WHAT IS EMM? ENTERPRISE MOBILITY MANAGEMENT EXPLAINED

Enterprise mobility has changed the IT landscape. Mobile device technologies are constantly evolving. Bring your own device (BYOD) power users demand support for an ever-expanding range of OS platforms, apps, and device models.

At the same time, this extended network of sensors and connected devices must:

- Communicate with corporate networks
- Engage with machines
- Serve as a new service and marketing channel to consumers

All of these touchpoints enable rapid innovation, new business opportunities, and new streams of revenues—but they also require management.

Let's take a look at enterprise mobility management (EMM), an ongoing, increasingly crucial practice for 21st century organizations.

What is enterprise mobility management?

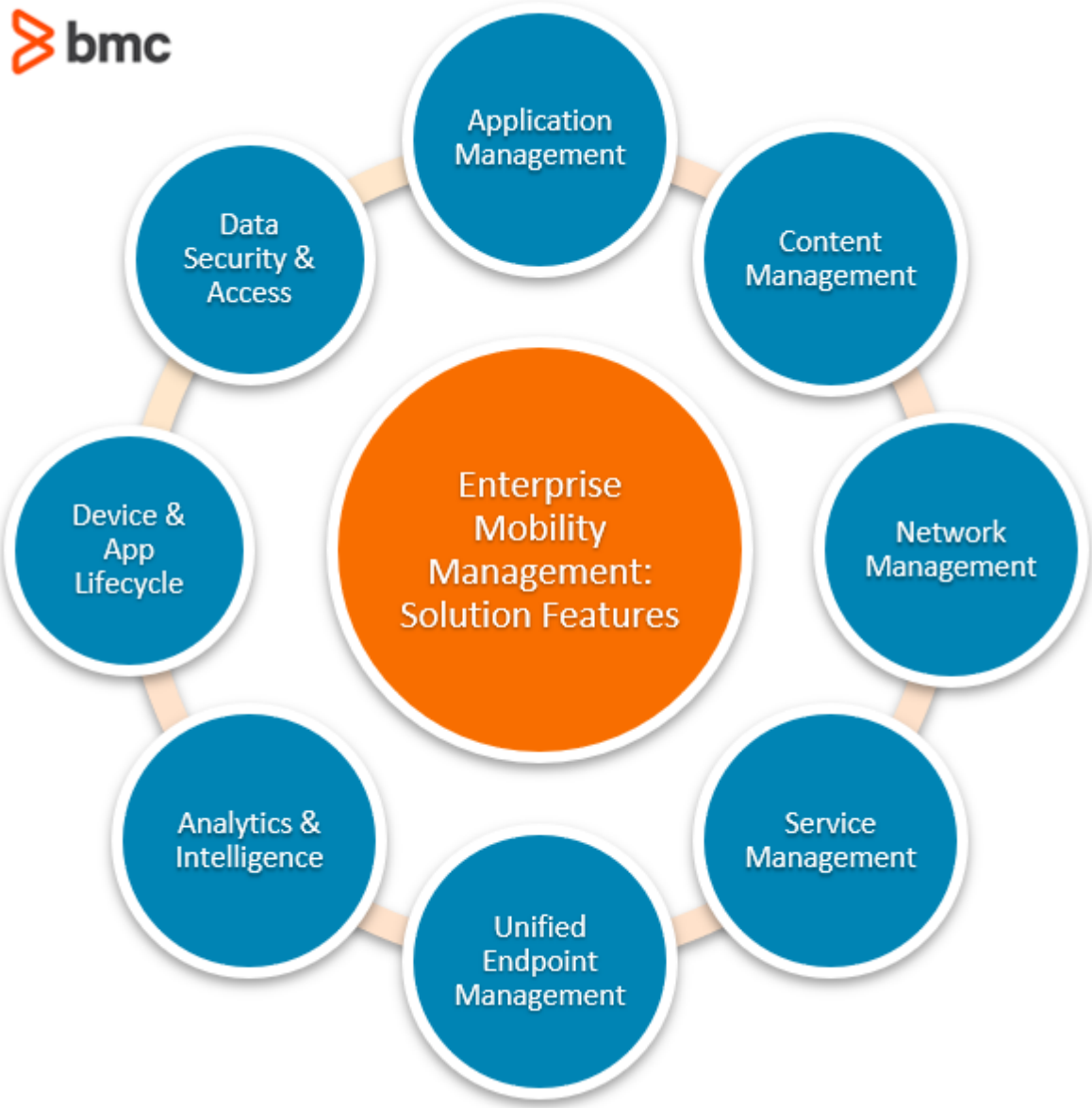
Enterprise Mobility Management (EMM) is a collective set of policies, practices, and technology solutions that allow organizations to manage and control mobile devices for corporate use. These devices may be corporate-owned or BYOD (Bring Your Own Device) devices used to access

sensitive business information.

EMM brings strong management capabilities to control the way mobile users, devices, and apps interact with the corporate network. The idea is to strike the right balance between productive mobile workforce operations and information security.

Features in EMM tools & solutions

An Enterprise Mobility Management tool integrates the enrolled devices with the corporate network, updating the necessary security configurations and applying a range of administrative controls.



An EMM solution typically includes the following set of features:

- **Application Management** controls which apps can be downloaded to the device, access corporate networks, and interact with accessed information.
- **Content Management** controls how organizational policies apply to the data stored in the device. Produces audit trails for activity around sensitive business information.
- **Network Management** controls network access, data transfer limitations, geofencing, and other Virtual Private Network (VPN) connections for enrolled devices connecting with the corporate network remotely. Devices can be remotely configured to the correct network

settings.
- **Service Management** administers self-service and push-updates of apps, configurations, settings, and IT service requests as controlled by IT admins. The technology integrated with the organization's ITSM tools can consistently apply the service management policies to mobile devices. It also helps control how devices consume the services, in the form of data usage and roaming cellular connectivity.
- **Unified Endpoint Management** manages and secures all endpoints from a unified platform. The centralized EMM platform can be used to manage devices including phones, tablets, laptops, mobile workstations, and IoT, enabling a unified experience for end-users with capabilities such as single sign-on management and Identity & Access Management (IAM).
- **Analytics and Intelligence** captures granular information on device, app, content and network activities, transforming that information into intuitive reports and intelligence on the productivity and performance of a mobile workforce.
- **Device and App Lifecycle Management** offers endpoint lifecycle management features, ranging from device onboarding and service provisioning to decommissioning and remote security measures such as data wipe.
- **Data Security and Access Management** applies additional layers of security to secure information, including encryption, password protection, and patching. This features helps control how devices and apps access corporate networks and sensitive data stored on the devices.

Enterprise mobility statistics

Research suggests that 67% of employees use BYOD devices at work and 87% rely on the organization for access management of corporate apps and data. As of 2020, there are already more than 10 billion personal devices in use and the BYOD market is expected to reach around $367 billion by the year 2022.

According to another research, the number of IoT devices are expected to reach 41 billion by the year 2027. 5G cellular subscriptions will be 1.9 billion by the year 2024. Business organizations will invest up to $1.1 trillion in IoT technologies with an expected economic impact of up to $11 trillion by the year 2025.

The proliferation of connected devices and rapid adoption for corporate use will make it necessary for organizations to manage and control the way these devices can be used to facilitate business operations.

EMM best practices

In this context, follow these enterprise mobility and data security guidelines in order to successfully set up effective EMM policies:

- Enforce the principle of least access privilege, which means that each employee can only access the bare minimum resources necessary to perform their job.
- Encrypt devices, apps, and the data—both at rest and in motion.
- Prepare for 5G: immersive data-intensive enterprise mobility experiences will boost workforce productivity.
- Establish data security policies against device loss, Man-in-the-Middle (MITM) attacks,

jailbroken devices, malware, and potential vulnerabilities.
- Account for the human element: Security threats from malicious insiders and unsuspecting employees can be more impactful when they can access sensitive information conveniently on their BYOD devices
- Automate governance, administrative, and service management controls for a diversified range of form factors, platforms, OS and models, and IoT technology standards.
- Design user-centric management controls to make enterprise mobility a productive experience for employees.

Related reading

- BMC The Business of IT Blog
- Mobile Device Management (MDM): An Introduction
- Cybersecurity: A Beginner's Guide
- What Is the Internet of Behavior? IoB Explained