CMT vs. MDM/EMM

WHO WILL WIN?

In one corner, we have the client management tool (CMT). Strong and sturdy, it gives IT visibility and control into their organizations' servers and operating systems (OSs). CMT has been a stalwart of IT management, responsible for much of the inventory and patching completed in the past few decades. CMT also enables the detection of vulnerabilities and attacks on endpoints and helps IT administrators shut them down.

In the other corner, we see mobile device management/enterprise mobility management (MDM/EMM). MDM was born to manage smartphones and tablets in the enterprise. EMM focuses on maximizing security and productivity simultaneously. It rose quickly in the ranks by enabling applications (apps), docs and content for users. By supporting bring your own device (BYOD), EMM reduces costs and increases user satisfaction.

ROUND 1

DEVICE AND OS SUPPORT

At the bell, both contenders are strong out of their corners.

CMT hits hard with its support for servers, Linux, UNIX and Microsoft Windows—the latter with limited Apple macOS support.

MDM/EMM, a southpaw, then catches CMT off guard with support for Apple iOS, Google Android, macOS and Windows.

As the round concludes, it's a draw. Boos are immediately heard from the crowd as their opponent seems to be able to manage wearable and Internet-of-Things (IoT) devices.

ROUND 2

DEVICE AND USER ENROLLMENT

CMT shows its size to start the round, boasting heavyweight agent enrollment with traditional Microsoft Win32 and Mac PKG/DMG packages. Taking a more hands-on approach to installation than its competitor, CMT likes to be manually installed via sneakernet, USB or a download site. One major advantage is the ability to be embedded or ghosted into an OS image.

Lean and nimble, MDM/EMM dances around its heavyweight opponent, unshackled from the requirements of on-domain registration. Users and their devices can be installed right over the air (OTA) and rarely require IT intervention. Showing its speed, MDM/EMM can support device enrollment programs, out-of-box enrollment and zero-touch deployment to make enterprise setup effortless. Continuing to pile on the jabs, MDM/EMM integrates with existing infrastructure such as Microsoft Active Directory/Lightweight Directory Access Protocol (AD/LDAP).

To finish the round, CMT is pummeled by MDM/EMM's app-based and application programming interface (API) enrollment options.

As both competitors head back to their corners, **MDM/EMM** seems to be taking the lead.

ROUND 3

APPS AND CONTENT

CMT and MDM/EMM enter the round swinging and connecting. Both can distribute apps, documents and files.

MDM/EMM extends its reach a bit farther with distribution options for smartphones and tablets. It continues gaining momentum by offering users access to encrypted content repositories as well as support for third-party file sharers like Box. In addition, it connects with public app stores to ease app distribution and accessibility.

The crowd is on their feet. They're wondering which competitor will enable single sign-on (SSO) to web and cloud apps via desktop and mobile devices to ensure quick, intuitive and secure access.

ROUND 4

PATCHING AND VERSION UPDATES

CMT pushes Microsoft, macOS and third-party patches, as well as client configuration, registry changes and client-based actions. Add some customized software packages for an even bigger punch.

Taking a beating on the ropes, MDM/EMM can do some patch management; however, it is limited by mobile OS platform restrictions. CMT, on the other hand, is optimized around traditional PC and Mac management.

CMT is hurting, but somehow outdid MDM/EMM in round 4.

ROUND 5

SECURITY AND POLICY ENFORCEMENT

Entering the final round, both opponents still have skin in the game with the ability to detect out-of-compliance devices and take real-time actions.

CMT can see threats, understand them and act on them—concentrating more on the security and compliance of servers, laptops and desktops. Instilling client confidence, CMT supports popular privacy and data regulations such as Center for Internet Security (CIS), Defense Information Systems Agency Security Technical Information Guides (DISA STIGs), United States Government Configuration Baseline (USGCB) and Payment Card Industry Data Security Standards (PCI-DSS).

MDM/EMM anticipates mobile mishaps, setting specific policies to try and counteract any that might impact their environment.

Out of nowhere, MDM/EMM swings a haymaker, proving a protected container for emails, contacts, calendars, chat and secure browser, too—a real advantage for a BYOD shop by preserving user privacy while separating work and personal data.

Both opponents head to their corners battered and bruised. Some boos and cheers are heard as CMT gets a "W" for the round. Many are shouting it's a questionable call.

THE NEWCOMER

UNIFIED ENDPOINT MANAGEMENT

Unified endpoint management (UEM) enters the ring to settle the score.

It enables security and productivity for users and all devices, including smartphones, tablets, laptops, desktops, wearables and IoT—all from the same modern IT management tool.

It does all the things that CMTs, MDMs and EMMs are known for—offering the broadest level of support from legacy platforms to Windows 10 and macOS. It can send patches and third-party app updates, as well as app distribution and installation for Win32, PKG/DMG and AppX payloads. It includes a universal app catalog with support for all major endpoint and mobile platforms.

As if the odds weren't already stacked in its favor, UEM provides consistent policy management and enforcement across all form factors—making it super easy to set-and-forget to secure all endpoints used for work. Vulnerability detection and remediation both pack a security punch.

And the new kid's got a mean right hook, delivering cognitive insights, contextual analytics and cloud-sourced benchmarking capabilities to its arsenal. UEM helps you make sense of the mobile minutiae you encounter daily—while protecting your endpoints, users, apps, docs and their data from one platform.

IT'S A KNOCKOUT!

IBM® MaaS360® with Watson™ UEM has the best of both CMT and MDM/EMM solutions.

CHECKING THE SCORECARD

Key: Supported ✓ Not supported ✗ Limited support ✧

Function	CMT	EMM	UEM
Patch and third-party updates (distribution and installation)	✓	✗	✓
Registry changes	✓	✗	✓
Hardware/software inventory	✓	✓	✓
Linux management	✓	✗	✓
OTA enrollment	✓	✓	✓
Win32 and PKG app distribution	✓	✗	✓
Imaging	✧	✧	✧
Unified app catalog	✗	✗	✓
Identity and access management	✗	✗	✓
Single pane of glass for all endpoints	✗	✗	✓
Policy management via API	✗	✓	✓
Integration with vendor stores	✗	✓	✓
Location-based policies	✗	✓	✓
Decrease total cost of ownership (TCO)	✗	✓	✓
Lightweight management	✗	✓	✓
User-based context	✗	✓	✓
Wi-Fi configurations	✗	✓	✓
Microsoft ActiveSync configurations	✗	✓	✓
AD/LDAP integrations	✗	✓	✓
Blacklisting/whitelisting of apps	✗	✓	✓
Real-time actions (wipe/selective wipe/locate and more)	✗	✓	✓
FileVault (Apple) BitLocker (Windows) management	✗	✓	✓
Microsoft Windows Information Protection (Windows only)	✗	✓	✓

CAN YOUR CURRENT SOLUTION GO TOE TO TOE WITH THE CHAMP?

Take the trial. **Witness the beatdown.**

IBM MaaS360 | With Watson

With unified endpoint management, you get all the features of MDM, EMM and CMT, with added cognitive insights and contextual analytics. For more information, visit **www.unifiedendpointmanagement.com**

WSL12374-USEN-01