



# ENSURING ROCK SOLID UNIFIED ENDPOINT MANAGEMENT

By Nathan O'Bryan

**Quest**<sup>TM</sup>



<https://quest.com>

**The IT landscape** that we all live in is an ever-evolving place. While many organizations would like to exercise tight control over the devices that end-users are using to access their corporate data, that just isn't a realistic possibility in many cases.

If we, as IT professionals, need to live in a world of Bring Your Own Device, then we must have the tools to manage those devices effectively. Many IT departments have to strike a balance between allowing end-users to use the devices they want while still protecting the organization's data and IT assets.



For these reasons, and many more, a rock solid Unified Endpoint Management plan is an absolute requirement for most IT departments operating today.

In this paper, we have taken some common questions about Unified Endpoint Management solutions from customers and provided the answers and information you need to make a decision on the right solution for your organization.

We've tried to stay away from "selling" you on a specific solution, and focus on providing good answers to the questions IT departments have about Unified Endpoint Management.

### **WHAT IS UNIFIED ENDPOINT MANAGEMENT?**

Before we can dive into all the questions around Unified Endpoint Management, we should ensure that we clearly define what we're talking about when we say "Unified Endpoint Management."

Unified Endpoint Management (UEM) is an approach to managing and securing

PCs, workstations, laptops, cell phones, tablets, and all other types of devices in a standard manner within a single console. UEM is similar to Mobile Device Management (MDM), but includes an expanded scope of more devices within a single control console.

A good UEM application can manage Windows machines as well as Apple and Linux computers too. Of course, the ability to manage both Apple and Android mobile devices is absolutely required.

### **WHY IS UNIFIED ENDPOINT MANAGEMENT IMPORTANT?**

We, as IT professionals, have to navigate a complex IT environment. The applications we support are constantly evolving new features and functionality. The compliance rule sets we have to satisfy are becoming more complicated, detailed, and involved. The BYOD devices that we are asked to support are becoming more prolific, varied, while end-users are becoming more reliant on having more services available on these devices.

It is a basic assumption of economics that everyone is asked to do more with less all the time. For that productivity growth to happen, we need to keep evolving better tools. Cobblers need to develop better tools and processes to make shoes, Doctors need to develop better tools and processes to heal the sick, and manufacturers need to develop better tools and processes to build their products. The same thing is true for IT professionals. We need better tools and processes to expand the services we provide to our customers.

As software gets more complex to deploy and support, the most efficient route is going to be for the company that creates that software to also manage it. This will allow for companies like Microsoft to provide more and better features on a faster time table with fewer support issues.

One effect of this move to cloud services is that end-users will have more opportunity to access corporate data from more places on more devices. Cloud applications are, by default, available to be accessed over the public internet at any time. This may not be the case with

## IT PROFESSIONALS NEED **BETTER TOOLS AND PROCESSES** TO EXPAND THE SERVICES WE PROVIDE TO OUR CUSTOMERS.

UEM is one of the improved tools that allow us to accomplish that growth. A UEM solution gives us a single console we can use to manage all the devices that attach to our corporate IT infrastructures.

### **HOW DOES THE EXPANSION OF CLOUD SERVICES EFFECT THE NEED FOR UEM?**

It is an undeniable fact that more and more IT services are moving to a cloud model. Microsoft, the largest software company in the world, has declared they are a “Cloud first, Mobile first” solution provider.

on-premises deployments of the same services.

While the ability to access corporate data from any device anywhere at any time is a great boon for productivity, it can be a significant security and compliance risk. The risk of all this access can be managed with a good UEM solution.

### **DOES OFFICE 365 NATIVELY PROVIDE A UEM SOLUTION?**

No.

Office 365 and the greater Microsoft cloud does provide several MDM solutions, but Microsoft does not currently

offer a single solution that rises to the level of a UEM solution.

Exchange Online includes some basic MDM functionality. Exchange Online can enforce limited password policies on devices connecting to Office 365 via ActiveSync, and wipe devices that have been reported lost or stolen. That is pretty much the limit of the MDM features built into Exchange Online.

If your organization purchases Azure Active Directory Premium, then you will

devices are connecting to your data and what is running on those devices is always going to be step one. Knowing who is using what devices to connect to your data, and what software is running on those devices is essential for both organizations that support BYOD initiatives and organizations that do not.

- **Software compliance and metering.**

Many organizations in many different verticals now need to function within the governance of one or more different compliance rule sets. HIPPA, Sar-

## THE VALUE IN A **GOOD UEM SOLUTION** IS IN THE FACT THAT IT HELPS YOU **MANAGE MANY TYPES** **OF DEVICES** IN MANY DIFFERENT WAYS.

get access to Conditional Access policies that give you greater control of who can access your organizational data from what devices.

### **WHAT FEATURES SHOULD I GET WITH MY UEM SOLUTION?**

The value in a good UEM solution is in the fact that it helps you manage many types of devices in many different ways. Below are a few of the features you may want to look for in an UEM solution.

- **Hardware and software inventory management.** This is really where you want to start with your new UEM solution. Having strong control over what

banes-Oxley, PCI, and many other rule sets each bring their own unique requirements for IT departments to navigate. While a UEM solution is never going to magically make your organization “compliant,” it can help you gather the data your organization needs to ensure compliance.

- **Software deployment, upgrades, and removal.** Once users have connected devices to your infrastructure, it is important to be able to manage the software installed on those devices. Your organization may need to remove specific applications from all devices connecting to your infrastructure, or maybe you need

to upgrade some subset of applications on certain devices. A good UEM solution will give you the tools you need to handle those and many other scenarios.

- **Patch management.** Everyone in IT is aware that security patch management on devices can be critical. At anytime an exploit can be found that compromises the integrity of your corporate IT infrastructure. We all know that these exploits can, do, and will happen on a regular basis, we just don't know when they will occur or what devices will be affected. A solid UEM solution will give your organization the ability to push emergency patches to multiple different types of devices on a short time scale.

**A SOLID UEM SOLUTION WILL GIVE YOUR ORGANIZATION THE ABILITY TO PUSH EMERGENCY PATCHES TO MULTIPLE DIFFERENT TYPES OF DEVICES ON A SHORT TIME SCALE.**

- **Remote control.** Anyone who has worked on a service desk will tell you that supporting users when you can not see what they are doing on their screen can be very difficult. A good UEM solution will give you the tools you need to be able to remote control user's devices. A

centralized console your help desk can use to be able to remote control all kinds of devices will quickly become invaluable.

- **Reporting.** Maybe the greatest features of a good UEM solution comes from the fact that all your organization's devices are managed with a single application. When all devices are managed with the same application, that application knows many things about those devices. With all devices reporting to the same console, that console has access to a much larger set of data about those devices than would be possible with other solutions.

#### **WHAT ARE THE ADVANTAGES OF HAVING A SINGLE SOLUTION TO MANAGE YOUR ENDPOINT ASSETS?**

The central benefit of a UEM solution is a single management solution for all your organization's devices. Having a central console where your IT department can access information about all devices connected to your infrastructure is a powerful feature that is going to be worth the cost of implementing a UEM solution.

Another advantage of using a single solution to manage all your organization's devices is that all the data collected in this single UEM solution is going to be available to be used together. Having a single repository that includes information like device type, patch levels, installed software, user name, and other important information allows that solution to provide

more powerful features than would be available from several solutions that did the same things but didn't have a central repository.

### **HOW DO CUSTOMERS USE UEM TOOLS TO COMPLETE WINDOWS 10 MIGRATIONS?**

An operating system upgrade project can be one of the more daunting projects for an IT department to undertake. Ensuring all the hardware, software, applications, and end users can work together without interruption to workflow is a huge challenge. Anything your support systems can do to ease that burden is going to make everyone's life so much better.

A solid UEM solution can help provide inventories of currently installed software, device information that can be used to build driver packages, and remote device management tools that can be used by your support desk for post migration support.

### **WRAPPING IT UP**

If your IT department needs to be able to manage a wide variety of devices from both BYOD and from company owned hardware, then your IT department will need a solid UEM solution that can help you navigate and manage all that complexity.

For the reason outlined above, and for many more, the right UEM system greatly improves your organization's control over these devices.

### **FIND OUT MORE**

<https://www.quest.com/>

The Quest logo is displayed in a large, orange, sans-serif font. A small trademark symbol (TM) is located at the top right of the letter 't'.

---

**Nathan O'Bryan** is a Microsoft Certified Solutions Master: Messaging and a Microsoft MVP for Office Servers and Services from Portland, OR. He specializes in Exchange, Office 365, Active Directory, Azure and a bit of Skype for Business.