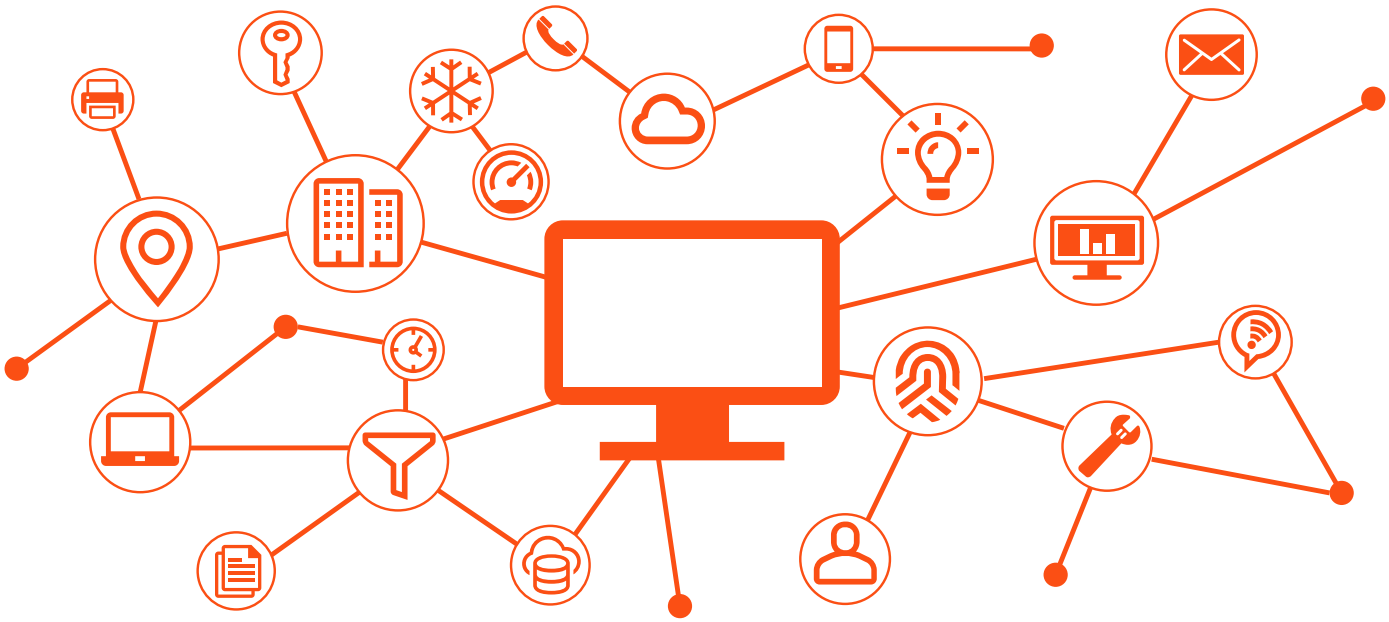
Managing All Devices the Same Way with Unified Endpoint Management (UEM)

A single approach for all platforms and form factors

Written by Dana Ragsdill, Product Manager, Quest



In the beginning, there was endpoint management and there was mobile device management (MDM). They required separate products because desktop computers and laptops were so different from smartphones and tablets. IT administrators were not happy managing in these separate worlds, but they made it work.

Then, consolidated endpoint management came with the second wave. The processes and workflows for desktop computers, laptops, smartphones and tablets were still different and separate, but at least admins could execute them from a single console. They were happy that they no longer needed separate tools, but they looked forward to the day when processes would be the same for all devices.

Now is the time of the third wave, and unified endpoint management (UEM) lets admins use the same processes to enroll, inventory, manage and secure all devices from a single product. Admins like it.

This paper explores the evolution of UEM and the most useful characteristics in a UEM product. Readers will take away ideas on unifying endpoint management for all devices in their organizations.

WHAT IS UEM?

UEM is an approach to securing and controlling desktop computers, laptops, smartphones and tablets in a connected, cohesive manner from a single console. It extends even further,

to the management of essentials such as printers, projectors, personally owned BYO devices, gateways and Internet of Things (IoT) devices.

The unified approach to endpoint management is necessary to secure the IT environment. Admins need the ability to see and manage all devices connected to the network, regardless of type. But different processes, workflows and device operating systems have historically resulted in admins having to jockey different management consoles, a time-consuming and inefficient endeavor. The promise of UEM is the same treatment and management of all devices connected to the network.

As noted above, endpoint management is evolving to give admins greater control over more types of devices from a single product.

> Admins have had to jockey different management consoles, a time-consuming and inefficient endeavor.

WHAT IS CAUSING THIS EVOLUTION?

First, homogeneity in the IT landscape is becoming rare. Admins look back fondly on the days when all they had to support was Windows; now, along with potentially multiple versions of Windows, the devices in their organization run macOS, Linux, iOS, Android and Chrome OS, with different versions of each. Form factors now include desktop computers, laptops, Chromebooks, tablets and smartphones. In particular, the proliferation of mobile devices greatly affects IT, whose mission is to support, secure and protect them against vulnerabilities.

Next, because the devices were so different, client management and mobile management products evolved separately, forcing admins to manage each device category differently. The operating systems running on the devices had a lot to do with that; before Windows 8.1, for instance, there was no way for MDM software to access, control or secure the OS and its apps. Now, with Windows 10 support for MDM APIs, truly unified endpoint management is possible on a vastly greater scale.

Then, IT's charter includes both corporate and personally owned (BYO) devices, such as laptops, smartphones and tablets. The extent of support expected in each organization may vary, but at a minimum IT is responsible for maintaining network security and keeping non-compliant devices from causing harm.

Finally, IoT and other computing devices are helping to build the business case for UEM. Whatever new IoT devices like sensors and voice-controlled units may be, they are not PCs, meaning that the ordinary approach to client management will not suffice for them. And the trend toward remote connectivity in devices like kiosks, ATMs, parking meters, thermostats, point-of-sale devices, signage, vending machines and wearables makes them eligible for centralized management as well. At the same time, nobody wants them to become yet another category of device to be managed with yet another console, so IoT and other peripheral devices are squarely on the evolutionary path toward UEM.

WHAT GOES INTO UEM?

The main consideration for a UEM product is that it should combine the main features of MDM tools and traditional client management tools, then apply those features to all endpoints:

- Manage configurations and settings
- Enforce policy and compliance
- Provide detailed reporting
- Manage security
- Integrate corporate identity and Single Sign-On (SSO)
- Integrate with enterprise systems
- Allow for containerization
- Push updates
- Allow for multi-user, single user or kiosk options with ease of management for all devices

The product should support the latest versions of the most popular operating systems in enterprise use today, including iOS, macOS, Android, Windows, Unix and Linux. It should also make migration possible from older versions such as Windows 7 to secure, modern versions like Windows 10.

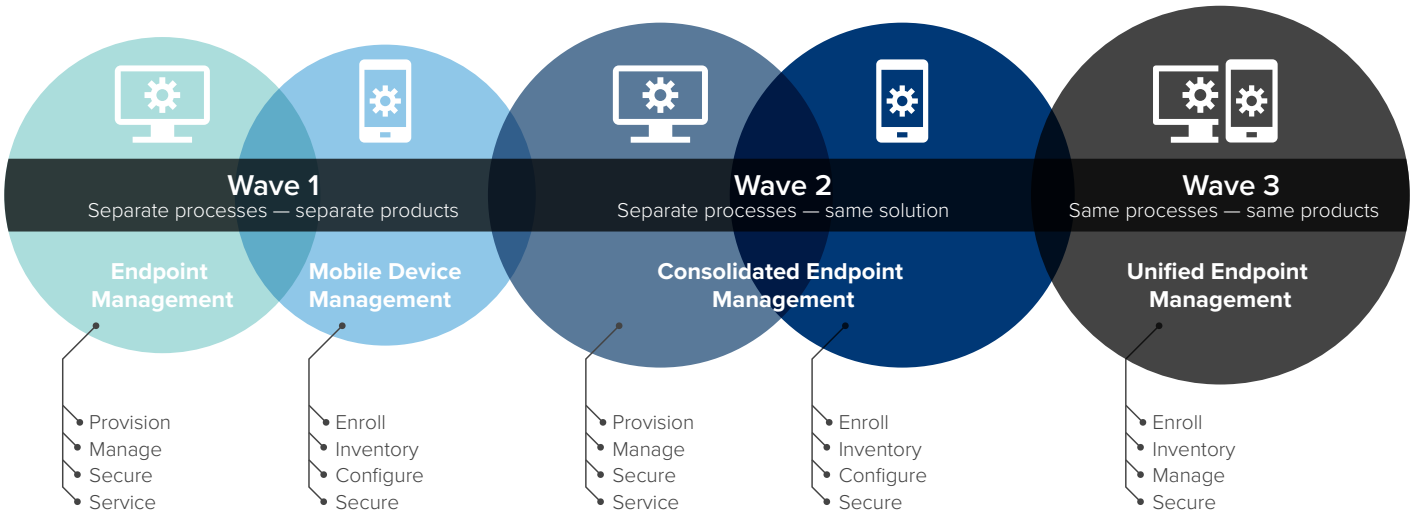


Figure 1: Three waves of UEM evolution

Employees are taking more of their personally owned, BYO devices into the office and connecting them to the network. They like the flexibility and the boost in productivity, but they do not want IT to configure the devices or access personal data on them. IT, of course, must enforce the organization's security standards on corporate data and resources without affecting the employees' ability to use their devices. To strike that balance, the ideal UEM product should meet several important criteria:

- Make user-owned devices trusted
- Apply device-level security policies
- Provide the apps needed for work
- Manage software licenses on personally owned BYO devices
- Minimize the time it takes to provision

THE PHASES OF IMPLEMENTING UEM

Every organization's history with client management and MDM puts it at a different point in its evolution toward UEM. As described in the introduction and as shown in Figure 1, Gartner has defined three waves in that evolution as a function of the processes and workflows required to manage the devices and the number of separate consoles required to manage them.[1]

Wave 1 is characterized by different management products because the processes are different. IT must provision, manage, secure and service traditional endpoints like PCs and laptops; and enroll, inventory, configure and secure mobile devices. Even if each product works efficiently for its respective device type, the overall result is inefficiency because IT has to work at separate consoles.

Wave 2 begins to reconcile the separate domains with a single console, but the processes remain different, as they were in Wave 1. IT has fewer solutions to manage and a more comprehensive view of what is on the network, but it must still manage the device types differently.

Wave 3 represents the true implementation of UEM: the same processes and workflows, managed through the same product. In this promised land of greatest efficiency, IT uses the same product and console and manages devices the same regardless of platform or form factor.

THE KACE APPROACH TO UEM

Approach A in building UEM products is to treat UEM as a descendent of enterprise mobility management (EMM). In effect, the products take advantage of the support for MDM APIs in macOS

> Client management and mobile management products evolved separately, forcing admins to manage each device category differently.

1 *Cosgrove, Terrence and Doheny, Rich, "Market Guide for Client Management Tools," Gartner, August 2016, https://www.gartner.com/doc/3408217/market-guide-client-management-tools*

Finite IT.

IoT and other peripheral devices are squarely on the evolutionary path toward UEM.

and Windows 10 to treat computers and laptops like mobile devices. However, Approach A leaves out devices running old operating systems.

Approach B takes traditional client management solutions that have APIs or integrations with MDM solutions and combines them with EMM.

In either case, the problem lies with mobile app management. Both approaches work properly with some of the built-in APIs for iOS and Android, but they leave uncovered several important aspects of iOS and Android, such as SDKs, app wrapping tools and productivity apps, on which enterprises depend. Furthermore, most organizations have made significant investments in and rely on Group Policy to manage their desktop computers and laptops. Unfortunately, mobile devices are managed differently.

KACE has followed Approach B, that of a traditional client management vendor moving to include and integrate MDM functionality. For several years, KACE has integrated MDM solutions, and now, the KACE Cloud Mobile Device Manager represents the most complete integration within its own products.

Through a single pane of glass, IT admins can inventory and report on all devices from the KACE Systems Management Appliance (SMA). Management of devices takes place in KACE Cloud Mobile Device Manager.

ABOUT KACE CLOUD MOBILE DEVICE MANAGER

IT admins working in the two different worlds of endpoint management and mobile device management have been obliged to use separate products and move between separate consoles. That has been unavoidable because of different processes and workflows for both device types, but the inclusion of MDM APIs in macOS and Windows 10 promises to bring the two worlds closer together.

Using KACE Cloud Mobile Device Manager, admins now have a comprehensive view of all devices in their organization through the KACE Systems Management Appliance. With the same processes and products, admins can manage all devices the same way with truly unified endpoint management.

ABOUT QUEST

Quest helps our customers reduce tedious administration tasks so they can focus on the innovation necessary for their businesses to grow. Quest® solutions are scalable, affordable and simple-to-use, and they deliver unmatched efficiency and productivity. Combined with Quest's invitation to the global community to be a part of its innovation, as well as our firm commitment to ensuring customer satisfaction, Quest will continue to accelerate the delivery of the most comprehensive solutions for Azure cloud management, SaaS, security, workforce mobility and data-driven insight.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.