

# Complete Guide to Unified Endpoint Management



In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

In this e-guide:

IT staff uses unified endpoint management software to manage a range of devices within the organization. Learn about all the components of UEM in this comprehensive guide.

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

## Complete guide to unified endpoint management

Jack Madden, TechTarget

Unified endpoint management ([UEM](#)) is a category of software that provides management, configuration and security controls for multiple types of enterprise devices and applications.

UEM and its predecessors -- the more narrowly focused enterprise mobility management ([EMM](#)) and mobile device management ([MDM](#)) -- were a response to the wave of new devices that came into the enterprise with the advent of iOS and Android smartphones and tablets, as well as cloud, SaaS, and mobile apps.

UEM is often associated with managing mobile devices and apps, but today's UEM software can manage many other devices, [including macOS](#) and Windows PCs, wearables, IoT devices and ruggedized and embedded devices. UEM can also manage security features and configurations embedded within client apps, on devices that are themselves not managed or owned by the company. Many UEM platforms now also include identity and access management functionality.

When creating a UEM strategy, organizations will have to consider many factors, including how to support different types of devices; how applications will be delivered; how to deal with personally owned devices ([BYOD](#)) and privacy; identity management; network access; and the overall employee experience.

In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

Evolution

Shortly after the arrival of smartphones, products arose to integrate them into the enterprise. Good for Enterprise and Nitrodesk TouchDown provided early enterprise email clients and mobile app management ([MAM](#)), and iOS 4 and Android 2.2 introduced MDM APIs that could be used for remote management by an MDM server.

The first modern MDM products were generally separate from traditional client management tools, which focused on PC management. Later, vendors started to consolidate MDM and MAM into a single platform, and the collective term for products in the [industry shifted](#) from MDM to EMM. EMM products included support for managing devices via MDM APIs and protocols, as well as support for managing apps.

➤ Image on the next page

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

# The evolution of endpoint management: MDM, EMM and UEM

|                 | Mobile device management (MDM)                                                                                                                                                              | Enterprise mobility management (EMM)                                                                                                                                                                                                | Unified endpoint management (UEM)*                                                                                                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION     | Tools that manage mobile devices, mobile users' data and some basic mobile application controls                                                                                             | Tools that manage everything that MDM does, plus offer more granular control over mobile applications                                                                                                                               | Tools that manage everything that EMM does, plus offer full desktop management including desktop OSes, apps and data                                                                                     |
| CHARACTERISTICS | <ul style="list-style-type: none"> <li>Enforce passcodes</li> <li>Install applications</li> <li>Perform remote device wipes</li> <li>Configure corporate profiles for BYOD, COPE</li> </ul> | <ul style="list-style-type: none"> <li>Enforce multifactor authentication</li> <li>Manage enterprise file sync and share</li> <li>Deploy device web browser security settings</li> <li>Apply conditional access policies</li> </ul> | <ul style="list-style-type: none"> <li>Apply EMM controls to PCs and desktops</li> <li>Configure and update desktop and mobile apps at the same time</li> <li>Manage IoT devices and printers</li> </ul> |
| PRODUCTS        | <ul style="list-style-type: none"> <li>VMware AirWatch MDM</li> <li>Citrix XenMobile</li> <li>MobileIron MDM</li> </ul>                                                                     | <ul style="list-style-type: none"> <li>VMware AirWatch EMM</li> <li>Citrix Endpoint Management</li> <li>MobileIron EMM</li> </ul>                                                                                                   | <ul style="list-style-type: none"> <li>VMware Workspace One</li> <li>Citrix Workspace</li> <li>MobileIron UEM</li> </ul>                                                                                 |

\*UEM platforms reflect current offerings, as vendors discontinue the older versions of their tools

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

As the EMM market matured, it transformed into UEM. UEM tools, which combine traditional client management with EMM, emerged via several different approaches.

Some client management tools simply added support for mobile devices via MDM protocols. In other cases, vendors took existing client management platforms and EMM platforms and found ways to link them together, providing a degree of common visibility over both halves.

At the same time, desktop [operating systems](#) started adding support for remote management via their own MDM APIs and protocols. This made it easier for UEM platforms to start supporting desktops, as it was simply a matter of adding more flavors of MDM for different devices. In time, these products incorporated more elements of traditional client management, as well.

UEM platforms continue to develop, largely by [integrating with even more categories of software](#). This can include endpoint security products, identity and access management, performance monitoring, and productivity tools, such as enterprise file sync and share and chat apps.

## UEM vs. MDM vs. EMM vs. client management tools

There are many different terms floating around in the device management industry. New customers must sort out the differences between UEM and MDM, EMM and client management tools. Here's [how UEM compares to other terms](#):

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

- **Mobile device management.** A decade ago, there were many freestanding products that focused on managing mobile devices via MDM APIs and protocols. Today, support for MDM is simply one of many functions in a modern UEM platform.
- **Mobile app management.** Like MDM, freestanding mobile app management products were once common, but this is now a component of UEM.
- **Enterprise mobility management.** Industry trends spread fast, so over the course of a few years, a wave of consolidation and product updates resulted in EMM platforms that included both MDM and MAM functionality. When EMM platforms began supporting macOS, Windows and other devices, industry trends again changed quickly, and *unified endpoint management* became the common term.
- **Client management tools.** Most organizations have likely been using traditional PC-focused client management tools for two decades. Going forward, these systems will likely be augmented or eventually replaced by UEM tools.

## Benefits of UEM

Many organizations waited to adopt UEM. Since smartphones and tablets are consumer devices, many users can configure basic functions on their own. There are plenty of reasons why most organizations [will benefit from UEM](#), however.

Organizations that are highly regulated, use mobile devices for business-critical functions or operate at enterprise scale will have to manage mobile devices no matter

In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

what. It's simply too much of a liability to go without, and managing devices manually can take significant amounts of support time.

Organizations can gain many efficiencies from managing all devices with a single platform, including unified visibility and policies. UEM provides many other benefits, such as management that works from anywhere, automation, [cloud-native platform architectures](#), easier integration with security products and analytics capabilities. Moving to UEM gives organizations a chance to transition to management products that are based on concepts that are two decades newer than traditional client management tools.

## Components

Unified endpoint management platforms encompass many components.

**Device management.** The primary component of UEM is device management, connecting devices to the service via an MDM protocol. MDM protocols allow the service to remotely interact with a device, sending it configurations, commands and queries. There's no need for a device to be on a corporate network or VPN, as MDM protocols are designed to work over the internet.

Device management tasks include configuring encryption; setting passcode policies; managing OS and app updates; configuring Wi-Fi and VPN connections; configuring

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

email and other accounts; device location tracking; remote lock, unlock, and wiping of the device; and configuring data loss prevention settings.

**OS and device support.** UEM often focuses on [mobile devices](#), but most offerings support multiple types of clients.

[Apple iOS](#) is supported by Apple's MDM protocol, which does not require an agent. IOS management involves several cloud services from Apple -- including the Apple Push Notification Service, and [Apple Business Manager](#) and Apple School Manager for purchasing apps, managing Apple IDs, and enrolling devices in bulk. Apple MDM has [several different modes for different scenarios](#), including User Enrollment mode for BYOD, Device Enrollment, and Automated Device Enrollment and Supervised mode for corporate devices. Apple has expanded its MDM protocol to cover macOS and tvOS devices, and macOS management [is a rapidly growing and evolving field](#).

In the past, [Android](#) management was fragmented. But, today, the Android Enterprise management framework -- which emerged in Android 5 and is now included in almost every Android device -- is quite powerful and flexible. Android Enterprise has [management modes](#) for [dedicated kiosk devices](#); corporate devices; and devices with mixed work and personal usage, via work profiles.

Windows management has long been the domain of traditional client management tools, but the addition of an MDM protocol in Windows opened up an opportunity for UEM vendors to more easily enter the market. The nature of legacy applications means

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

that it will take many years for the enterprise to transition completely from client management to MDM, so today, the state of the art is to combine elements of both.

UEM can also manage several other types of devices:

- Chromebooks and Chrome OS devices connect to a proprietary cloud service offered by Google, but several UEM platforms integrate with Google, using it as a middleware service.
- [Many ruggedized devices](#) -- as well as wearable devices, such as smart glasses and virtual or augmented reality goggles --, run Android OS or inherit management capabilities from paired smartphones. Managing these devices is [possible with some UEM products](#).
- Some UEM platforms also manage or integrate with virtual desktops.

➤ **Image on the next page**

## In this e-guide

- Complete guide to unified endpoint management p. 2
- Evolution p. 3
- UEM vs. MDM vs. EMM vs. client management tools p. 5
- Benefits of UEM p. 6
- Components p. 7
- UEM software vendors p. 18
- Choosing the right UEM product p. 20
- Deploying UEM p. 22
- UEM market p. 23
- Further reading p. 24

## UEM product support for IoT and wearables

| VENDOR     | PRODUCTS                    | SIMPLIFIED PROVISIONING | LIFECYCLE MANAGEMENT | SECURITY          | APP DEPLOYMENT / CONFIGURATION | KIOSK SUPPORT | REMOTE MGMT/ SUPPORT | OS SUPPORT                              |
|------------|-----------------------------|-------------------------|----------------------|-------------------|--------------------------------|---------------|----------------------|-----------------------------------------|
| VMware     | Workspace One               | Yes                     | Yes                  | Yes               | Yes                            | Yes           | Yes                  | Android Enterprise, Windows 10 IoT      |
| 42Gears    | SureMDM SureLock            | N/A – smart-watches     | Yes                  | Yes               | Yes                            |               | Yes                  | Wear OS                                 |
| Microsoft  | Endpoint Manager            | Yes – Windows Autopilot |                      | Device-based only |                                | Yes           |                      | Android, Windows 10 IoT                 |
| SOTI       | MobiControl                 | Yes                     |                      | Yes               | Yes                            |               | Yes                  | Android, Linux                          |
| IBM        | MaaS360                     | Yes                     |                      | Yes               | Yes                            | Yes           |                      | Android, Windows 10 IoT, Android Things |
| BlackBerry | Unified Endpoint Management |                         |                      |                   | Yes                            |               |                      | Android                                 |
| MobileIron | Unified Endpoint Management |                         |                      |                   |                                |               |                      | WatchOS, Wear OS, Android               |
| Citrix     | Citrix Endpoint Management  |                         |                      |                   |                                |               |                      | Android                                 |



NOTE: BLANK CELLS INDICATE INFORMATION IS NOT AVAILABLE. ILLUSTRATION: ARTRESPIR/ADOBE STOCK

©2020 TECHTARGET. ALL RIGHTS RESERVED. TechTarget

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

**Deployment and enrollment.** Traditional client deployment involves a labor-intensive process of device imaging, but MDM protocols and UEM platforms offer a much more convenient process.

Apple iOS, Android, macOS and Windows 10 devices can be enrolled manually through the user interface, but these OSes also offer new automatic enrollment and provisioning processes. Examples include Apple Automated Device Enrollment, Windows Autopilot and Android zero-touch enrollment.

When almost any modern device is powered on for the very first time, it will check in with a cloud service. If it's a corporate device, it can be redirected to the appropriate UEM platform, on which the device can be enrolled and configured automatically. Since there's no need for IT staff to perform a traditional imaging process, OEMs can ship devices directly to end users.

**BYOD and privacy.** In many enterprises, the first iOS and Android devices were often personally owned devices that users purchased on their own and then wanted to use for work. This resulted in corporate data and apps existing on the same device as personal apps and data, which brought unprecedented security and privacy challenges. Many components of UEM platforms exist and have evolved over the years specifically to deal with BYOD and privacy.

Many IT departments realized that they just couldn't treat a personal device like a corporate device, with a blanket of locked-down policies. Instead, they introduced MAM to apply corporate policies to specific apps and data, while leaving other apps

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

and data alone. This can be done by using specialized applications that connect directly to the UEM server, [even if the device itself is not enrolled](#), or via operating systems that can [separate work from personal features](#).



ART: AKINDO/GETTY IMAGES

©2020 TECHTARGET. ALL RIGHTS RESERVED TechTarget

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

UEM platforms can also limit administrator roles so that admins cannot see or do anything that may affect the personal side of a device, or platforms may have roles dedicated specifically to privacy auditing and control.

Some UEM vendors provide end user-facing resources that explain what their company can and can't do. For example, no MDM protocol allows a UEM server to read personal text messages, personal emails, or see personal photos.

**Mobile app management.** MDM protocols can enable UEM services to install apps on devices and manage settings within the apps if they are exposed using [app configuration standards](#). MDM protocols also have features that can define how corporate apps interact with personally installed apps, such as file-sharing controls and per-app VPNs.

When devices aren't enrolled in MDM -- for example, devices used by contract employees, partners and some employees' personal devices -- UEM platforms can treat the app as an endpoint rather than a device and focus on building management features into an application. Encryption, passcode challenges, [remote wipe](#), data loss prevention controls, settings configuration, VPNs and other features can all be integrated directly into the code of an app.

These apps must be specifically developed, however, so only certain apps will have these features. UEM vendors generally provide basic apps like email clients and browsers, and offer SDKs and [app wrapping](#) tools for customers and independent

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

software vendors that want to create their own apps that are compatible with a particular UEM platform.

UEM platforms generally provide a repository for enterprises to host their in-house apps, or they can direct devices to install apps that are hosted in public app stores. For end users, UEM platforms provide an application catalog so that users can install apps via self-service. Some of these app catalogs have evolved into complete [digital workspace](#) offerings, with links to launch web and mobile apps with single sign-on, integration with remote desktop clients and other features, such as micro apps, content repositories, company directories and even virtual assistants.

**Identity and access management.** The usage of SaaS apps rose concurrently with the spread of mobile devices. Just as UEM arose to deal with mobility, so did new cloud-based identity and access management ([IAM](#)) products and standards. Many SaaS apps use standards such as Security Assertion Markup Language and OAuth to federate user identities and provide single sign-on.

Since then, UEM and IAM have [gone hand in hand](#), and some UEM platforms even provide their own identity provider functionality.

There are many ways that UEM and identity management can work together, whether they're part of the same platform or separate products. UEM can distribute certificates to mobile devices, which then can be used to authenticate to an identity provider. This ensures that only devices that are enrolled in UEM can access enterprise apps, and since entering passwords on a small screen can be challenging, single sign-on is

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

especially important for providing a pleasing and secure user experience on mobile devices.

UEM can provide additional context for access and authentication decisions. For example, a conditional access policy may consider the device location, management status, patching status and other signals from the UEM when deciding whether to grant access, ask for additional authentication factors, block access, or take other actions.

**Security.** Mobile operating systems have very different security models than traditional desktop operating systems. Mobile devices are always connected to the internet, and they can easily be lost.

Mobile OSes are [sandboxed](#), so apps only interact with each other and the OS in a very limited and supervised way; there are user-controlled permissions protecting sensitive data. Mobile apps must be signed and generally come from curated app stores with security reviews and mechanisms for revoking apps.

A significant proportion of mobile security tasks are a matter of monitoring and configuring devices via MDM. For example, is the device free of [sideloaded applications](#)? Is it patched and encrypted? Are enterprise apps configured to connect via a VPN? Are proper data loss prevention restrictions in place? IT can also remotely lock or erase devices using over-the-air technology.

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

This is not to say that [mobile devices are completely secure](#). Just like any operating system, there are vulnerabilities that IT admins must patch. In particular, organizations also worry about [phishing](#), [social engineering](#) and other identity and authentication issues on mobile devices.

Mobile threat defense (MTD) products have emerged [to augment UEM](#). MTD tools generally cover four different areas, including device integrity, which includes jailbreak and root detection; network security to prevent man-in-the-middle attacks; mobile app reputation service; and phishing prevention.

Phishing prevention is especially important because many of the visual cues that help users spot phishing attacks are obscured on mobile devices, and mobile chat apps generally don't run through filtering systems the way that enterprise emails do.

MTD can be deployed to devices as a freestanding agent or via an SDK that is integrated into other apps. MTD deployments [benefit greatly from UEM integration](#), as UEM platforms can provide more visibility than agent apps alone and offer multiple ways to remediate threats.

**UEM and artificial intelligence.** Many products in the security and management space have been marketing artificial intelligence and machine learning features, and UEM is no exception. [AI and machine learning can augment UEM products](#) in a variety of ways. Vendors may train AI and machine learning models using data from their entire customer base, from a single customer or from a single user, depending on the application.

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

# Adding intelligence to 5 UEM apps

When assisted by AI, critical applications in unified endpoint management get a lot smarter and faster.



ILLUSTRATION: GIGABONITO/GETTY IMAGES

©2019 TECHTARGET. ALL RIGHTS RESERVED. TechTarget

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

AI and machine learning can recommend device management policies and spot configuration anomalies so that administrators don't have to create policies manually. For security purposes, AI and machine learning are often used to identify anomalous device, user or application behavior and configurations, alerting IT to any issues. This is especially common in access management flows, where the technology can be used to adjust authentication requirements.

For end users, AI and machine learning often appear in the form of natural language processing and chatbots. For example, a user could make a request to enroll a new device, install an application or even access helpdesk resources via interfaces in UEM products.

## UEM software vendors

While a few very broad UEM products receive the most attention in the industry, there are still a [wide variety of vendors](#) that support various combinations of different MDM APIs and protocols, security, mobile app management, client management and other related features.

These vendors provide the broadest UEM offerings:

- **Microsoft.** For many years, Microsoft dominated client management with System Center Configuration Manager (SCCM). [Microsoft's EMM platform](#), Intune, was a bit later to the market than other offerings, a strategy that is

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

typical of Microsoft. Microsoft is now [bringing Intune and SCCM together](#) as Microsoft Endpoint Manager and is taking advantage of [sales of Windows and Office 365](#) to get it in front of many customers.

- **VMware.** VMware acquired EMM vendor AirWatch in 2014, and now sells its very broad UEM platform [under the Workspace One brand](#). Workspace One now has integrations for security, identity management, micro apps and desktop virtualization. Lately, VMware has been investing [heavily in Windows 10 management](#).
- **MobileIron.** MobileIron is one of the few independent, pure-play UEM vendors left. [Recent efforts](#) have focused on conditional access, mobile threat defense and passwordless authentication.
- **Citrix.** Desktop virtualization vendor Citrix acquired EMM vendor Zenprise in 2013 and micro-app platform Sapho in 2018. Citrix is seeking to move beyond their core desktop virtualization market to general purpose uses.
- **BlackBerry.** BlackBerry began offering support for iOS and Android management in 2012, but it really became a player in the UEM space with the acquisition of Good Technology in 2015. BlackBerry has undergone a transition from a hardware vendor to a software vendor, and the company now focuses on security, most recently with the acquisition of Cylance.
- **IBM.** IBM is active in the UEM market with MaaS360, which IBM acquired from Fiberlink Communications in 2013. MaaS360 benefits from IBM's broad portfolio of related products, including identity management, cloud access security brokering and mobile threat defense. MaaS360 has also integrated both administrator and end user-facing artificial intelligence features from IBM Watson.

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

## Choosing the right UEM product

Unified endpoint management is a "sticky" product; once devices are enrolled, it's difficult to unenroll them and connect to a different product without manual, in-person support. Therefore, [choosing a UEM product](#) is an important decision.

Customers should consider the following questions:

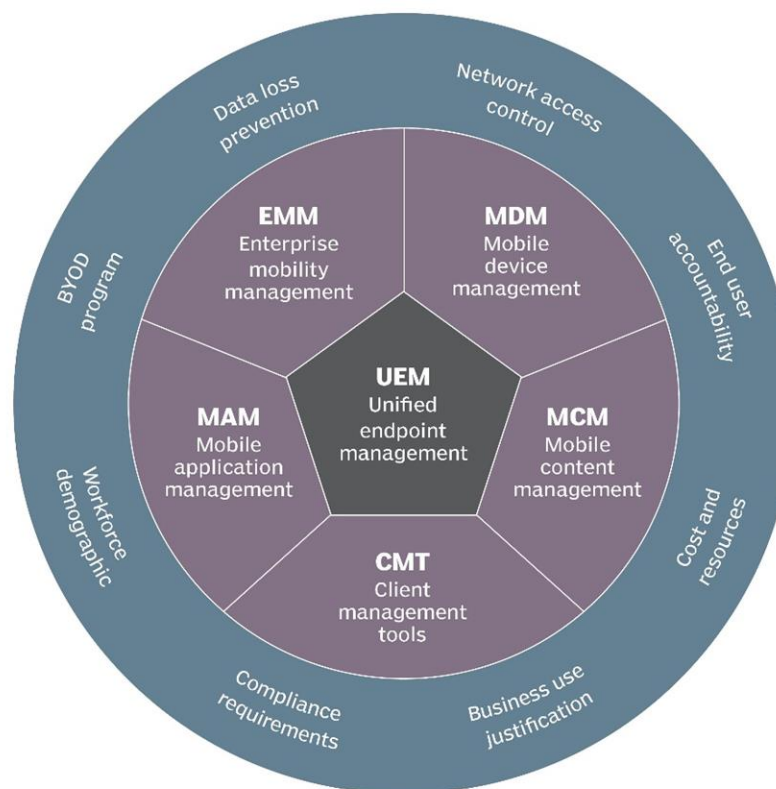
- Does the product support all the operating systems and deployment models -- for example, BYOD, ruggedized or corporate -- that the organization uses?
- Will the product support future deployment scenarios, such as IoT devices, Linux, macOS or Windows 10?
- Besides endpoint management, what other services -- such as app catalogs, browsers, email clients, productivity apps or micro apps -- does the product offer?
- Does the UEM integrate with the appropriate identity and security products? Or, what bundled security and identity features are available? Do they provide timely support for new iOS, Android and other features?

Like any software buying decision, customers must consider whether the vendor can meet their desired service-level agreement and regulatory certification requirements, and whether the vendor has an established relationship and trust with the customer. Finally, customers should pay attention to the vendor's approach to BYOD, privacy and user experience.

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

# The components of UEM



## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

## Deploying UEM

Like any project, deploying UEM requires careful planning. But when end users, BYOD and personal privacy are involved, IT must take extra care. [Organizations must inform users](#) of what the company can and cannot do and see on their personal devices. IT departments must be aware that many decisions about BYOD policies are not theirs to make alone; they must consult human resources and legal departments, as well.

Device enrollment is often one of the most challenging aspects of a UEM deployment. [Automatic device enrollment](#) can save significant amounts of labor but requires coordination between the UEM platform and the device reseller. Getting end users to enroll devices requires training programs. Even then, achieving compliance can be a challenge.

When [expanding UEM to Windows](#) and macOS, a whole new set of challenges arises. Companies must decide how they're going to translate traditional client management policies to MDM policies, while possibly adopting a new device management platform. It's likely that many organizations will transition to UEM for Windows and macOS over several years, moving department by department, or via attrition.

IT must take precautions when migrating devices from one product to another. Since this process generally involves unenrolling and reenrolling devices, there are several products on the market designed to keep track of devices during the transition.

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

A UEM deployment is not a single project; it is constantly changing. Apple iOS, Android and other [operating systems change every year](#), with new MDM APIs and new features for the enterprise to manage. In addition, users' attitudes towards BYOD change over time as well, and new generations of employees may have different feelings about enterprise management on personal devices.

## UEM market

The UEM market will be evolving rapidly over the next several years. Microsoft is investing in ways to make Windows 10 management and Windows application management easier, including technologies like MSIX App Attach. More organizations are deploying macOS devices. SaaS and mobile app usage continues to expand. As a result, UEM platforms, which today mostly are used for mobile devices, [will be more appropriate for handling all enterprise endpoints](#).

Since UEM, as a concept, is designed around handling diverse endpoints and integrations, it should be well positioned for new types of devices and operating systems that emerge in the future. This is in contrast to traditional client management platforms, which were often designed around a single client OS and management paradigm.

The arrival of iPhones, Android and SaaS apps was a disruption to the Windows-centric IT world of the 2000s. Unified endpoint management will leave enterprises in [a better position for the future](#).

## In this e-guide

|                                                 |       |
|-------------------------------------------------|-------|
| Complete guide to unified endpoint management   | p. 2  |
| Evolution                                       | p. 3  |
| UEM vs. MDM vs. EMM vs. client management tools | p. 5  |
| Benefits of UEM                                 | p. 6  |
| Components                                      | p. 7  |
| UEM software vendors                            | p. 18 |
| Choosing the right UEM product                  | p. 20 |
| Deploying UEM                                   | p. 22 |
| UEM market                                      | p. 23 |
| Further reading                                 | p. 24 |

## About SearchEnterpriseDesktop

With new desktop OSes being released regularly, mobile devices infiltrating the workplace and security risks higher than ever, desktop admins are constantly looking for tools and strategies to help them better deploy new technologies and manage their desktop environments.

Our independent editorial team and expert contributors at SearchEnterpriseDesktop.com, such as 15-year desktop editor, Serdar Yegulalp, offer up news, tips, tutorials, advice and trends on an array of topics—from enterprise application managements and system security management, to overviews of all Windows operating systems—SearchEnterpriseDesktop.com is your home for all things desktop management- and security-related.

**For further reading, visit us at:**  
[SearchEnterpriseDesktop.com](https://www.searchenterprisedesktop.com)

Images: Fotolia

©2020 TechTarget. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher.