The Ultimate Guide to Mobile Device Management

April 2023

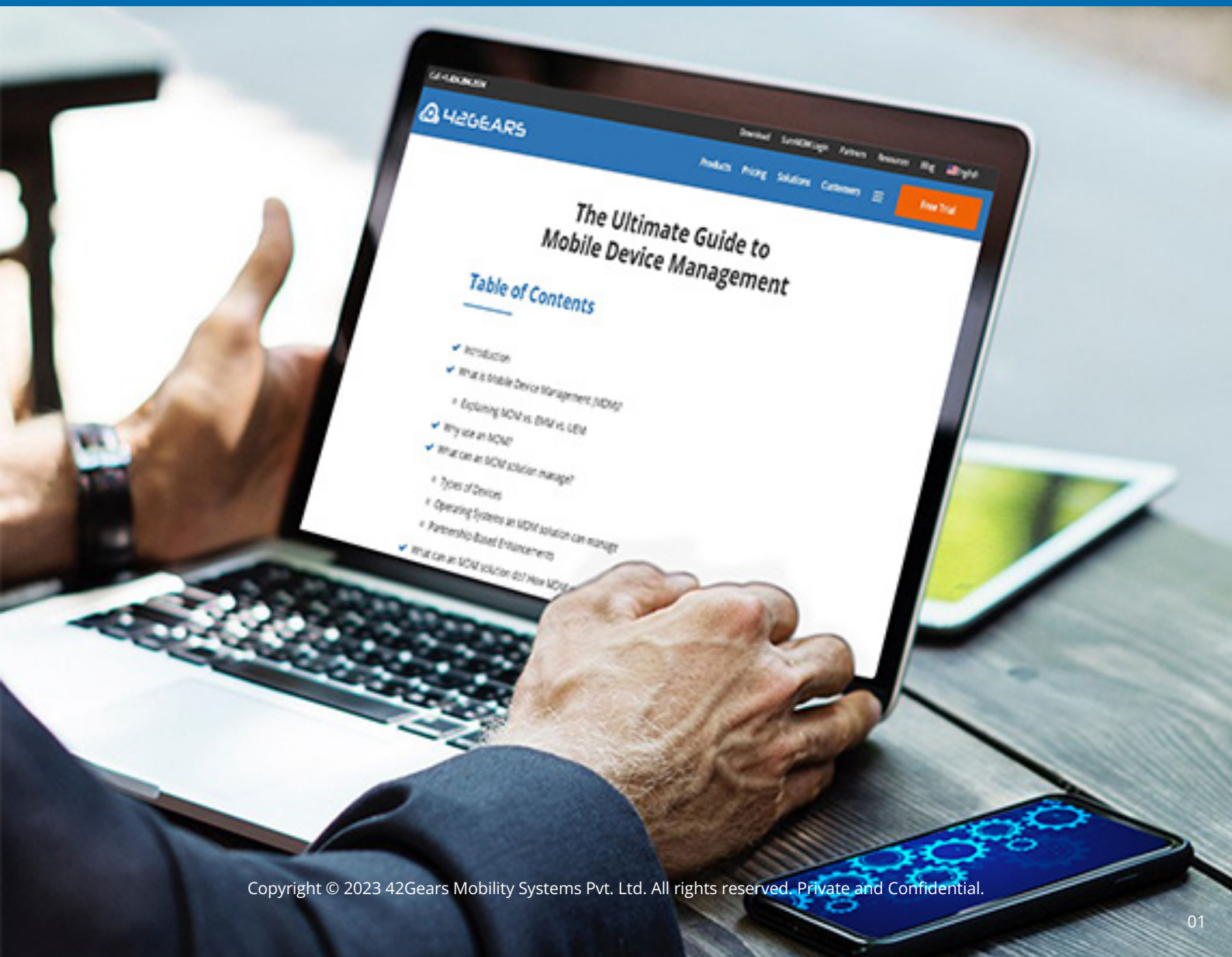


Table of contents

Introduction to Mobile Device Management

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.

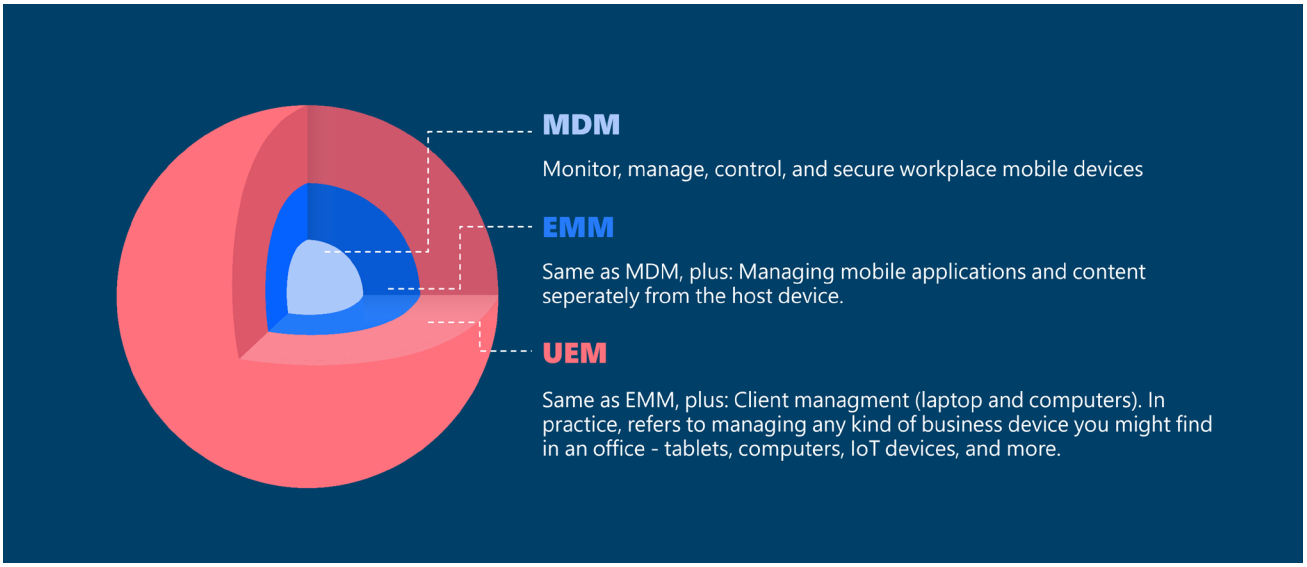
MDM can manage more than mobile devices. You can use MDM technology to manage smartphones, tablets, desktops, and almost any other technology. For this reason, implementing MDM software is a smart idea for almost any company.

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 mobile devices and the applications and content** on those devices. 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.

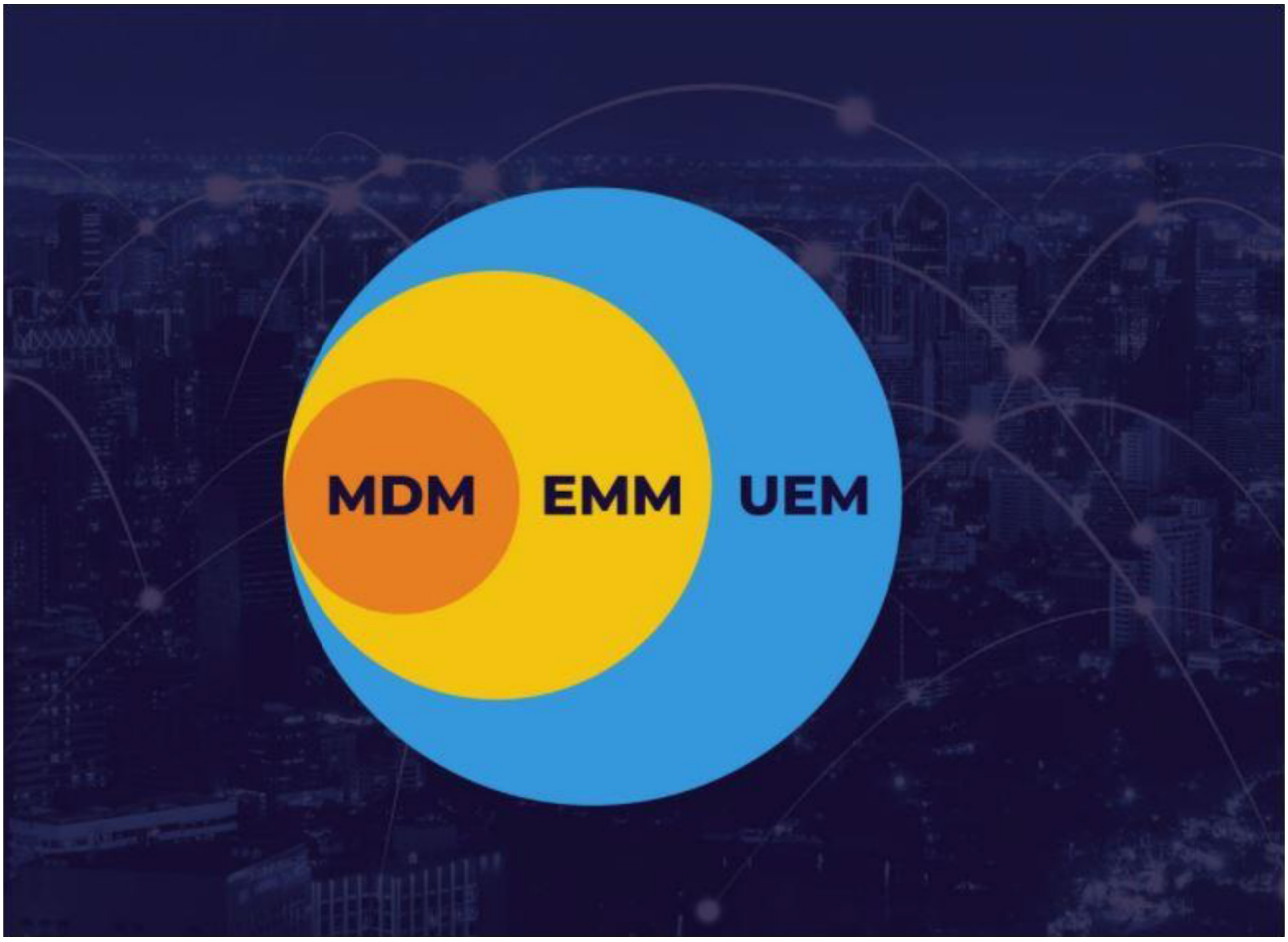
What is UEM (unified endpoint management)?

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 previous approaches, and also far more powerful.

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.

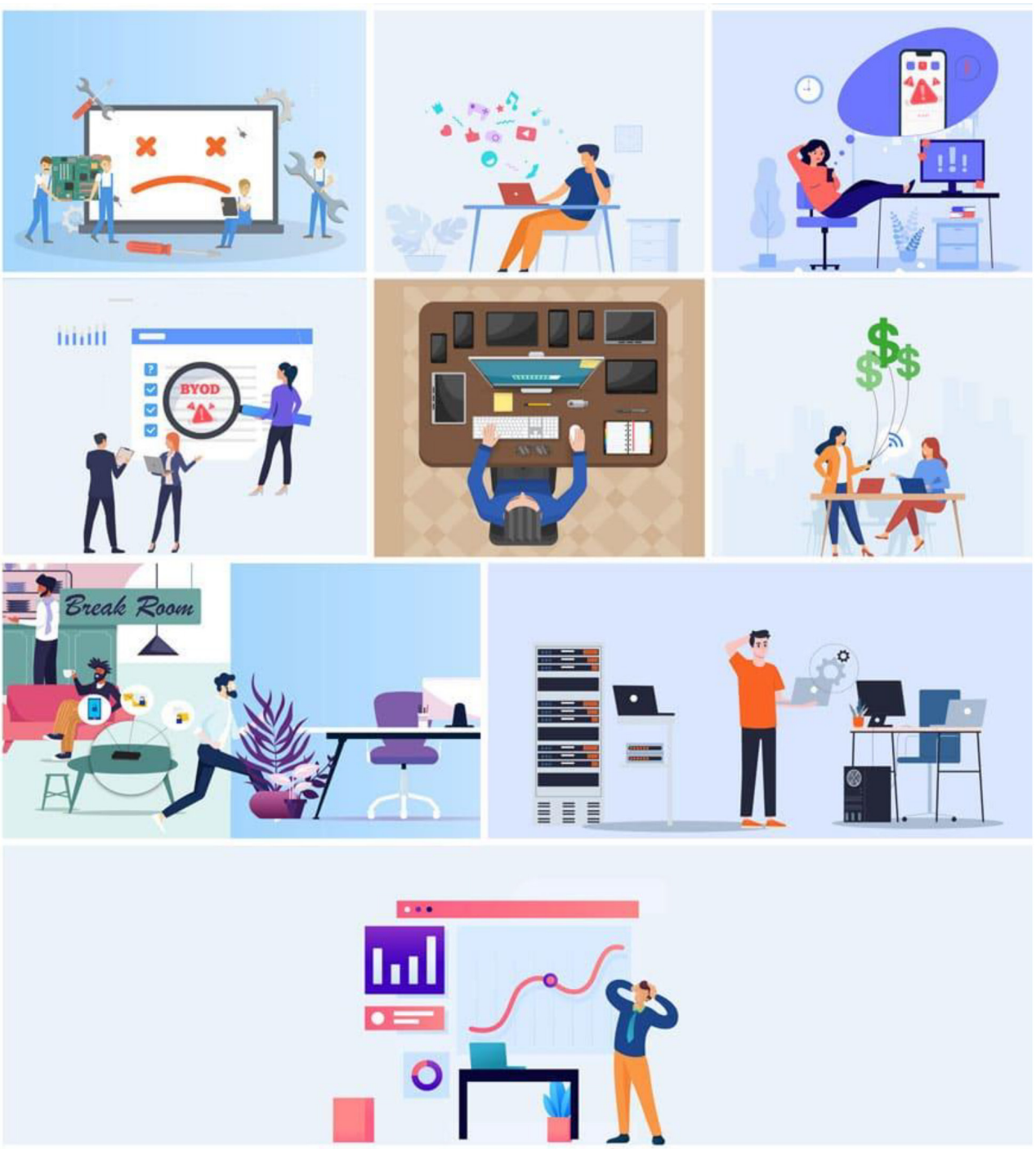
MDM and EMM remain popular terms because they are widely recognized. Of course, there is always the chance that MDM and EMM offerings have fewer features, and are therefore not UEM solutions. You should always make the effort to ensure any MDM or EMM solution you find is actually a UEM solution.



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?



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 admion-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 that supports the mobile devices your team uses.

- ✓ **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.

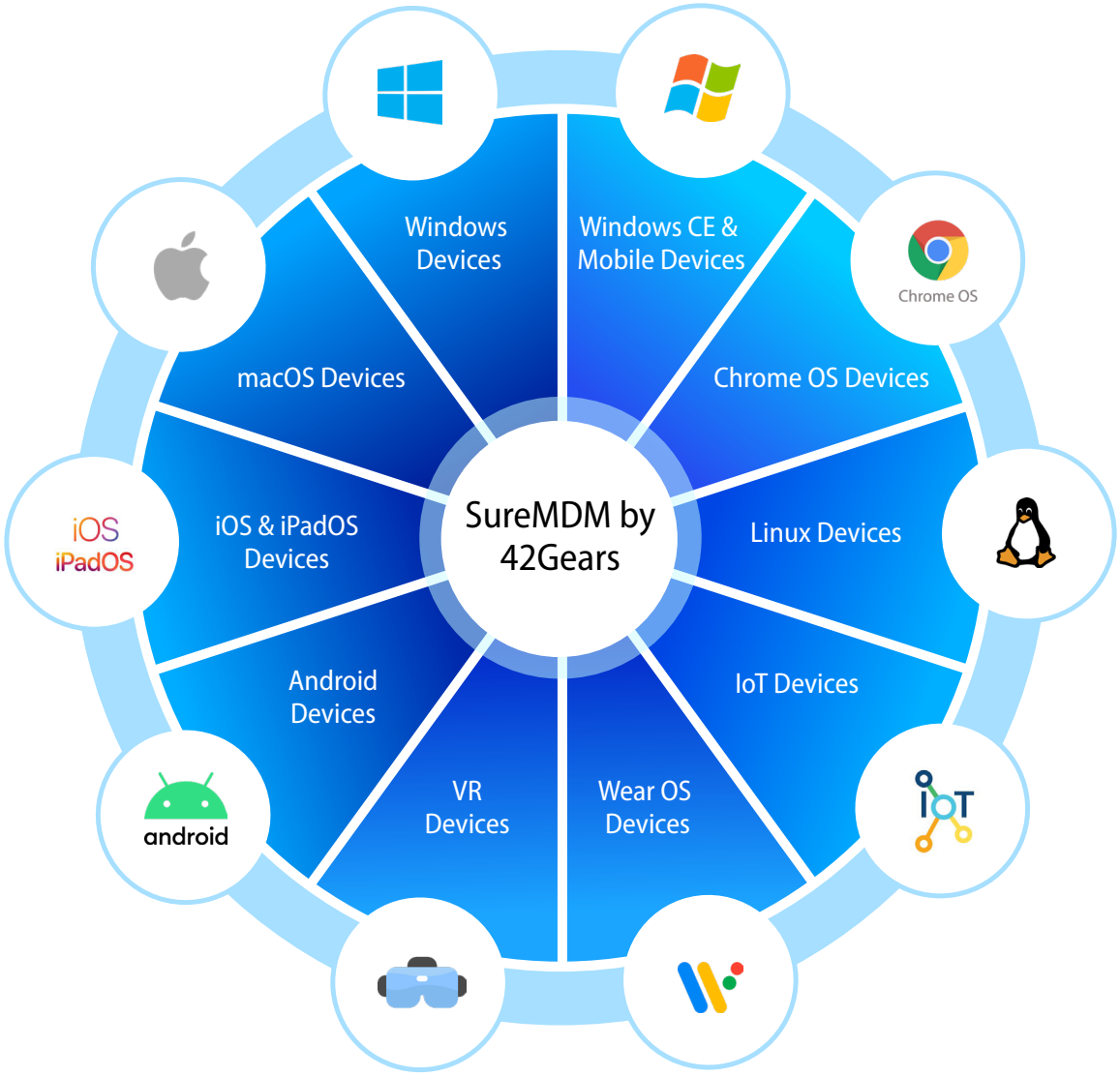
- ✓ **Virtual Reality (VR):** One of the biggest new trends in business is the use of Virtual Reality (VR) or Augmented Reality (AR) devices. In response, most MDMs offer support for **select VR/AR headsets.** They are also known as head-mounted displays.

- ✓ **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 is Device Lifecycle Management?

The Stages of Device Lifecycle Management

While it is essential to understand the general concepts underlying MDM, this is only the first step towards actually implementing it for your business. You will need to plan for the entire device lifecycle, which can be analyzed as a sequence of five steps. These include:

- ✓ Enrollment: Bringing newly-acquired devices into your business network.
- ✓ Provisioning: Setting up initial configuration, security settings, apps, and content for employees and users to get started.
- ✓ Deployment: Getting provisioned devices in workers' hands.
- ✓ Management: Monitor devices for compliance, push app updates, troubleshoot application and performance issues.
- ✓ Retirement: Removing devices from the system once they reach end-of-life (EOL).

Of course, some of these steps are more involved than others; deployment will likely be a quick process, while management is an ongoing process over several years. Yet each step has its own challenges and potential pitfalls, so it is worth addressing them in sequence.

Enrollment

The process of enrolling devices into a management framework is a daunting task, but it is essential. Depending on the tools available, this process may be almost fully automated, or it may require substantial effort on your business' behalf.

If you are enrolling Android devices, you can rely on Android Enterprise to help with some steps of the enrollment process. If you are enrolling newly-released devices from select suppliers, you will be able to partake in Zero-Touch Enrollment (ZTE), This will allow you to set up and enroll devices before even turning them on.

If this is not supported, however, MDM solutions like SureMDM present a wide array of enrollment methods on Android, giving your business flexibility in how it begins the lifecycle management process. These include fast and easy techniques like scanning a QR code with each device to instantly enroll it.

If you are enrolling Apple devices, you can streamline enrollment by purchasing devices from Apple Authorized Resellers. They will be able to help you register and enroll devices into Apple Business Manager (ABM) before you turn them on for the first time. Of course, you can also manually enroll devices into ABM via Apple Configurator.

For Windows devices, you can use the Windows Autopilot program if you purchase devices through select resellers. Otherwise, you will need to enroll devices manually. You can accomplish this by downloading an MDM agent directly onto a given device, and connecting it to the MDM console. Alternatively, you can use Windows' device management capabilities to enroll devices through Windows, provided you connect an associated MDM solution.

For any other device type not covered above, you will mostly need to use manual enrollment methods. This means you (or an employee) will need to download an on-device agent, and then connect the device to the central console by hand. Some of the steps can be automated, but it's often a time-consuming method.

It's worth noting that you may also wish to enroll employee-owned devices, in addition to business-owned devices. For these so-called BYO ("bring-your-own") devices, or BYOD, enrollment depends on the operating system. Android and Apple devices allow employers to register employee-owned devices through Android work profiles and the Apple User Enrollment program, For Mac, Windows, and Linux devices, you will need to ask employees to download the on-device agent instead.

If you are a veteran to the use of MDM, you may actually be looking to switch MDMs, rather than enrolling from scratch. In that case, it's very important to talk with the company behind the MDM you are migrating towards, to ensure that a smooth transition is possible. You'll also need to make sure that every device is unenrolled from the existing MDM and then enrolled into the new solution.

This may seem obvious, but inventory-keeping between MDM solutions is quite difficult; you will save yourself an enormous headache by double-checking inventory at every step. On another note, different MDMs allow admins to assign device hierarchies in different ways; this may require manually mapping the hierarchies of one MDM solution onto another.

Provisioning

Now you have connected all your devices. It's time to set them up with the apps and content they need, while preventing them from accessing irrelevant apps and content. This is tedious to do by hand for a small organization, and effectively impossible for larger ones; thankfully, you can rely on MDM to speed up the process substantially.

Different operating systems offer different ways to provision apps and content. On Apple devices, like iPhones and iPads, you can do this through ABM (Apple Business Manager). ABM has now subsumed the Volume Purchase Program (VPP) functionality that admins once needed to make this possible. For Android devices, on the other hand, admins will need to use the Managed Google Play Store for Android devices.

On these and other platforms, you can use MDM functionality to create an Enterprise App Store. This is a private storage space for the apps that your employees and users can access at will. Rather than forcibly downloading the apps to the devices, an Enterprise App Store allows employees to access and download apps on their own time and when they need them. You can also implement an Enterprise File Store that follows the same logic, providing a safe space for employees to download essential files and documents.

Device Lockdown

If the devices you are provisioning will serve a dedicated purpose, you should consider locking the devices down. This means you are restricting the device from performing any activities you haven't approved beforehand. Admins can choose either between single-app mode or multi-app mode, based on the needs of their employees.

Device manufacturers often provide simple lockdown mechanisms of their own, but they typically require manual interaction with each device, which is infeasible at scale. This is another circumstance in which MDM can help you get a grip on many devices at once.

On Windows devices, you can choose between using an MDM to set up a Kiosk Profile, or using a dedicated device lockdown solution like SureLock for Windows. For its part, Android offers a default Screen Pinning option, but this is very limited and requires manual setup and deactivation on each device. For this reason, most businesses use a device lockdown tool like **SureLock** instead.

For iPhones and iPads, you can use Guided Access, a built-in feature, but its functionality is quite limited. It's generally wiser to activate single-app mode, either

through Apple Configurator or an MDM solution. Using an MDM solution provides you with the most management capabilities.

You can extend device lockdown to Internet usage as well, if you need to keep users on specific websites. Some MDM solutions come with their own internet browsers, like SureFox by 42Gears. This way, you can prevent users from accessing suspicious websites and downloading any kind of malware that can jeopardize user and organizational data safety.

Deployment

Once you have provisioned devices, you can now begin the deployment process, sending devices out to the employees or users who will be using them. While this is a relatively straightforward process, there are a number of things that can go wrong. It's worth reviewing what those things are, so you can make sure to avoid them and have a successful deployment.

One important aspect of deployment that sometimes goes overlooked is making sure that every device has the appropriate security certificates installed. If there is any error in this regard, employees may be locked out of essential functions on the devices you provide them. As a result, it's important to ensure users can report issues immediately, and get them fixed right away. Particularly for frontline workers using devices to stay safe in tough environments, security certificate issues could put users at serious risk.

Another concern related to deployment is ensuring that network connectivity is always available. If a user gets a device with improperly configured Wi-Fi or data consumption settings, there should always be a way to configure a connection again. This can be a challenge many businesses face when devices are locked down and do not allow access to settings menus. With 42Gears' lockdown software, you can choose to have connectivity settings menus automatically open when a device no longer senses a connection, making sure employees won't be locked out of resources they need. Be aware that you must turn on these options before you deploy the devices.

In some instances, deployment may also see device users enrolling their new devices into an MDM solution. If admins don't rely on resellers, and don't want to manually set up each device, users can enroll devices themselves. Those users will need to follow on-screen instructions, but those instructions should be fairly straightforward. For example, they may need to scan a QR code to enroll devices.

You should make sure that devices can complete authentication while being enrolled, especially if employees are enrolling devices themselves. Whether you choose Active

Directory or another method, you should complete a proof-of-concept in advance to make sure it will work for your employees.

Management

Once employees have properly-provisioned devices in their hands, it is time to manage those devices. This is (ideally) by far the longest phase of lifecycle management, as most devices have a lifespan of at least a few years.

It's a daunting task to keep devices compliant, up-to-date, and functional for several years, but it's made substantially easier through the use of mobile device management software. MDM software allows you to automate many aspects of management, and even when automation isn't feasible, an MDM solution helps to resolve issues faster.

Oftentimes, a single device needs access to a given resource at one time of day or location, but not at others. In these cases, an admin can create contextual rules known as fences. If devices are within the fence, a certain policy activates, but once the criterion for the fence is no longer fulfilled, the policy deactivates. Location-based geofencing, time-based time-fencing, and network security-based network-fencing can all go a long way towards ensuring responsible device use.

You can also rely on the MDM console to update apps on devices remotely without the need for employees to take any action. This can take place as a silent update on devices employees are actively using, or you can choose to wait for periods of time when employees are not actively using devices. Remotely updating apps also confers a range of benefits, such as reducing device downtime and raising employee productivity.

That said, it's not always ideal to update every app as soon as updates become available. Sometimes updates have major issues that need to be resolved before it's safe to download them. In these cases, admins can use MDM software to keep every device from updating that app, ensuring everyone stays on the same version of any given app. Without an MDM solution, keeping devices up to date is effectively impossible, requiring admins to manually inspect each device.

One of the greatest challenges associated with any enterprise deployment is troubleshooting devices. If software stops working properly, this normally requires a technician to come fix a device in-person, or for employees to ship the device to the technician. Both possibilities are very expensive. Thankfully, in many instances, you can use an MDM solution's remote control features to take control of devices remotely, and repair them remotely. This makes repairs faster and easier.

Another challenge tied to device management is the possibility of users consuming too much data. If the company is forced to pay for excess data consumption, it can be prohibitively costly to cover these costs at scale. With an MDM solution, you can monitor each device's data consumption, send messages to users consuming too much data, and if necessary block data consumption altogether. The same goes for battery consumption; whether through irresponsible device use or failing device health, excessive battery use is a major problem. By tracking and notifying users when device battery levels decline, an MDM solution can keep devices from losing charge for longer.

Retirement

When devices are no longer supported by their manufacturers, and there's no way to secure them, it's time to retire them. While resetting and relinquishing a device is relatively simple, there are a few important things to keep in mind.

If you've enrolled your devices into an MDM solution, you should keep in mind that the device licenses do not need to end along with the device. As long as a given license is not yet expired, you can apply the remaining length of the license to another device.

You may need to forcibly retire devices ahead of schedule if they are lost or stolen. Using an MDM solution, you can remotely purge device data (in a process called a "remote wipe") on any enrolled device with an Internet connection, including one that is lost. Still, you should understand that wiping the device will in most cases remove the on-device agent app, meaning the device is no longer connected to the MDM console. You'll also need to uncouple devices from the central console, in order to free up their licenses for use on other machines

When you are unenrolling employee-owned devices from the MDM solution, the process is generally the same. Rather than removing all content from each device, the wipe operation instead just removes all enterprise-related data, and the virtual container holding that data. This leaves the employee's personal data completely untouched and unaffected.

It's worth noting that there are ways to push back the need to retire a device. Some device manufacturers offer programs that extend security support well past a device's end-of-sale date, such as Zebra's LifeGuard program. If you have not yet purchased the devices you wish to deploy, take the time to investigate whether your potential devices will offer something like this.

What can an MDM solution do? How MDM works

Mobile device management can help in dozens of ways, organized into a few larger categories. They are as follows:

- ✓ MDM (Mobile Device Management)
- ✓ MAM (Mobile Application Management)
- ✓ MCM (Mobile Content Management)
- ✓ MIM (Mobile Identity Management)
- ✓ Bring Your Own Device (BYOD)
- ✓ 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 employees 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.