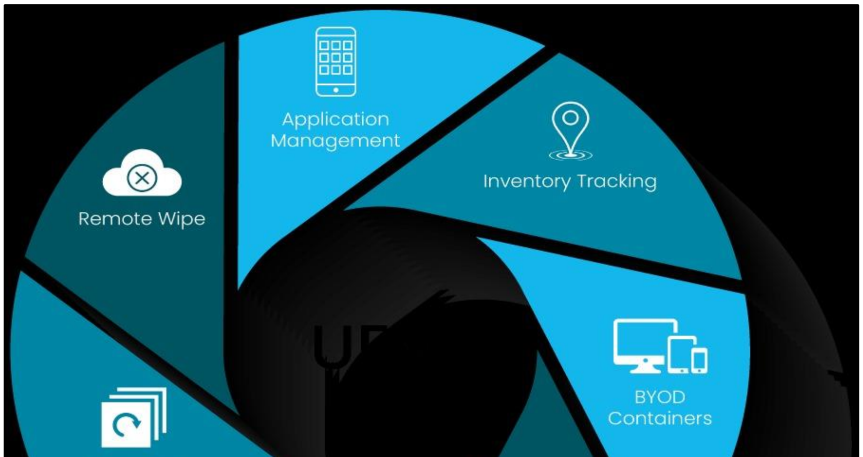
What is unified endpoint management (UEM)?

What is UEM?

UEM (unified endpoint management) is software that enables IT and security teams to monitor, manage and secure all of an organization’s end-user devices, such as desktops and laptops, smartphones, tablets, wearables and more, in a consistent manner with a single tool, regardless of operating system or location.

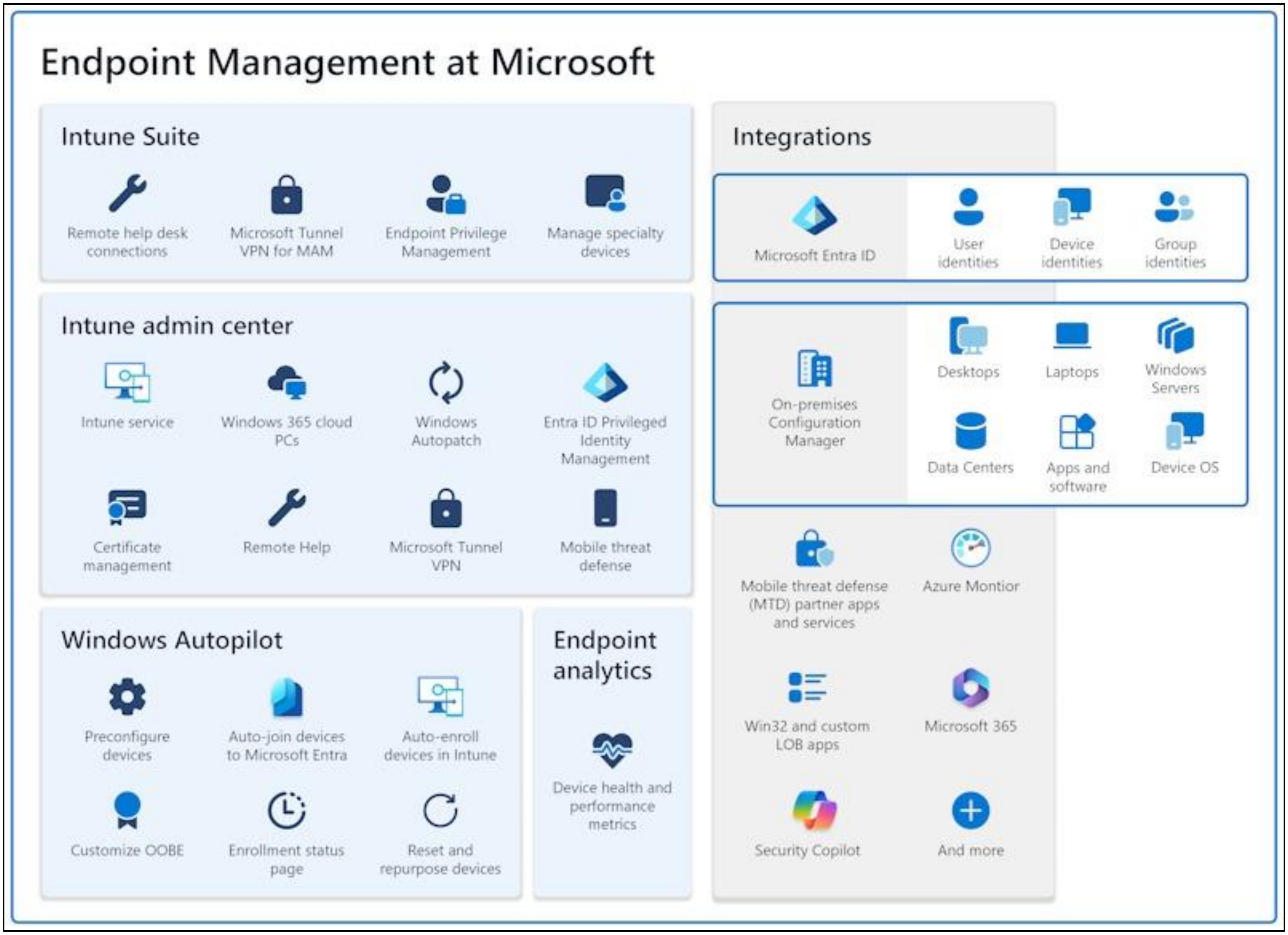


UEM strengthens endpoint security by simplifying it, enabling security and IT teams to protect all endpoint devices by using one tool in one consistent way.

A relatively new technology, UEM combines the capabilities of legacy mobile management solutions, including mobile device management (MDM) and mobile application management (MAM), with those tools used to manage on-premises and remote PCs.

Unified Endpoint Management (UEM) was already widely used for handling bring your own device (BYOD) programs and hybrid workforces that combine on-premises and remote setups. Its adoption surged as security and IT teams adjusted to support expanded work-from-home (WFH) initiatives following the onset of the COVID-19 pandemic.

Endpoint Management at Microsoft



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 Montior

Win32 and custom LOB apps

Microsoft 365

Security Copilot

And more

The evolution of UEM

UEM is the latest in a series of mobile security management tools, which are tools that emerged and evolved in response to the changing relationship between organizations, employees, mobile devices and working styles over the last two decades.

From MDM...

The first mobile devices introduced in the workplace were company-owned and mobile device management (MDM) tools were developed to enable IT administrators to manage and secure these devices. MDM tools gave administrators total control over all features of a device. They might provision, enroll and encrypt devices, configure and control wireless access, install and manage enterprise apps, track the location of the devices, and lock and wipe a device if it was lost of stolen.

...to MAM...

MDM was an acceptable mobile management solution until smartphones became so popular that employees wanted to use their personal smartphones for work (instead of carrying both a work and a personal device). BYOD was born. And soon, employees bristled at surrendering total control of their personal phones and personal data to MDM.

A new solution, mobile application management (MAM), emerged. Rather than managing the entire mobile device, Mobile Application Management (MAM) specifically focuses on app oversight and control. With MAM, administrators might take total control over corporate apps and the corporate data associated with them; they might also exercise enough control over employees' personal apps to protect corporate data, without touching or even seeing employees' personal data.

...to EMM...

But MAM solutions also found their limits, most of which resulted from their sheer inability to keep pace with the explosion of new apps employees might add to their iOS or Android devices.

In response, vendors combined MDM, MAM and some related tools to create enterprise mobility management (EMM) suites. EMM provided the corporate data security of MDM, the superior employee experience of MAM, and management and security control over all devices used outside of the office—not only smartphones, but off-site laptops and PCs too.

...to UEM

EMM left one final endpoint management gap (and potential security vulnerability). Because it didn’t offer capabilities for managing onsite end-user devices, it required administrators to use separate tools and policies for onsite and off-site device management and security. This created more work, confusion and opportunity for error, right about the same time that more employers were trying to let more employees work from home.

Evolution

With new types of devices being used in the workplace, administration of traditional laptops, desktops and new devices was a challenging task for IT administrators. Traditional CMTs (client management tools) lacked some features for a complete approach to endpoint management. The rise of UEM was also a result of the adoption of newer enterprise friendly platforms like Windows 10, and iOS 11.
Differences between MDM, EMM and UEM

- MDM controls mobile device functionality and converts it into a single purpose or dedicated device. It has features like device enrollment, remote control, device lockdown, and location tracking
- EMM offers all MDM features, and also provides Mobile Information Management, Bring Your Own Device, Mobile Application Management and Mobile Content Management.
- UEM provides enterprises management of mobile devices as well as endpoints like desktops, printers, IoT devices and wearables from a single management platform.

Key Processes in UEM:

1. Enrollment:

Devices are enrolled into the UEM system using methods like QR codes, bulk enrollment programs (like Apple's DEP or Android's ZTE), or manual registration.

2. Configuration Management:

UEM allows administrators to configure device settings, including password policies, encryption, network configurations (Wi-Fi, VPN), and application settings.

3. Software Distribution:

UEM enables the deployment of applications, updates, and patches to managed devices, ensuring they have the necessary software and are up-to-date.

4. Security Policy Enforcement:

UEM enforces security policies across all managed devices, including password complexity, data encryption, remote lock and wipe capabilities, and restrictions on file sharing.

5. Monitoring and Management:

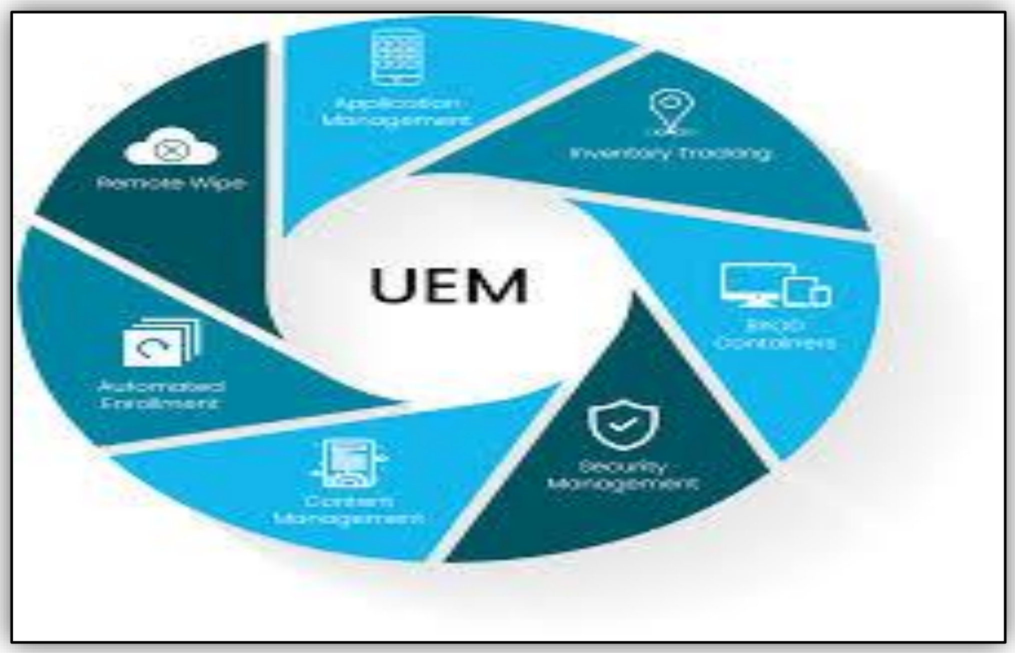
UEM provides real-time monitoring of device status, user activity, and security threats, enabling proactive management and response to potential issues.

6. Remote Actions:

UEM allows administrators to perform remote actions on devices, such as locking, wiping, or restarting them, particularly in cases of lost or stolen devices.

7. Compliance Management:

UEM helps organizations meet compliance requirements by ensuring that devices adhere to security policies and regulations.



Examples of UEM in Action:

- ### Secure Access to Corporate Resources:

A company uses UEM to ensure that all employees connecting to the corporate network with their mobile devices meet specific security requirements (e.g., strong passwords, encryption) before granting access.

- ### Remote Troubleshooting:

An IT administrator uses UEM to remotely troubleshoot a user's laptop that is experiencing issues, without needing physical access to the device.

- ### Protecting Sensitive Data:

If a company-issued laptop is lost or stolen, the IT team can use UEM to remotely lock the device and wipe all sensitive data from it, preventing a data breach.

- ### Managing Application Updates:

UEM automatically pushes out software updates to all managed devices, ensuring that employees are using the latest and most secure versions of applications.

- ### Separating Work and Personal Data:

UEM can create separate work profiles on personal devices, ensuring that company data is kept separate from personal data and preventing it from being shared with unauthorized users.