**What Is Enterprise Mobility Management (EMM)?**

Presently, when mobile devices are the preferred tool at work, EMM is becoming a critical IT requirement. Smartphones and tablets have become much more advanced in recent years and offer numerous features that make them ideal for several business tasks. They also offer employees the convenience to work from anywhere and at any time. However, if not managed properly, they can put a company’s data and network security at risk. Therefore, companies need EMM solutions that let IT teams manage mobile devices across multiple platforms such as iOS, Android and Windows 10.

EMM solutions come with a set of tools and features that let IT teams monitor, control and manage mobile devices for enhanced security. Typically, an EMM tool offers solutions like mobile device management (MDM), mobile applications management (MAM), mobile content management (MCM) and mobile identity (MIM). Having access to both mobility and security services ensures that employees can access company applications, tools and data at any time without putting the integrity of the device or network at risk.

**The Evolution of Enterprise Mobility Management**

The roots of EMM tools date back to the early 2000s when Blackberry phones became hugely popular in the business world for bringing email to mobile devices. Businesses purchased these phones in large numbers to expand their mobile device infrastructure. It enabled companies to boost productivity through wireless capabilities. But it also necessitated the need for a mobile device management (MDM) tool to secure the various Blackberry models in use. You can think of MDM as a simple predecessor of the sophisticated EMM tools of today.

As iPhones and Android phones became more available, employees found they offered better functionality and connectivity than Blackberry devices and began using them for work purposes. Due to the consumerization of IT, employees started asking companies to let them use the same devices for both work and personal use, triggering the bring-your-own-device (BYOD) wave.

Companies realized that allowing (BYOD) had many benefits. It enhanced employee productivity, efficiency and happiness, while also simplifying and reducing IT costs. It was a win-win situation for everyone.

A combination of the BYOD phenomenon and an expanding smartphone apps market led to the creation of mobile application management tools (MAMs) that managed the security and functionality of business apps. Over the years, MDM and MAM tools got coupled with mobile content management (MCM) and mobile identity management (MIM) features to provide enterprises with a more comprehensive mobile device management tool.

In other words, an EMM solution, as we know it today, is an integrated set of single-feature mobile device management tools such as MDM and MAM. IT teams store business data and applications in containers on mobile devices that can be managed and secured remotely via an EMM tool. Nowadays, mobile device operating systems provide native device management support, commoditizing the EMM industry.

**What Companies Need Enterprise Mobility?**

Enterprise mobility refers to the system where employees can work remotely and use whichever devices they choose. This system leverages cloud technology to share business applications and data wirelessly. Now, more than ever before, companies need a robust enterprise mobility framework to ensure business continuity under all circumstances.

The COVID-19 pandemic highlighted the need to be prepared for all contingencies. According to the International Data Corporation (IDC), the number of mobile workers in the U.S. will continue to grow over the next four years from 78.5 million in 2020 to 93.5 million in 2024. IDC expects mobile workers to make up more than 60% of the total U.S. workforce at the end of its forecast period.

Business organizations are increasingly adopting enterprise mobility systems because they help reduce costs, increase productivity and offer employees better work-life balance. This framework is likely to benefit companies interested in switching permanently to a remote or hybrid working environment. It ensures that employee onboarding, training, data sharing and transferring, and collaboration activities can occur remotely and safely. Additionally, enterprise mobility frameworks can also help streamline and secure a blended work environment where employees work across different locations and time zones.

**How Does Enterprise Mobility Management Work?**

Companies use EMM tools to monitor work-related applications and data on mobile devices owned by their employees. This helps protect enterprise data while safeguarding the privacy of employers.

With an EMM tool, device enrollments can be done in bulk both on-premise and remotely, saving the IT team time, effort and cost associated with individual sign-ups. Companies can even send SMS and email invitations to employees and have them self-enroll in the company’s BYOD or enterprise mobility management program.

Using an EMM tool, companies can remotely implement security policies, change device settings and remove data and apps used for work. In addition, the tool allows IT professionals to wipe out sensitive business data in case a device is lost, stolen, hacked or damaged, without deleting personal data.

EMM tools combine a multitude of features and are improved continuously to meet the changing demands of businesses. EMM tools, as we know them today, are essentially amalgamated and upgraded versions of the single-feature mobile management tools of the past. While EMM tools offer holistic security and management for mobile devices used for work, when you look closely, you will see that these tools consist of many individual features, each focused on a specific aspect of mobile device management. Let’s take a closer look at single EMM features that can be used independently or combined with other features to form a more effective EMM solution.

**Mobile Device Management (MDM)**

MDM refers to managing all mobile devices employees use for work such as laptops, smartphones and tablets. It involves using MDM software to remotely manage the entire lifecycle of a mobile device and its operating systems like device inventory, configuration management and remote wipe.

An MDM console can configure and manage devices only after the devices have been enrolled in the server using vendor-specific enrollment programs, such as those offered by Apple, Google and Microsoft, or manually through QR codes, email and SMS. Once enrolled, a device can be configured and managed remotely. The MDM software can either run locally or in the cloud. MDM solutions available as Software-as-a-Service are cost-efficient, scalable and easy to manage.

**Mobile Application Management (MAM)**

MAM involves deploying, monitoring and patching enterprise mobile applications that employees use for work. IT professionals can deploy security and corporate policies on business apps and segregate them from personal apps to limit the sharing of corporate data among them.

A MAM solution also allows employees to access the necessary application from the enterprise app store remotely. App configuration, inventory management, application lifecycle management and software license management are tasks performed using a MAM solution. In the event of a security issue, it can also help remove applications.

**Mobile Content Management (MCM)**

Employees need to access company data on their devices to be productive. MCM tools enable employees to access, share and store work files on their mobile devices without sacrificing security. An MCM can help determine access rights each employee has to the company’s data and network. By restricting access, companies can isolate the affected areas of their network during a cyberattack, saving the rest of the IT infrastructure from getting taken over. A good MCM solution will also integrate seamlessly with productivity tools so employees can collaborate more effectively.

**Mobile Identity Management (MIM)**

Data is valuable, and only authorized individuals should have access to it. Companies must adopt a zero-trust security policy as their workforces become more mobile, distributed and remote. They can do this by asking employees to authenticate their identity each time they log into a company network.

A MIM solution can restrict or deny access based on policies in the case of a potential security threat. It relies on multifactor authentication (MFA), biometrics or device-specific information to verify user identity. MIM goes beyond password management to perform identity checks.

**Unified Endpoint Management (UEM)**

While EMM followed in the footsteps of MDM and MAM, the next stage of development in the enterprise mobility management industry is the Unified Endpoint Management (UEM) tool.

Using a UEM tool, companies can manage mobile devices plus all endpoints like servers, PCs, printers, wearables and IoT devices connected to the corporate network. Companies do not need to invest in an EMM tool separately if they have a UEM tool. It reduces IT costs and increases the IT department’s ability to manage devices on a company’s network from a single console.

**What Is the Importance of Enterprise Mobility Management?**

The business world faces a significant threat from cybercrime. Since people now work from different locations and use a range of devices and platforms to accomplish their tasks, steps must be taken to protect and secure business data to avoid organizational risks.

Organizations can use EMM tools to provide employees with secure and safe access to work apps and data. The COVID-19 pandemic taught us that companies need to take steps to protect their employees, devices and data even outside secure office networks. A good EMM solution can be a valuable tool for the following reasons:

* **Device Security:**The cybersecurity threats a company potentially faces increase manifold as they add more devices to their network. Every connected device creates a node that threat actors can exploit to breach the digital perimeter of the company. With an EMM tool, companies can ensure that employees install an endpoint security solution on their device before registering it for the BYOD program or using it for work.Using an EMM solution, companies can monitor all systems on their network for unusual behavior that could indicate whether the device has fallen into the wrong hands. A company can limit the access of specific endpoints to its network and data with features like identity and access management and add another layer of security.

Consider that according to the Verizon Mobile Security Index 2021 Report, more than half (54%) of the companies that had experienced a mobile-related security breach attribute the breach to user behavior such as falling for a phishing attack, downloading unapproved apps or making unintentional errors.

* **Data Security:**A stolen or lost mobile device can allow malicious agents to access a company’s network. As well as increasing the risk of data theft from the phone, it also increases the vulnerability of passwords saved on devices. With an EMM solution, your company’s IT team can remotely wipe corporate data stored on a lost or stolen device and use it to deploy location apps to find a misplaced device.

**What Are the Benefits of Enterprise Mobility Management?**

By adding an EMM solution to the IT stack, companies can offer work flexibility to their employees and simultaneously protect themselves from modern and sophisticated cyberattacks. This section explains how EMM tools help businesses remain safe and secure while supporting agile enterprise structures.

* **Better Control Over Mobile Data and Apps:**When devices and work-related apps are not protected, hackers can exploit them and gain access to a company’s network. Using an EMM solution, companies can remotely manage devices and apps so that employees have access to the data and apps they need. The tool also ensures that data sharing takes place securely and that employees do not download apps that could pose a security risk. Additionally, the solution can be used to host a personal enterprise app store from which employees can download apps that have been verified for security.
* **Supports BYOD Programs:**According to the Verizon Mobile Security Index 2021 Report, more than one in three (36%) organizations opened access to corporate resources and systems to employees using personal devices — that’s on top of those that already allowed it.By using an EMM solution, companies can monitor and evaluate all BYOD resources from a single console. It allows them to act swiftly as soon as they learn about a device getting compromised. EMM solutions can provide businesses with the visibility they need to monitor external and internal threat actors, as well as ensure that their employees proactively adhere to their device policies.
* **Improves Employee Productivity:**Having access to company data and information anywhere and anytime helps employees respond to work tasks in real time and facilitates easy collaboration with peers. It also allows employees to use their own devices for work, with which they enjoy familiarity and comfort, and hence helps them produce better quality work in less turnaround time.

**Who Uses Enterprise Mobility Management?**

Due to mobile devices, employees are no longer dependent on the office environment for work, which has improved productivity. Even though the needs of every company are different, EMM solutions will benefit companies that have a hybrid or remote work environment or employees who are always on the move. Let’s look at some industries where an EMM system would be a good fit.

* **Healthcare:**During the COVID-19 pandemic, many healthcare professionals provided consultation to patients over the phone. They shared prescription and test results over mobile devices. An EMM solution enables healthcare brands to secure patient communications while storing and sharing all patient information in a secure environment. Deloitte’s 2021 Connectivity and Mobile Trends Survey found that virtual medical visits enabled patients to receive quality care during the pandemic — drawing positive feedback from them.
* **Construction:**Most construction employees like architects, site managers and engineers are always in the field. With access to company tools and applications on mobile devices, they can share ideas, designs and tasks from the ground and check on inventory without visiting the office or the warehouses. This helps streamline the workflow and increase productivity.
* **Retail:**Equipping sales staff at retail outlets with mobile devices will help them personalize the user experience on hand and maintain better communication with inventory teams, warehouse teams and sales staff at other outlets.

Having an EMM Solution that supports BYOD policies can benefit many small and midsize businesses that wish to scale while keeping their costs low.

**Implementing Enterprise Mobility Management**

An EMM policy will not only improve security for your business but will lay the groundwork for a BYOD policy that can reduce IT costs, make your employees more productive and the work culture more flexible. A structured roadmap is key to ensuring your EMM plan carries more advantages than disadvantages. Here’s how you can go about it:

* **Permitted Devices:**To make EMM management simple and easy, you must first decide which devices you will allow employees to use. You need to consider the device models and operating systems that best suit your business needs. It will also help you determine how often employees must upgrade their devices. Also, you should decide if you will be subsidizing the device purchase and paying a certain amount for its upkeep and repair. Maintaining a consistent standard will help you simplify policy decisions.
* **Type of Enterprise Mobility Management Solution:**The next question to consider is the type of EMM solution you should purchase. Do you want a tool that offers a whole host of features or specific features like MDM, MAM and such?
* **Device Management and Registration:**When the type of devices is selected, rules will need to be established about registering and adding them to the company’s IT directory. It is a good time to figure out how much and what kind of access will be given to employees based on their job roles. This policy area will also look into how much access the company will have to the device if it is used for personal use as well.
* **Information Storage:**Do employees have the option of downloading and storing company data on their devices in a secure container? Would data access be granted only via a cloud application that is accessible only after multiple authentications? The trick is to strike a balance between productivity and security.
* **Compliance:**The government has different compliance and mandates that industries must follow. Know the compliance requirements of your company and ensure that mobile management fits within the guidelines. Compliance with security standards is essential, especially when employees have access to confidential client or customer information.
* **Risk Management:**How will the company secure devices and data if they are lost or stolen? A step-by-step procedure must be outlined and well documented so that IT technicians are not entangled in looking for solutions.
* **Policy Stakeholder Involvement:**A company should ensure that stakeholders from across sectors participate in the implementation of an EMM policy. This will prevent policy conflicts and ensure everyone’s goals are met.