

CMT vs UEM

WHY IT'S TIME FOR YOUR BUSINESS TO MAKE THE SWITCH

As UEM technologies witness substantial growth, a viable solution to replace CMTs is emerging.

" The widespread growth of BYOD has led to a significant rise in the use of mobile devices at work. "

58%

of the global market share comprises of mobile devices.

64%

higher smartphone conversion rates compared to desktops.

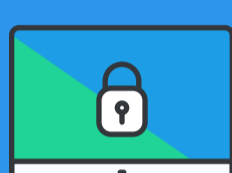
Businesses can no longer solely rely on legacy management tools like CMTs to secure and manage mobile devices.

Which is why they're now making the switch to UEM.

50%

of businesses will be using UEM as their primary PC management tool by 2023, up from **10%** in 2019.

Let's see why CMTs are dropping behind the competition.



CLIENT MANAGEMENT TOOL (CMT)

VS



UNIFIED ENDPOINT MANAGEMENT (UEM)

1: MULTI - PLATFORM SUPPORT

- CMTs provide support for on-premises servers and infrastructure.
- Supports platforms including Linux, UNIX and Windows, along with limited macOS support.
- Lacks support for mobile devices and IoT.

- UEMs primarily support cloud-based infrastructure.
- Provides support for desktops, mobile devices, and IoT, including Apple iOS, Google Android, macOS and Windows.
- Limited support for desktop environments such as Linux and UNIX.

2: DEVICE ONBOARDING

- Supports onboarding via traditional Microsoft Win32 and Mac PKG/DMG packages.
- Admins must manually install packages via a download site, or an external media.
- Admins can embed the device management client/agent into an OS image.

- Supports zero-touch, OTA enrollment to offer effortless enterprise setup.
- Supports BYOD enrollment techniques for Android and iOS.
- Admins can sync existing user accounts from Active Directory, and LDAP, to streamline user onboarding.

3: APP & CONTENT DISTRIBUTION

- Admins can distribute apps, documents and files to client devices.
- Limited support for app distribution to mobile devices.
- Lacks integration with third-party app deployment services.

- Admins can distribute apps, documents and files to endpoints.
- Connects with public app stores, while also supporting private app deployment.
- Integrates with services including Apple Apps & Books, Managed Google Play, and more.

4: UPDATES AND PATCHING

- Supports Windows, macOS, and third-party patch deployment.
- Admins can customize software packages, perform registry changes, client configurations, and more.
- Patch management is limited on mobile devices.

- Provides limited patch management capabilities.
- Admins can schedule, enforce, and delay OS updates
- Supports OTA updates for a range of devices and platforms including iOS, macOS, Android, Windows, and tvOS.

5: ENDPOINT & DATA SECURITY

- CMTs offer software and functionalities to proactively identify and resolve threats.
- Focuses on the security and compliance of servers, laptops and desktops.
- Offers limited security towards mobile devices.

- Focuses on the security and compliance of mobile devices.
- Offers protected containers for BYOD security.
- Provides limited functionality towards desktop security.

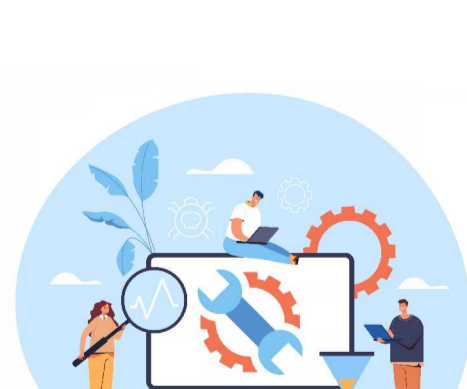
" Although CMTs provide advanced **desktop management** capabilities, better **on-premises** support, and superior **patch management**, UEM is the better choice for businesses aiming to secure and manage **all their corporate and BYO endpoints** from a single **centralized console**. "

Why switch to Unified Endpoint Management (UEM)



UEMs provide flexible licensing, enabling SMBs to scale according to their business growth.

Scalability



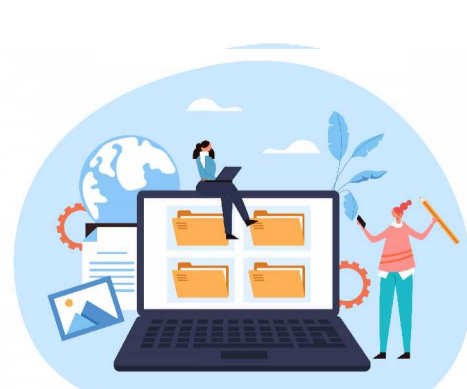
UEMs offer integrations with a host of services, thereby complementing your existing infrastructure.

Third-party integrations



UEMs offer a centralized dashboard, which enables IT to streamline their endpoint management processes.

Centralized management



UEMs provide the ability to secure and manage BYOD devices while enforcing strict data privacy measures.

BYOD support