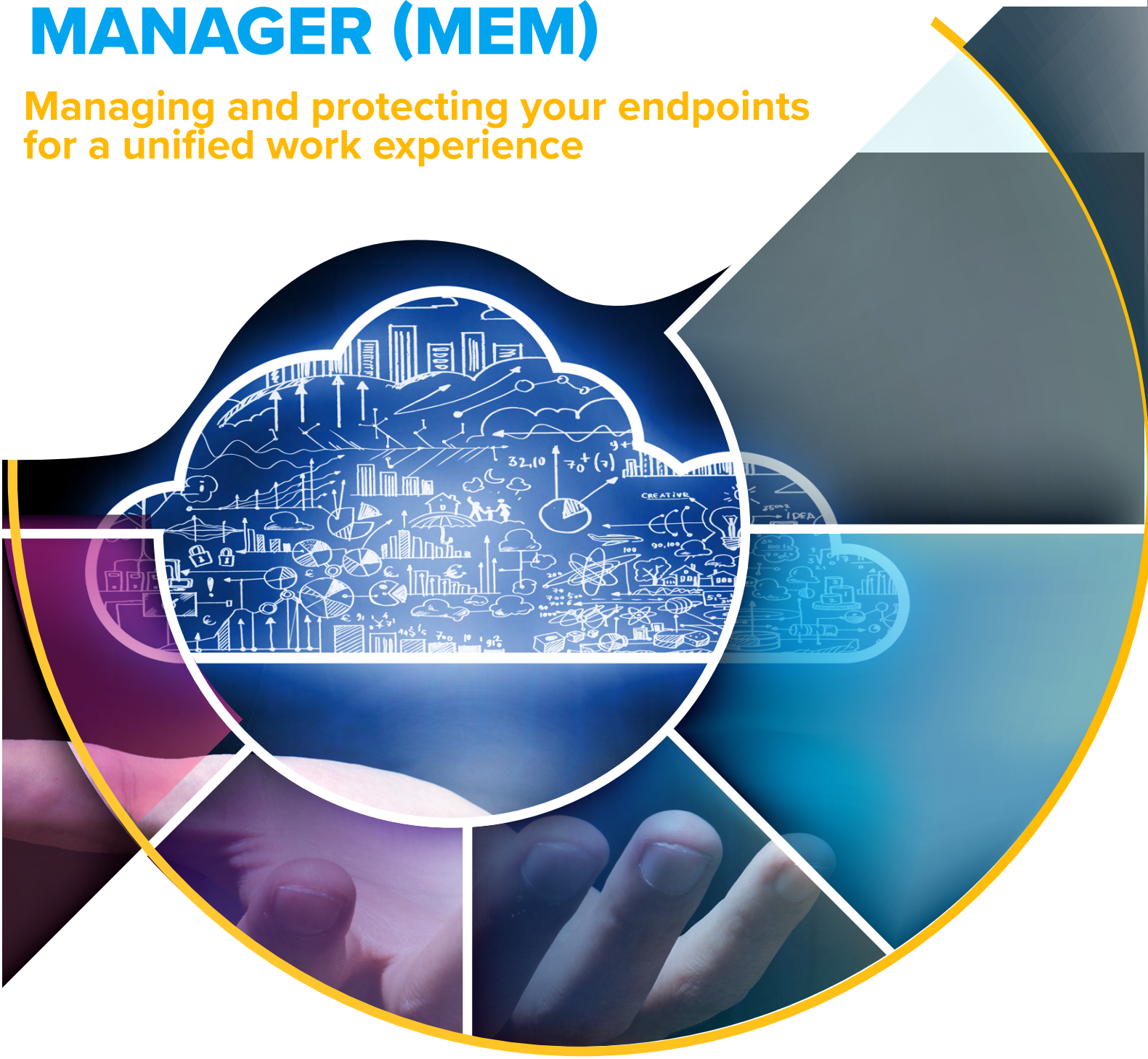
happiest minds
The Mindful IT Company
Born Digital . Born Agile

MICROSOFT ENDPOINT MANAGER (MEM)

Managing and protecting your endpoints for a unified work experience



Since 2020, there has been a significant increase in co-management and cloud management of endpoints. Businesses still need help in providing work flexibility from anywhere, through any device with secure and reliable connectivity. While most companies are moving their entire IT Infrastructure services to cloud platforms, they need to build streamlined support to bring flexibility, security, and better collaboration over their diverse corporate and Bring Your Own Device (BYOD) environment.

Microsoft Endpoint Manager is one such cloud-based platform that lets you manage all your endpoints with multiple features for users and devices and provides support for companies of all sizes while saving you money and time. Users can experience the modern Microsoft 365 cloud telemetry, which has brought many areas such as Endpoint Manager (Intune), Office 365, OneDrive, Teams, SharePoint, Exchange Online, Advanced Threat Protection (ATP), and Defender Antivirus.

In this whitepaper, we have detailed how Microsoft Endpoint Manager (MEM) can enable your modern workplace by managing and protecting your endpoints for better hybrid work experiences while reducing your total ownership cost.

Why Microsoft Endpoint Manager?

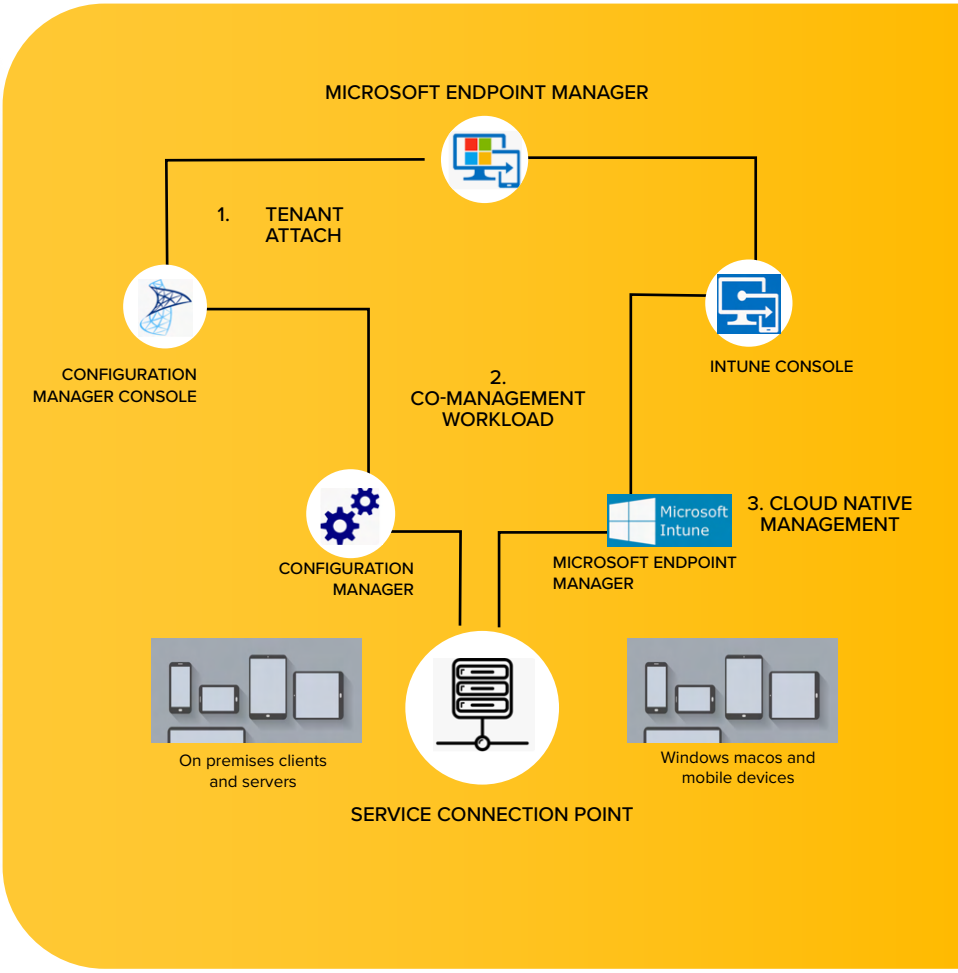
Endpoint Manager combines the on-premises solution of Configuration Manager with Microsoft Intune cloud services attached called Co-management.

Co-management combines existing on-premises investments with cloud-based features of Intune, where organizations use this to utilize all services of both technologies.

This gradually helps to move the workloads from on-premises to the cloud, where most configuration manager features are already implemented in Intune.

Benefits

- Cost Effective
- Scalability
- Data Recovery
- Operational Flexibility



Advantage of MEM over MECM

CONFIGURATION MANAGER (MECM)	MICROSOFT ENDPOINT MANAGER (INTUNE)
Hardware and Software dependency to install and configure into the on-premises physical and virtual servers	Web-based SaaS Platform/link with Intune subscriptions to login
Support Windows, Linux and Mac OS Client and Server Devices	Supports Windows, Mac OS Devices and Mobile Devices such as Android, Apple iPad/iOS, Chrome OS mobile devices
MECM supports apps to users/devices, security updates, Data/User/Device Protection, Antivirus, Microsoft 365 services	Intune supports apps to users/devices, security updates, Data/User/Device Protection, Antivirus, Microsoft 365 services
Included in major platforms such as Patch Management, Image Management, Software Deployment and Defender Antivirus	Included in major platforms such as Patch Management, Windows Autopilot, Software Deployment and Defender Antivirus
Desktop Analytics is in use for Optimization	Endpoint Analytics with various PowerBI or Data warehouse integration
Security Baselines, compliances, policy creations and servicing plans for Office 365 and Windows Updates, SQL Reports, Windows Software Update Services	Security Baselines, compliances, policy creations and servicing plans for Office 365 and Windows Updates, Reports, Windows Update for Business (WufB)
Remote Features include VPN, and Wi-Fi enabled to access internet devices	Remote Help or Remote Deployment to access BYOD devices

Features of Microsoft Endpoint Manager

Microsoft Endpoint Manager cloud-based solution is designed to address many challenges associated with devices in terms of asset handling, identity, mobility and security, Antivirus, compliance, and Analytics. All these features are introduced within MEM (Intune) and enable integration with other management tools such as MECM (Configuration Manager). Below are the various features we have tried to detail and explain the use of each.

01 Microsoft Intune

Intune is a Cloud based Unified management platform service that focuses on mobile device Management (MDM), Mobile Application Management (MAM) support with lot of services such as apps to users, device protection, device migration, Role Based Access Control (RBAC), Identity, Compliance Reports

02 Configuration Manager

MECM is On-premises and Cloud based management service that focuses on all kind of devices includes clients, servers except mobile devices such as Android, Apple iOS/iPad, Chrome OS and respective support such as apps to users/devices, protection to devices, device migration, Image and Patch management, Compliance Reports

03 Windows Autopilot

Simplified device deployment, there is no need to reimage or manually set up before handing device to users, hardware vendor can ship for ready to use directly with just domain credentials which is called as OOBE (Out of the Box Experience)

04 Endpoint Analytics

Analytics gives insights of your organization is working and quality of experience delivered to users. Endpoint Analytics identify policies, hardware and software issues before end user request a help desk ticket to identify issues. Provides detailed report to customers

05 Endpoint Protection

Endpoint Protection from Cyberthreats. This is epicenter for comprehensive endpoint security, rapidly stops the attacks, scale security resources and evolve defenses across operating system and network devices

06 Azure Active Directory

Universal platform to manage and secure identities for users and control access to your apps, data and resources

Detailed View

CONFIGURATION MANAGER INTEGRATION WITH MEM

Configurations Manager, called MECM, is the earlier version of the on-premises management tool used to manage device deployments, image management , patch updates , and other infra support. Most of the features of on-premises are slowly migrating to Intune.

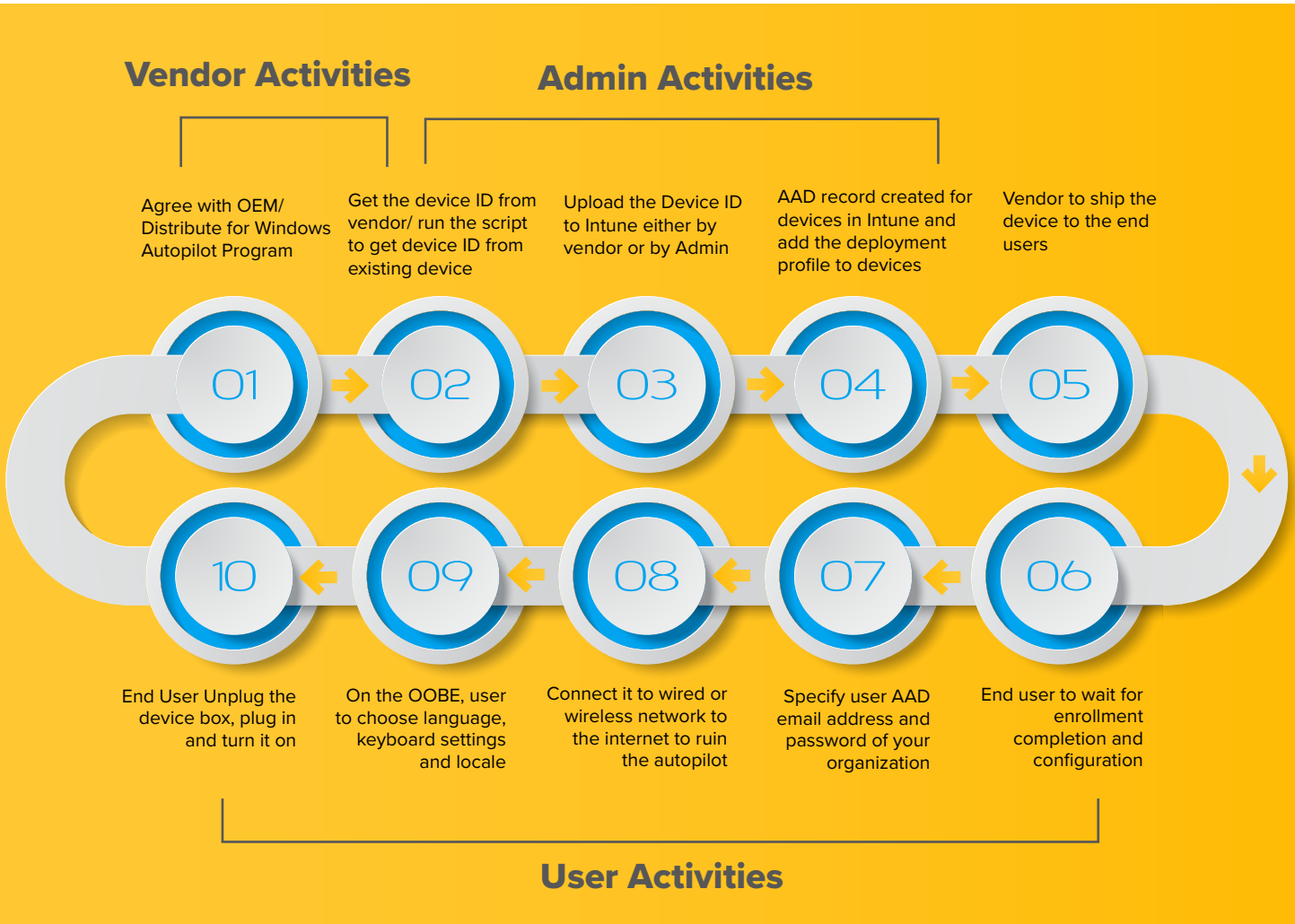
Recent times have seen modern infrastructure platforms, and organizations opting for Cloud Unified platformswhich they wanted to integrate for certain years and then decommission later.

WINDOWS AUTOPILOT

One of the major concerns in the IT infrastructure market is Image Management and Maintenance. But the Intune feature called "Windows Autopilot," enrolls devices faster by assigning all the required user profile settings to devices just by considering the box experience (OOBE) concept introduced by Microsoft. This OOBE profile checks the operating system provided by Original Equipment Manufacturers (OEMs) and decides to enroll the devices without applying OS from scratch helping organizations reduce the cost and time consumption of image activities.

Windows Autopilot is a cloud-native service that sets up and pre-configures new devices, preparing them for use. It can also reset and repurpose existing devices. Moreover, it's designed to simplify the lifecycle of Windows devices from initial deployment through end-of-life, benefitting IT and end users.

The Windows Autopilot is also used to pre-configure devices, automatically join them to Azure AD, enroll them in Intune, customize the box experience (OOBE), and more. You can also integrate Windows Autopilot with Configuration Manager and co-management for more device configurations.



Currently, only a few of the components of MECM are moved to Intune, such as server supports, customized images, and some policies. Therefore organizations wanted to utilize both management due to which Microsoft introduced a feature called ‘co-manage’ which integrates Intune and MECM, and Endpoints/users utilize both management.

Endpoint Analytics

Endpoint analytics aims to improve user productivity and reduce IT support costs by providing insights into the user experience. The insights enable IT to optimize the end-user experience with proactive support and detect regressions in the user experience by assessing the user impact of configuration changes. There are 3rd party tools, such as PowerBI, and data warehousing, which are successfully integrated with Endpoint analytics to utilize more graphical insights for organizations to view while submitting the reports of various requirements.

Endpoint Protection

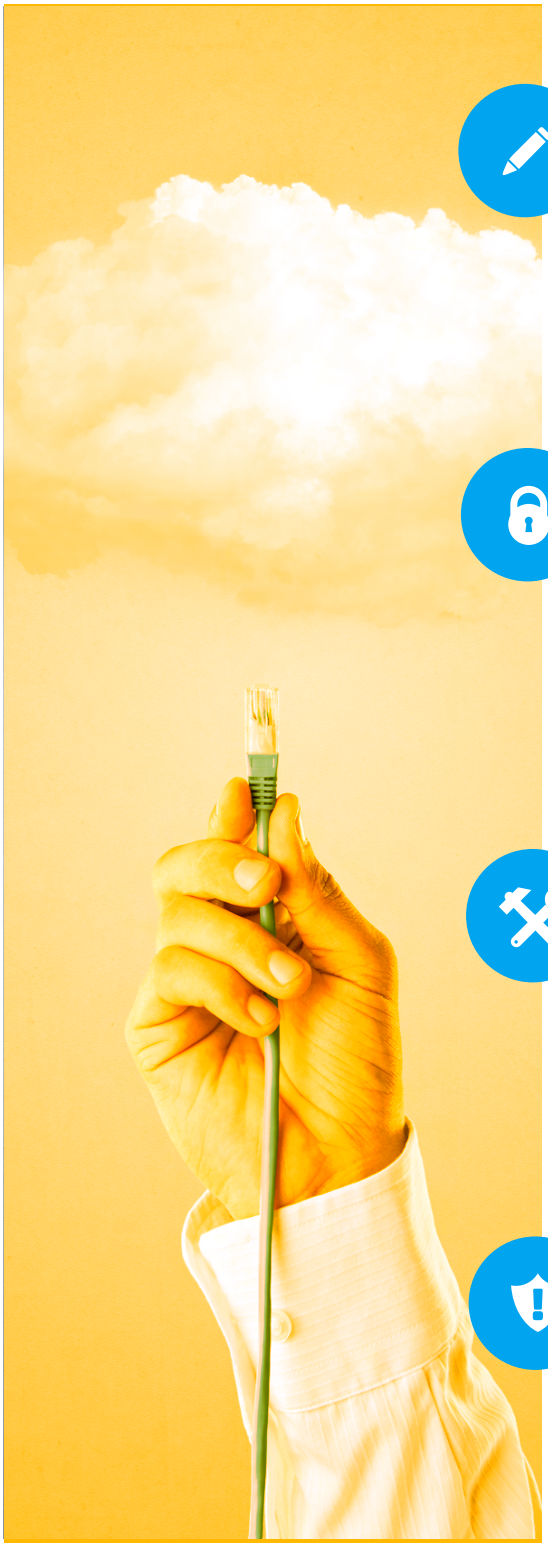
Device management not only requires installation and configuration of endpoints but also more concern about security perspective by protecting from hackers or attackers. The Endpoint Protection feature of Intune can manage devices by updating with Antivirus (Microsoft Defender or 3rd party), Bitlocker encryption , attack surface reduction, Microsoft ATP, device restrictions by applying protection policies, etc. Many policies related to devising protections have been introduced in Intune, which secure both corporate or external (BYOD)) devices.

Azure Active Directory

Azure Active Directory is an identity and access management platform for all users and devices, while Intune is AAD-dependent in terms of identity and access management. Here Multi Factor Authentication (MFA) is introduced to secure the devices.
The features mentioned above of Microsoft Endpoint Manager (MEM) are uniquely called with one name as Microsoft Intune, which has benefits of integration with MECM, Identity & Access Dependence with Azure Active Directory, and enhanced features such as Windows Autopilot, Endpoint Protection, Endpoint Analytics, and other standard features like security (Defender), Application and device management.

Microsoft Endpoint Manager (Intune) Device Life Cycle

All the devices that you manage have a lifecycle. Intune can help you manage this lifecycle from enrollment, through configuration and protection, to retiring the device when it's no longer required.



ENROLL

- Users can Self Enroll their BYOD or CORP Windows device, Mobile Devices using Company Portal
- IT Admin can configure Windows device with Hybrid Azure AD join, Co-Management, DEM (Device Enrollment Manager), Bulk Enroll, GPO and Mobile Devices with MDM Push certificates, ADE, Google Play Store

PROTECT

- Antivirus
- Disk Encryption
- Firewall
- Endpoint Detection and Response
- Attack Surface Reduction
- Account Protection

CONFIGURE

- Configure various policies for Devices, Users and Applications to protect them from Cyberthreats
- Conditional Access
- Windows Quality, Feature Updates and Autopatch Configuration
- Group Policies creation, Export and Import from another Device Management Platform
- Device Compliance

RETIRE

- There might be frequent situations where devices may steal, lost or decommission. In such situation Intune has capability to retire devices

Critical Capabilities of Microsoft Endpoint Manager (MEM)

Native Cloud Integration controls security and risk based conditional access for apps and data

Secure and Intelligent

Intelligent security
- Windows Hello for Business
- Security Baselines
- Bitlocker Management
- ATP (Advanced Threat Protection)
- Secure score

Risk Based Control
- Endpoints compliance and Risk
- Conditional Access
- App Protection Policy
- Third Part risk and compliance signaling

Flexible support for diverse corporate and BYOD scenarios while increasing productivity and collaboration

Scalable and Flexible

Unified Management
- Mobile Device Management
- M365 Admin Center
- Guided deployments
- Office 365 Pro Plus
- Microsoft Edge

Zero Touch Provisioning
- Windows Autopilot
- Android Enterprise
- Apple DEP
- Samsung Knox
- Windows Autopatch

Maximize your investment and accelerate time to value with fast rollout of services and devices with end-to-end integration across familiar Microsoft stack

Maximize Investment

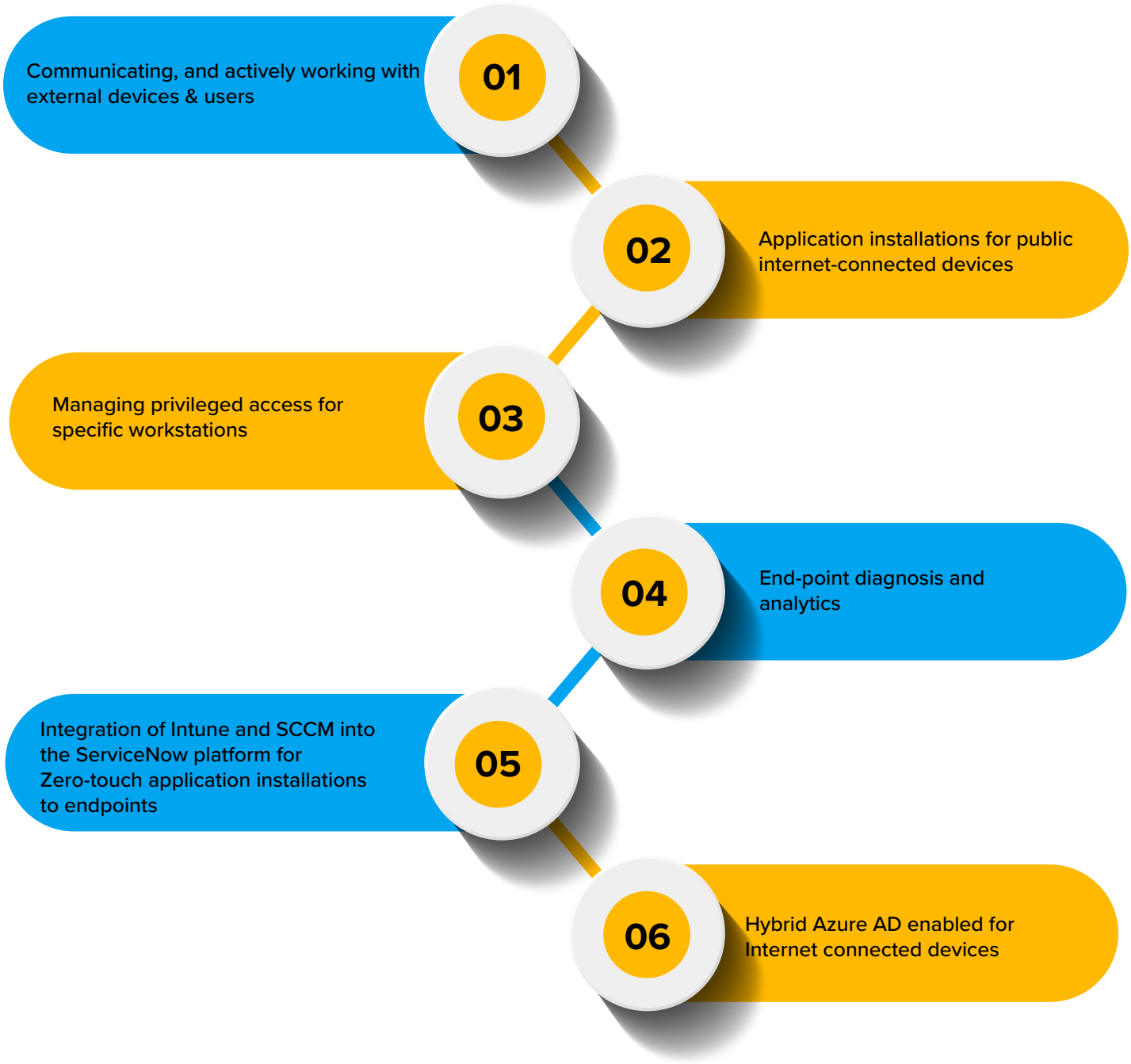
Advanced Analytics
- Desktop Analytics
- Log Analytics
- Endpoint Analytics
- Real Time Advanced Threat Protection
- Dynamic User Risk

Microsoft 365 Integration
- Role-Based Access Control (RBAC)
- Graph API
- PowerShell
- Audit
- Cloud Optimization

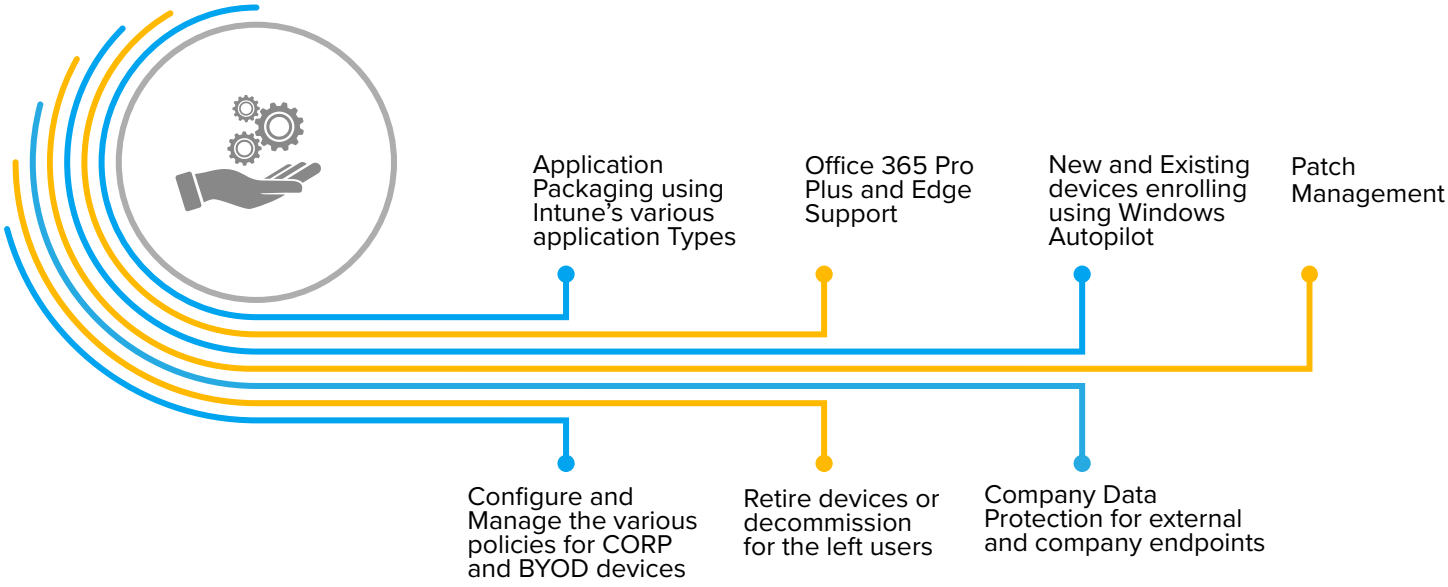
How Happiest Minds is effectively utilizing Microsoft MEM to add value to our customers

Here is a scenario where we have helped one of the leading global pharmaceutical companies by enhancing their Master Data Management (MDM), and Mobile Application Management (MAM) platforms.

Challenges



What we offered



Value Delivered

01

Automation use cases resulting in better efficiency and reduced errors

02

Streamlined processes for device enrollment, client applications, device protection with RBAC and Conditional access, autopatch for Windows devices

03

Improved business decisions by introducing a unified cloud platform, streamlined asset management, and their infra services

04

High-end user satisfaction and better compliance

Summary

Irrespective of the kind of work and the device in place, organizations need to adopt technology that allows them to manage all endpoints in a secure and flexible environment contributing to increased productivity and collaboration. As an Infra Management Service provider, we have dedicated digital workspace platform services where we transitioned and transformed many of the customers' on-premise platforms to the cloud with respect to device management and infrastructure services. Happiest Minds has a dedicated digital workspace service team that continuously works and implements the latest market strategies to support our customers on Microsoft365 services, Unified Endpoint Management and other infra-areas across the globe.

Author Bio

Sachin SK is a Digital Workspace Service Architect with over 16+ Years of experience in End User Computing and Cloud Services (EUCS). He has spent many years in consulting services for EUCS platforms, involved in Transition and Transformation projects with the successful implementation of Infra technologies such as VDI, SCCM, Intune MDM, and MAM configurations, Patch Management for Windows, Servers, Image Management for Windows and MacOS migrations. He has supported plenty of application migration with repackaging for many platforms by delivering various format types such as MSI, App-V, MSIX, Intune Win32, LoB, and VMWare AppStack to all global customers. Sachin is responsible for DWS Practice delivery with respect to planning, designing, and implementing the infrastructure core deliverables.

Happiest Minds Technologies Limited (NSE: HAPPSTMNDS), a Mindful IT Company, enables digital transformation for enterprises and technology providers by delivering seamless customer experiences, business efficiency and actionable insights. We do this by leveraging a spectrum of disruptive technologies such as: artificial intelligence, blockchain, cloud, digital process automation, internet of things, robotics/drones, security, virtual/augmented reality, etc. Positioned as 'Born Digital . Born Agile', our capabilities span digital solutions, infrastructure, product engineering and security. We deliver these services across industry sectors such as automotive, BFSI, consumer packaged goods, e-commerce, edutech, engineering R&D, hi-tech, manufacturing, retail and travel/transportation/hospitality.

A Great Place to Work-Certified™ company, Happiest Minds is headquartered in Bangalore, India with operations in the U.S., UK, Canada, Australia and Middle East.

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

www.happiestminds.com

business@happiestminds.com