Benefits of an Enterprise Mobility Management Solution

Technology is dynamic, more so, communication devices technology. Mobile phone devices have undergone a huge revolution since Nokia's dominance in the 2000s. Samsung, Apple, and Huawei phones now dominate the market, creating devices that can do just about anything, thanks to a rise in application use.

Consequently, businesses have found it difficult to keep up with annual changes in device technology because of budgetary constraints. For this reason, many organizations have 'Bring Your Own Device (BYOD)', policies that allow employees to use their electronic devices for work purposes.

While these policies may save a company from hefty and continuous device plus technology updates, and lower employee device learning curve, BYOD policies pose significant risks for business. Some of these risks include exposure to data security threats, increased complexity in disparate IT technology management and support, and loss of company and employee privacy.

For this reason, businesses are adopting enterprise mobility management policies to secure their data in the face of the rising use of employee technology and devices. Enterprise mobility management is a business term that combines a set of processes, technologies, and policies that enhance the management and security of mobile devices within a company.

It is an developing suite of services and systems that accommodates the dynamic nature of mobile device technology use within organizations. Today EMM encompasses the use and support of macOS and Windows 10 applications, devices and access management protocols.

Additionally, EMM supports the design and rollout of productive and engaging mobile experiences for employees. Eventually, enterprise mobility management will evolve to a unified endpoint management protocol status. Below are the definitions of various EMM protocols.

MCMK

Mobile Device Management (MDM)

Over 94% of all mobile and remote workers today depend on smartphones for connectivity and productivity. Mobile device management technology installs unique user profiles on these devices, helping them encrypt, control, and enforce workplace data access and device use policies.

MDM technology can supply an IT department with device use metrics such as OS configuration, inventory, and provisions. Through MDM, businesses can configure robust security policies on these devices, making them fit for enterprise use.

Mobile Application Management (MDM)

Data by the Synopsys Cybersecurity Research Center (CyRC) shows that 63% of mobile applications use vulnerable open source components. Additionally, these applications may expose sensitive data via excessive device permissions and application code.

A consecutive review of popular financial and banking applications shows that 88% of them have vulnerabilities that may lead to a security breach. Mobile application management policies can control and supervise mobile applications deployment. These tools will help organizations remove any vulnerable apps and protect sensitive data.

Mobile Identity Management (MIM)

Do you know that 70% of staff always have their phones near at hand while at work? Mobile identity management processes in EMM keep watch on an organization's data network, ensuring that only trusted users or devices access it.

Mobile Identity Management (MIM)

Do you know that 70% of staff always have their phones near at hand while at work? Mobile identity management processes in EMM keep watch on an organization's data network, ensuring that only trusted users or devices access it.

Mobile Content Management (MCM)

Mobile content management is an EMM variant that oversees content access, security, and push and protection of mobile device files.

Mobile Expense Management (MEM)

Mobile expense management is the enterprise mobility management accounting hand. It controls costs through analysis of procurement, BYOD stipends, communication expenses, and device user data.

EMM Best Practices

Mobile devices are a core part of the employees' work-life, seamlessly integrating with office diaries and personal contacts. A smartphone can add two more hours of work to your day, supporting work functions from the moment that you wake up, and in your commute. The mobile employee works 240 hours more per year than the average population.

Flexible working devices have become especially crucial during COVID-19 lockdowns and work-from-home setups. EMM solutions allow for the flexible use of mobile devices in the work environment, giving your business's IT department control of several aspects of mobile device usage.

Enterprise mobility management tools, processes, and technology will enhance enterprise-level security and lower devices management and support complexity.