A Definitive Guide to Enterprise Mobility Management

Enterprise mobility continues changing the IT landscape. Mobile device frameworks and technologies continuously keep evolving. BYOD (Bring Your Own Device) enables users to demand support for the rapidly expanding range of apps, OS platforms, and device platforms.

In addition to this, the extended network of connected devices and sensors should be capable of:

- Communicating with corporate networks
- Engaging with machines & models
- Serving as a new marketing and service channel to the customers

The given set of touchpoints ensure innovation, new streams of revenues, and new business opportunities. Additionally, these components also require effective management. Let us help you know all about Enterprise Mobility Management or EMM through this e-book.

A Definitive Guide to Enterprise Mobility Management

EMM refers to the specific set of policies, technology solutions, and practices that enable enterprises to manage as well as monitor mobile devices for corporate use. The given set of mobile devices can be BYOD (Bring Your Own Devices) or corporate¬ controlled devices. These devices are utilized for accessing sensitive business centric information.

EMM brings into effect robust management capabilities for controlling the manner mobile devices, users, and apps tend to interact with the respective corporate network.

The concept here is to bring about an effective balance between information security and productive mobile workforce operations.

Essential Components of the EMM Technology.

EMM serves to be a methodology or practice for ensuring that mobile device utilization is simple and secure. A dedicated EMM strategy usually includes a blend of three core technologies. These are:

MAM (Mobile Application Management): It offers improved security and granular management. With MAM, admins can look forward to specifying policies for a certain app or a group of apps. Some apps are available with built in MAM APIs. On the other hand, there are others that depend on device level MAM APIs.

MDM (Mobile Device Management): It is regarded as the foundation for any given mobility suite. It depends on the combination of the agent application. It gets installed on the server software and end-point devices running along the cloud or the corporate data center. Admins can make use of MDM's server management console for specifying different policies and configuring multiple settings.

The given set of policies are further put into implementation by agents. These settings can be configured through API integration into different operating systems of the mobile device.

MIM (Mobile Information Management): These are described as "Dropbox¬ like" services that are cloud¬ based and used for syncing files as well as documents across multiple devices.

When the given set of technologies are synced and used together with a proper strategy, it can help in solving every issue arising out of enterprise mobility in any organization.

EMM Tools & Solutions Features

A dedicated EMM (Enterprise Mobility Management) tool is useful in integrating the involved devices with the given corporate network, implementing a wide range of useful administrative controls, and upgrading important security configurations.

An EMM solution is typically known to include the given set of features:

- **Network Management:** Responsible for controlling data transfer limitations, network access, and other VPN (Virtual Private Network) connections for involved devices that remotely connect with the available corporate network. Devices can be configured remotely to the connected network settings.

- **Application Management:** For controlling which specific apps can be downloaded to the respective devices for accessing corporate networks and interacting with accessed information.

- **Content Management:** For controlling how organizational policies tend to apply to the device's stored data. Content management also helps in producing audit trails for activity surrounding confidential business information.

- **Analytics & Intelligence:** For gathering granular information on the app, device, content, and network specific activities and transforming the available information into intelligence and intuitive reports on the overall performance and productivity of the mobile workforce.

unified experience for the users having capabilities like IAM (Identity & Access Management) and single sign on management. devices like phones, mobile workstations, tablets, Iot, and laptops. As such, it enables a single, unified platform. The centralized EMM platform is used for managing multiple Unified Endpoint Management: For managing and securing all endpoints with the help of a.

Data Security and Access Management: For implementing additional security layers for securing information ¬like encryption, patching, and password protection. The given feature helps in controlling how devices as well as apps access sensitive data and corporate networks on the devices.

EMM Best Practices

As an enterprise, you can abide by the following guidelines to set up EMM policies effectively:

Enforcing the principle of least access privilege. This implies that every employee has access to only minimum resources required for performing their jobs.

Ensuring encryption of devices, data, and apps both in motion and at rest.

Preparing for 5G. The delivery of data intensive, immersive enterprise mobility experiences will help in boosting workforce productivity.

Establishing data security policies against MITM (Manin the Middle) attacks, device loss, malware, potential vulnerabilities.

and jailbroken devices

Accounting for the human element. Security related threats from unsuspecting employees and malicious insiders can be highly impactful upon accessing sensitive information conveniently on the BYOD devices.

Automating governance, service management, and administrative controls for a wide range of platforms, form factors, IoT technology standards, models, and Operating Systems.

Designing user centric management controls for making enterprise mobility a profitable experience for employees.

Productivity Maximization with EMM

The primary objective of EMM is not only to provide the users with a highly secure environment to work across mobile devices, but also to become highly productive. EMMS solutions are useful in providing built for business mobile-based productivity apps including a secure web browser, calendar, email, remote access, and document editing for enabling mobile employees to be highly productive as well as secure.

Conclusion

The overall market of EMM is growing at a rapid rate. As such, EMM solutions have become a necessity for mobilizing as well as optimizing the entire workflow.