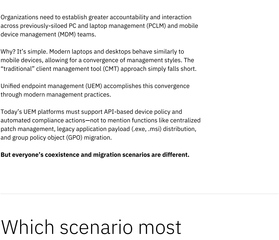
IBM Security

2020 and beyond:

Four essential strategies for endpoint modern management

"Adoption of Windows 10, Google Chrome OS, and Apple macOS will drive the need for a combined endpoint management console in greater than 70% of organizations by 2024."[1]



Organizations need to establish greater accountability and interaction across previously-siloed PC and laptop management (PCLM) and mobile device management (MDM) teams.

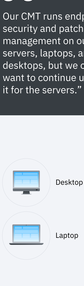
Why? It's simple. Modern laptops and desktops behave similarly to mobile devices, allowing for a convergence of management styles. The "traditional" client management tool (CMT) approach simply falls short.

Unified endpoint management (UEM) accomplishes this convergence through modern management practices.

Today's UEM platforms must support API-based device policy and automated compliance actions—not to mention functions like centralized patch management, legacy application payload (*.exe, .msi*) distribution, and group policy object (GPO) migration.

But everyone's coexistence and migration scenarios are different.

Which scenario most applies to you?



Strategy 1

"I have a CMT running endpoint security and patch management on our servers, laptops and desktops—and I want to continue using it for all three endpoints."

Desktop

Laptop

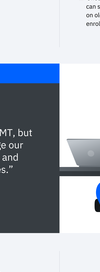
Solution:

Achieving coexistence without disrupting your business is quick and easy:

- Enroll your PCs and laptops in UEM while keeping the CMT installed.
- Let your administrator decide which processes are run by the CMT and which are run by UEM.
- Voilà! Business isn't disrupted, and coexistence has been achieved.

Strategy 2

"Our CMT runs endpoint security and patch management on our servers, laptops, and desktops, but we only want to continue using it for the servers."



Desktop

Laptop

Solution:

This scenario requires UEM to support a phased migration, starting with a period of CMT and UEM coexistence.

- Devices will be enrolled in both UEM and CMT.
- Both tools manage the appropriate processes on your laptops and desktops—but devices are gradually removed from the CMT.
- In the end, your servers remain untouched, all employee devices are on one platform, and new devices can simply enroll in the UEM.

Strategy 3

"Only our laptops and desktops have endpoint security and patch management running through a CMT. We don't want to use it moving forward."

Desktop

Laptop

Solution:

According to analysts, your scenario is the future of endpoint management.

- Start with a period of coexistence where both the UEM and CMT agents are installed on your laptops and desktops.
- Once it has been verified that your UEM can support traditional CMT processes on older devices, retire the CMT and enroll new devices solely in UEM.

Strategy 4

"We don't have a CMT, but we want to manage our Windows, macOS, and Chrome OS devices."

Desktop

Laptop

Smartphone

Smart Glasses

Solution:

This is the easiest scenario of all because you're not concerned with coexistence with or migration from a CMT.

- Get a UEM that supports patching and distribution of legacy apps and files and delivers modern API-based management.
- Enroll all of your laptops, desktops, smartphones, tablets, and every other connected device directly into your UEM platform. No coexistence required!

A UEM for every scenario

Regardless of your journey to modern management, IBM Security MaaS360 with Watson, an industry leader in UEM, can help you achieve your endpoint management and mobile security goals. In *The Forrester Total Economic Impact of IBM MaaS360 with Watson*, an IBM-commissioned study, a composite organization developed through conversations with existing MaaS360 customers derived a significant return on investment.

"Before adopting MaaS360, the composite organization's ability to audit and patch endpoints were uneven and varied based on device type."[2]

MaaS360 yielded "a three-year risk-adjusted total Present Value ROI of $22,960" in the category of auditing and patching endpoints.[2]

"After adopting MaaS360, the auditing and patching of endpoints became far more simplified."[2]

While modern management is the goal here, it's important to consider all aspects of a UEM deployment to ensure your endpoints are managed and secured in a way that fits your organization and the needs of the end users.

With mobile threat defense (MTD), out-of-the-box single sign-on (SSO), risk-based conditional access, and AI risk insights, MaaS360 provides the robust risk management posture organizations need without disrupting employee productivity.

Want to learn more? Request a demo of MaaS360 today.

Talk to an expert

1. 2019 Gartner Magic Quadrant for Unified Endpoint Management Tools
2. The Total Economic Impact™ Of IBM MaaS360 With Watson, a commissioned study conducted by Forrester Consulting on behalf of IBM, April 2019