



MICROSOFT
INTUNIE









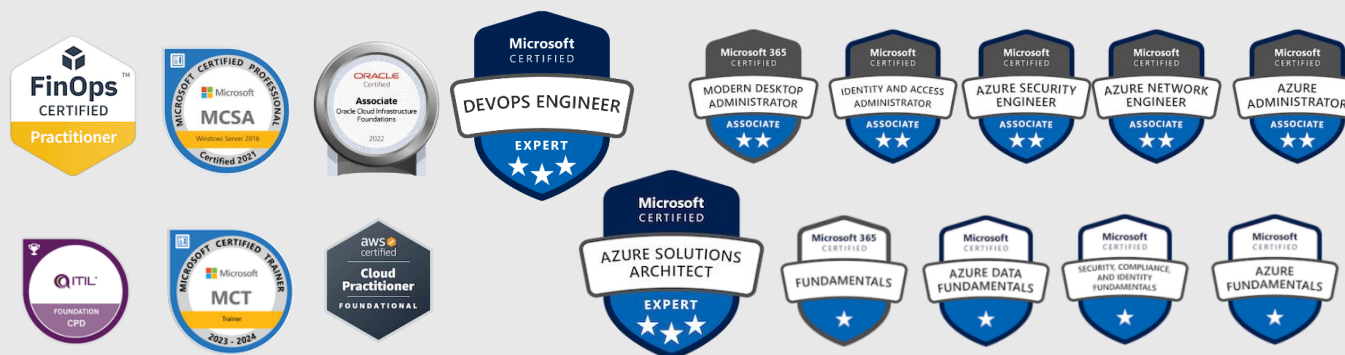
Uma Visão Abrangente do Gerenciamento Moderno de Endpoints



WHOIAM

 Rafael
Ferreira

- 10+ anos de XP 
- Senior DevOps Engineer @ CI&T
- Algumas Certificações técnicas
- Ciências da Computação 
- Geek, Gamer 
- Filmes  séries 
- Pai de uma golden 

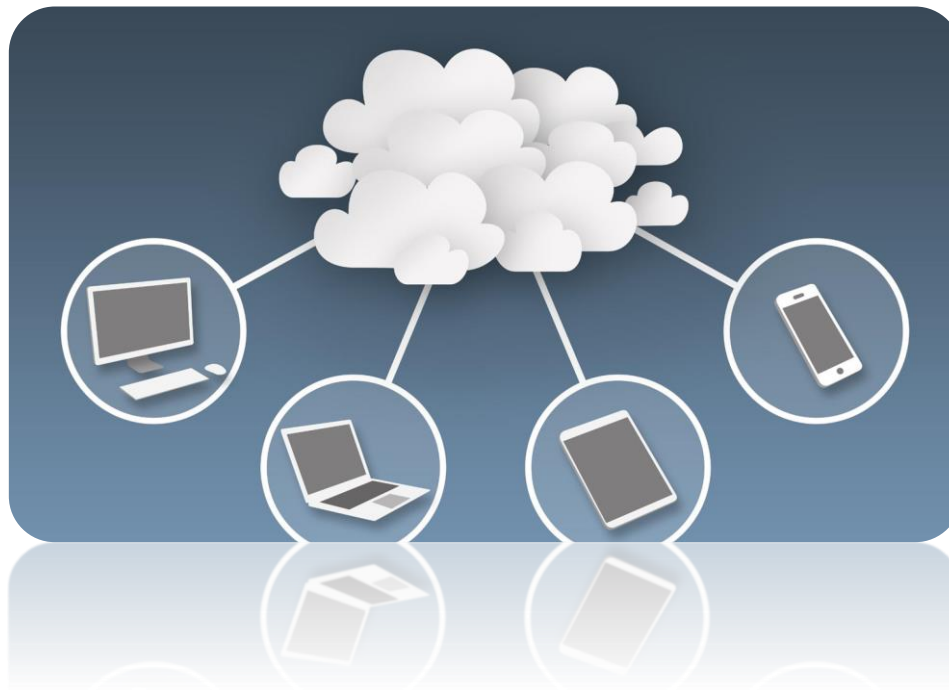


What is Microsoft Intune?

O Intune é um serviço baseado em nuvem que fornece recursos de gerenciamento de dispositivos, permitindo que você gerencie e proteja seus dispositivos, registre novos dispositivos, defina políticas e configurações e garanta a conformidade do dispositivo



Baseado em Nuvem?



SaaS?

Software as a Service



Gerenciadores de Endpoint

- NinjaOne Endpoint Management
- Citrix Endpoint Management
- Microsoft Intune
- ManageEngine Endpoint Central
- Atera





Como funciona o Microsoft Intune?



Registro de dispositivo

Os usuários registram os dispositivos no Intune e os administradores gerenciam os dispositivos e os aplicativos instalados neles.

Gerenciamento de políticas

O Intune permite que os administradores criem políticas que são automaticamente aplicadas em todos os dispositivos registrados, incluindo gerenciamento de dispositivos e aplicativos.





Microsoft Intune

Microsoft Intune admin center

Synchronize users from Microsoft 365



Synchronize users from on-premises to Microsoft Entra



Import via CSV



User- and service-based authentication



Policies

- Security rules
- Application protection
- Device access
- Device configuration
- Compliance policies
- Conditional access
- And more

Security admins



Dedicated kiosk devices



Zebra devices



End users



Device sign-in

User affinity links user with device and applies policies based on group membership

Security admins



Dedicated kiosk devices



Zebra devices



End users



Visão Geral do Microsoft Intune

Gerenciamento Unificado de Dispositivos:

- Plataforma única para dispositivos móveis, desktops e virtuais.
- Administração centralizada simplificada.

Gerenciamento de Aplicativos:

- Implantação remota de aplicativos.
- Atualizações sem intervenção do usuário.

Gerenciamento de Dispositivos:

- Atualização de políticas de dispositivo.
- Implantação de atualizações de software.
- Monitoramento da integridade do dispositivo.



- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Welcome to the fresh look for Intune

Explore the updated homepage. Inside is still the familiar unified management solution for all your endpoints.

[Give us your feedback](#)



Status

- Devices not in compliance: **1**
- Configuration policies with error or conflict: **1**
- Client app install failure: **0**
- Connector errors: **1**
- Service health: **Healthy**
- Account status: **Active**

Spotlight



Introducing the Microsoft Intune Suite

The unified solution includes Remote Help, Endpoint Privilege Management, AI-powered advanced analytics, and more.

[Explore](#)



Increase productivity with Cloud PCs

Easily provision Windows 365 Cloud PCs and manage them alongside your physical devices.

[Explore](#)

Get more out of Intune



Microsoft Intune Blog

Discuss best practices, get the latest news, and engage in conversations around Microsoft Intune.

What's new in Microsoft Intune July 2024

Microsoft recognized as a Leader in UEM Software 2024 IDC MarketScape reports

What's new in Microsoft Intune June 2024



Intune Customer Success

Get the deep technical knowledge to help you be successful using Intune.

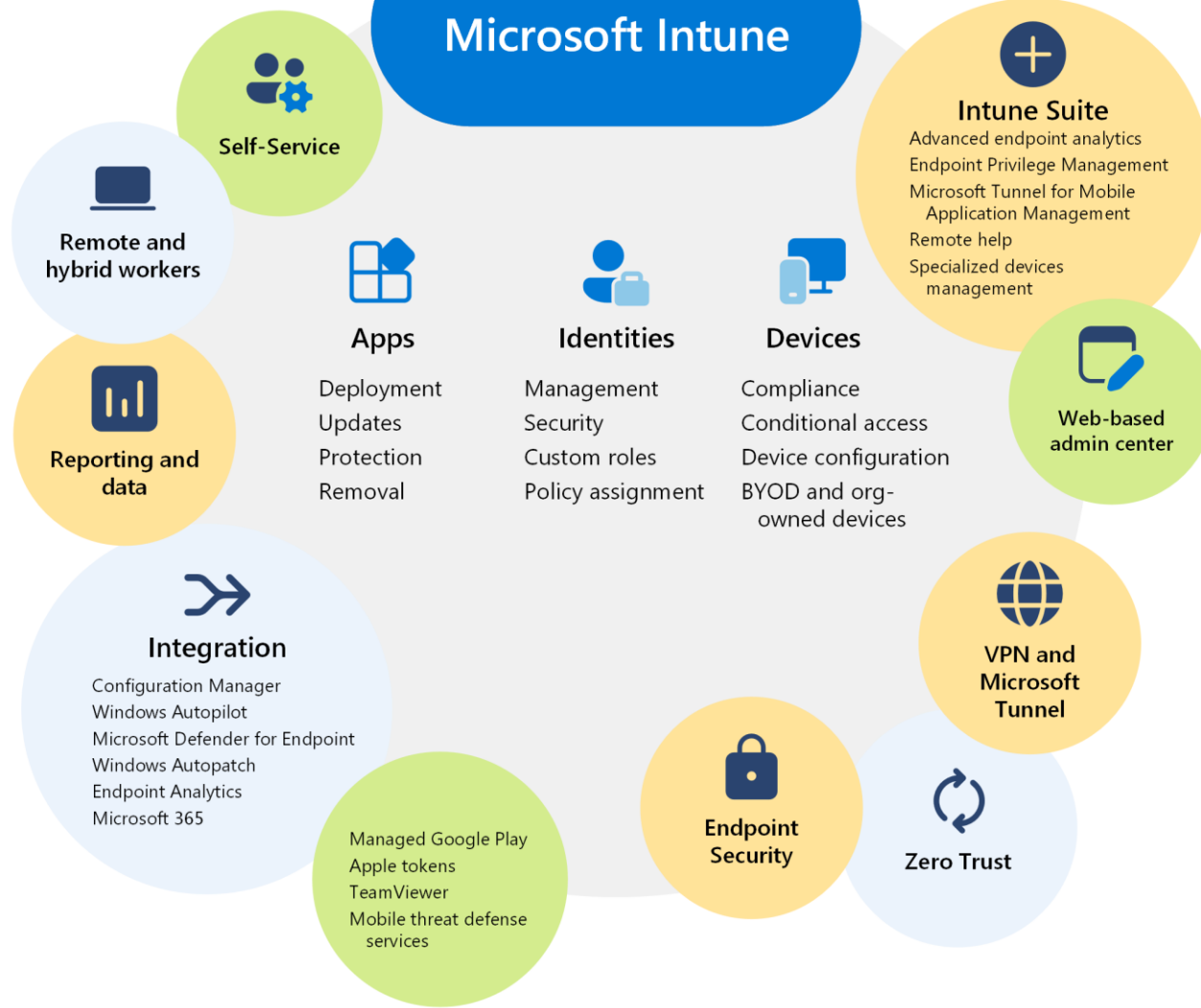
Use JIT registration and JIT compliance remediation for all your iOS/iPadOS enrollments

New Recovery Tool to help with CrowdStrike issue impacting Windows endpoints

New permission prompt to improve macOS notification experience for users when using



Microsoft Intune





MDM vs MAM



MDM (GERENCIAMENTO DE DISPOSITIVOS MÓVEIS): PERMITE O CONTROLE ADMINISTRATIVO COMPLETO SOBRE DISPOSITIVOS CORPORATIVOS.



MAM (GERENCIAMENTO DE APLICATIVOS MÓVEIS): PERMITE O CONTROLE ADMINISTRATIVO BASEADO EM APLICATIVOS PARA PROTEGER DADOS CORPORATIVOS.

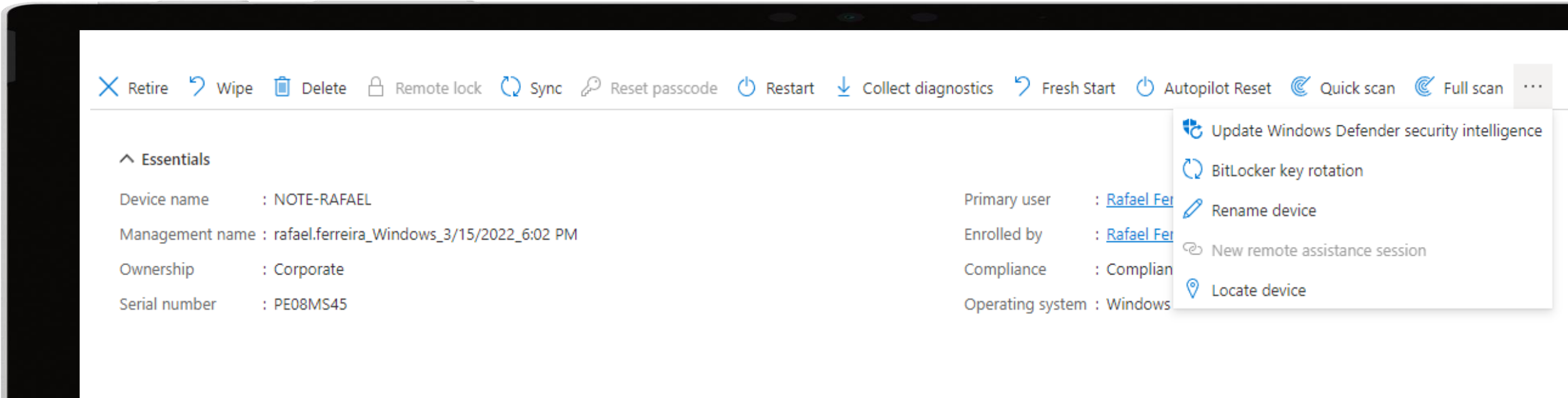


MDM

No Intune, podemos controlar o dispositivo com base no MDM: Gerenciamento de Dispositivos Móveis.

Por exemplo, um dispositivo corporativo de usuários que trabalham em home office.

O Gerenciamento de Dispositivos Móveis fornece ao administrador controle, limpeza, reinicialização, coleta diagnósticos, renomeação ou localização do dispositivo, como você pode ver abaixo:



The screenshot displays the Microsoft Intune MDM console interface. At the top, a horizontal toolbar contains various management actions: Retire, Wipe, Delete, Remote lock, Sync, Reset passcode, Restart, Collect diagnostics, Fresh Start, Autopilot Reset, Quick scan, and Full scan. Below this toolbar, the 'Essentials' section is expanded, showing device details for a device named 'NOTE-RAFAEL'. The details are organized into two columns:

Device name	: NOTE-RAFAEL	Primary user	: Rafael Fer
Management name	: raphael.ferreira_Windows_3/15/2022_6:02 PM	Enrolled by	: Rafael Fer
Ownership	: Corporate	Compliance	: Compliant
Serial number	: PE08MS45	Operating system	: Windows

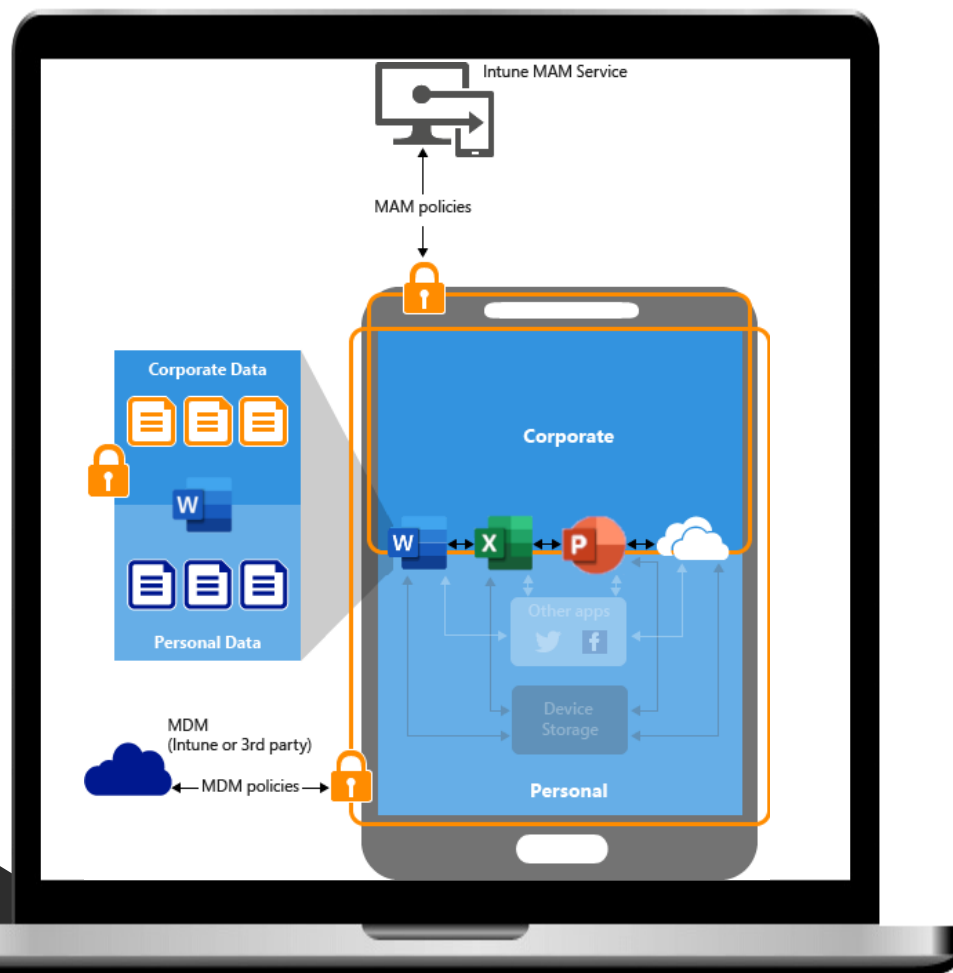
To the right of the device details, a context menu is open, listing several management actions:

- Update Windows Defender security intelligence
- BitLocker key rotation
- Rename device
- New remote assistance session
- Locate device



MAM

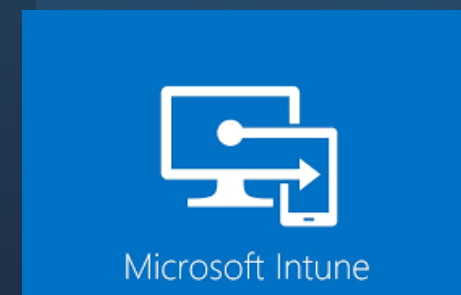
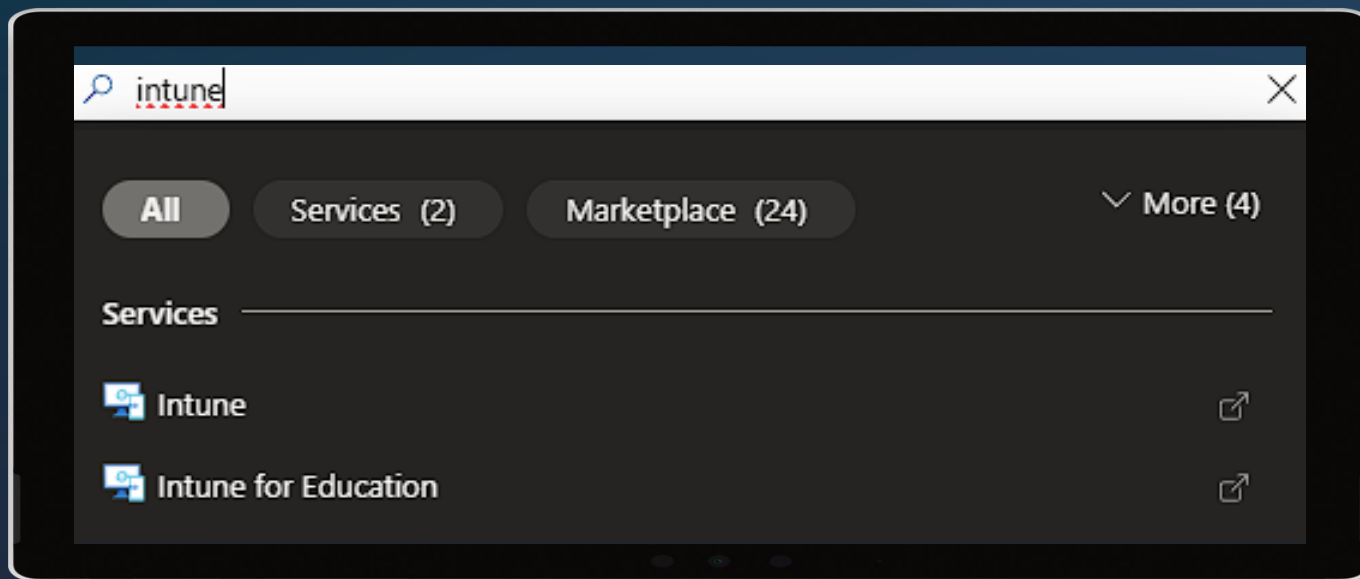
E temos um nível MAM: Mobile Application Management
O Gerenciamento de Aplicativos Móveis fornece o controle de administrador do dispositivo? NÃO!



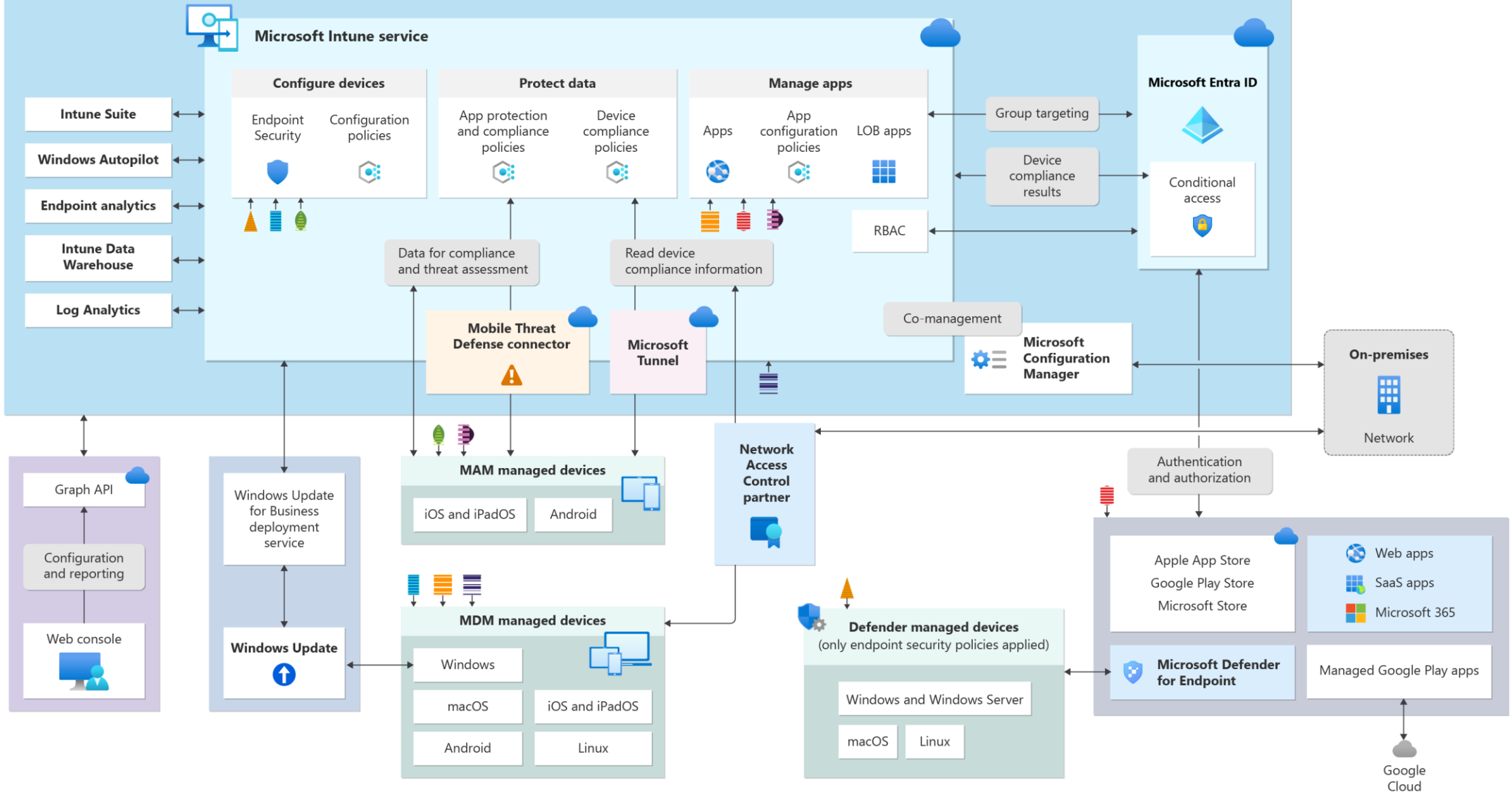
O Gerenciamento de Aplicativos Móveis permite que o administrador controle um aplicativo baseado em níveis. Proteja os dados corporativos, e-mails e informações do cliente

Microsoft Intune

O Microsoft Intune no passado fazia parte do portal Azure, mas ficou tão poderoso que, evoluiu e hoje existe um portal e tornou-se um produto dos produtos mais conhecidos da Microsoft no assunto de Segur.



Microsoft Intune product family



Falando de SEGURANÇA



SEGURANÇA ACIMA DE TUDO



Single Sign-On





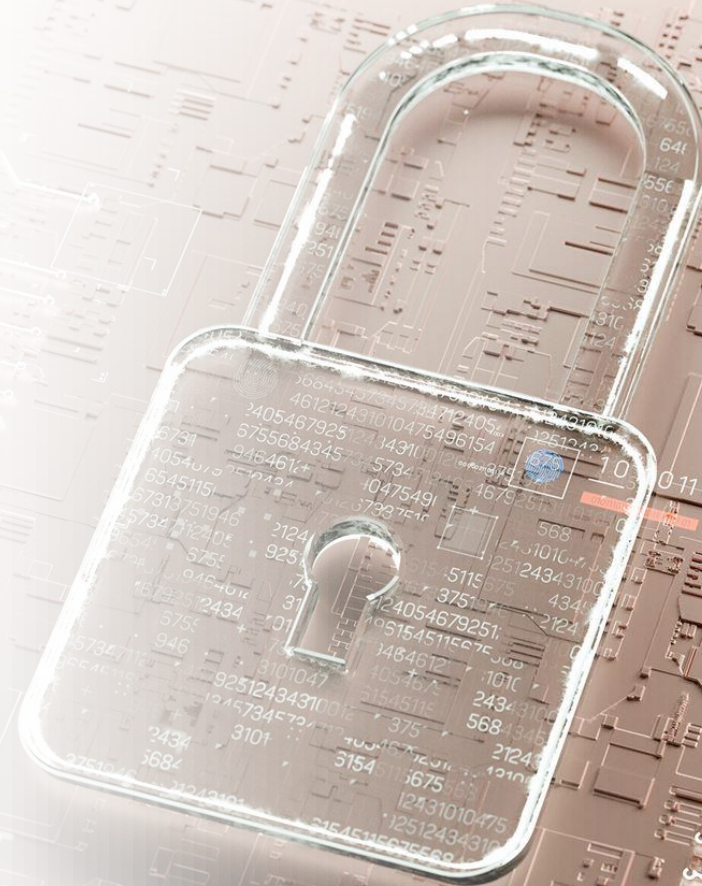
Políticas de acesso condicional



Wipe

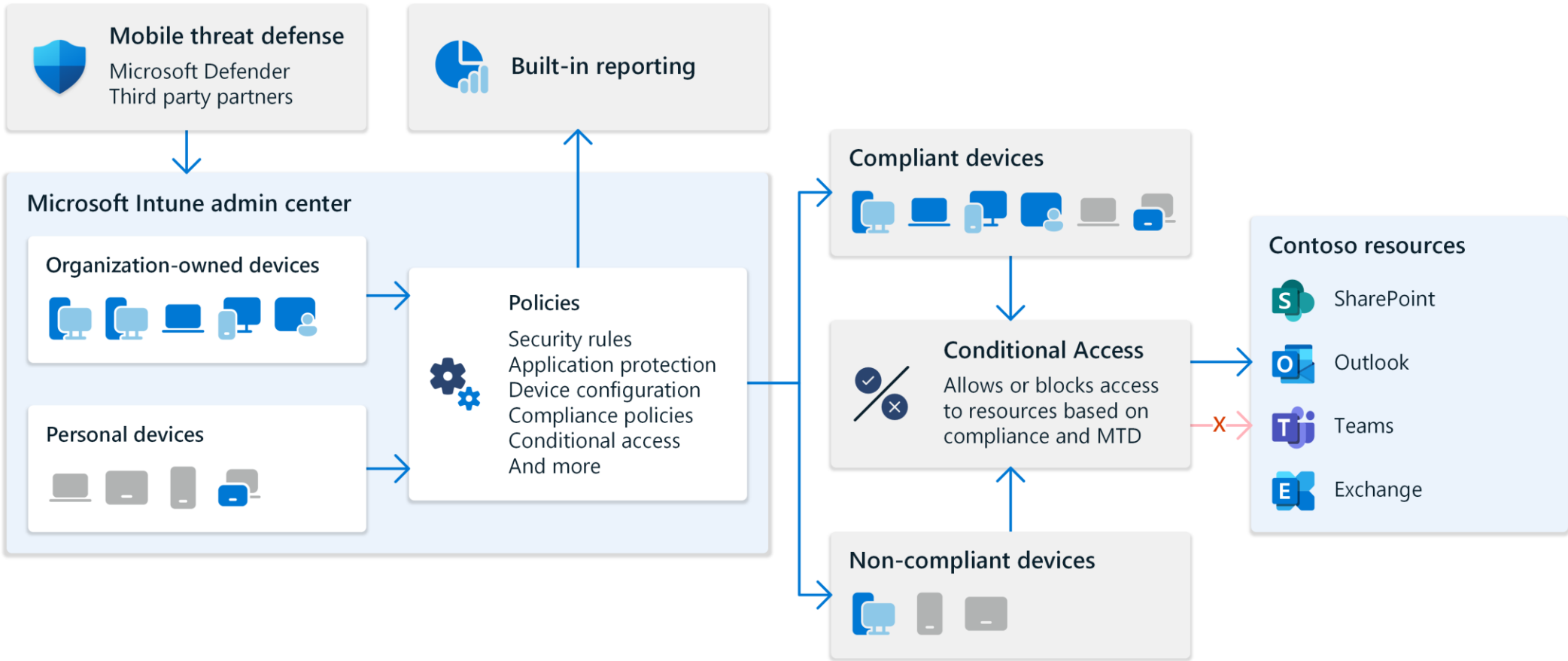


Criptografia















Microsoft Intune











Microsoft Intune

Features and benefits

-  Manage devices from a central console
-  Deploy and update software
-  Configure settings
-  Enforce policies
-  Monitor with data and reports
-  Remote administration
-  Maintain networks of common OS
-  Optimize devices for business use
-  Automate policy management
-  Cloud-attach on-prem Configuration Manager

Mobile Device Management

-  Enroll user devices
-  Push apps on devices
-  Restrict devices to a specific OS
-  Block personal devices
-  Remove data from lost or stolen devices
-  Security and protection

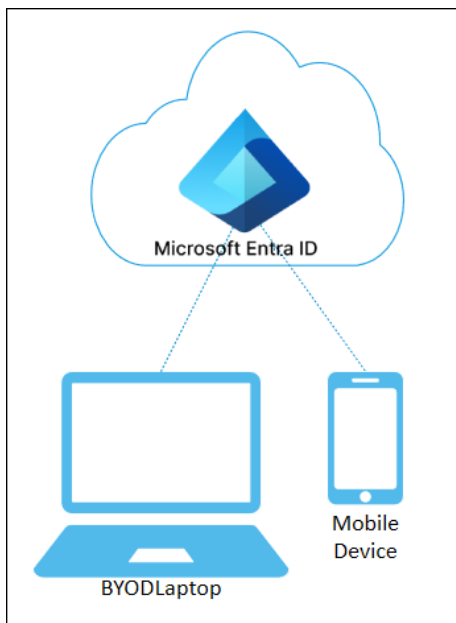
Mobile Application Management

-  Allow personal devices to access org resources
-  Prompt users to authenticate
-  Remove data from lost or stolen devices
-  Security and protection



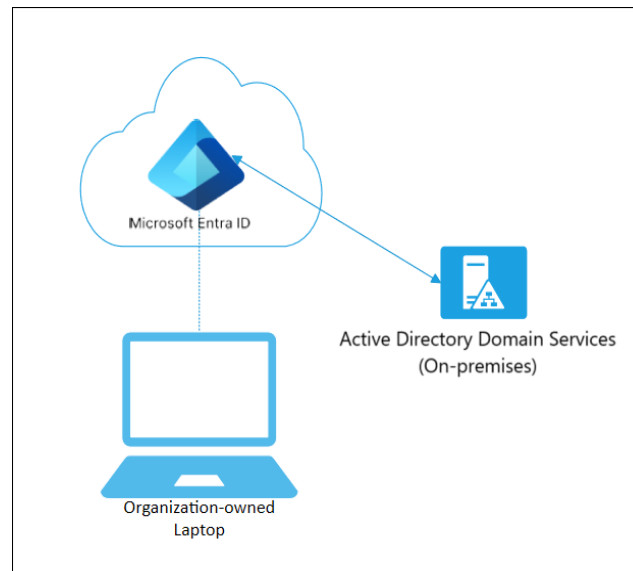


Microsoft Entra Registered



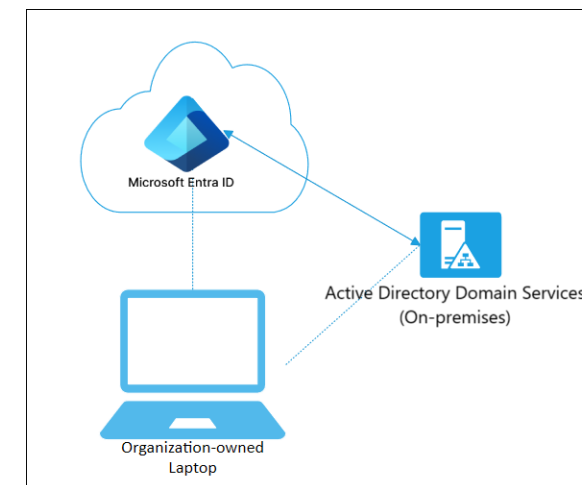
- Para dispositivos BYOD.
- Acesso a aplicativos como Outlook e Word.

Microsoft Entra joined



- Dispositivos associados ao Entra ID.
- Controle administrativo completo.

Microsoft Entra hybrid joined








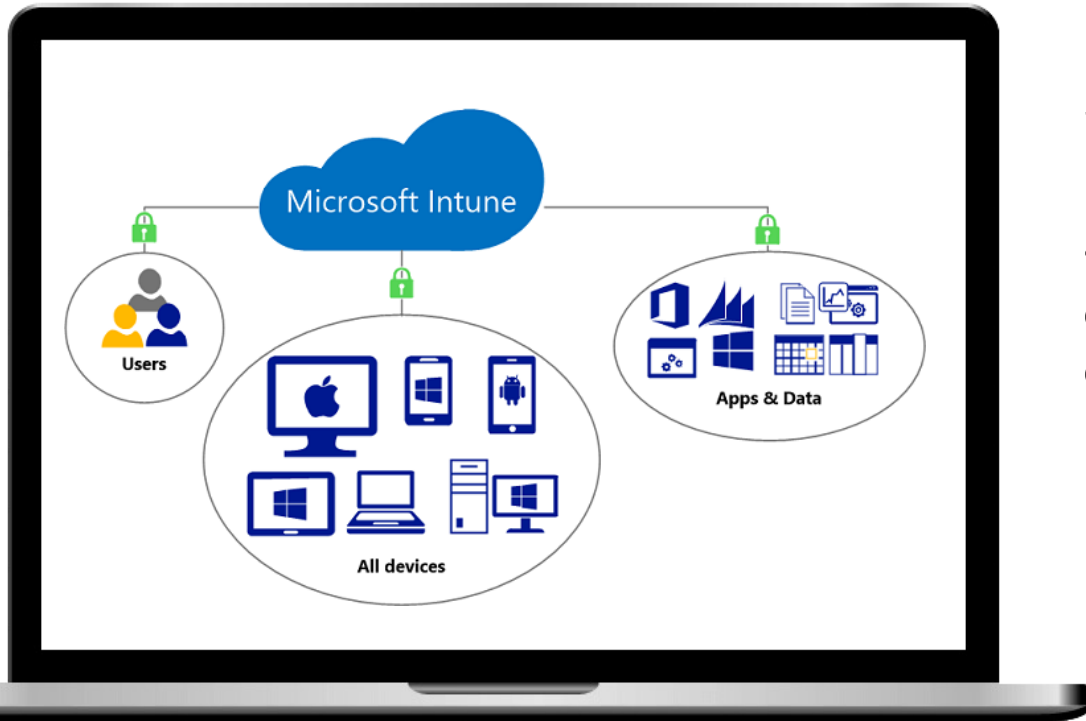
- Cenários híbridos com Active Directory On-premises e Entra ID.
- Conexão e sincronização de políticas.



Plataforma - Nível do sistema operacional

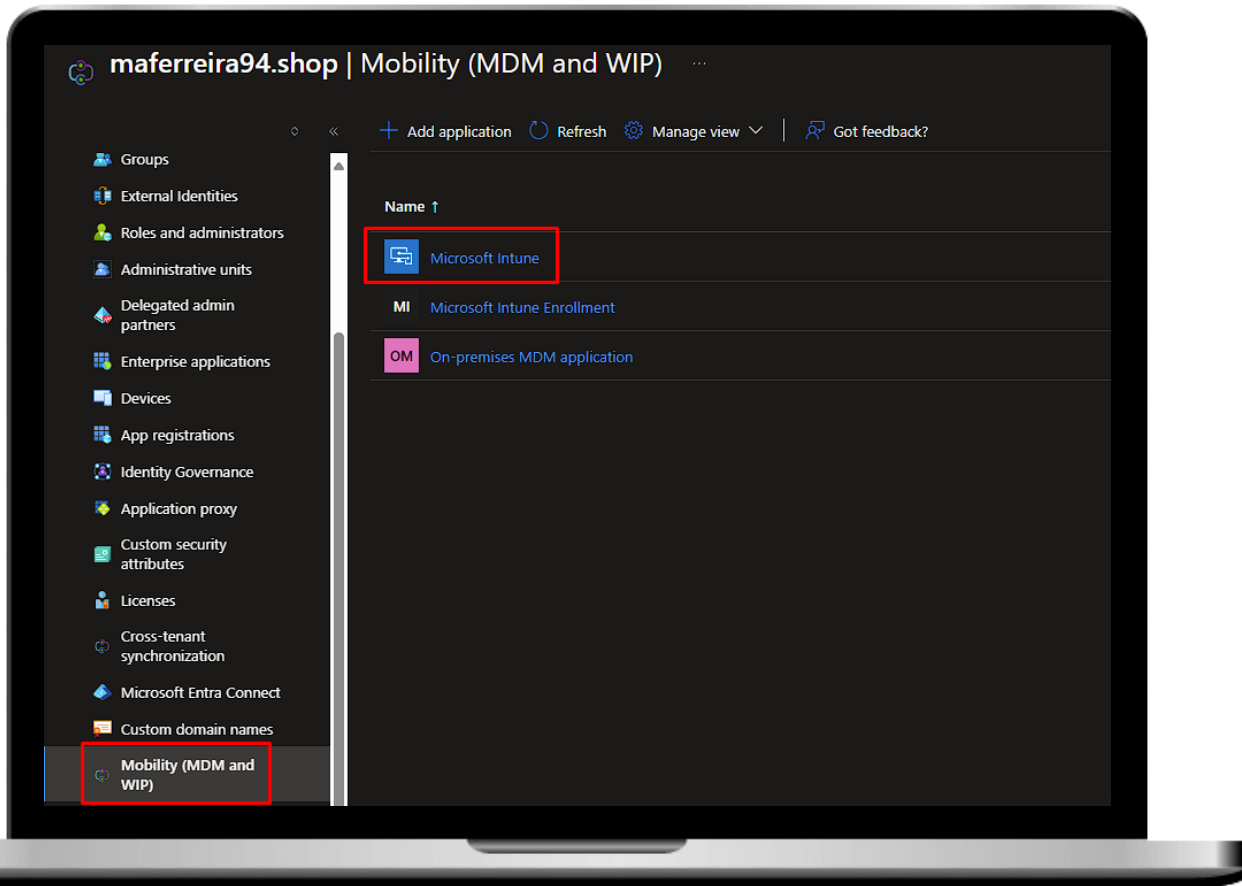
- Agora que temos conhecimento sobre o que o Intune faz. Qual sistema operacional é compatível com o Intune?

-  Windows
-  iOS/iPadOS
-  macOS
-  Android
-  Linux



Windows enrollment

- Em primeiro lugar, recisa definir a mobilidade (MDM e MAM) para Microsoft Intune no Portal do Azure



Windows enrollment

Aqui você tem as configurações sobre o registro do Windows.

Automatic Enrollment:

Home > Devices | Windows > Windows

Windows | Enrollment

Learn about the different ways a Windows 10/11 PC can be enrolled into Intune by users or admins. [Learn more.](#)

Enrollment options

- Automatic Enrollment** - Configure Windows devices to enroll when they join or register with Azure Active Directory.
- CNAME Validation** - Test company domain CNAME registration for Windows enrollment.
- Co-management Settings** - Configure co-management settings for Configuration Manager integration.
- Device platform restriction** - Configure which platform versions can enroll.
- Device limit restriction** - Define how many devices each user can enroll.
- Enrollment notifications** - Send email or push notifications to devices after they enroll.
- Windows Hello for Business** - Replace passwords with strong two-factor authentication.

Windows Autopilot device preparation

Use Windows Autopilot device preparation to streamline configuration, reporting, and troubleshooting experiences. [Learn more about Windows Autopilot device preparation](#)

- Device preparation policies** - Configure devices for initial provisioning.

Windows Autopilot

Use Windows Autopilot to customize the Windows onboarding out of box experience and workflow. [Learn more about Windows Autopilot](#)

- Devices** - Manage Windows Autopilot devices.

Microsoft Intune

MDM user scope

None Some All

MDM terms of use URL

MDM discovery URL

MDM compliance URL

[Restore default MDM URLs](#)

Windows Information Protection (WIP) user scope

None Some All

WIP terms of use URL

WIP discovery URL

WIP compliance URL





[Restore default WIP URLs](#)

Creating new WIP without enrollment policies (WIP-ME) is no longer supported. For more information, see [Windows Information Protection](#)



Endpoint Management at Microsoft







Intune Suite

-  Remote help desk connections
-  Microsoft Tunnel VPN for MAM
-  Endpoint Privilege Management
-  Manage specialty devices

Intune admin center

-  Intune service
-  Windows 365 cloud PCs
-  Windows Autopatch
-  Entra ID Privileged Identity Management
-  Certificate management
-  Remote Help
-  Microsoft Tunnel VPN
-  Mobile threat defense


















Windows Autopilot

-  Preconfigure devices
-  Auto-join devices to Microsoft Entra
-  Auto-enroll devices in Intune
-  Customize OOBE
-  Enrollment status page
-  Reset and repurpose devices

Endpoint analytics

-  Device health and performance metrics

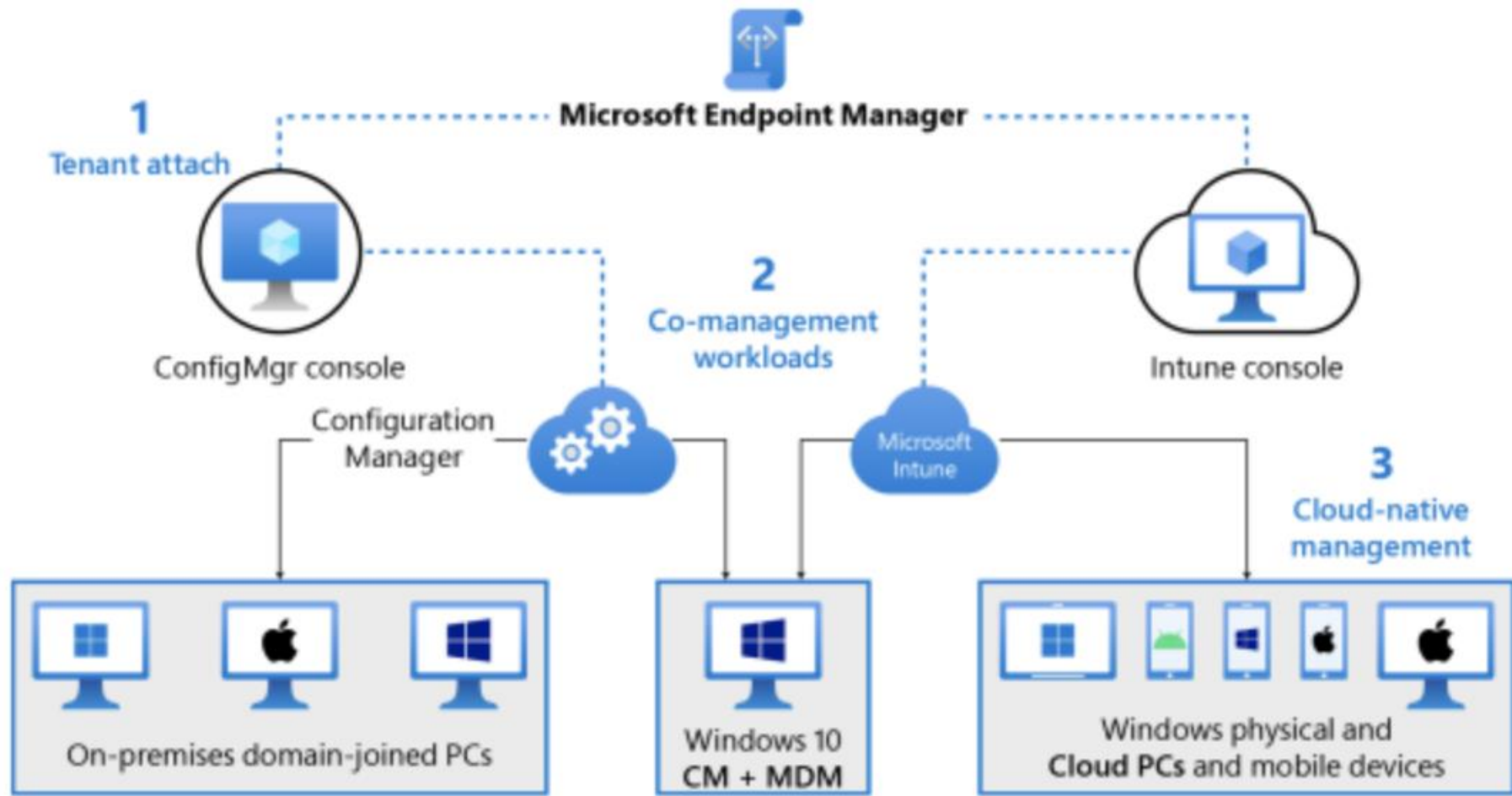
Integrations

-  Microsoft Entra ID
-  User identities
-  Device identities
-  Group identities
-  On-premises Configuration Manager
-  Desktops
-  Laptops
-  Windows Servers
-  Data Centers
-  Apps and software
-  Device OS
-  Mobile threat defense (MTD) partner apps and services
-  Azure Monitor
-  Win32 and custom LOB apps
-  Microsoft 365
-  Security Copilot
-  And more



Dando super poderes ao intune







Microsoft Endpoint Manager



Microsoft
System Center
Configuration Manager



Microsoft
Intune



Hardware



Regional
Distribution Points

Branch
Cache



Server-side
Peering

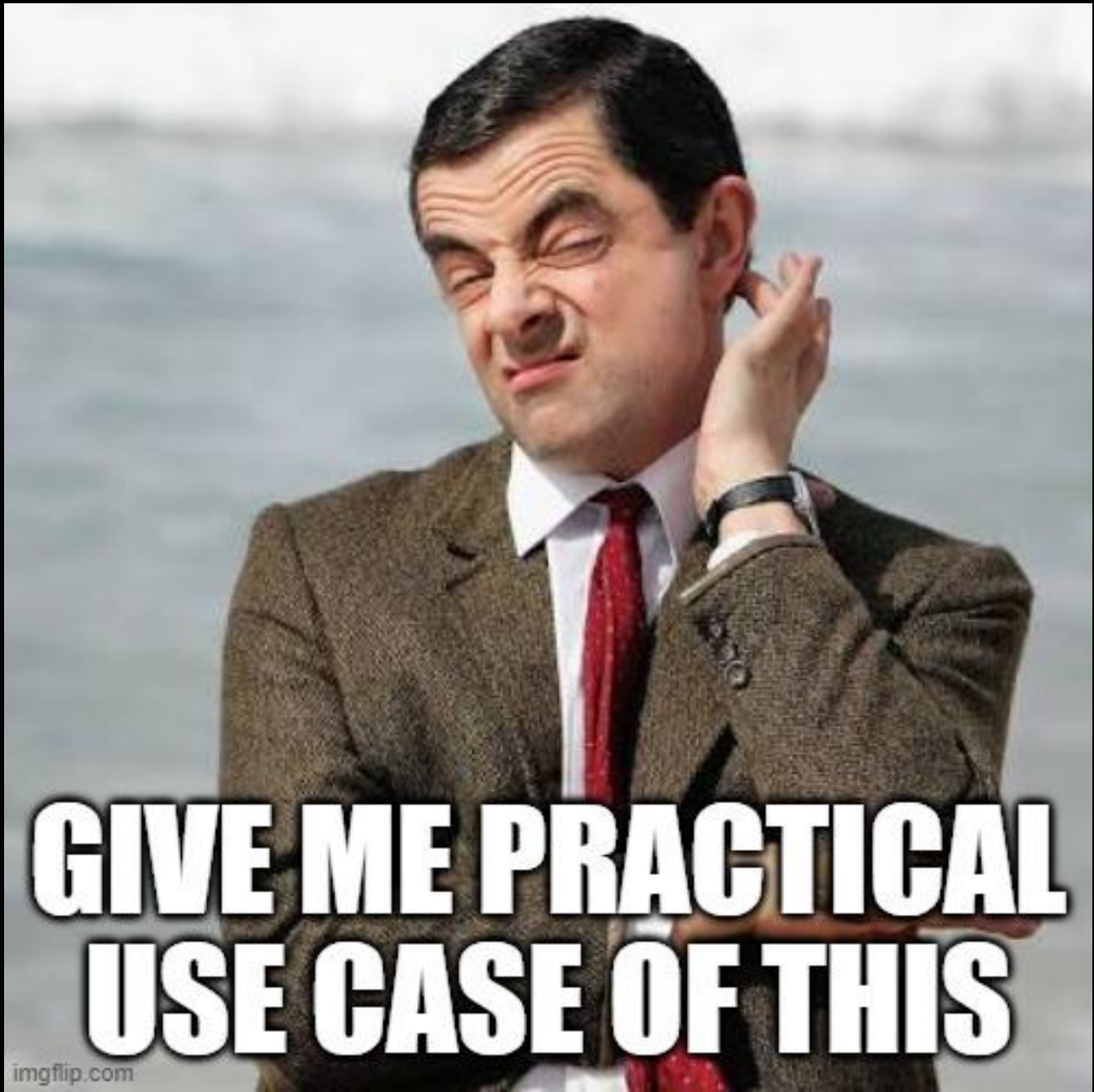
Peer
Cache



Client-side
Peering

Delivery
Optimization





imgflip.com



Casos de uso

Um colaborador recém entrou na empresa e precisa ter diversos softwares e políticas configurados.

OBS1: O colaborador é do Sul e a empresa está localizada no Nordeste.

OBS2: O colaborador é da área administrativa e não possui conhecimento avançado em informática.

Um colaborador mal intencionado entra recente na empresa com conhecimento avançado em informática. Como proteger o dispositivo de más intenções?





HANDS-ON



Certificação

Microsoft 365 Certified: Endpoint Administrator Associate

Exame MD-102: Administrador de Ponto de Extremidade

Habilidades medidas:

- Implantar o cliente Windows
- Gerenciar a identidade e a conformidade
- Gerenciar, fazer a manutenção e proteger dispositivos
- Gerenciar aplicativos



Agradecimentos



ChatGPT



DALL-E



Copilot



Google



Microsoft



Obrigado!

Vocês podem me encontrar em



rafaelmaferreira

