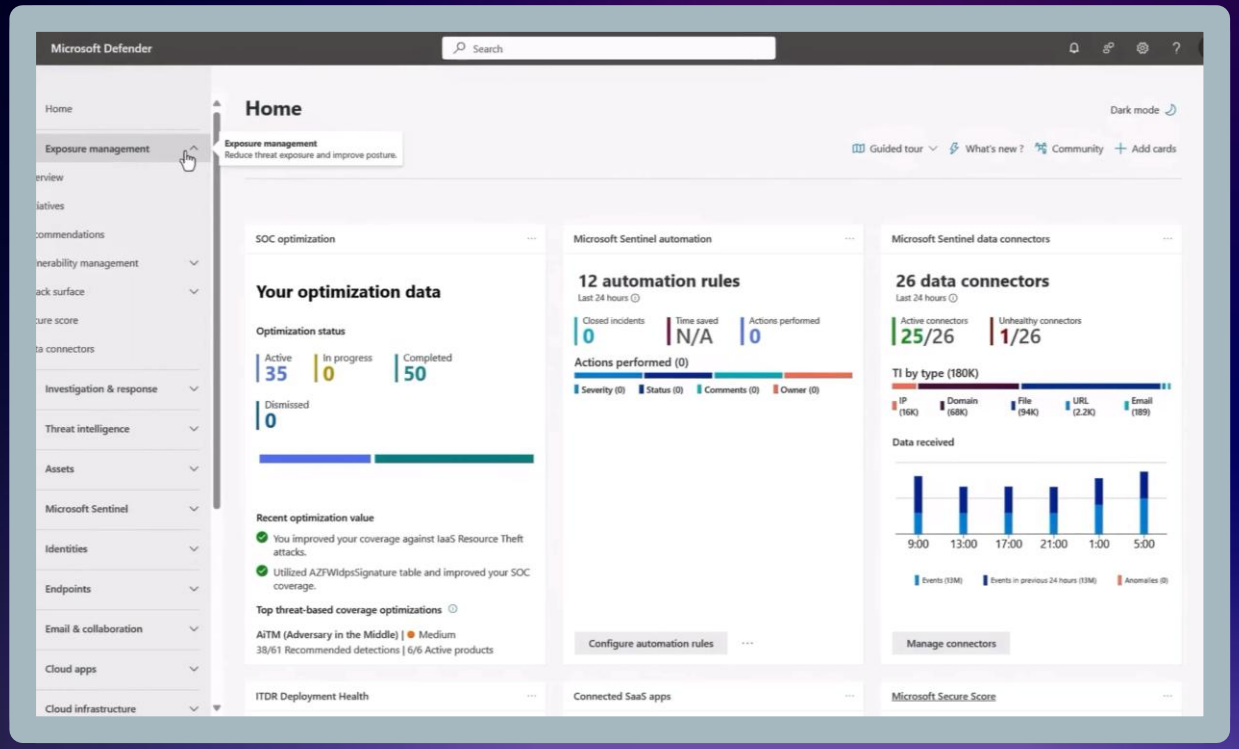
Monitors and reevaluates vulnerabilities over 90 days, identifying newly emerging threats.

Prioritize and expedite critical patches

Uses AI-driven analysis to analyze impact and determine which vulnerabilities need immediate attention.

Remediate faster with full context

Provides clear reasoning for urgency, enabling faster, informed remediation without unnecessary disruptions.



Your homework

- ✓ Set the stage with the Zero Trust assessment tool
- ✓ Get ready for E3 & E5 Intune Suite Inclusion
- ✓ Print it, and place it in your office! The 7 requirements for Minimum Viable Trust Fabric for Enterprise AI

Take action on Zero Trust

Follow our comprehensive technical guide to adopting Zero Trust

https://aka.ms/zerotrustworkshop

Thank You

Lior Bela
Intune Business Director

Sangeetha Visweswaran
Intune VP of Engineering