

WHITE PAPER

The Best Path to UEM is Unified Co-Management

Foreword by
Lee C Stonehouse
VC Experience

Dear Reader,

I am pleased to introduce this excellent white paper entitled 'The Best Path to UEM is Unified Co-Management' from MobileIron (an Ivanti company).

The content delves into the mobile UEM component of standardising the mobile estate, a subject core to our mission at VC Experience.

At VC Experience we build applications that are integrated into MobileIron's UEM and we recommend this as a core component of standardising your corporate mobile estate.

Thank you for your interest.

Lee C. Stonehouse

Co-Founder, VC Experience



The Best Path to UEM is Unified Co-Management



Contents

Customers Want a Common Management Experience	4
Co-Management: The Bridge to Modern Management	6
How Does This Timeline Apply to You?	7
You're Doing Co-Management Already.....With GPOs	7
Security is Another Reason for a Co-Management Approach	7
Ivanti Co-Management Stands Out with a Unified Experience	7
Integrated Security Capabilities in the Same Console	8
How Do You Plan to Bridge the Gap?	8
Conclusion	9
References	9

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti"), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.Ivanti.com.

© 2019, Ivanti. All rights reserved. IVI-2263 02/12/19. AS/JR/BB/DL

Introduction

IT's primary function is to secure and enable workers and organizations, using automation, processes, and shared data. More and more, IT administrators are wanting to manage computing and network environments from a single management experience. So, when talking about modern management or Unified Endpoint Management (UEM), we need to consider two aspects: 1) whether the endpoint management experience of your IT administrators is a unified one; and 2) what the underlying technologies should be to enable this.

Forrester Research defines UEM or modern management as: "Products that provide a centralized policy engine for managing and securing employee laptops and mobile devices from a single console."¹

As reported by Gartner Inc. in its July 23, 2018 *Magic Quadrant for Unified Endpoint Management Tools*, the vision of Unified Endpoint Management (UEM) encompasses a new class of tools for IT administrators that can act as a *single management interface* for mobile, PC, and other devices. The movement towards UEM is in its early stages.

As stated on page 1 of the report, this vision of UEM encompasses tools that perform these functions:

- Configure, manage and monitor iOS, Android, Windows 10 and macOS, and manage some Internet of Things (IoT) and wearable endpoints.
- Unify the application of configurations, management profiles, device compliance and data protection.
- Provide a single view of multidevice users, enhancing efficacy of end-user support and gathering detailed workplace analytics.
- Act as a coordination point to orchestrate the activities of related endpoint technologies such as identity services and security infrastructure.²

Page 1 of the report also states:

- Vendors in this analysis fall into two categories: those that are heavily invested in mobile and modern management with very little client management tool (CMT) functionality, and those that have integrated an

existing CMT or explicitly built CMT features into their UEM.

- Modern OSs favor UEM-only management; Google's Chrome OS and Windows 10 S are two examples. Presently, the majority of organizations have yet to adopt UEM as the primary management tool for all endpoints, making the inclusion of features that bridge CMT and UEM strong differentiators today. The value of these features will diminish as fewer devices require them and Gartner will adapt future analyses of this market accordingly.³

The focus of this white paper centers on this concept of combining features that bridge client management tools (CMT) and enterprise mobility management (EMM) to provide solutions that answer the day-to-day demands placed on IT operations, security, and service management, while also helping to enable organizations in their advancement towards this broader vision of single-console UEM. This "bridging" is often referred to as "co-management."

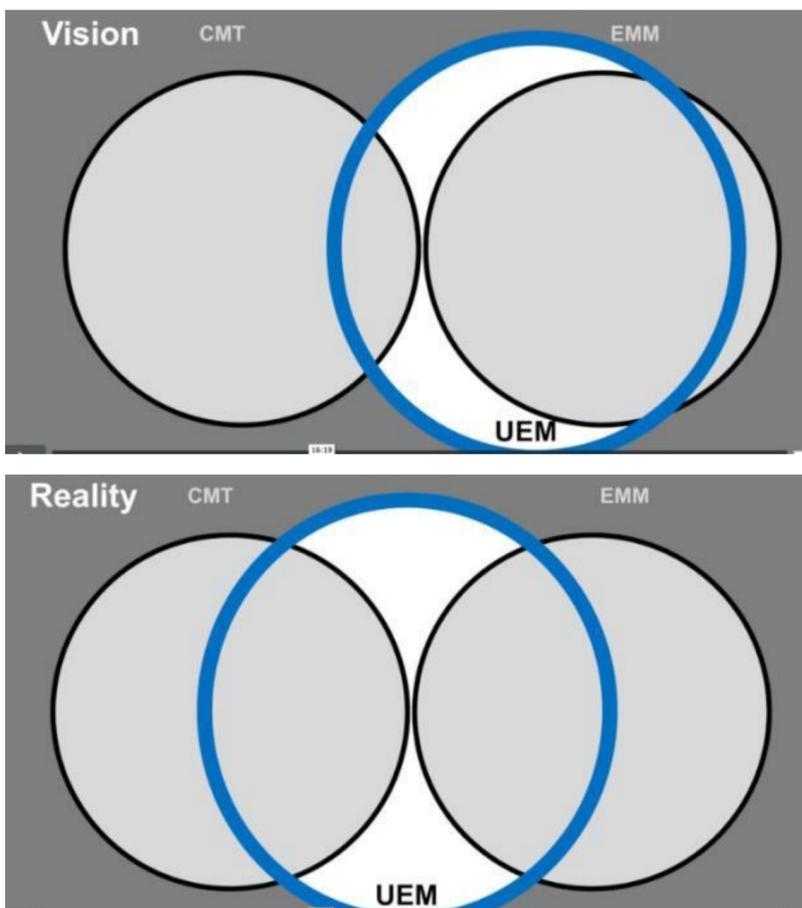
Customers Want a Common Management Experience

Without question, IT administrators desire a common management experience across all devices in their environment, yet this can't be accomplished using modern management technologies alone. What's needed is co-management to continue progressing towards a state of UEM.

You would be hard-pressed to find any sizeable enterprise that manages all its endpoints exclusively with modern

management. The only scenarios that analysts cite are start-up companies or divisions of companies that are starting fresh or that have dictated they will only supply devices such as a smartphone and a Chromebook. It will be some time before large organizations can standardize on devices that are all easily managed using MDM-styled management with the same level of management you'll find in a CMT tool.

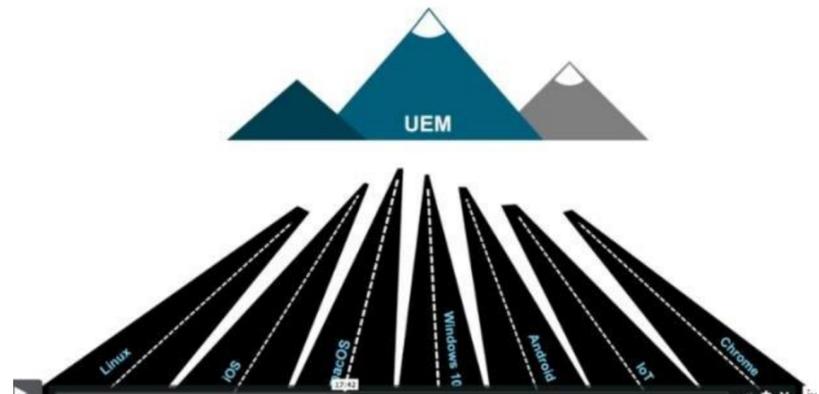
There are also differing points of view in the industry concerning the balance needed between EMM and CMT capabilities to assist in that forward progression. For some, the balance is weighted towards EMM. From Ivanti's view of reality, the balance is equal.



Whatever your view is, co-management's flexibility provides the deeper control of CMT with the simpler management capabilities in EMM where needed. While EMM provides a standard way for managing devices, CMT offers capabilities for deeper management and fine-tuning of management processes developed over the years.

Another reason for bridging CMT and EMM through an equal balance versus making a gigantic leap to UEM primarily via EMM is this: while OS vendors are starting to build modern management technologies into their systems, they aren't moving at the same pace.

Not moving at same pace



Let's say the Mac OS is out in front of Windows in one area, and the opposite is true in another. If you apply a particular policy to a user, will it filter out to all of the other operating systems? Not necessarily because they may not have the same feature in their configurations. In actuality, how unified is the endpoint management if OS advancements aren't at the same level?

In addition, there are some management elements to Windows 10 that can only be managed through a Mobile Device Management (MDM) or EMM solution.

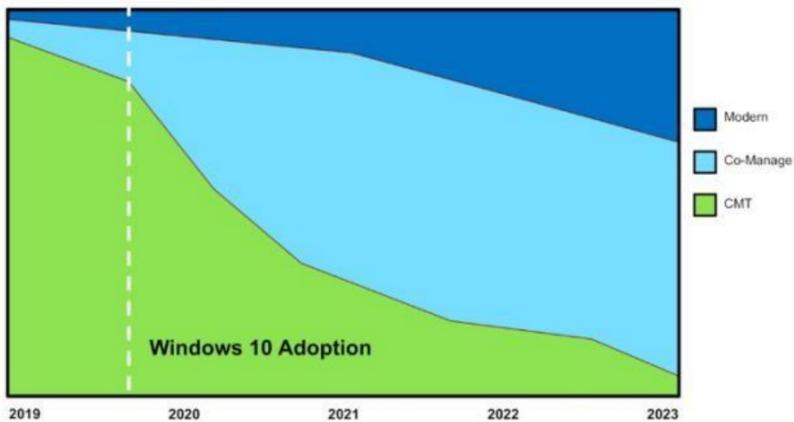
Action:

Ask yourself, is it important to get the benefits of a unified management experience now through co-management and transition gradually to a more streamlined management through UEM, or do you push through the obstacles and the difficulties to get to UEM, only to wait for all the OS vendors to "level up" to the point where an enterprise would have the same level of control?

Co-Management: The Bridge to Modern Management

In the chart that follows, modern management is represented in blue, co-management in light blue, and CMT in green. Based on consultations with analysts and customers, Ivanti foresees that co-management will be an essential strategy or component of endpoint management overall for the next five years and beyond.

Moving to Windows 10 and rolling out rapid updates was one of the driving factors for the adoption of UEM. However, Microsoft has relaxed its cadence of updates. Therefore, the drop off of CMT usage may not be as steep as shown.



The adoption of Windows 10 makes a strong case for using co-management for several years to come vs. a CMT-only strategy. There will be a continued need to manage multiple platforms from 2020 through 2022. From the year 2021 going forward, there will also be an uptick in the number of features that will require MDM-styled management. Currently, many of those capabilities are fulfilled through CMT-styled tools.

How Does This Timeline Apply to You?

What is your mix of devices, and do you see that mix changing drastically in the next three years? If it's anything more than 25 percent laptops/desktops, you should consider co-management with Ivanti, especially if you want to perform more management than what is currently available through vendors' MDM APIs. You should also consider Ivanti if you want integrated management workflows or integration with other areas of IT.

You're Doing Co-Management Already—with GPOs

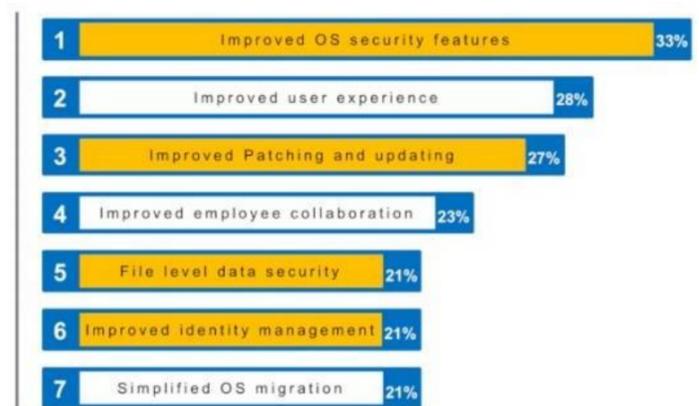
The reality is, you're already pursuing a type of co-management strategy with Group Policy Objects (GPOs). You can perform a certain amount of management, and then add scripting on top of that for device and configuration management. Many IT departments are using both agents and GPOs to cover the gaps that the agents either don't do, or that can be done just as well or more easily with GPOs. One of the advantages of modern management is eliminating the need for GPOs. Ivanti® Unified Endpoint Manager (Ivanti UEM) does the same thing. It eliminates the need for extensive GPOs to modify the user experience at login.

Security Is Another Reason for a Co-Management Approach

An Enterprise Strategy Group (ESG) survey on Unified Endpoint Management Trends reported that four of the top seven benefits for migrating to Windows 10 were security related.⁴ This matches up well with the EMA Group's top seven challenges to endpoint management in its March 2018 report *Orchestrating Digital Workspaces – The Evolving State of Endpoint Management*.⁵

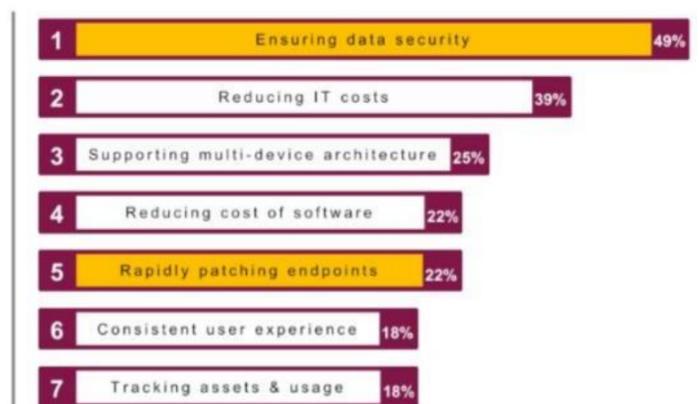
ESG Survey on UEM Trends

Top 7 benefits to Windows 10



EMA Group's Top 7 Challenges

Top 7 challenges to Endpoint Management



Ivanti Co-Management Stands Apart with a Unified Experience

While the ultimate goal is still UEM—managing everything from a single management console or common management experience—the vendors in the “Leaders” quadrant of Gartner's *Magic Quadrant for Unified Endpoint Management Tools* report referenced earlier require at least two consoles to manage all devices.⁶ Examples include:



- Microsoft with SCCM and Intune
- IBM with MaaS360
- VMware/AirWatch
- MobileIron with Microsoft SCCM

Many of these vendors will need to rely on MDM-related features from Microsoft to deploy and manage Windows 10.

One of Ivanti's main development themes is around Windows 10, including Autopilot and MDM features that will help organizations move to and manage their growing Windows 10 environments. Windows Autopilot is a perfect example of how Ivanti can provision a Windows 10 device without requiring Microsoft Intune.

Ivanti Unified Endpoint Manager (Ivanti UEM) allows you to migrate users' personal settings and files easily to Windows 10. However, migration is only the start of the Windows 10 journey. It automates the large, frequent Windows-as-a Service updates with minimized network overhead. The solution also helps you onboard new Windows devices quickly by leveraging Windows Autopilot, without requiring Microsoft Intune, giving you a way to provision users' devices with "zero-touch" from IT. When the user receives their new Windows 10 device, powers it on for the first time, and it connects to the network, it's ready to go.

Integrated Security Capabilities in the Same Console

Accessible within the same Ivanti UEM console are the add-on endpoint security capabilities of Ivanti® Endpoint Security for Endpoint Manager that prevent, detect, and remediate even the most sophisticated threats, including ransomware. You can see everything necessary to find and remediate malware, diagnose problems, and identify faulty or nonapproved processes. If ransomware invades your network, Endpoint Security will catch it, kill it, notify other connected machines, and block the malware from running on them.

Powerful remote capabilities allow you to isolate, investigate, and remediate or re-image endpoints across the network. Additionally, device blocking and connection control let you monitor and restrict I/O device access.

Application control guards against zero-day exploits, stealth attacks, and other sophisticated threats. And data protection features prevent malicious software from encrypting your files.

How Do You Plan to Bridge the Gap?

In Gartner's Magic Quadrant report referenced earlier within the context of CMT and MDM, they discuss the following three waves:⁷

- Wave 1: Completely separate tools—CMT for PCs, UEM for mobile—and processes for management to PCs and mobile.
- Wave 2: Concurrent use of tools for mobile and PC devices, with PCs being addressed by CMT or a combination of CMT and UEM. Wearable and some IoT devices fall under EMM.
- Wave 3: Tools, processes and policies for PC and mobile devices merge. Note that a subset of IoT devices, where applicable, and wearable devices, where applicable, can be managed in this same console.

Ivanti is firmly in the second wave moving into the third wave. Microsoft on the other hand is still in Wave 1 with SCCM and Intune. They do however, talk about co-management, which we can do as well, but our workflows and console are integrated, while theirs are not.

The "Challengers" quadrant in the Gartner report illustrates that Ivanti can execute against customer needs. You might consider Ivanti as "trusted" versus highly "innovative" in this space. We are, however, innovating in areas that apply to UEM, but that innovation won't be reflected in the Magic Quadrant for a few years. These include capabilities such as real-time discovery and visualization via cloud components that provide contextual suggestions based on your data and that of other peer organizations, plus the ability to take action to remediate or make adjustments to your environment.

You could say that Ivanti "challenges" the common definition of UEM that it's mostly the same as EMM. Our definition is captured within the single console experience

and the integrated workflows between devices that leverage multiple technologies.

Ivanti is recognized as one of only two vendors with a full CMT stack, which means we're the only ones with a full CMT stack integrated with MDM-styled management. It's still one of the only solutions that allows you to apply common configurations and applications to multiple devices all at once in the same workflow—from the same console.

Ovum Analyst Group wrote a favorable short report that helps position Ivanti Unified Endpoint Manager.⁸

“With end of life looming for Windows 7, more businesses are embarking on projects to upgrade to Windows 10. Technologies that can support this migration will be of great interest to businesses over the next few years. We believe this is driving interest among IT leaders globally in tools that support a more unified approach to endpoint management.”

—Ovum Analyst Group

Conclusion

As mentioned earlier, IT administrators desire a common management experience across all devices in their environment, yet they won't be able to accomplish this over the next several years using modern management technologies alone. What's needed is co-management to continue progressing towards a state of UEM.

Ivanti Unified Endpoint Manager is proven, reliable endpoint and user-profile management software that is

core to: 1) discovering everything that touches your network; 2) automating software delivery; 3) reducing headaches with login performance; and 4) integrating actions with multiple IT solutions. Ivanti Unified Endpoint Manager lets IT analysts and admins do their magic for all devices from one management experience—not through two, three, four or more consoles.

Please visit our [Ivanti Unified Endpoint Manager page to learn more.](#)

References

1. Forrester Research blogs, “Implement UEM To Improve Employee Experience And Protect Customer Trust,” June 28, 2018; <https://go.forrester.com/blogs/forrester-unified-endpoint-management-uem/>
2. Gartner Inc., Magic Quadrant for Unified Endpoint Management Tools, July 23, 2018; ID: G00354834
3. Ibid.
4. Enterprise Strategy Group (ESG) Survey on Unified Endpoint Management Trends
5. EMA Group, Orchestrating Digital Workspaces – The Evolving State of Endpoint Management; March 2018
6. Gartner Inc., Magic Quadrant for Unified Endpoint Management Tools, July 23, 2018; ID: G00354834
7. Ibid
8. Ovum Analyst Group, “Ivanti releases Unified Endpoint Manager solution to support organizations workspace modernization efforts”; 26 July, 2018; Product code: ENS001-000034

Learn More

-  [anti.com](https://www.ivanti.com)
-  **800 982 2130**
-  [ales@ivanti.com](mailto:sales@ivanti.com)