ICT POWER.IT

Microsoft

#POWERCON2023

Microsoft Intune: il braccio operativo della sicurezza sugli endpoint

Riccardo Corna

MVP Security – Senior Consultant

(Coautore: Davide Salsi – MVP Enterprise Mobility)

@itspecialcloud

/riccardocorna

83 %

Organizzazioni che hanno subito almeno 1 attacco negli ultimi 2 anni

25 %

Organizzazioni che hanno identificato l'accesso non autorizzato ai dati sensibili come una delle principali minacce alla sicurezza

90 %

di tutti gli attacchi ransomware riusciti hanno origine da dispositivi non gestiti

Rif: Microsoft Digital Defense Report – October 2023

Agenda

- Zero Trust
- Intune come un «Maestro» d'orchestra
- Perché "Maestro"?
- Band lineup
  - Endpoint Security
  - Threat Defense
  - Identità del device
  - Identità dell'utente
  - Privilegi minimi
- Q&A

Principi Zero Trust

Verifica esplicita

Autenticare e autorizzare sempre verificando l'identità e lo stato del device senza presupporre che questi siano attendibili

Assumere il breach

Segmentare gli accessi per prevenire movimenti laterali e protegge le comunicazioni attraverso la crittografia end-to-end

Privilegi minimi

Limitare l'accesso mediante: accessi "just-in-time" (JIT) e "just-enough-access" (JEA), policy adattive basate sul rischio e protezione dei dati

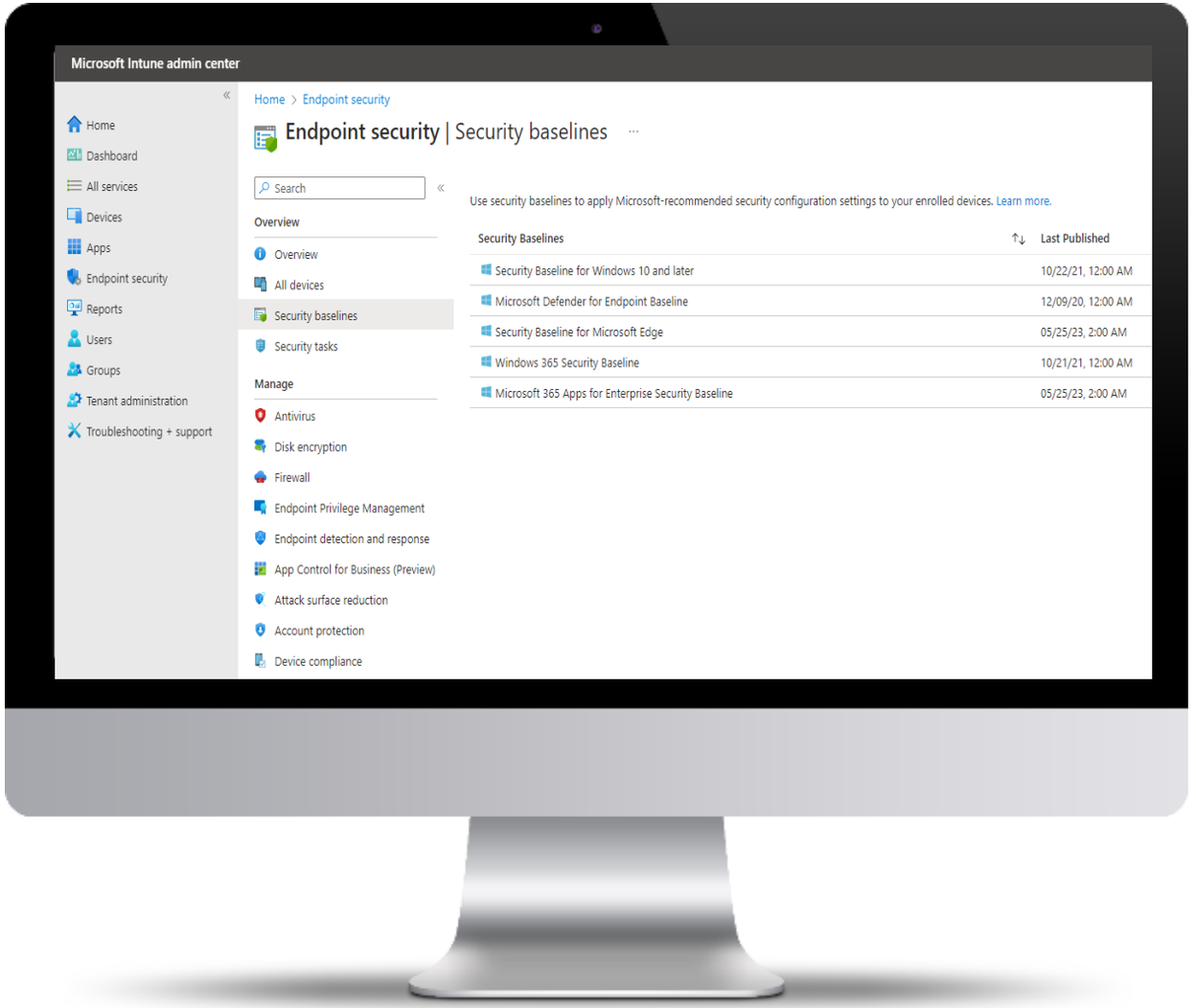
Microsoft Intune come un «Maestro» d'orchestra

Perché «Maestro» Microsoft Intune?

- Perché non serve solo a gestire dispositivi.
- Perché è il braccio operativo degli strumenti di sicurezza Microsoft per gli endpoint:
  - Cosa significa?
  - Molte delle configurazioni e delle informazioni che permettono di "calcolare" lo stato di salute e di sicurezza di un endpoint, sono veicolate da/attraverso Intune.

Endpoint Security

- Scenario:
  - Endpoint Security
- Piattaforme coinvolte:
  - Windows
  - macOS
  - iOS/iPadOS
  - Android
- Sezione:
  - Endpoint Security
  - Devices -> Configuration Profiles
- Strumento musicale:
  - Batteria



Security Baseline

01 Insieme di settings per Windows 10 che rappresentano le best practices di Microsoft per la sicurezza e la protezione del sistema operativo, di Edge, Defender for Endpoint, Microsoft 365 Apps e Windows 365

02 Vengono rilasciate periodicamente nuove versioni

03 Sono il risultato di un confronto da parte del team di security Microsoft con le raccomandazioni del Center for Internet Security (CIS) e di altre organizzazioni

Security Configuration Framework

Il Security Configuration Framework è una serie di raccomandazioni fornite da Microsoft per la configurazione e la conformità dei dispositivi:

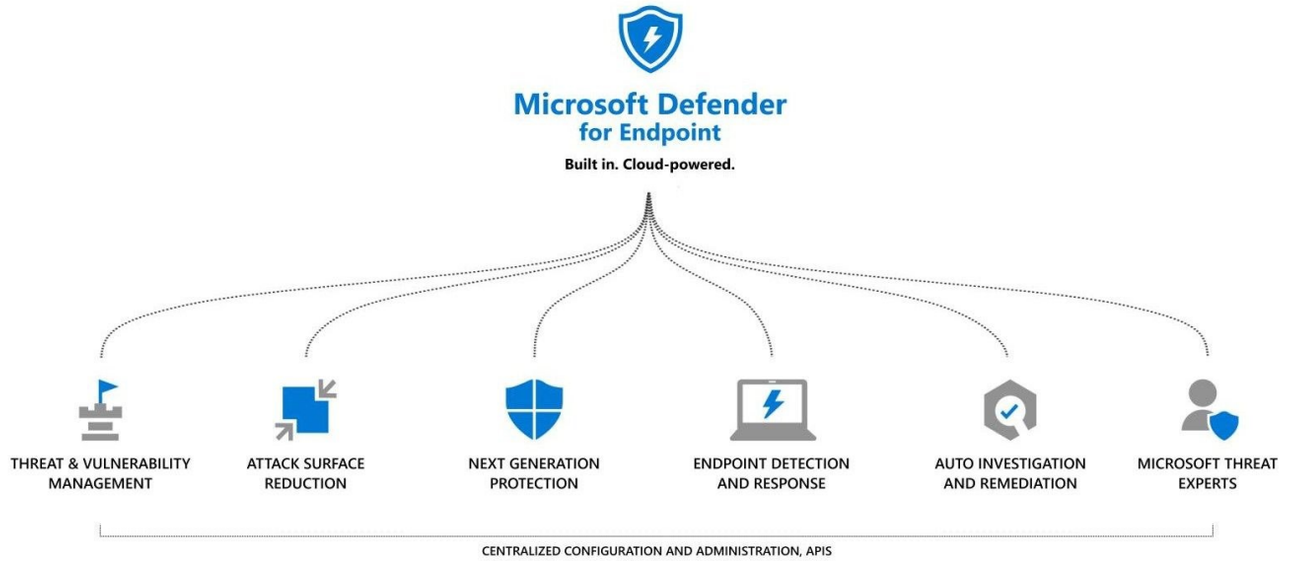
- iOS/iPadOS (Personal – Supervised)
- Android (Personal – Fully Managed)

- Suddivide i dispositivi in uno dei seguenti 3 livelli di sicurezza:
  - Basic (solo per device Corporate)
  - Enhanced
  - High

Threat Defense

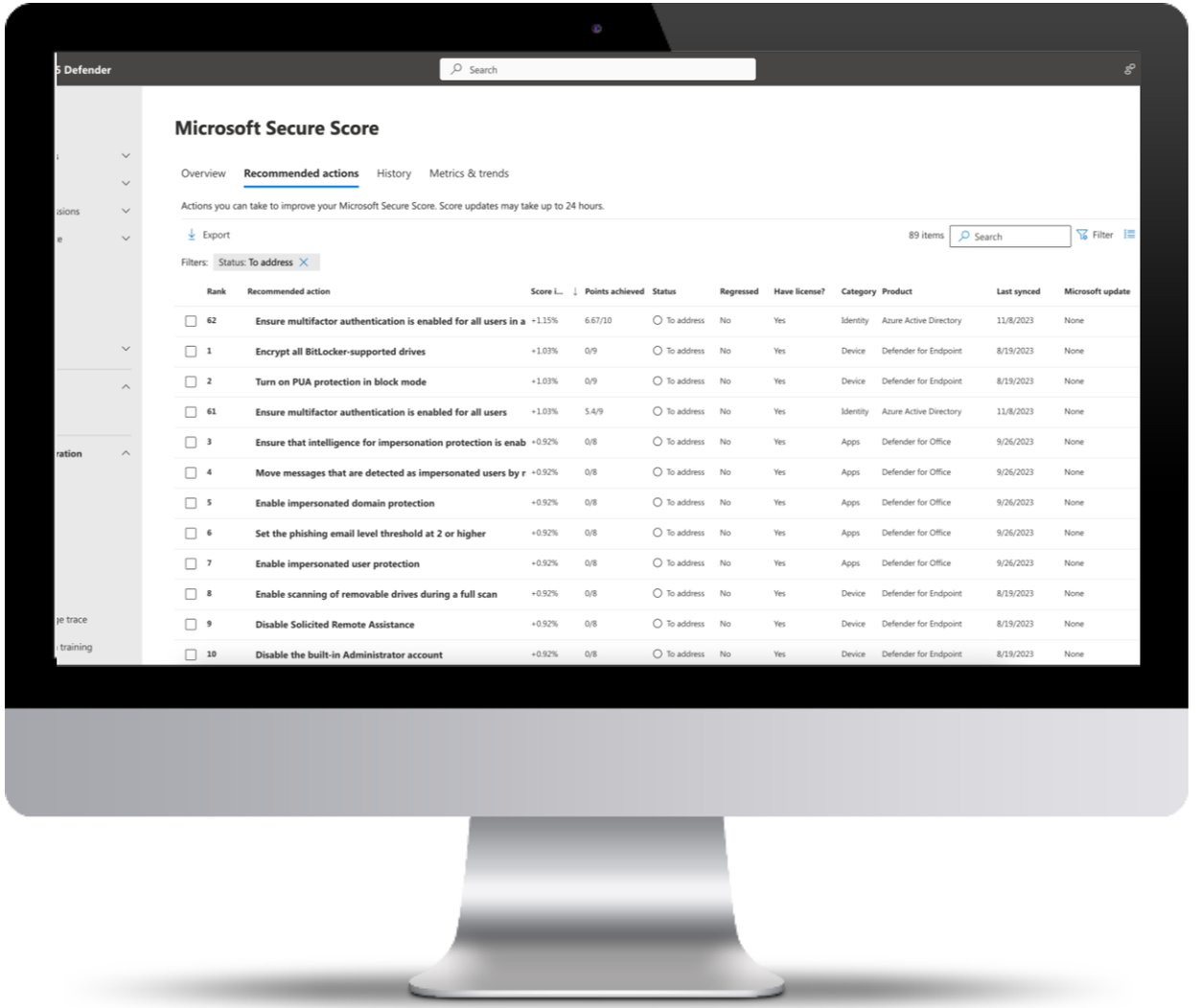
- Scenario:
  - Threat Defense
- Piattaforme coinvolte:
  - Windows
  - macOS
  - iOS/iPadOS
  - Android
- Sezione:
  - Endpoint Security -> Antivirus
  - Devices -> Configuration Profiles
- Strumento musicale:
  - Chitarra (virtuoso)

Microsoft Defender for Endpoint



Quali funzionalità e configurazioni di MDE vengono veicolate attraverso Intune?

- Endpoint Detection and Response
- Antivirus
  - Pianificazione scansioni
  - Aggiornamento firme
  - Esclusioni
  - Tanto altro ☺
- Attack Surface Reduction (ASR) Rules
- Account protection
- Web Protection (iOS e Android)



Piano di hardening

01 Il sensore di MDE analizza le configurazioni di macchina e l'ambiente circostante

02 I dati vengono analizzati dall'intelligenza del cloud Microsoft

03 Viene generato un elenco di azioni raccomandate per aumentare la postura di sicurezza

04 Si distribuiscono le configurazioni per implementare le remediation… con **Intune**!

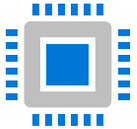
Identità del device

- Scenario:
  - Identità del device
- Piattaforme coinvolte:
  - Windows
  - macOS
  - iOS/iPadOS
  - Android
- Sezione:
  - Devices -> Compliance Policies
  - Devices -> Conditional Access
  - Apps -> App protection policies
- Strumento musicale:
  - Chitarra (ritmica)

Compliance Policy

Configurazioni device

Esempio: richiesta PIN, encryption, ecc..



Caratteristiche OS

Esempio: versione min/max OS, integrità device, ecc…

Sicurezza app installate

Esempio: app installate da fonti sconosciute, ecc…

Livello di minaccia

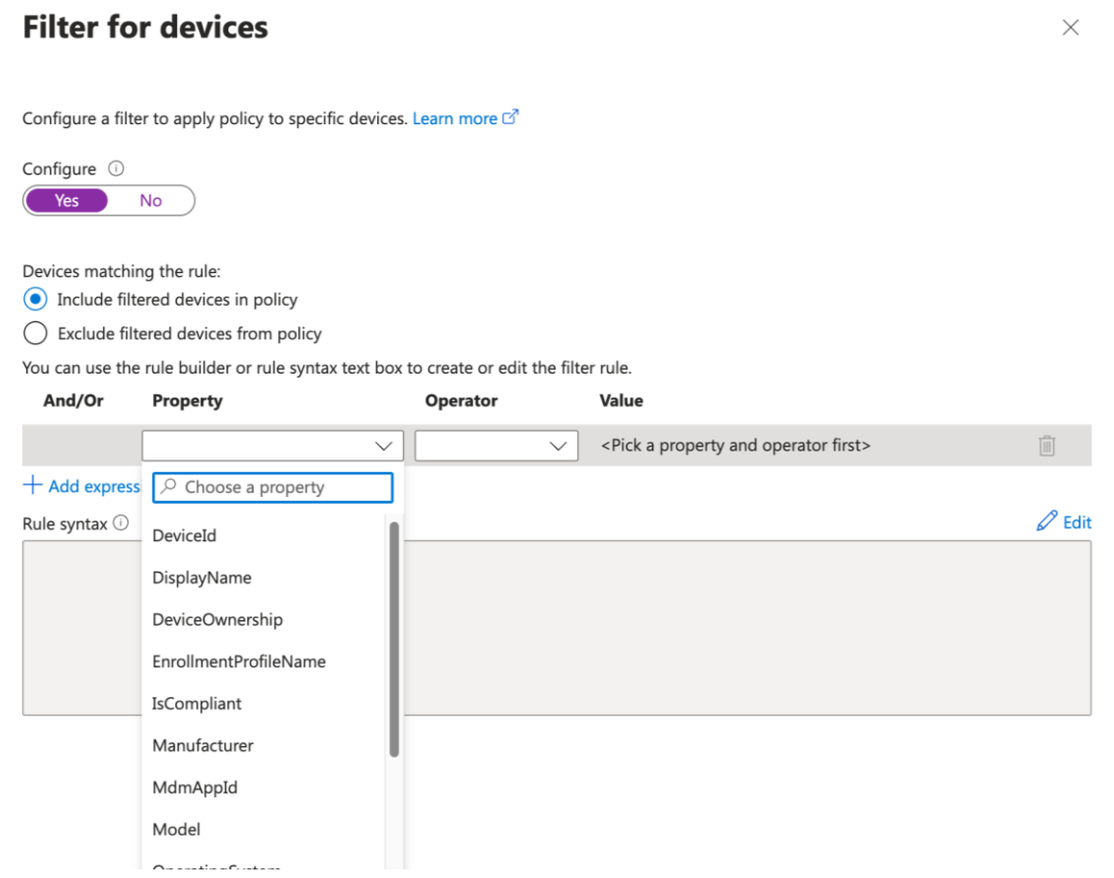
Esempio: livello rischio determinato da MDE

- Regole e impostazioni che un dispositivo deve rispettare per essere considerato **conforme allo standard aziendale**
- Possono essere utilizzate per **monitorare e risolvere** le situazioni di difformità
- Possono essere sfruttate dal servizio di **Conditional Access**

Conditional Access

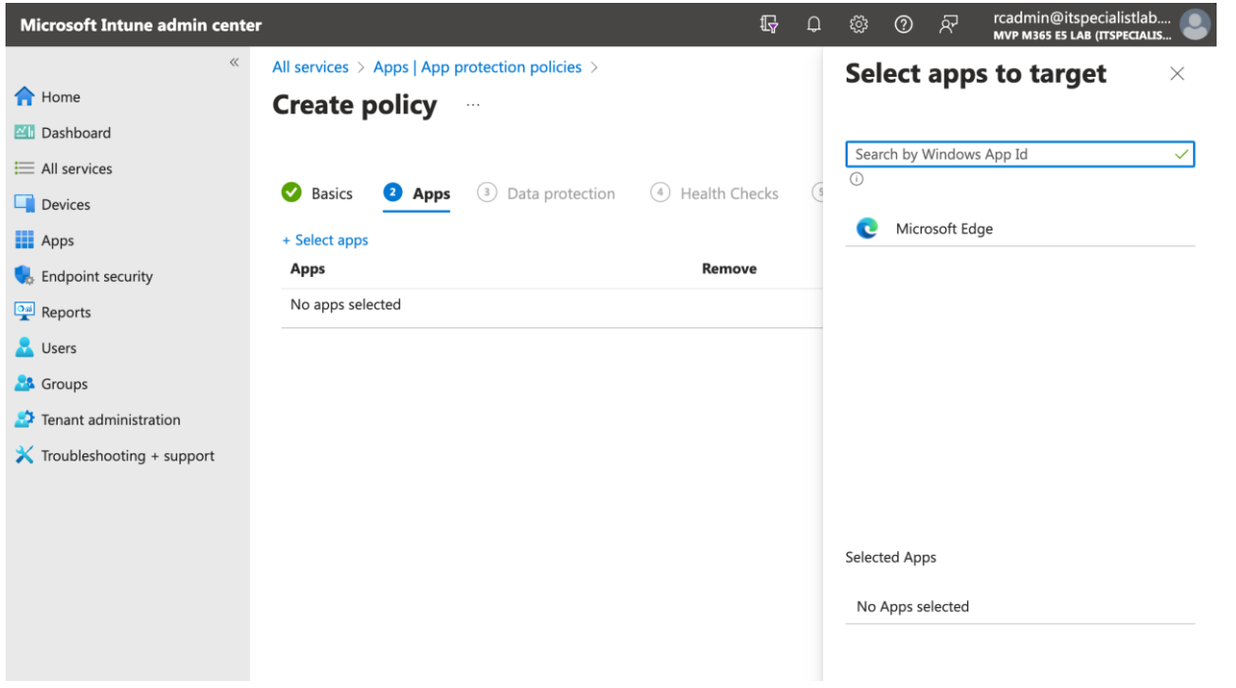
- Come interviene Intune nel Conditional Access oltre alla conformità?
- Filtri dispositivo
  - Possiamo definire dei filtri per includere o escludere dispositivi con specifiche proprietà
  - I filtri possono essere definiti anche tenant-wide dal menu

    Tenant administration -> **Filters**

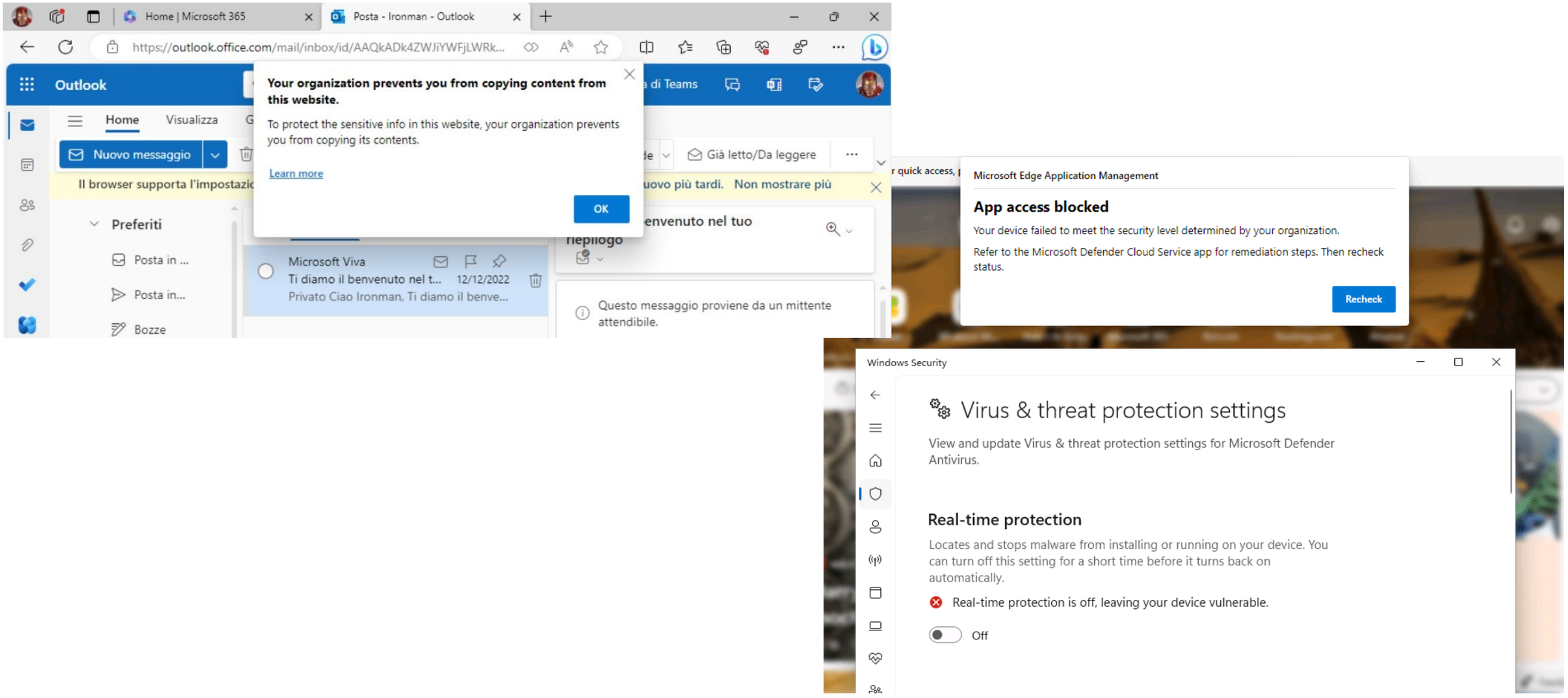


MAM per Windows

- Nuova funzionalità da poco in GA
- Supera alcuni limiti che aveva WIP
- Aiuta a separare in maniera chiara dati utente dai dati lavorativi
- Esperienza MAM simile a quella dei dispositivi mobile
- Il comportamento dell'app dipende esclusivamente dall'identità usata dall'utente



MAM per Windows

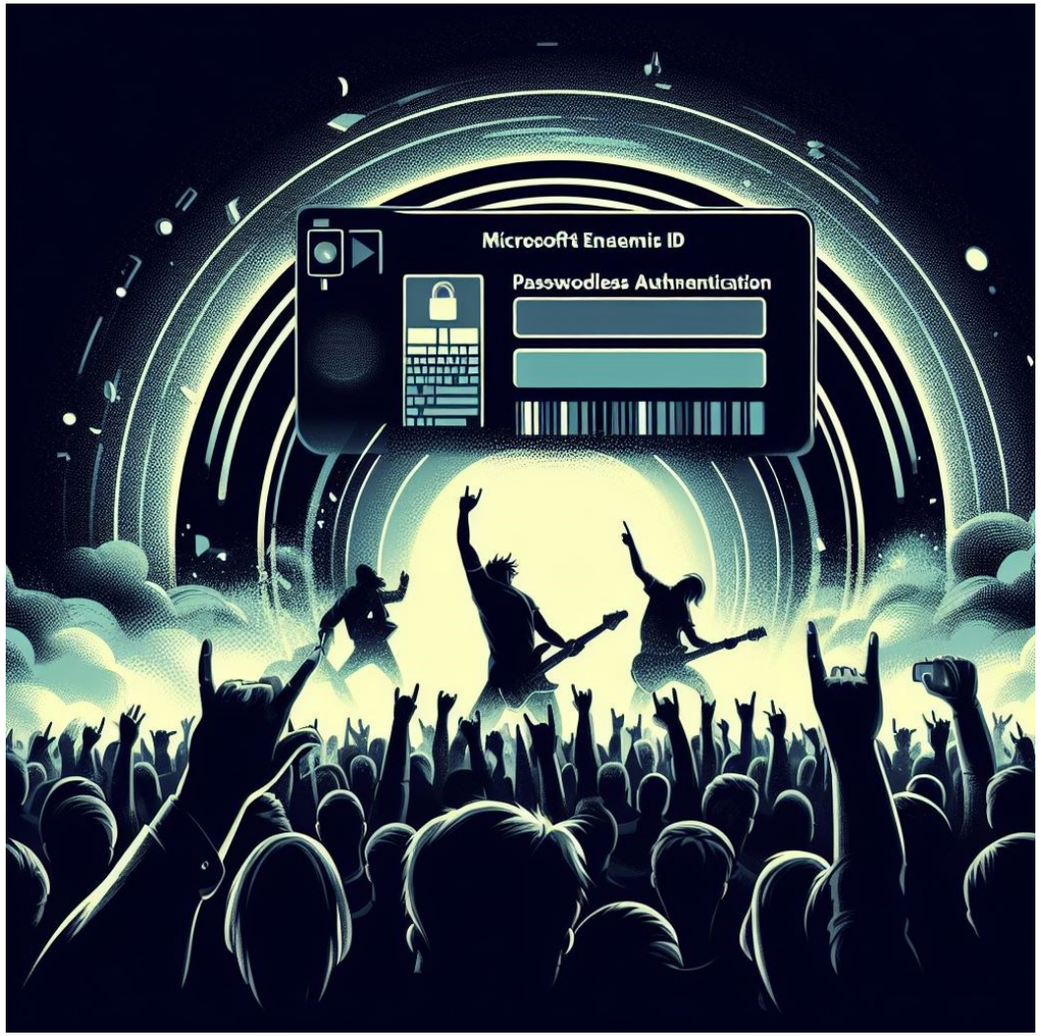


Identità dell'utente

- Scenario:
  - Identità dell'utente
- Piattaforme coinvolte:
  - Windows
- Sezione:
  - Devices -> Configuration Profiles
  - Endpoint Security -> Account Protection
- Strumento musicale:
  - Voce

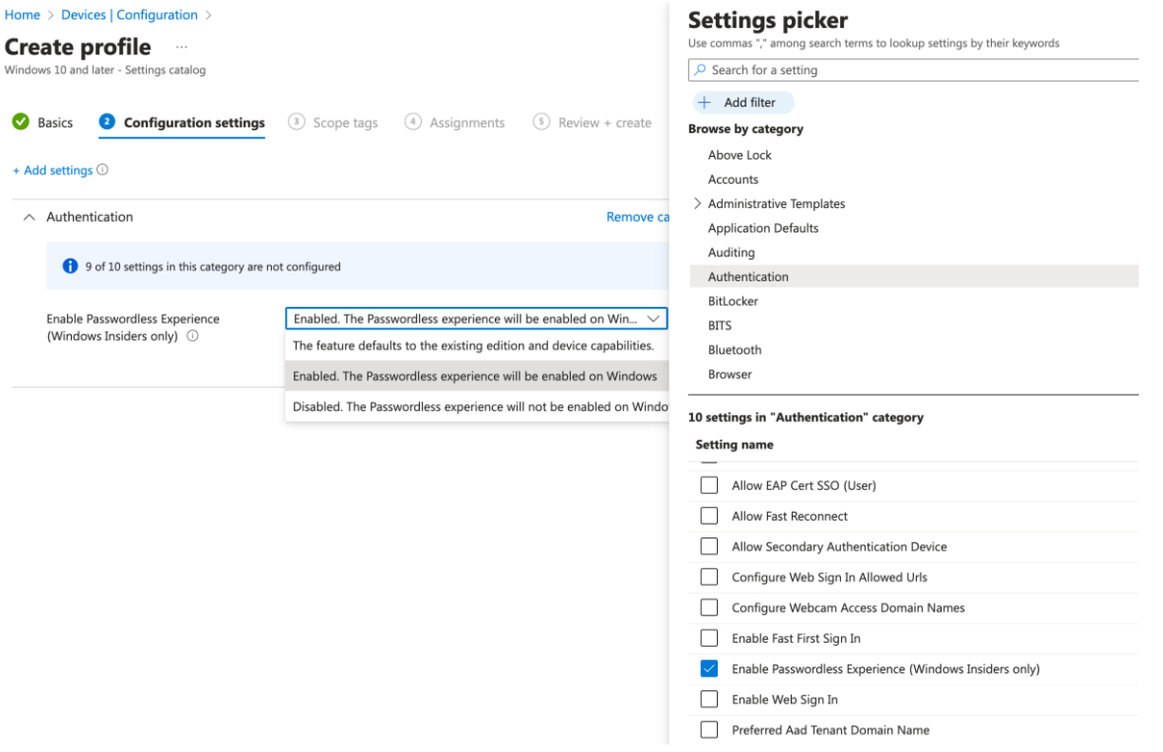
Passwordless

- Quali funzionalità e impostazioni passano da Intune per un'esperienza passwordless?
- Windows Hello for Business
- Abilitazione Web Sign-In (+ TAP)
- Self Service Password Reset da login Windows
- NOVITÀ: Passwordless experience

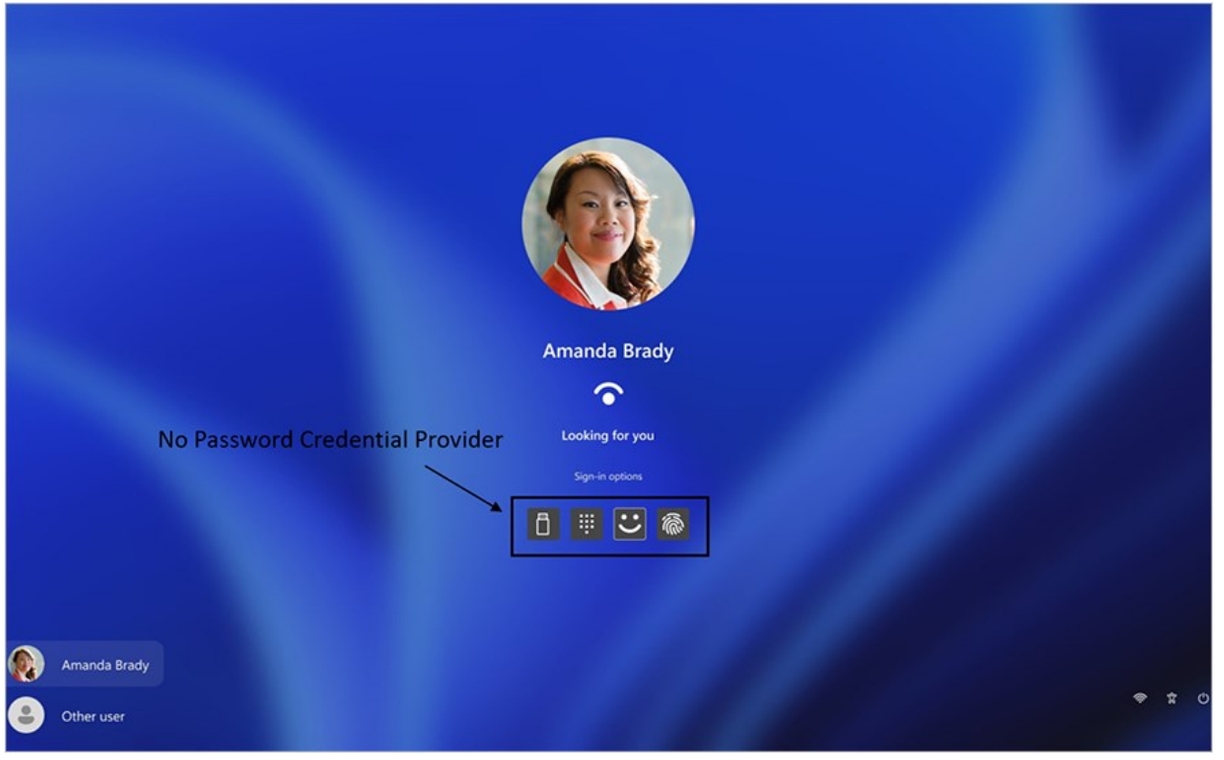


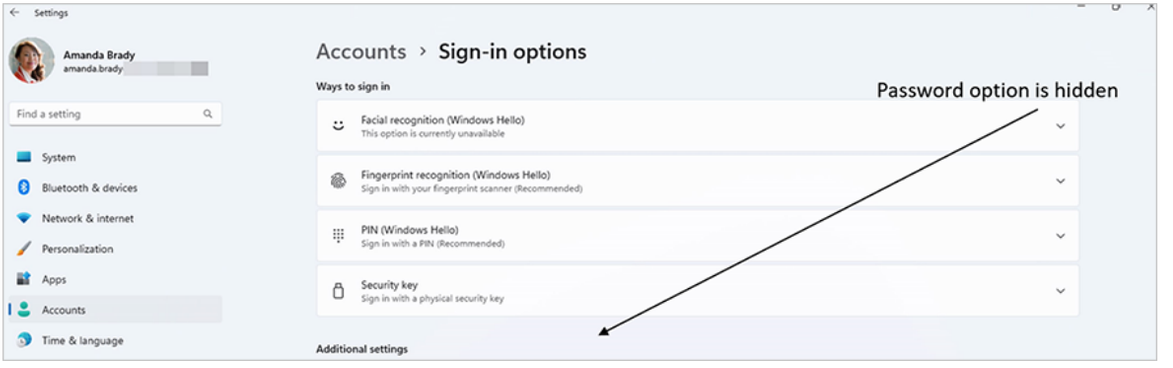
Passwordless Experience

- Gli utenti che accedono con WHfB o una chiave FIDO2:
  - Non possono utilizzare la password sulla schermata di blocco di Windows.
  - Non vengono sollecitati a utilizzare una password durante autenticazioni in sessione (elevazione UAC, gestore password nel browser, ecc.).
  - Non hanno l'opzione "Account > Cambia password" nelle Impostazioni.
- Non impatta account locali
  - Utile se l'admin locale sotto LAPS deve fare help-desk
- È comunque permesso ad un utente di accedere con password quando utilizza l'opzione *Altro utente* nella schermata di blocco.
- Il provider di credenziali della password è nascosto solo per l'ultimo utente che ha effettuato l'accesso con WHfB o una chiave FIDO2
- La Passwordless Experience di Windows non mira a impedire agli utenti di usare le password, ma piuttosto a guidarli ed educarli nel ridurre il suo utilizzo



Passwordless Experience



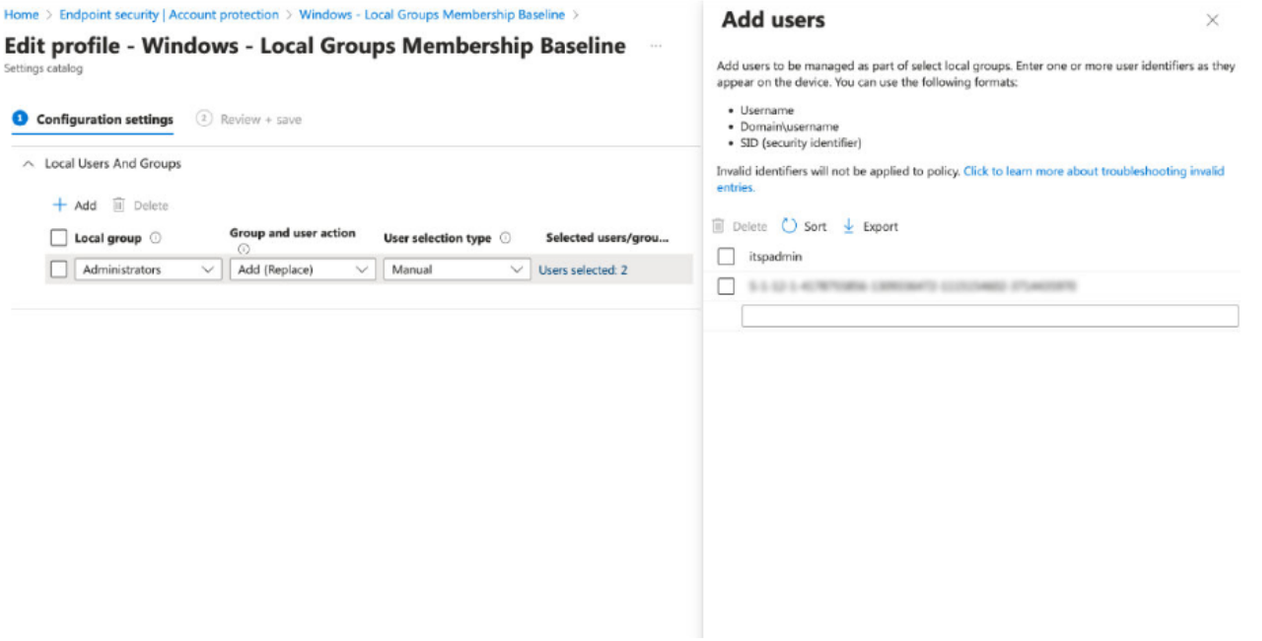


Privilegi Minimi

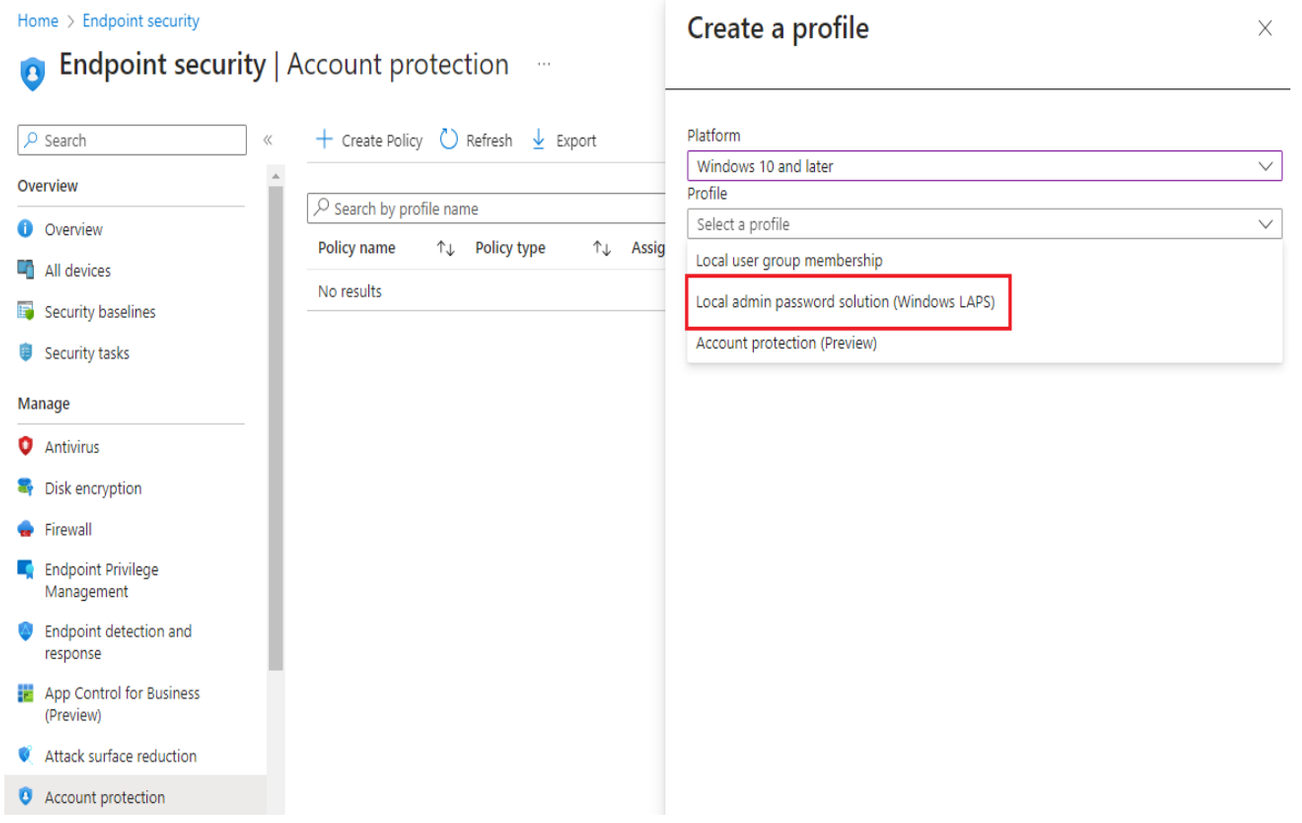
- Scenario:
  - Privilegi Minimi
- Piattaforme coinvolte:
  - Windows
- Sezione:
  - Endpoint Security -> Account protection
  - Endpoint Security -> Endpoint Privilege Management
- Strumento musicale:
  - Basso

Local User Group Policy

- Un utente che joina manualmente il proprio client ad Entra ID, diventa amministratore di macchina
- Inoltre, chi ha ruolo Global Admin o di Entra Joined Device Local Administrator, è amministratore
- Con le **Local User Group Policy** possiamo aggiungere, rimuovere o aggiornare le membership dei gruppi locali di macchina!



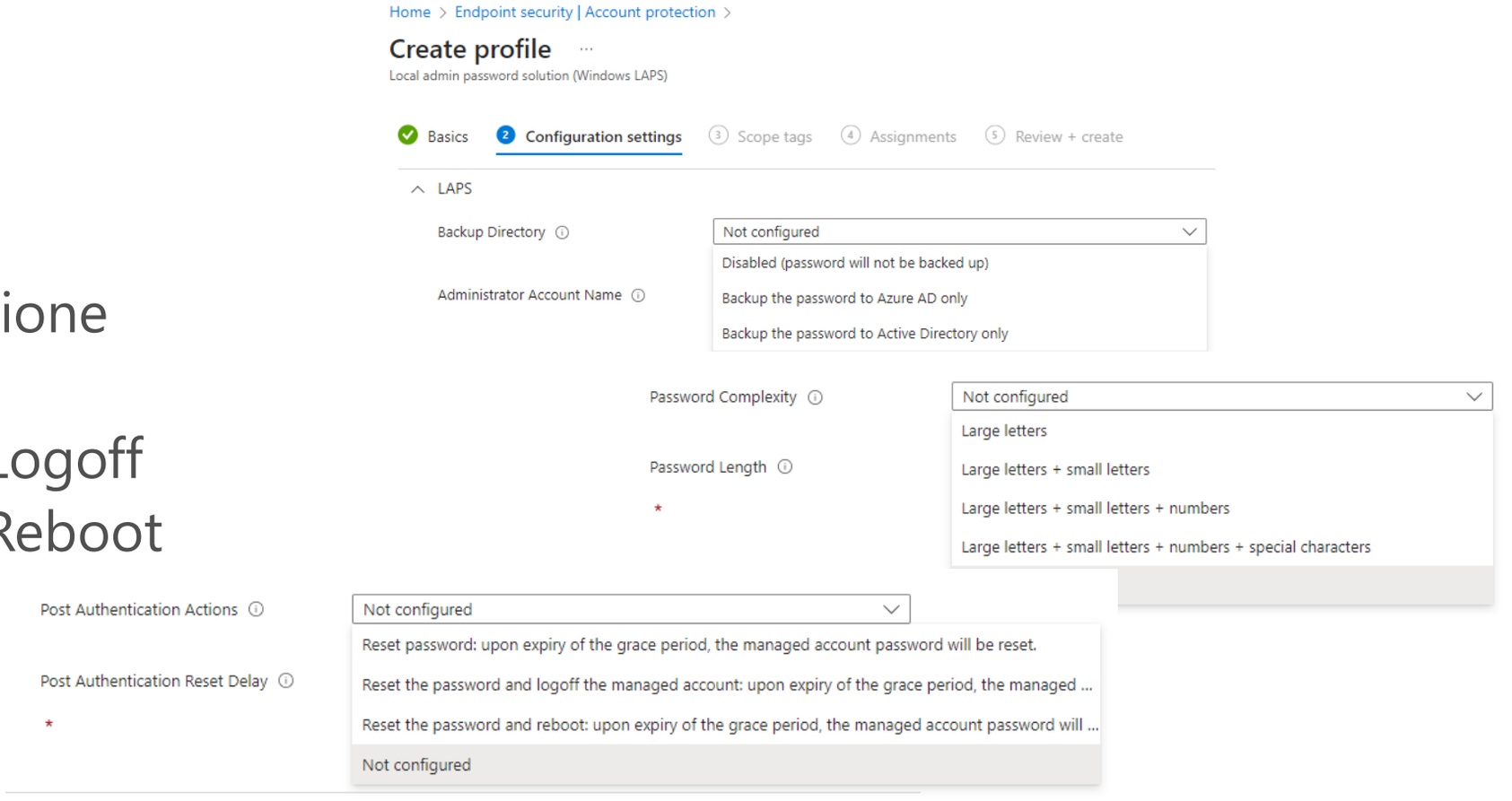
Windows LAPS



- Soluzione di Just in Time (JIT) local admin password
- Le password sono quindi:
  - Uniche per ogni sistema
  - Generate casualmente
  - Memorizzate in Entra ID o in Active Directory
- Architettura basata su:
  - Group Policy Client Extension (AD)
  - Endpoint Security Policy (Intune)

Windows LAPS - configurazione

- Backup password:
  - Azure AD
  - Active Directory
- Complessità password
- Lunghezza password
- Azioni post-autenticazione
  - Reset password
  - Reset password + Logoff
  - Reset password + Reboot



Privilegi minimi - Use Case

Applicazione legacy installata sul device che richiede privilegi elevati per scrittura su folder e/o chiavi di registry di sistema

Privilegi minimi (Soluzioni disponibili)

- Local Admin

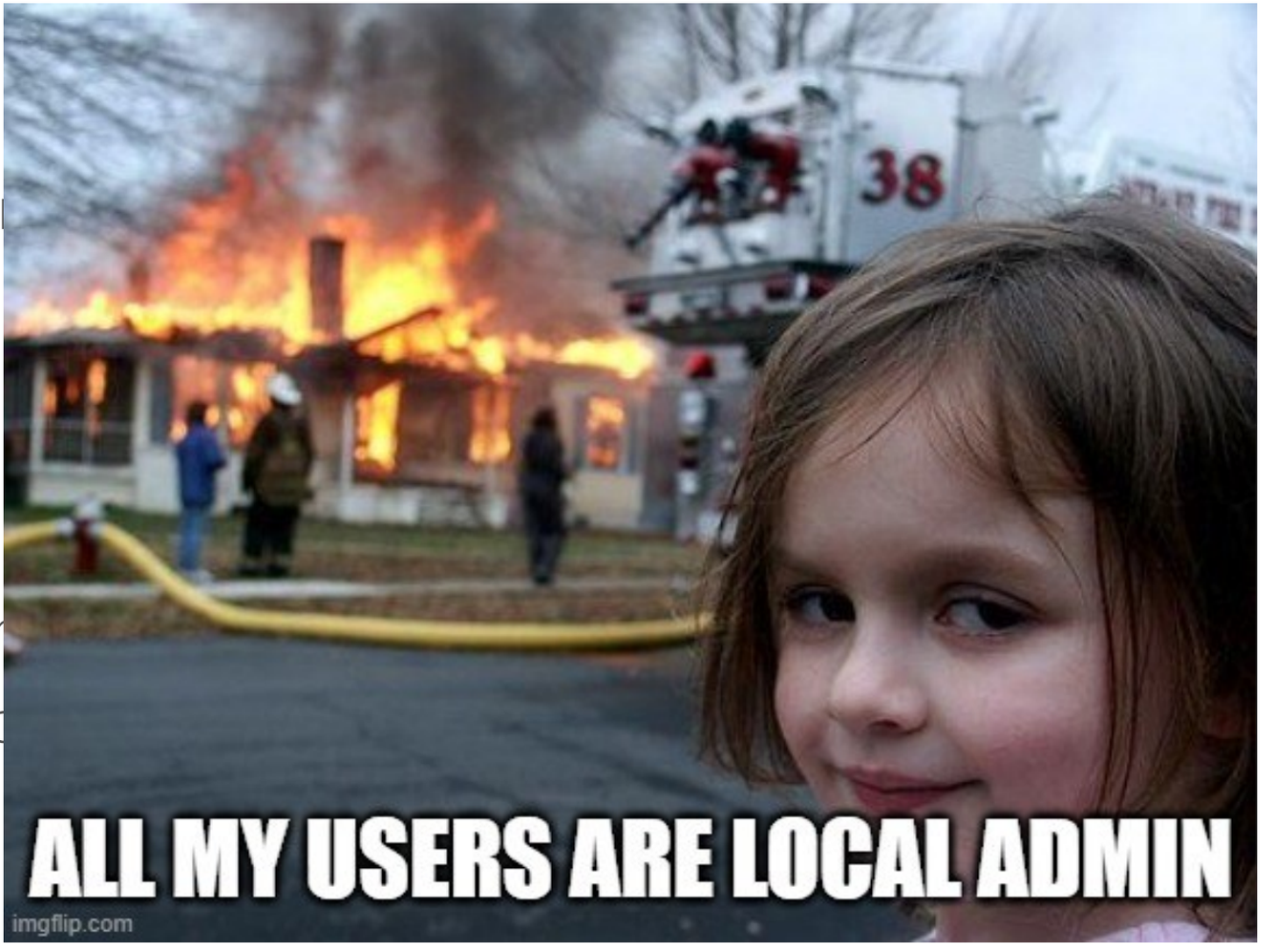
Local Admin

PRO:

- Massima (troppa) autonomia agli ute

CONTRO:

- Elevata esposiz compromissior
- Possibilità di modifiche a basso livell
- Installazione/esecuzione di software autorizzato



Privilegi minimi (Soluzioni disponibili)

- Local Admin

- Windows LAPS

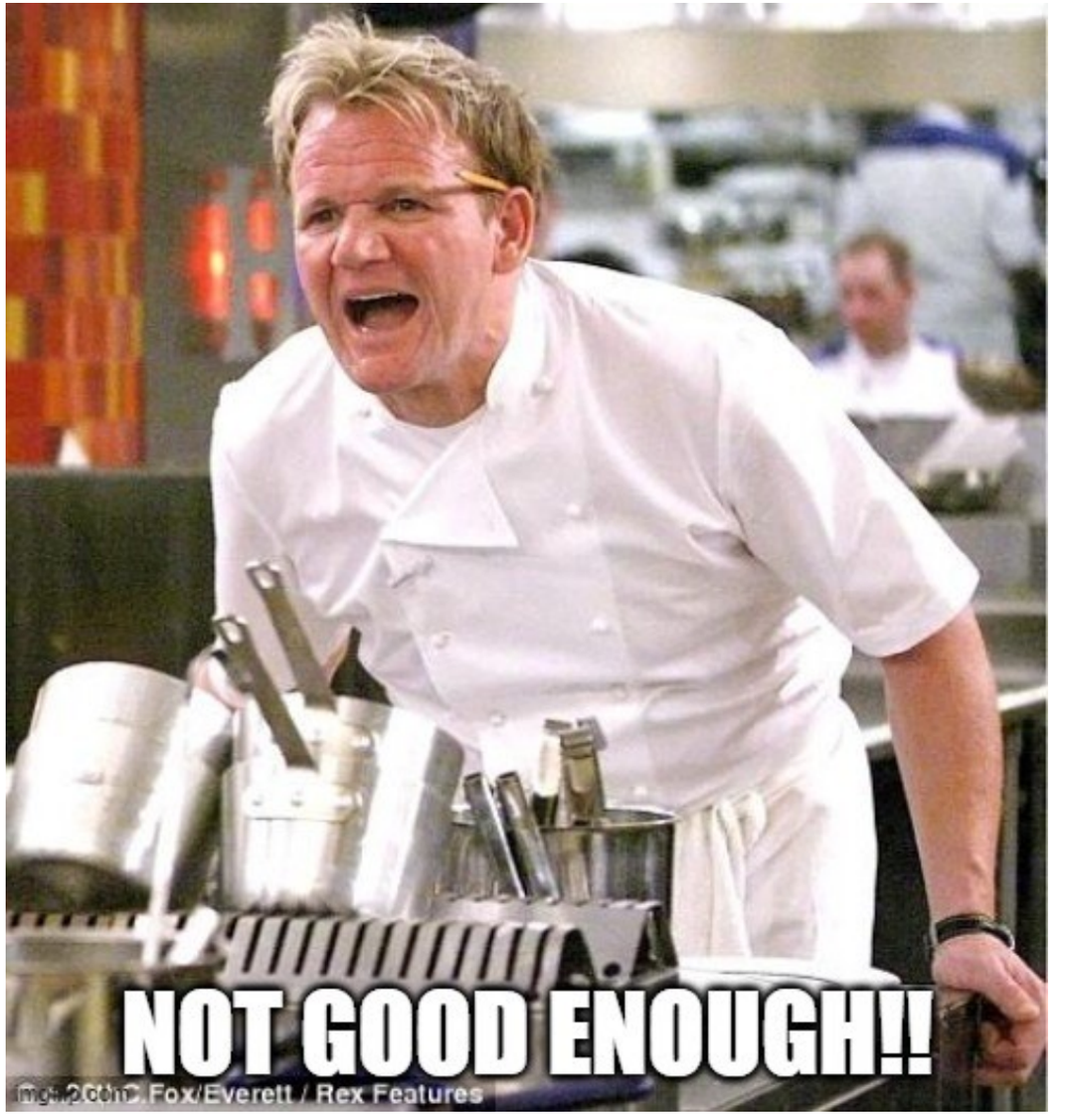
Windows LAPS

PRO:

- Processo di autorizzazione controllato
- Rotazione della password admin locale

CONTRO:

- Necessario [illegible] IT
- Possibilità di esecuzione di qualsiasi processo
- Effort di implementazione su AD *



Privilegi minimi (Soluzioni disponibili)

- Local Admin
- Windows LAPS
- Endpoint Privilege Management

Endpoint Privilege Management

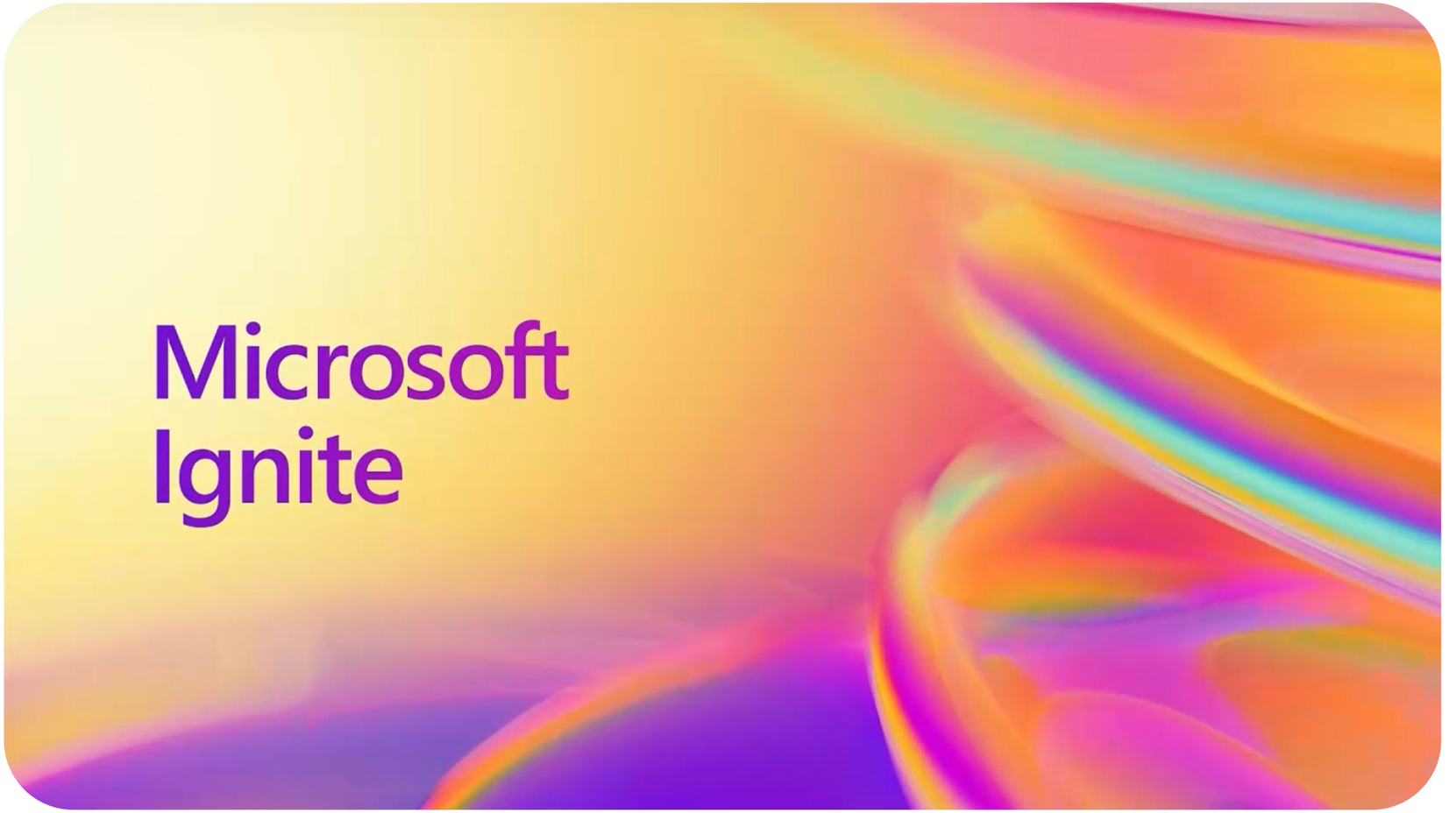
PRO:

- Processo di autorizzazione controllato
- Possibilità di e di specifici processi co
- Ridotto co T per l'esecuzion
- "Integrato" n erativo

CONTRO:

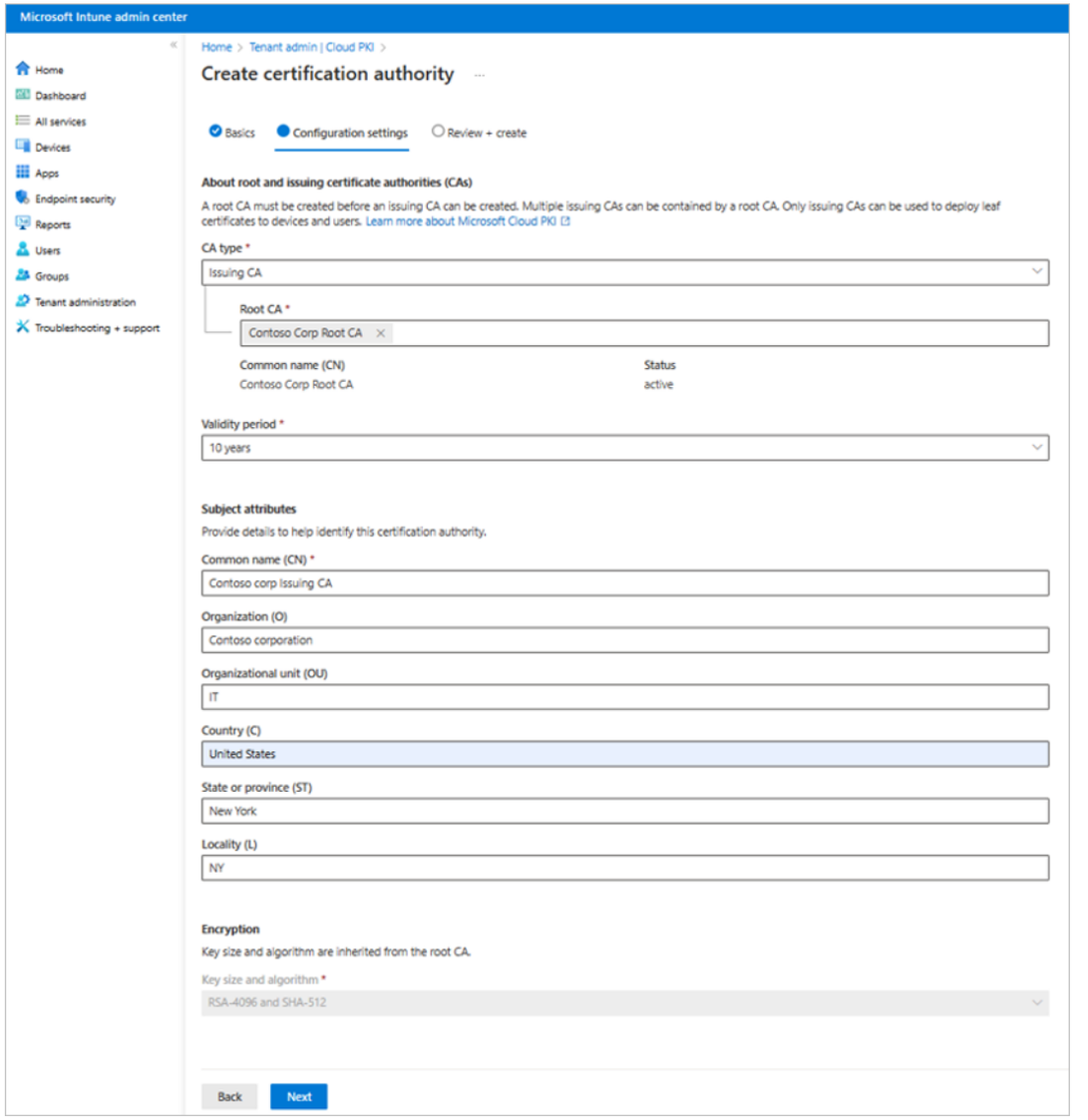
- Definizione preventiva delle regole

What's New Ignite 2023



Microsoft Cloud PKI

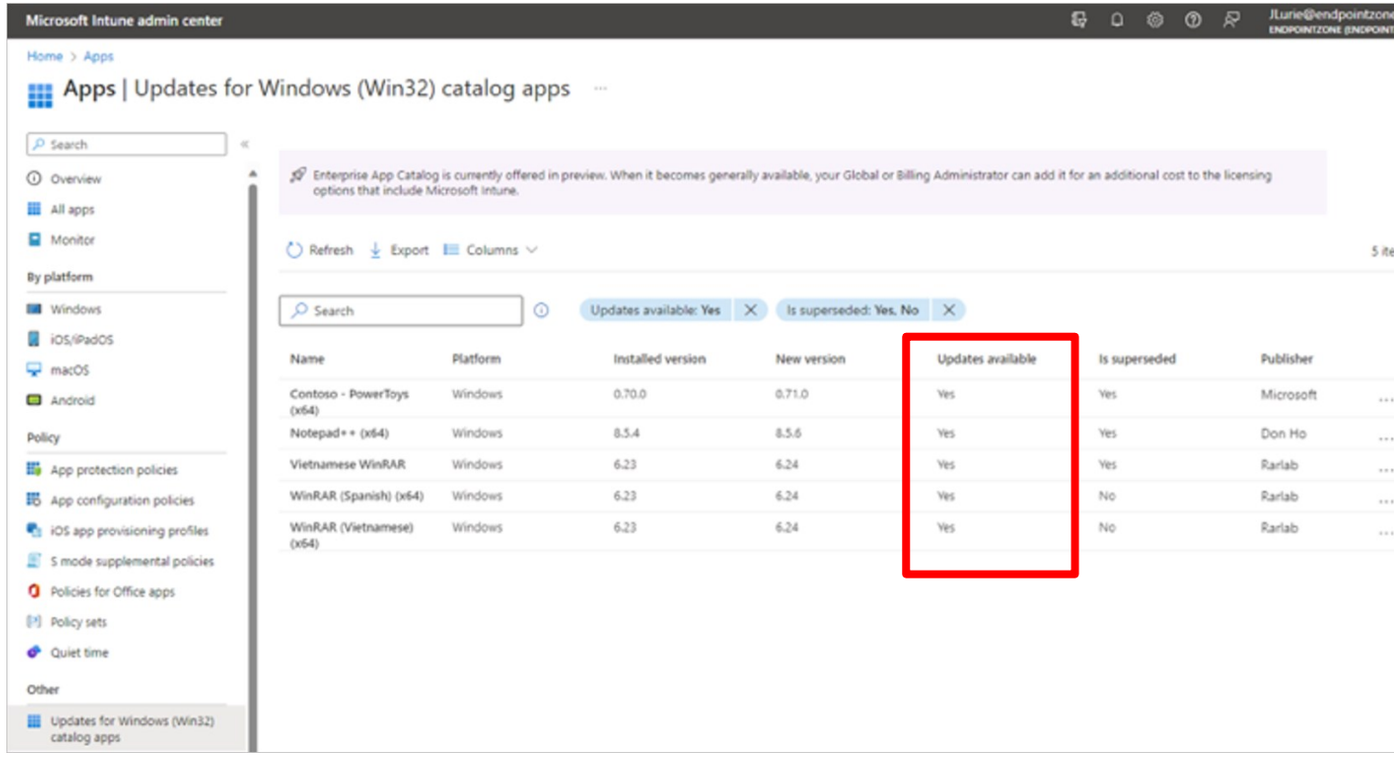
- Cloud-based Public key infrastructure (PKI)
- Permette di semplificare la gestione dei certificati:
  - Rimozione dei server on-premise
  - Possibilità di rilascio certificati su multi-piattaforma (Windows, iOS, macOS, Android)
  - Riduzione costi legati a servizi come Network Device Enrollment Service (NDES) e reverse proxy



Enterprise App Management

- Il ritardo nell'applicazione delle patch e nell'aggiornamento delle applicazioni è una delle principali vulnerabilità a cui sono esposte le aziende

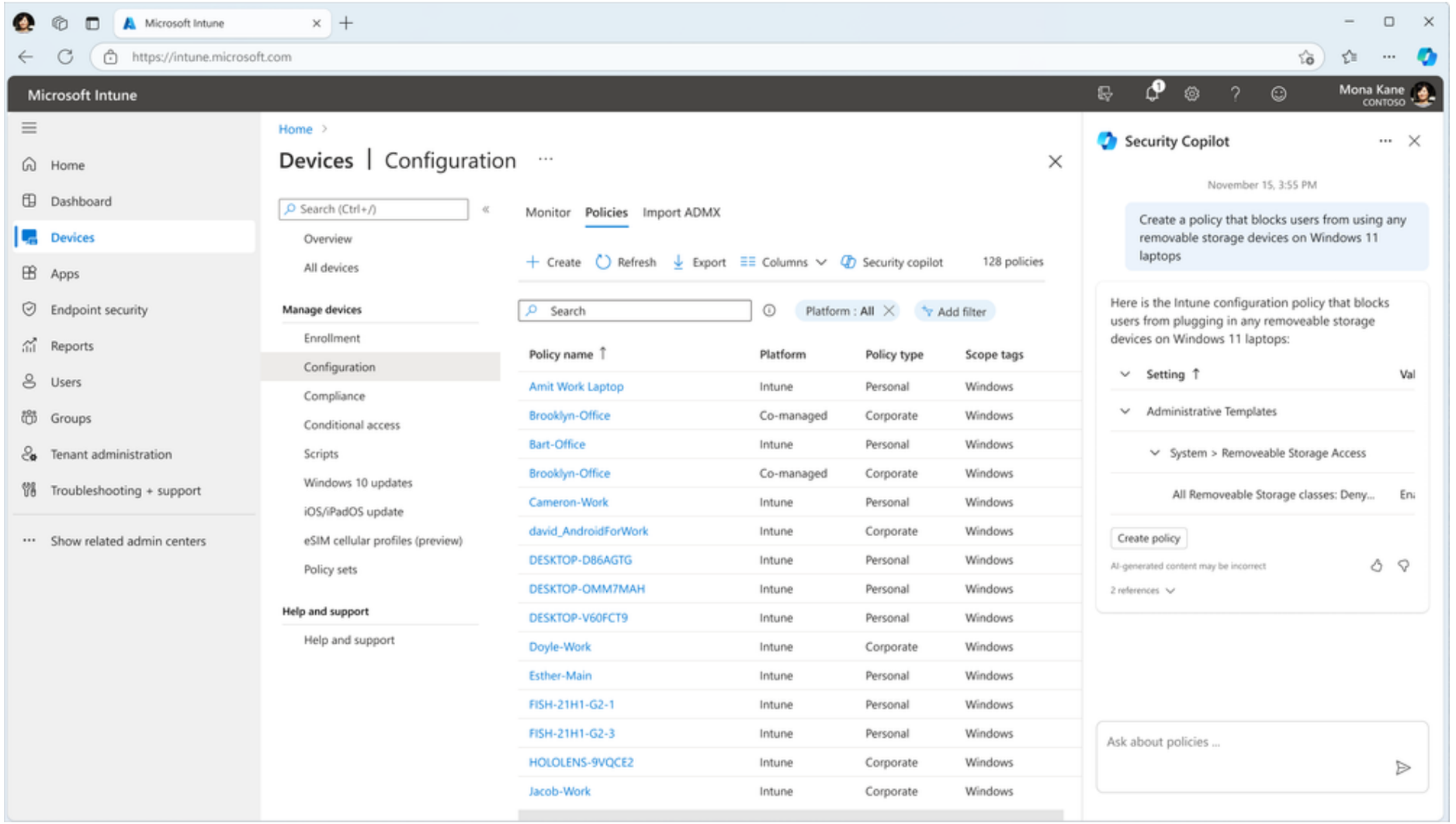
- Semplifica il ciclo di vita della gestione delle applicazioni
- Riduce l'effort da parte degli IT Admin nella creazione e nell'aggiornamento delle app



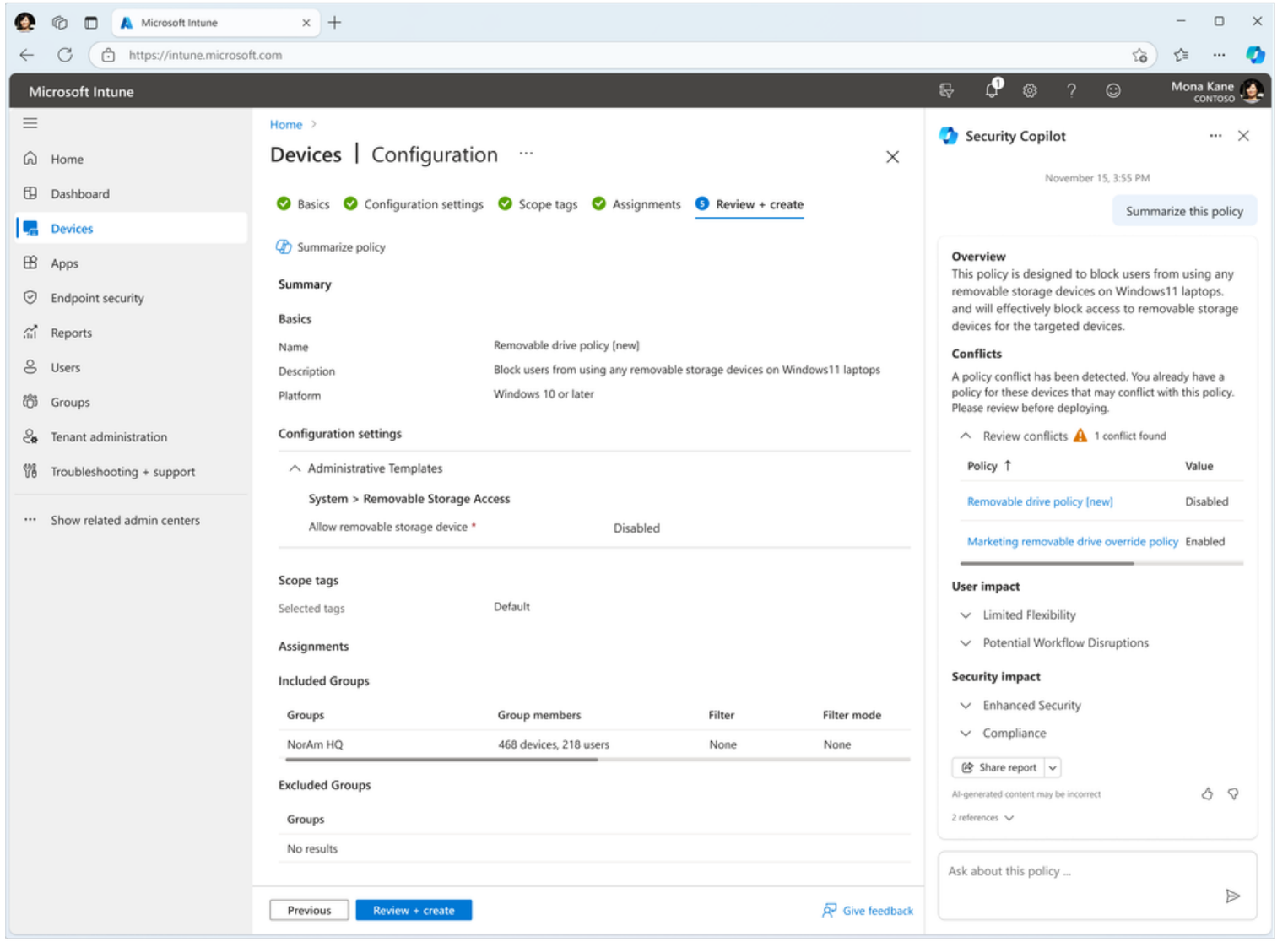
Security Copilot + Intune

- Security Copilot è una piattaforma basata su cloud AI che offre un'esperienza basata su linguaggio naturale
- Può aiutare i professionisti della sicurezza in diversi scenari: incident response, threat hunting e raccolta di informazioni
- Come funzionerà insieme ad Intune?
  - Prompt specifici innescheranno la cooperazione con Intune
  - Nelle prossima slide alcuni esempi

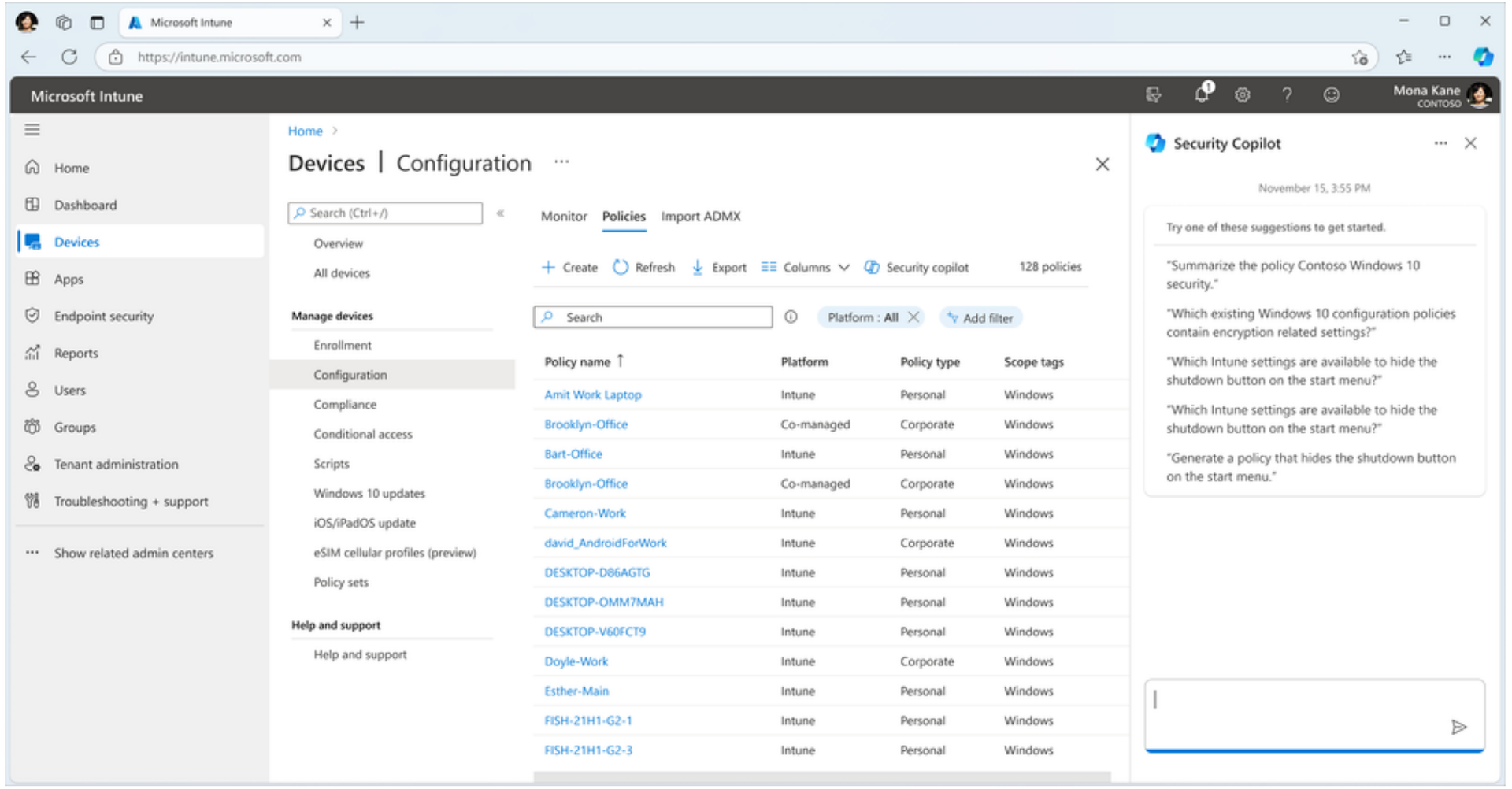
Security Copilot + Intune (Policy)



Security Copilot + Intune (Policy)



Security Copilot + Intune (Remediation)




SIGNORI
E' STATO UN ONORE SUONARE CON VOI
imgflip.com

Seguiteci!

Microsoft Security Italian User Group

Microsoft Intune Italian User Group

AVD & W365 Italian User Group

ITSpecialist.cloud

ICT POWER.IT

Microsoft

Grazie

Riccardo Corna

MVP Security – Senior Consultant

@riccardocorna

/riccardocorna