WHITEPAPER

Understanding Unified Endpoint Management

By 42Gears Team

Table of Contents

Introduction

The enterprise workplace has come a long way from accommodating largely Windows-based desktops and laptops to mobile users working on personally-owned laptops, tablets and smartphones. At the beginning, when the need was limited to managing desktops, IT used traditional **Client Management Tools** (CMT) to supervise hundreds or thousands of IT distributed Windows systems.

Client Management Tools (previously known as **PC Configuration Lifecycle Management** [**PCCLM**] tools) manage the configurations of client systems. Specific functionality includes OS deployment, inventory, software distribution, patch management, software usage monitoring and remote control. Desktop support organizations used client management tools to automate system administration and support functions that would otherwise be done manually.

But with the advent of enterprise mobility followed by BYOD and the Internet of Things (IoT), client management tools (CMT) started falling short when it came to managing new devices and technologies.

Evolution of UEM

In the last few years, organizations have started using **EMM** tools to manage and secure their mobile devices, laptops and Macs. As more and more companies across the globe are transitioning to Windows 10, iOS11, macOS High Sierra and ChromeOS, the demand for a common management platform has increased substantially. Also, the rise of new technologies such as **Enterprise of Things** (**EoT**), including sensors, beacons and other similar devices, are encouraging organizations to look for a single solution that will provide a unified approach towards mobility management.

As per Gartner Magic Quadrant Report for EMM: "EMM is quickly no longer meeting the requirements for organizations as client computing merges with mobile computing to form end-user computing groups. This has created the need for a single solution to manage both traditional client devices as well as mobile devices. Both Apple and Microsoft have been adding MDM APIs in their platforms to facilitate this convergence".

CMT and EMM tools have very different ways of functioning. Organizations moving towards EMM would require a separate set of staff and an extensive training schedule for their IT workers to adapt to the new solution. It made sense to find a unified platform that could manage all devices from a single platform.

IT admins using legacy CMT solutions have to spend time and effort to create custom and complex distribution packages that are pushed out to network connected desktops or devices over the LAN. This makes it difficult to add new devices to the system as they have to be updated with all the requisite applications again. It is a resource and time-consuming process. On the other hand, EMM supports device roaming and remote device and data management. Users can acquire any device, operating on any operating system and use an EMM portal to configure apps and settings on the device over the air, as per corporate settings and policies. Using a corporate app store, IT can also push out enterprise applications and updates to thousands of devices roaming globally.

Connectivity and consistency in management and security of devices is important to ensure user productivity and enterprise data protection. Differences in security and management policies to control devices, applications and information are one of the main reasons for breaches in the security infrastructure of a company. It is also important for enterprises to offer consistent mobile access to necessary applications and data for uninterrupted user productivity. A single set of enterprise management and security policies that can be applied across all devices and users will work much better than two separate sets of tools.

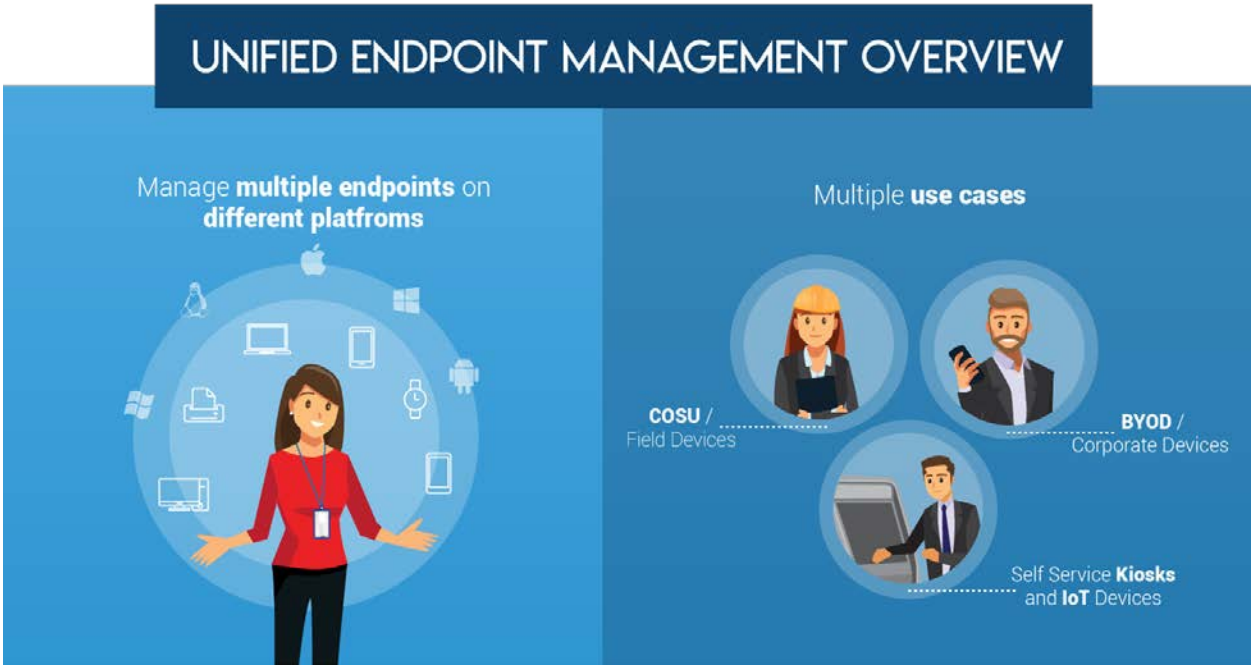
UEM Market trends and Size

Rise of New Technologies; driving the shift to Unified Endpoint Management

With Windows 10 introducing tools for app development and a set of API's for desktop and mobile devices, IT admins can push all necessary applications from a single secure and corporate approved app store. It can manage applications and information on devices as well as the corporate network in a much more streamlined manner. Windows 10 also delivers several other critical enterprise management features that are required by IT admins across devices. In essence, Windows 10 has been a huge driving force for adoption of EMM across industries.

Windows 10, ChromeOS and macOS Sierra has helped Enterprise Mobility Management Solutions to evolve and deliver a unified capability to manage all laptops and desktop mobile devices and applications. Convergence of technology will enable support of common platforms like iOS11 for iPhones and iPads, Mac High Sierra for iMacs and MacBooks, Windows 10 for rugged and mobile devices.

Enterprises are expanding their IT capabilities to adopt a Unified Endpoint Management platform that not only simplifies managing and securing of devices but also helps to cut the cost of running a mobile workplace, pushing mobile enterprises into the age of IoT.



Components of UEM

The adoption of traditional and non-traditional mobile devices across organizations on a large scale is one of the key drivers of UEM. UEM addresses all the problems faced by IT managers by extending the MDM and EMM solutions beyond smartphones and tablets.

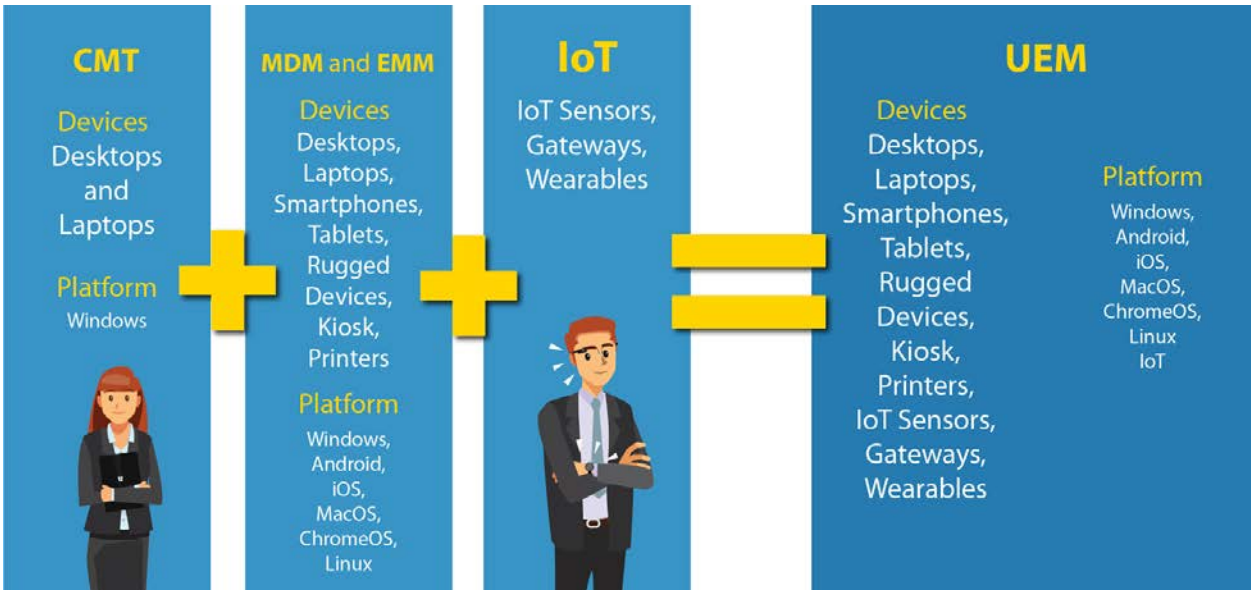
Here are the essential components which define the attributes of UEM solution.

Client Management Tools (CMT):

Until a decade ago, IT managers were using Client Management Tools to combat different challenges in the computing environment which were limited to desktops and laptops. CMT allowed organizations to keep the desktop and mobile environment running smoothly and efficiently while improving service to end-user customers.

Mobile Device Management (MDM):

Eventually new mobile devices started entering the fray, and IT had to manage additional devices along with the existing Windows PCs. Thus, the proliferation of multiple endpoints led to the rise of Mobile Device Management solution.



IT admins had to remotely manage different devices based on different operating system. There was a greater need to access, control and secure the OS and the apps used in it. This was the time when Windows 8.1 dominated the market.

An MDM solution allowed the admins remotely manage all endpoints and enable the deployment, enrolment, grouping, provisioning, decommissioning and platform management of mobile devices. Enterprises were able to to secure, monitor and manage any ownership-based devices such as laptops, smartphones and tablets through MDM solution.

MDM solution enabled admins to configure Wi-Fi access, install and manage enterprise apps as well as remote lock and wipe corporate data to ensure security in cases when the device was lost or stolen.

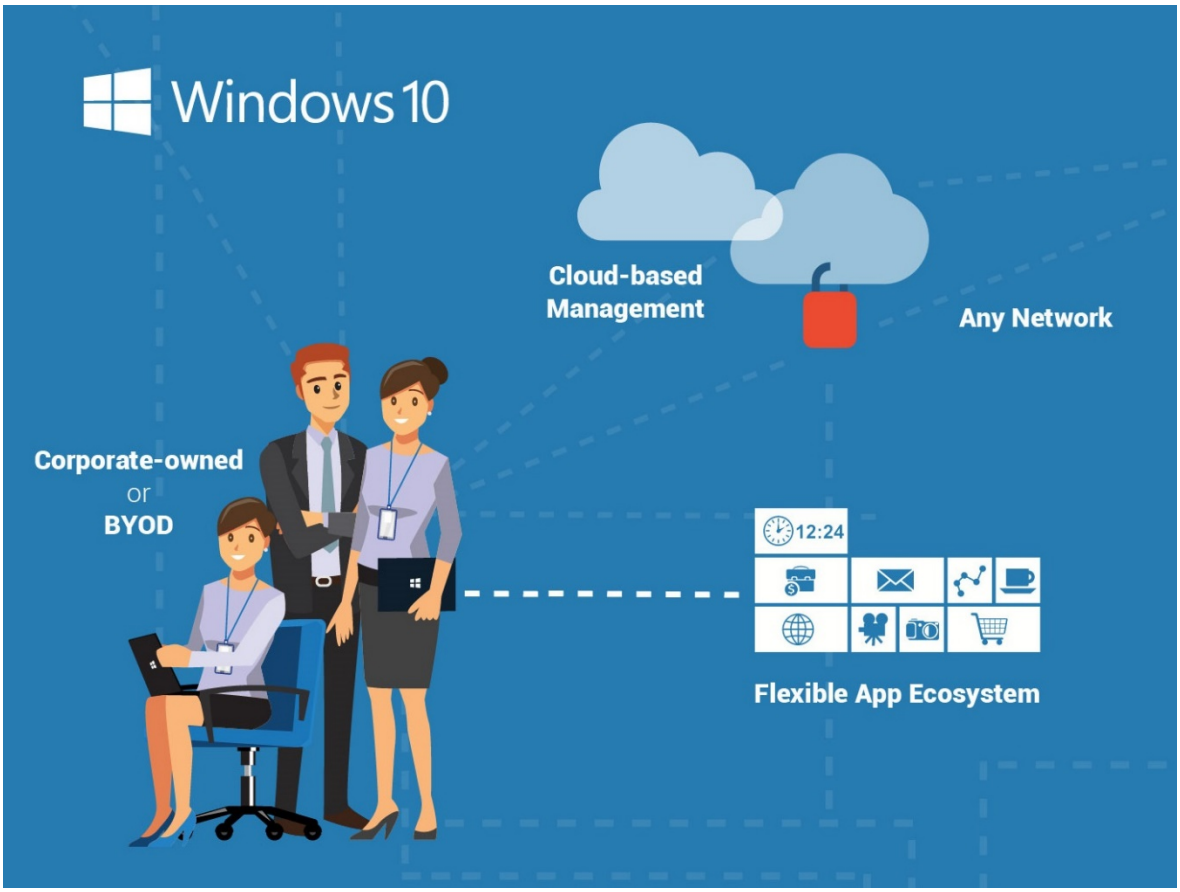
However, the rapid rise in other versions of each endpoint such as Chromebooks, Android and iOS devices called for the need to develop an efficient solution – Enterprise Mobility Management (EMM) which could manage them all.

Enterprise Mobility Management (EMM):

The Enterprise Mobility Management (EMM) tool evolved from MDM and was equipped with features such as containerization, identity and access management, application management and content management.

Mobile Application Management (MAM) allows enterprises to apply management and security policies such as app distribution, app license management, administrative push, whitelist or blacklist applications and data encryption. It also protects corporate data by restricting access to applications based on user role.

Identity and access management policies focus on verifying the identity of users and devices through digital certificates. Single Sign-On (SSO), certificate management, authentication through device enrolment are some of the core features of Mobile Identity Management (MIM).



The Mobile Content Management feature secures corporate data distribution to mobile devices by allowing enterprises to apply content level policies such as device independent encryption keys, authentication and file sharing.

IoT

IoT sensors, gateways and wearables are defying the traditional approach of securing and managing mobile devices. These devices have remote connectivity challenges, limited interfaces and unclear security implications which qualifies them for central management.

Benefits of UEM

UEM platform integrates with a wide range of management tools, existing enterprise software systems and third-party technical platforms to better control and drive value from IT assets. At its core, UEM is about viewing all IT assets through "**a single pane of glass**" as part of a broader business strategy, rather than a separate technology category.

Here are some of the key benefits that enterprises can derive from UEM:

1. UEM removes the hassle of managing multiple tools, improves user experience and reduces IT management cost

UEM solves the daunting task of managing several different endpoints with multiple tools. In today's business ecosystem, employees use at least two or more devices to perform various business tasks based on various OS and different versions. The centralized nature of UEM provides a high degree of visibility to manage every device, platform, configuration and application.

This results in a consistent user experience across all devices and enables them to work according to their convenience, thereby increasing productivity.

Further, UEM automates IT processes such as provisioning, auditing and tracking endpoints, and Data Loss Functions (DLP) which reduces IT management costs.

2. UEM enhances IT Security

A UEM platform acts as a strict defense against any threat by enforcing policies on the users based on various levels. UEM can help IT to provide seamless access to corporate data and ensure that all the endpoints comply with standard security policies.

UEM lets IT admins provide personalized access to specific applications and corporate data based on an advanced level such as user business role, location and usage patterns, regardless of the device ownership or network. Maintaining a single set of user profile for access rights, privileges and configurations get rid of the struggle of duplicate management while ensuring a consistent experience.

Apart from this, admins can also enforce timeout values, passcodes and logout policies.

3. UEM enables better informed business decisions

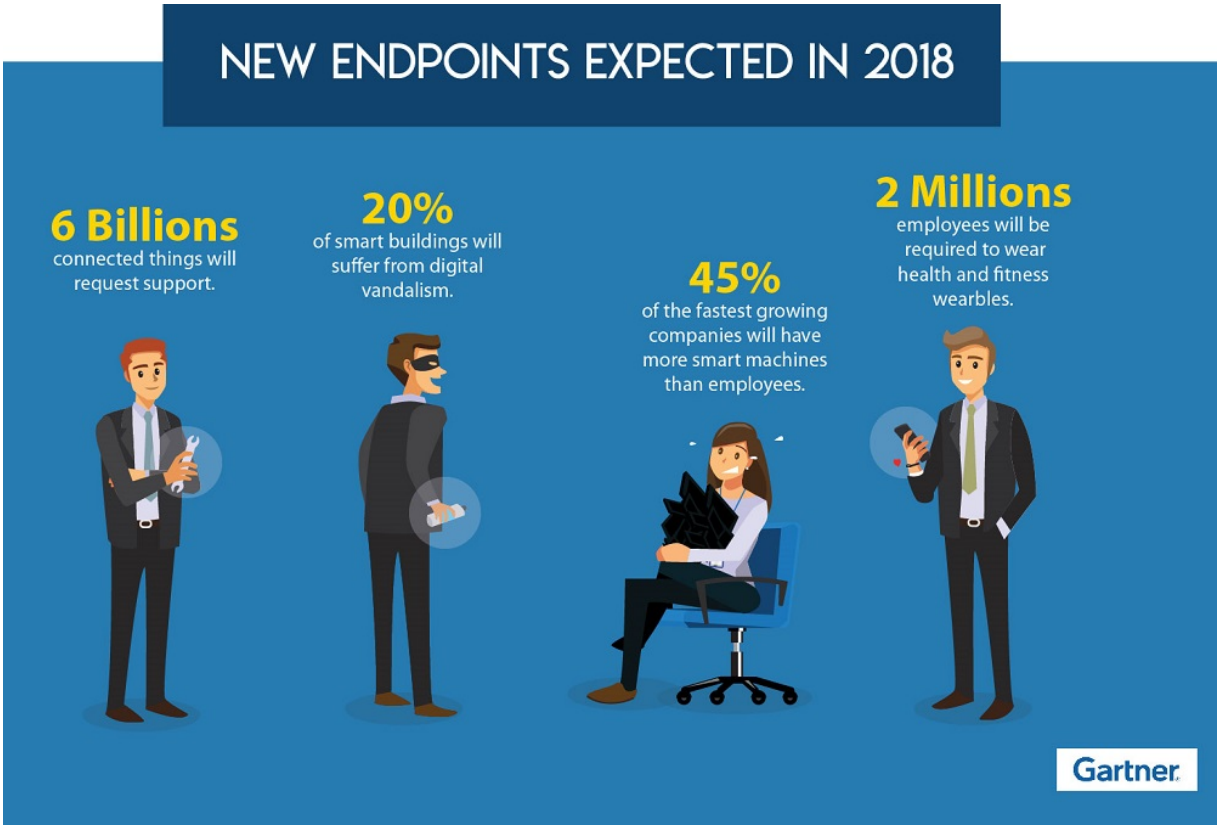
As modern day businesses have already started to integrate artificial intelligence for data crunching and predictive analysis, cognitive-enabled-UEM can analyze massive amounts of data generated through all endpoints. The cognitive approach of UEM can offer diagnostic and predictive tools to analysts through which analysts can process and interpret the data. This data is generated through all endpoints and their users, apps and content. Security teams and analysts can use this data to quickly identify threat events and prepare for impact.

Hence, it is easier for business decision makers to track the data, prepare customized reports and make informed decisions. The UEM solution can be customized as per the needs and infrastructure of different enterprises and their respective vulnerabilities.

Who needs UEM?

Security managers and system administrators who face trouble in ensuring security compliance and managing multiple device types, user accounts and permissions should consider UEM solution. It will keep them a step ahead while assessing the security of endpoints, maintaining network uptime and providing an improved user experience.

According to a report from Gartner, 2017, "20.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020. Total spending on endpoints and services will reach almost $2 trillion in 2017." As the traditional approach is no more enough to manage the newly evolved non-Windows endpoints such as IoT sensors, point-of-sale devices, ATM machines, thermostats, rugged kiosks and voice control units. Clearly, organizations that are unable to adopt new digital business models and improve the end user expectations of consumers are going to fall behind. UEM has the capacity to tame all the endpoints and centrally manage them.



What to consider when looking for a UEM solution?

The following criteria should be considered by enterprises when adopting UEM solution so that it meets modern day requirements:

- It must provide one single platform to view and manage endpoint activities across devices such as - desktops, laptops, smartphones, tablets, laptops, wearables, ruggedized devices, and IoT sensors and gateways, kiosks and printers.
- Support multiple platforms (both existing and emerging) - iOS, MacOS, ChromeOS, Linux, Android, Windows and more.

- Smoothen the transitioning process of the endpoints from older versions to newer versions - Windows XP SP3, Windows Vista, Windows 7 and Microsoft Windows 8 (Windows 7 to Windows 10).
- Enable granular device management policies and patch management policies, allowing IT admins to maintain and manage legacy devices.
- Robust security policies which include automated rules enforcement and data loss protection.
- Provide out-of-the-box access to corporate email, Privileged Identity Management (PIM), Intranet and apps.
- Enable admins to detect jailbreaking and rooting on iOS, Android and Windows Phone devices.
- Auditing, tracking, reporting and endpoint inventory capabilities for devices, application and content.
- Support device lifecycle management from deployment, onboarding, management, security, enforcement and decommissioning.
- Streamline and automate tasks which helps to reduce IT overhead cost and reduce hardware expenses.

For a large number of IT organizations, the future lies in Unified Endpoint Management (UEM). It combines the simplicity of CMT with the inclusivity EMM (Enterprise Mobility Management) to offer a single solution that can manage and secure both old and new devices and operating systems, whether laptops, smartphones, tablets or any other device. UEM enables a single unified workspace that makes it easy and consistent to collaborate and access information from any device.

42Gears UEM is an all-powerful management platform that extends the comprehensive capabilities of device, app, content and identity management provided by an EMM solution. It offers over-the-air management of mobile devices, laptops and desktops built on Windows 10, ChromeOS, Linux and MacOS.