



The Ultimate Guide To Mobile Device Management

Table of Contents

● Introduction	3
● What is Mobile Device Management (MDM)?	3
Explaining MDM vs. EMM vs. UEM	4
● Why use an MDM?	5
● What can an MDM solution manage?	8
Types of Devices	8
Operating Systems an MDM solution can manage	9
Partnership-Based Enhancements	10
● What can an MDM solution do? How MDM works	11
Mobile Device Management (MDM)	12
Mobile Application Management (MAM)	12
Mobile Content Management (MCM)	13
Mobile Identity Management (MIM)	13
Bring Your Own Device (BYOD)	13
Non-Traditional Endpoint Support	14
● Options for deploying an MDM solution	15
Deploying a cloud-hosted MDM solution	15
Deploying an on-premise MDM solution	16
● Choosing the best MDM solution for your needs	18

Introduction

Mobile device management (MDM) is one of the most essential and widely-used technologies in 2021 – but that doesn't mean everyone understands it. People may use the term mobile device management meaning something else, or not understand what they need for their ideal mobile device management system. While it is easy to find mobile device management solutions, it can be hard to choose which mobile device management free trials to try.

You'll find the answers to many common questions here, as well as clear steps for implementing mobile device management in your business.

What is **Mobile Device Management (MDM)**?

Mobile Device Management (MDM) software is the approach used by companies to remotely monitor, manage, and secure devices of all kinds, including (but not limited to) mobile devices. Just as a store manager watches over and disciplines store employees, someone with MDM software can watch over and control phones and other devices.

MDM can manage more than mobile devices. You can use MDM technology to manage smartphones, tablets, desktops, and almost any other technology. For this reason, implementing MDM software is a smart idea for almost any company.

MDM technology is more important now than ever before. Workers worldwide are increasingly going mobile, and mobile devices have become crucial to all kinds of jobs. Businesses need ways to manage, monitor, and secure these devices.



Explaining MDM vs. EMM vs. UEM

MDM, EMM and UEM are the three most common terms you will see when researching MDM solutions. You may already be wondering what each one stands for, and how they relate to each other. Read on for a short version; if you'd like more detail, here's an extensive guide to these terms and their history.

Many people use MDM, EMM, and UEM interchangeably, but each one has a distinct meaning. It's essential to understand that these terms have evolved over time. The term mobile device management came first, followed by enterprise mobility management, and finally unified endpoint management.

Mobile device management (MDM) is used to monitor, manage, control, and secure all workplace mobile devices. The term is a holdover from an era where cell phones didn't interface with any other devices in the office. As a result, IT teams focused on managing office-owned phones separately from other devices. There was no way to ethically manage employee personal devices if they even owned any. Plus, in this era, admins did not need to have ways to manage files and other on-device content, as this was almost always unnecessary on older phones.

What is EMM (Enterprise Mobility Management)?

The term enterprise mobility management (EMM) represents managing both mobile devices and the content on them. EMM includes mobile device management (MDM), mobile application management (MAM), and mobile content management (MCM). Importantly, EMM also includes the ability to manage both company-owned and employee-owned phones. Together, these changes helped businesses accommodate highly mobile employees.

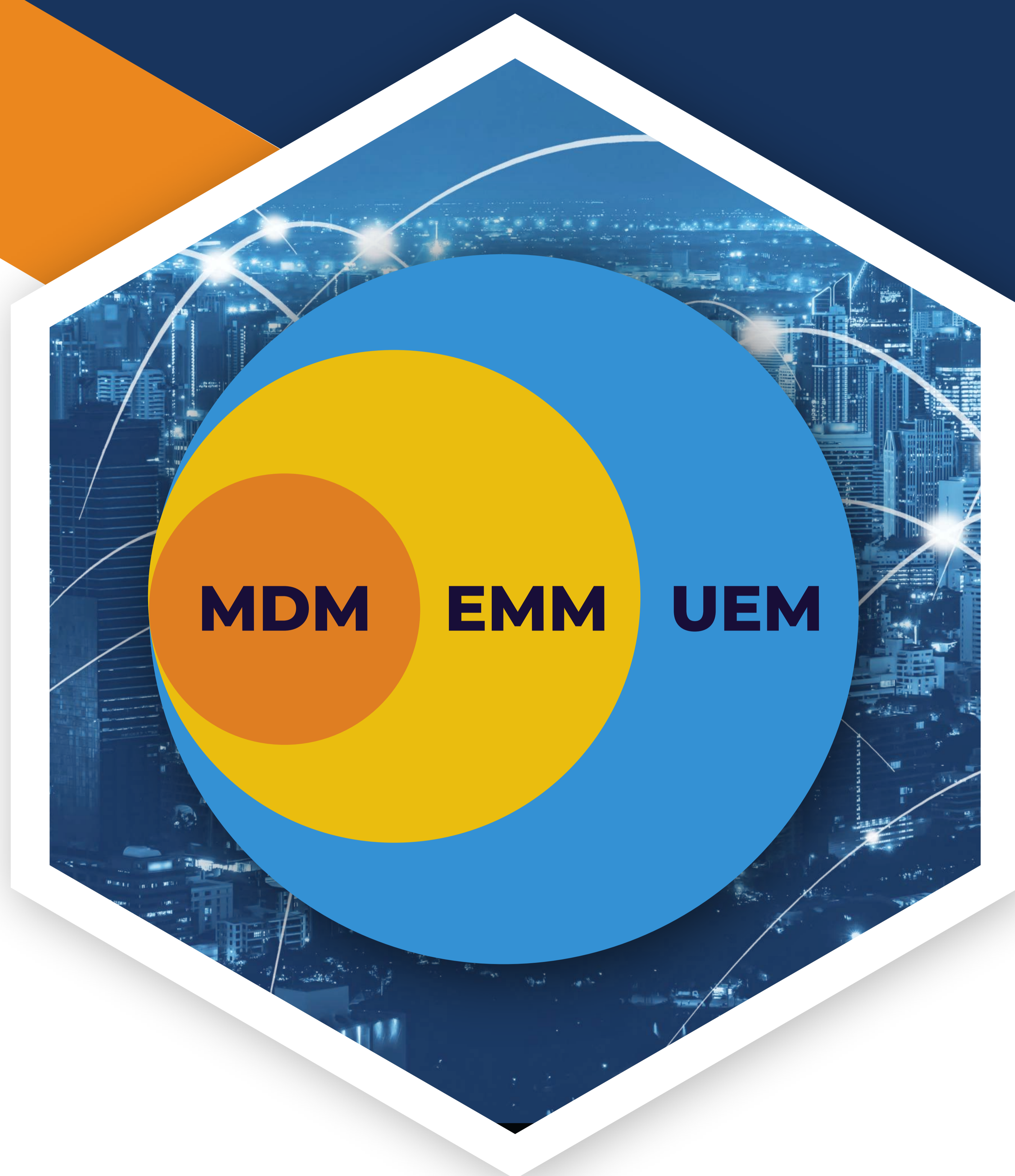


What Is UEM (Unified Endpoint Management)?

The term unified endpoint management (UEM) reflects the strategy of using a single management framework to **manage all kinds of business endpoints or devices**. This includes phones, tablets, computers, Internet of Things (IoT) devices, and much more across a range of operating systems. This is far more convenient than

What Is a UEM solution?

Any good modern MDM solution is really a UEM solution. Leading MDM solutions all offer the ability to manage almost any office device from one console. Plus, these solutions can all manage the content on those devices, too. Major industry benchmarks like the Gartner Magic Quadrant for UEM Solutions have now adopted the term UEM in place of MDM or EMM.

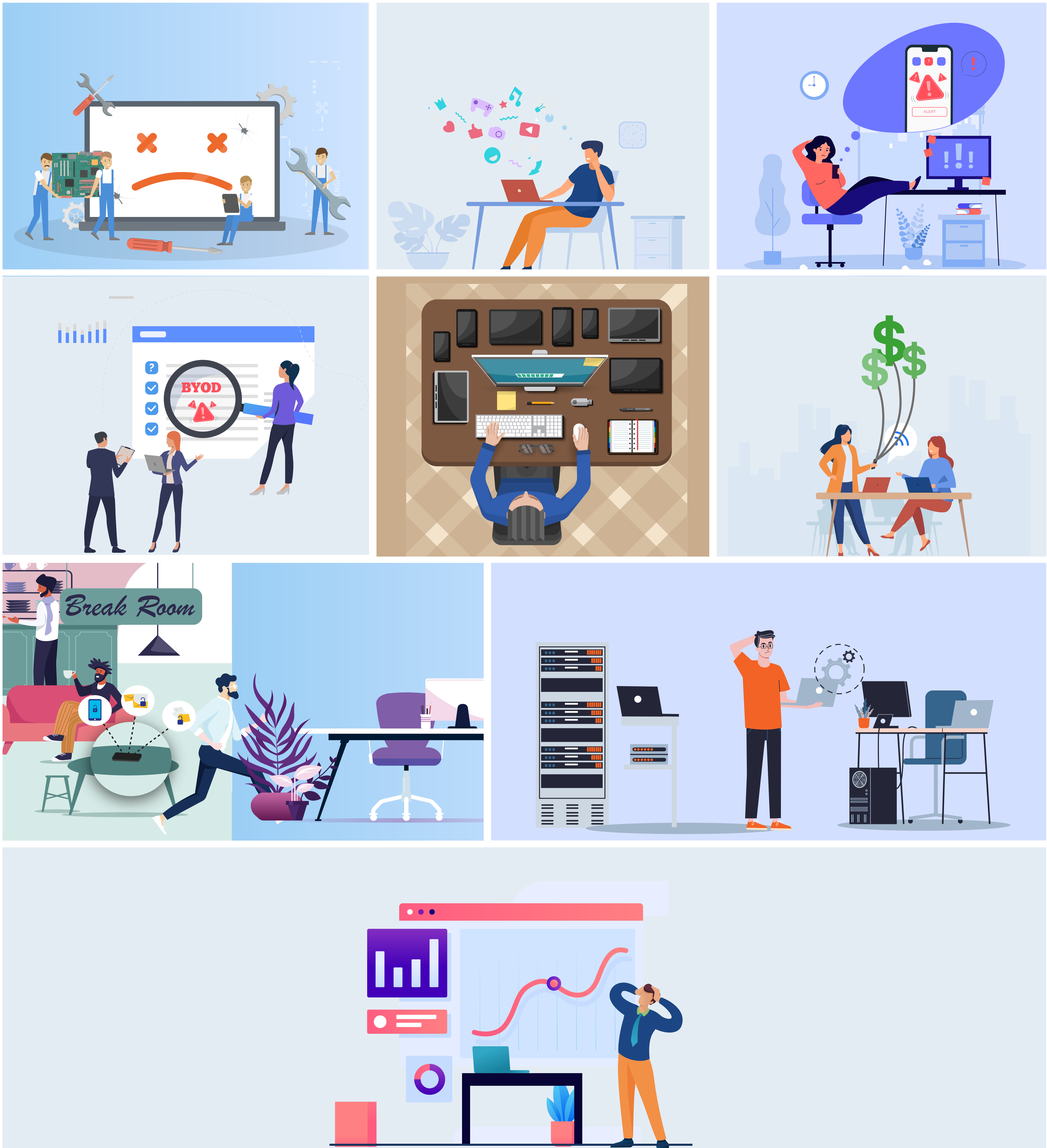


Why Use An MDM?

An MDM solution lets you improve many aspects of your organization at once, instead of making improvements one-by-one. Although setting up an MDM solution requires time and planning, it will show its value quickly, with sustained benefits over time.

When To Use MDM

An MDM solution lets you improve many aspects of your organization at once, instead of making improvements one-by-one. Although setting up an MDM solution requires time and planning, it will show its value quickly, with sustained benefits over time.



If any of the following statements match your concerns, the right MDM solution can resolve all of these at the same time:

- *When software issues cause devices to malfunction, IT admins need to travel on-site to make repairs, adding unnecessary transit costs.*
- *Employees don't get work done because they watch YouTube, play games, and use social media while at work.*
- *Some apps that employees download for fun end up being scams, resulting in the device being compromised by malware.*
- *Admins are not comfortable touching workers' personal devices for fear of invading privacy, meaning business data on those devices goes unsecured.*
- *Setting up new apps and devices takes too much time.*
- *There is no control on data consumption costs incurred on company-owned devices due to negligent use by workers.*
- *Employees could leak sensitive emails and files, with no contingency plan if that happens.*
- *Even if most employees use devices responsibly, admins have no emergency plans if one worker loses or misuses a device.*
- *Admins have separate systems for managing phones and computers, and jumping between them is cumbersome.*
- *Most device manufacturers provide some management tools, but there is no way to bring these tools together to manage the wide variety of devices found in most offices.*
- *There is no easy way for the IT department to collect and analyze data like device use patterns.*

When you implement a strong MDM solution, you can resolve all of these concerns quickly. Of course, admins will need to remain vigilant to ensure nothing goes wrong. But rather than solving these concerns one-by-one, admins with an MDM solution can address them all at the same time.

What Can An MDM Solution Manage?

As mentioned above, modern MDM solutions can manage almost every kind of business device (also called an endpoint). This is why the term unified endpoint management (UEM) is more accurate.

When researching an MDM solution, ask what types of devices and what operating systems the solution supports. Some solutions only support one operating system on a given type of device (for example, they might only support iPhones). This means it's important to find a solution that fits your particular needs.

Types Of Devices An MDM Solution Can Manage



Mobile phones: Of course, mobile device management includes the ability to manage mobile phones! Still, there are all kinds of mobile phones, including classic cell phones (or feature phones), and modern smartphones. You will need to make sure that you choose an MDM solution



Tablets: Some MDM solutions support both standard tablets and rugged tablets.



Computers: MDM solutions can manage both desktop and laptop computers



Wearables: Wearables in the workplace are becoming more and more important, and you can manage smartwatches and rugged wearable computers with most MDMs.



Rugged Devices: MDM solutions should support ruggedized phones, tablets, and other devices designed for physically demanding work environments. For example, an MDM solution may partner with a rugged device manufacturer to ensure the solution is optimized for warehouses employing that manufacturer's devices.



Virtual Reality (VR): One of the biggest new trends in business is the use of Virtual Reality (VR) or Augmented Reality (AR) devices. In response, most MDMs offer support for select VR/AR headsets. They are also known as head-mounted displays.



Industrial Internet of Things (IIoT): Some MDM solutions can also manage sensor-based devices, industrial routers, and other data collection devices used in industrial settings. 42Gears' Things Management is a powerful, yet scalable solution for the management of Industrial IoT devices.



Non-Traditional Endpoints: Some MDM solutions offer support for IoT devices and devices without traditional operating systems. These devices include office essentials like printers, scanners, and battery cradles that were built before IoT technology became so popular.

Operating Systems An MDM Solution Can Manage

● **Android:**

Google's mobile OS, now on its eleventh iteration, is at the heart of many companies worldwide. For this reason, a good MDM solution should support Android Enterprise along with additional useful functionality. In order to manage Android devices from different manufacturers, an MDM solution should also have OEMConfig support.

- **Android VR:**

Some major VR headsets run on Android, and an MDM may be able to support them as well.

- **Wear OS:**

Google's OS for smartwatches, formerly known as Android Wear, can be managed through some MDM solutions.

● **iOS and iPadOS:**

Apple split the iOS operating system in 2019, naming the iPad version iPadOS. However, admins can manage both iOS and iPadOS devices through Apple Business Manager (ABM), and most MDM solutions interface with ABM.

- **Watch OS:**

MDMs cannot manage Apple Watches independently, but can do so by managing the iPhones to which the watches are tethered.

● **macOS:**

Apple's laptop and desktop OS has thrived thanks to its stellar reputation and performance. Apple provides management tools through Apple Business Manager (ABM), but many offices use macOS in addition to Windows systems, and ABM is not sufficient by itself in that context.

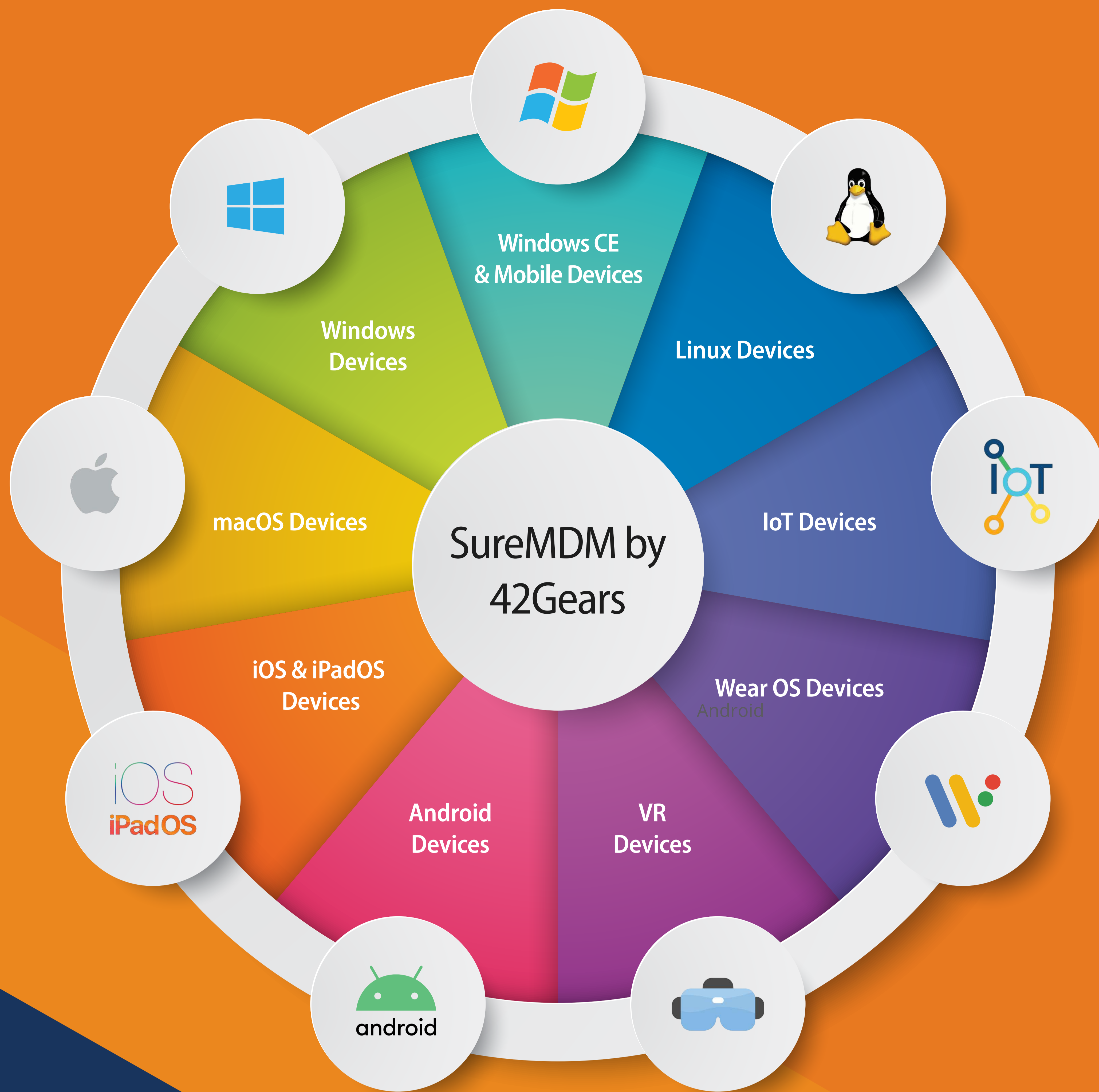
● **Windows:**

Given how widely Microsoft's OS is used worldwide, a good MDM solution should support Windows 10 devices. Many MDM solutions also offer limited support for deprecated versions of Windows (including Windows 7 and 8).

- **Windows CE and Windows Mobile:**

A surprising number of companies still rely on older devices running these deprecated versions of Windows. An MDM solution may be able to remotely monitor and support these devices alongside more modern ones.

● **Linux:** As an open-source OS, Linux requires skill to set up effectively and to maintain. Robust MDMs solutions support every available Linux distribution.



Partnerships Between MDM Solutions And Manufacturers

Some device manufacturers (known as “original equipment manufacturer,” or OEM) have exclusive programs that build on the OS their devices use. For example, Zebra Technologies, which produces rugged devices, offers a program known as Zebra LifeGuard. Enrolled devices get LifeGuard firmware updates even after Google stops supporting those devices. MDM solutions often partner with specific OEMs to optimize an MDM solution for a particular OEM’s products. For example, 42Gears has partnered with Zebra to offer enhanced support for Zebra LifeGuard updates and has partnered with Samsung to optimize SureMDM (42Gears’ UEM solution) support for the Samsung Knox security initiative.

If your organization uses devices from a specific OEM, you should check to see whether any MDM solutions have partnered with that OEM.” to “If your organization uses devices from a specific OEM, you should check to see whether any MDM solution providers have partnered with that OEM.





What Can An MDM Solution Do? How MDM Works

- ◆ **MDM**
Mobile Device Management
- ◆ **MIM**
Mobile Identity Management
- ◆ **MAM**
Mobile Application Management
- ◆ **BYOD**
Bring Your Own Device
- ◆ **MCM**
Mobile Content Management
- ◆ **Non-Traditional
Endpoint Support**

Although several categories include “mobile” in their names, they apply to both mobile devices and computers. These category names are holdovers from an earlier era, just like the term “mobile device management” itself.

Mobile Device Management (MDM)

These are features that impact the entire device and everything on it. These were the first features offered by MDM solutions, which is why they are known by this name. Over ten years later, these features are still necessary for implementing any kind of MDM.

Review [this list of common mobile device management features](#) to see some of the most important actions an MDM solution can perform:

Setting up many devices at once: You can use an MDM solution to quickly enroll many devices into your organization. As part of this process, you can add apps and other content to many devices at once (a process known as provisioning).

Monitoring many devices at once: Once you enroll devices into an MDM solution, you can choose what information admins receive about them. For example, you can track the location of company-owned devices or lookout for signs of poor “device health” (such as short battery life).

Applying contextual policies: You can apply policies to a device based on location (known as “geofencing”), time of day (known as “time-fencing”), and whether the device is connected to a certain Wi-Fi network (also known as “network-fencing”).

Neutralizing security risks: If someone loses a device or does something dangerous with it, admins can remotely secure the device. This ranges from locking down a device to completely wiping it and restoring it to factory settings.

Remotely troubleshooting devices: If device users experience issues, you can use the MDM solution’s central console to remotely view the device screen. From here, you can simulate screen taps and button presses to troubleshoot devices.

Mobile Application Management (MAM)

Newcomers often find the overlap between MDM and MAM confusing, as evidenced by popular online questions like “what is MDM and MAM?” Still, it is not hard to understand.

MAM features manage specific apps, rather than controlling the way the entire device works. Effectively using an MDM solution’s app management features will improve security and keep employees on-task.

Review [this list of common mobile application management features](#) to see how an MDM solution can help streamline the way employee’s access and use apps.

Distributing the same app, or the same group of apps, to every device: An MDM solution can ensure that every device has the apps it needs to function. You no longer need to worry about employees forgetting to download the apps they need.

Ensuring every device has the same version of an app installed: Outdated apps are vulnerable to attack. On the other hand, sometimes you need to wait to install the latest version of an app. An MDM solution can automate the update process, or you can manually approve the latest updates.

Mobile Content Management (MCM)

The purpose of Mobile Content Management is to manage files and other content, with a focus on protecting sensitive data. If used consistently, content management tools significantly reduce the likelihood of sensitive documents being leaked to third-parties.

Review [this list of common mobile content management features](#) to see how an MDM solution can keep your files safe.

Sending files to many devices at once: If you need to send important documents or media to some or all employees, you can use an MDM solution to do it quickly and at scale.

Keeping files within your organization: You can prevent employees from exfiltrating important data (such as through copy-pasting text) with an MDM solution.

Automatically destroying endangered content: If an MDM solution determines that a device has broken your organization's rules, the console can automatically destroy sensitive content on that device and alert admins.

Mobile Identity Management (MIM)

These features control how devices access your network, providing safeguards against attacks. By implementing these features across every device in your business, you can make it almost impossible for hackers to pose as legitimate employees.

Review [this list of common mobile identity management features](#) to see how you can use an MDM solution to make your network secure.

Distributing security certificates to approved devices: You can use an MDM solution to distribute and update security certificates as needed.

Single Sign-On: You can integrate many MDM solutions with SSO identity providers like Microsoft Active Directory Federation Services, in order to streamline the authentication process.

Bring Your Own Device (BYOD)

You can use an MDM solution to create a virtual "workspace" on employee-owned devices that doesn't invade personal privacy. You can manage, alter, or delete the virtual workspace remotely without impacting any personal-use apps or data. This is called containerization, as you create a container on each device.

Review [this list of common BYOD features](#) to understand what an MDM solution can do on employee devices.

Registering employee devices on business networks: BYOD support makes it easy to safely transfer Wi-Fi credentials and business email access to employee-owned devices.

VPN Configuration: You can use some MDM solutions to configure per-app virtual private network (VPN) connections on BYOD devices. This makes individual app activity secure even when the entire device is not using a VPN.

Controlling work data without seeing personal data: A good MDM solution will work with tools provided by Apple, Google, and others to create a virtual container for sensitive business data. As IT admins can only modify data within the container, they cannot see or alter personal data. Even if employees break company rules on their own devices, the company can wipe business data without wiping anything else.

Non-Traditional Endpoint Support

You can use 42Gears' Things Management Technology to manage equipment that wasn't designed with connectivity in mind, such as printers. Many companies are trying to figure out how to turn the Internet of Things into an "Enterprise of Things," but there are some major obstacles. This is where 42Gears' technology, specifically, can help.

Review this list of non-traditional management features that can be found in SureMDM by 42Gears:

Managing IoT devices with an MDM solution: If your business relies on sensors and other kinds of embedded devices, you can monitor and manage them through SureMDM.

Managing "not-so-smart" devices that don't have a modern OS: 42Gears has developed a framework to manage "not so smart" accessories like older printers. Companies can write their own code (or "Things Connectors") to make accessories accessible to SureMDM through their host machines, or check the 42Gears Things Connectors Marketplace. Once implemented, this turns the host machine into a proxy for older devices to be managed through SureMDM.

Creating a central framework for smart and "not-so-smart" devices alike: Once enrolled in SureMDM, smart and "not-so-smart" devices can both appear on a single central console. Admins can then remotely monitor and manage every device from a single console.



Options For Deploying An MDM Solution

When setting up an MDM solution, firms must choose between two deployment methods. This is an important choice, as it will have a significant impact on how you operate and maintain the MDM solution later on. These two methods – on-premise and cloud-based – both have advantages and disadvantages, and there is no “right answer” that applies to every organization.

Deploying A Cloud-Hosted MDM Solution

In a cloud-hosted MDM solution deployment, the provider who runs the MDM solution hosts all of your company’s data on servers actually hosted by cloud-infrastructure service providers such as AWS, Azure, or Google Cloud Platform.

Cloud-hosted MDM solutions are a good choice for anyone looking for a straightforward way to quickly set up an MDM solution. This includes most SMBs (small- and medium-sized businesses), along with many larger companies who want to optimize efficiency.

Review this list of reasons why to adopt (or avoid) a SaaS MDM solution (also known as a “plug and play” solution) to decide if it is a good fit for your organization.



Pros Of Using A SaaS MDM Solution:

You can save substantial time and money by relying on pre-existing infrastructure. Because you do not need to purchase or coordinate tech infrastructure on-site, you can jump right in and begin enrolling devices straight away.

No need for maintenance. The MDM solution provider will handle all maintenance, so you do not need to worry about the logistics behind-the-scenes.

You can scale up as needed. If you decide you need to support more devices, there will be more space in the server for you to occupy. With on-premise infrastructure, scaling up is much more costly, as you would need to create more space on your own servers. Plus, the MDM provider will automatically include upgrades as part of the service you pay for.

Cons Of Using A SaaS MDM Solution:

You have to trust the provider to keep your data safe. Some businesses may not like the idea of storing sensitive data in an external location. Any reputable MDM solution provider is well-aware of this concern and will place all sorts of safeguards to ensure data stays safe.

Deploying An On-Premise MDM Solution



In an on-premise deployment, an MDM solution provider leases its software for use on a client's own servers. This means that the client is now fully responsible for maintaining and protecting the MDM infrastructure.

On-premise MDM solutions are ideal for companies that need to keep all data in-house, provided they have the time and money to spare. This profile includes large healthcare and banking firms, where privacy is of the utmost importance but does not include most small or mid-size businesses, as well as any company without a large IT team.

Review **this list of reasons why to adopt (or avoid) an on-premise solution** to decide if it is a good fit for your organization.

Pros Of Using An On-Premise MDM Solution:

There is no risk associated with storing data externally. Industries such as finance need to consolidate data on-premise to maintain customer trust. An on-premise MDM deployment will allow them to do just that.

Cons Of Using An On-Premise MDM Solution:

Purchasing and maintaining the infrastructure you need demands time, effort, and money. You will need to build and set up your on-site infrastructure, and then maintain and update it regularly. You will also need to consider the time needed to train IT workers for these tasks. If you want to scale up your MDM deployment, you will be responsible for expanding your infrastructure as needed.

Choosing **The Best MDM Solution For Your Needs**

There is a fairly short decision-making process that will help you make the right choices regarding which MDM solution to choose. Even though each company that uses this method may come up with a different answer, the process itself is universally applicable.

1

Identify your overall goal(s). This should include solving specific problems with measurable results, if possible. For example, a good goal would be “I want my employees to stay focused at work. I want to cut the amount of time anyone spends playing games at work down to zero.”

2

Understand what endpoints you need to manage. If you make sure you know what needs to be managed, you will be in a better position to find the MDM solution that best suits your needs. Alternately, you can choose an MDM solution that is capable of managing most kinds of office devices, like SureMDM

3

Determine your budget and personnel. An MDM solution should make your organization easier to run. This means you need a clear sense of what your budget and IT team can handle in terms of set-up and maintenance.

4

Choose whether to use company- or employee-owned devices (or both). MDM solutions provide more options on company-owned devices, as admins do not need to worry about personal data. However, paying for devices can be expensive, and employees are most proficient at using their own devices.

5

Choose whether to deploy an MDM solution on-premise or via the cloud. As mentioned earlier, your organization does not have to worry about the upkeep of cloud infrastructure. On the other hand, to maintain complete on-site control over all sensitive data, an on-premise solution is the right choice.

6

Assign roles and responsibilities. Most good MDM solutions allow you to designate different admin roles, with different levels of authority. Setting these rules in place early on will avoid potential disputes.

7

Unique Needs. Every organization is unique, and so is every MDM solution. Finding what makes an MDM solution unique shouldn't be hard.

Learning as much as you can about step-by-step MDM deployments is essential. In fact, by reading this guide, you've just begun that process!



Conclusion

Modern IT teams focus on mobile device management as one of their core IT practices; once you understand it, you've taken a major step towards modernizing your workplace. Most MDM solutions can now manage almost any device or endpoint in the workplace environment, as befitting of the term "unified endpoint management." Using an MDM solution will help thwart all kinds of security threats; as you can streamline managing and securing apps and content, control access to sensitive data, and above all, improve workforce productivity.

Of course, each MDM solution offers a slightly different feature set. By determining what you must secure, monitor, and manage, and by assessing the importance of BYOD programs and non-traditional device management, you can figure out which MDM is right for you. If you are interested in trying a well-rounded MDM solution with support for all kinds of endpoints and use-cases, you can start with a free trial of SureMDM, the 42Gears MDM solution.



www.42gears.com