



## Microsoft 365: MDM Migration

**Our Next Generation MDM Migration solution provides, options for Migrating a 3<sup>rd</sup> Party MDM Solution to Microsoft Endpoint Manager to enable the Management of Devices for a Modern Workforce catering for a Hybrid work environment.**

Microsoft  
Partner

Silver Windows and Devices  
Silver Messaging  
Silver DevOps  
Silver Application Development  
Silver Collaboration and Content





## Table of Contents

1. Executive Summary .....	2
2. Migration Approach.....	2
3. High Level Device Architecture .....	3
4. Scope Definition .....	4
5. Steps to Complete Engagement .....	5
1. Our Migration Approach .....	8
6. Project Management.....	<b>Error! Bookmark not defined.</b>
7. Implementation Approach .....	<b>Error! Bookmark not defined.</b>
8. Risk Management and Change Management.....	<b>Error! Bookmark not defined.</b>
9. Client Responsibilities.....	<b>Error! Bookmark not defined.</b>
10. Access Requirements .....	<b>Error! Bookmark not defined.</b>





## 1. Executive Summary

Several organizations worldwide have been forced to change the way they work due to the current norm, where we are now exposed to Pandemics that cripple the way we work, customers have been forced to adapt and change from being an office-based workforce to a hybrid approach where we work from home and at the office. This brings a new challenge where our data and applications must follow us wherever we go. Another challenge is that customers are faced with Mobile Device Management (MDM) solutions that cannot easily adapt to this new norm or cannot scale or integrate with other applications and tools. Based on this challenge we have crafted a solution to assist customers to migrate 3<sup>rd</sup> Party MDM Solutions to Microsoft Endpoint Management.

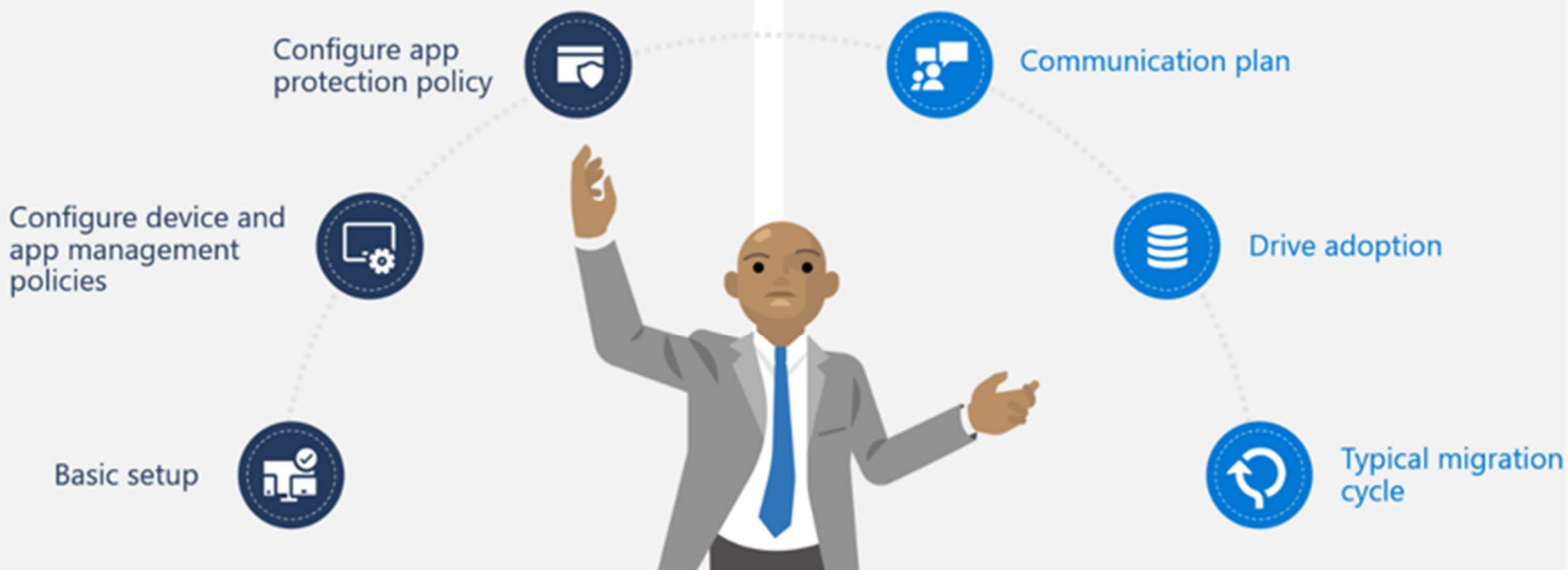
A successful adoption or migration to Microsoft Intune starts with a plan. This plan depends on your current mobile device management (MDM) environment, business goals, and technical requirements. Additionally, you need to include the key stakeholders who will support and collaborate with your plan.

## 2. Migration Approach



### Phase 1: Prepare Intune for MDM

### Phase 2: Migration campaign





### 3. High Level Platform Architecture

### 4. High Level Device Architecture

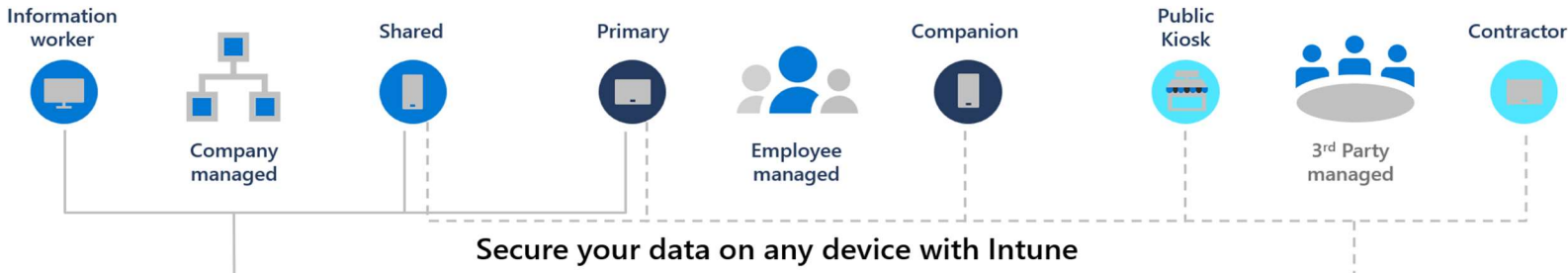
Complexity is inherent in today's mobile landscape – with the multiple needs and scenarios naturally presenting themselves in even the simplest environments.

- Organizations have company-managed devices; these may be dedicated to a specific user or devices that are shared across multiple employees.
- Organizations have devices that are employee-managed – whether it's a primary device they're using (their iPhone or PC) or what we call a companion device – something they are using to get online from time to time (like their daughter's iPad or a family computer).
- And, finally, there are 3<sup>rd</sup> party-managed devices – these are devices that may be managed by other entities or perhaps unmanaged but unfamiliar to you. Think about your partners and contractors that you want to enable – or public kiosk scenarios.

These various needs naturally show up in today's corporate environment. Intune's app management and device management capabilities are designed to help you solve for them all – in a way that enables you to get access to data securely based on your needs.



Microsoft Intune gives you the flexibility and control to secure your data on any device – even those you don’t manage



### Intune device management

### Intune app management



Enroll devices for management



Provision settings, certs, profiles



Report and measure device compliance



Remove corporate data from devices

Conditional access: Restrict access to managed and compliant devices



Publish mobile apps to users



Configure and update apps



Report app inventory and usage



Secure and remove corporate data within mobile apps

Conditional access: Restrict access to apps with app protection policy

## 5. Scope Definition

This engagement is a collaborative effort between our Customers and OnDemand. Ultimately, the success of this engagement depends on all parties understanding the roles and responsibilities and executing on their tasks effectively. A successful Microsoft Intune deployment or migration starts with planning.





The following section defines the scope of this engagement. It should therefore be noted that unless a deliverable is explicitly included in the tables below, it is to be regarded as implicitly excluded from the scope of delivery.



## 6. Steps to Complete Engagement

### Assessment Phase

In this phase we collect information from the existing MDM Solution:

<b>Devices</b>	<p><b>Number of devices:</b></p> <p>  XXXXX Android   XXXXX iOS         </p>	<b>Management modes</b>	<p>  <b>iOS:</b> device enrollment, user enrollment   <b>Android:</b> Android device administrator  <b>Android Enterprise:</b> Fully managed, dedicated, work profile         </p>
<b>Configurations and compliance</b>	<ul style="list-style-type: none"> <li>✓ XX Configuration profiles</li> <li>✓ XX Compliance profiles</li> </ul>	<b>Device provisioning</b>	<ul style="list-style-type: none"> <li>✓ Manual provisioning or</li> <li>✓ Automatic provisioning</li> </ul>
<b>Apps and Content</b>	<ul style="list-style-type: none"> <li>✓ XX Public apps</li> <li>✓ XX LoB apps</li> <li>✓ XX Web links</li> <li>✓ XX Content</li> </ul>	<b>On-prem connectors and features</b>	<ul style="list-style-type: none"> <li>✓ Certificate distribution (NDES)</li> <li>✓ VPN</li> <li>✓ Content distribution</li> <li>✓ On-prem Exchange connector</li> <li>✓ 3rd party integrations</li> </ul>
<b>Groups and Users</b>	<ul style="list-style-type: none"> <li>✓ XX Groups               <ul style="list-style-type: none"> <li>✓ X Smart groups</li> <li>✓ X Organization groups</li> <li>✓ X User groups</li> </ul> </li> <li>✓ XXXXX Users</li> </ul>	<b>Organization impacts</b>	<ul style="list-style-type: none"> <li>✓ Intune &amp; Azure AD RBAC model</li> <li>✓ Processes (enrollment, provisioning, etc.)</li> <li>✓ Android Enterprise readiness</li> <li>✓ Other</li> </ul>



From there we prepare prerequisites for the Migration:

<b>Devices</b>	<ul style="list-style-type: none"><li>✓ List of all active devices with all relevant information (OS version, model, serial number/IMEI, assigned user, etc.)</li><li>✓ List of all serial numbers or IMEI to be included in Corporate Device Identifiers (if applicable)</li></ul>
<b>Configurations and compliance</b>	<ul style="list-style-type: none"><li>✓ Assignment strategy (device-based or user-based)</li><li>✓ Devices enrollment modes strategy (e.g.: Android device administrator, Android Enterprise dedicated, etc.)</li><li>✓ Configuration profiles with parameters details and group assignments</li><li>✓ Compliance profiles with parameters details and group assignments</li></ul>
<b>Apps and Content</b>	<ul style="list-style-type: none"><li>✓ List of app categories</li><li>✓ LoB apps sources, icons, descriptions, and group assignments</li><li>✓ Web links URLs, icons, descriptions, and group assignments</li><li>✓ Content files and group assignments</li><li>✓ List of approved public apps and group assignments</li><li>✓ App whitelist / blacklist and group assignments</li></ul>
<b>Groups and Users</b>	<ul style="list-style-type: none"><li>✓ List of groups used with current MDM (user groups, organizational groups, admin groups, smart groups, etc.)</li><li>✓ Group type (static, dynamic) and belonging criteria</li><li>✓ List of users included in each group</li><li>✓ List of admins and roles</li></ul>
<b>Intune</b>	<ul style="list-style-type: none"><li>✓ Service accounts (Apple ID, Google ID)</li><li>✓ Third party services (Apple Business Manager, KNOX Mobile Enrollment, etc.)</li><li>✓ Current configuration assessment</li><li>✓ Licenses</li><li>✓ Administrator accounts for project team</li></ul>



If possible, Microsoft recommends optimizing the number of profiles and groups before migration for simplification and better administration



Below are Design activities we will complete as part of this engagement. To ensure we have a solid solution for our customers we ensure that we input all design decisions into the final step of the engagement before we implement the migration process. We cater for small to large and complex solutions.



**Design and implement Microsoft Endpoint Manager solution**



**Design and implement automatic provisioning including:**  
Apple ADE, Samsung KME, Google Zero Touch, Autopilot



**Design and implement Android Enterprise enrollment scenarios including:**  
dedicated, fully managed, work profile



**Design and implement device configuration and security features including:**  
Configuration profiles, Application Protection profiles, Endpoint Security profiles and security baselines



**Design and implement apps deployment for:**  
Mobile apps, LoB applications, Microsoft 365 apps for Enterprise, Microsoft Edge, etc.





## 1. Our Migration Approach

### Our MDM devices migration plan?

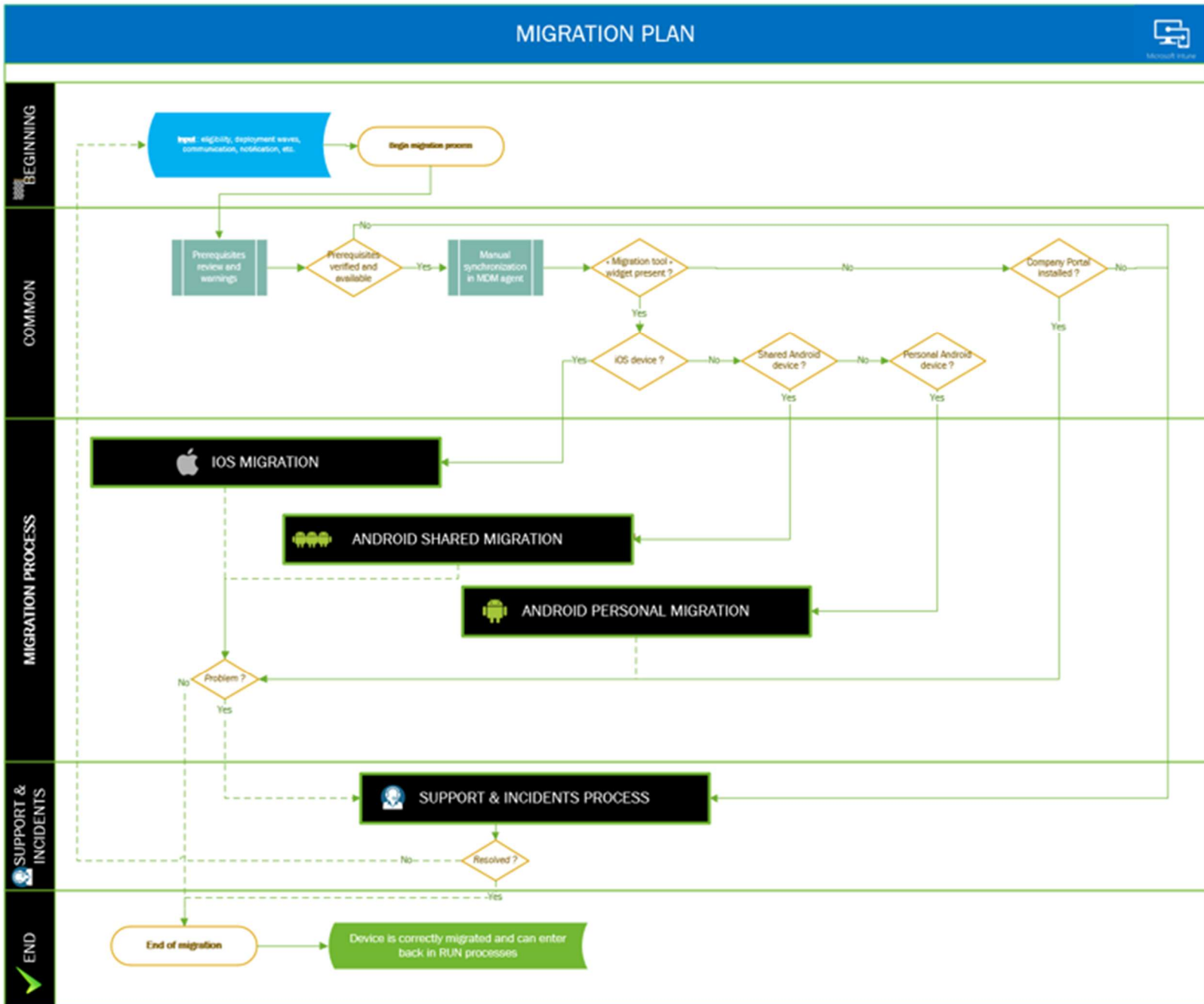
- ✓ MDM Migration Kickoff
- ✓ initial state with current MDM
- ✓ Initial and target management modes
- ✓ Migration criteria
- ✓ Process and tools





## 2. Migration Plan Design

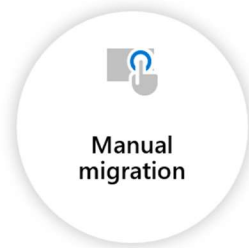
Below is the scale migration approach documented by Microsoft that we deliver solution





### 3. Migration Tooling

We use tools to Migration MDM 3<sup>rd</sup> party solutions to Microsoft Endpoint Manager/Intune; however, we prefer a strong Change Management plan for driving customer success in the customers environment.



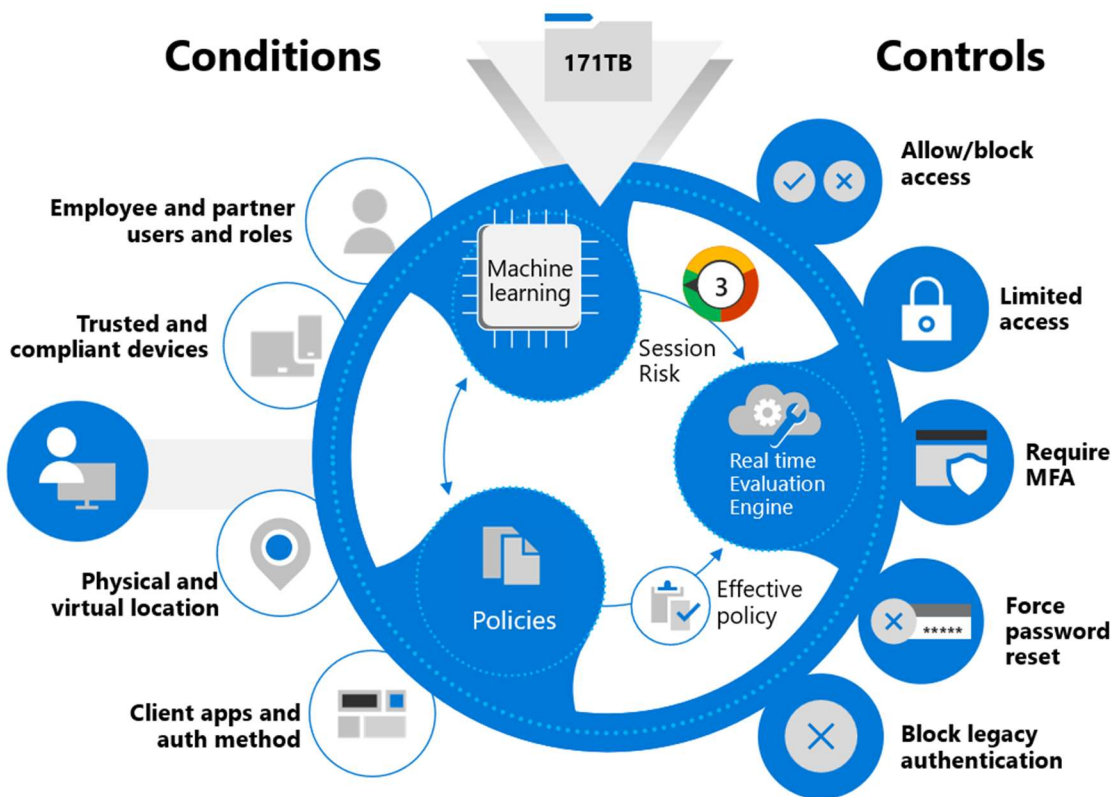
*Although MDM migration solutions or custom development can ease migrations in some cases, a strong change management strategy and communication is the most important key success factor for an MDM migration*





## 4. Drive end-user Adoption with Conditional Access

We are concerned about driving end user adoption with Conditional Access to ensure that set conditional access polices, for all user and ensure that all users, however users from the old MDM Provider will be considered as we continue with the migration.





## 5. Take A Flexible Path to Microsoft Endpoint Management

### Cloud security across endpoints

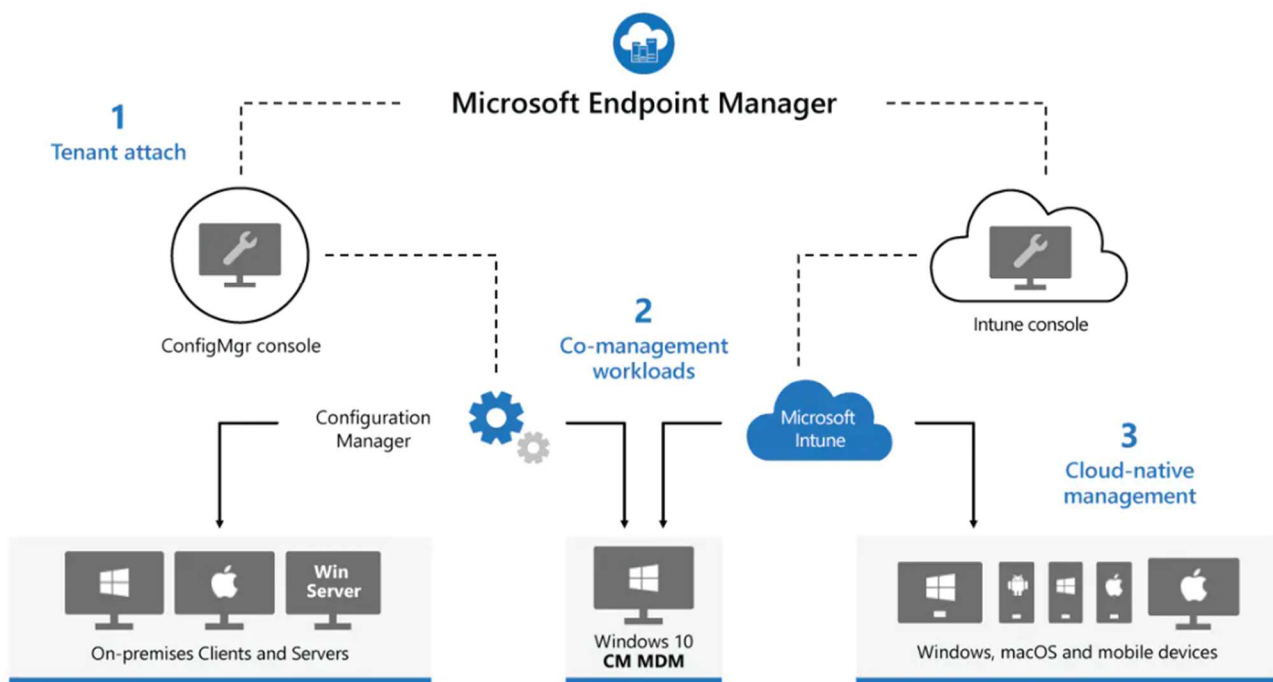
Help protect user devices against threats using Microsoft Zero Trust technology with unique capabilities.

### Comprehensive Windows 11 management

Simplify automated provisioning, configuration management, and software updates for all your endpoints.

### Maximum return on investment

Take advantage of existing investments to modernize the user experience with Microsoft 365 cloud telemetry.



A unified platform including both Configuration Manager and Microsoft Intune