MOBILE DEVICE MANAGEMENT (MDM): AN INTRODUCTION

Business organizations are rapidly adopting the trends of enterprise mobility and the bring your own device (BYOD) movement. These options offer workforce productivity as well as the ability for employees to work from anywhere, at any time, using any device.

Managing the growing pool of mobile devices connected to your corporate network is a pressing business and legal challenge. Failure to manage this appropriately is a major risk—just think of the sensitive business information that could be exposed. In order to cope with these concerns, companies can adopt mobile device management solutions in order to manage end users and their endpoint devices.

What is mobile device management?

Mobile device management (MDM) refers to software solutions and best practices that allow companies to manage and secure diverse mobile devices in compliance with corporate policies. MDM functionality includes the security of device and data, management of devices, software, configurations and services, and device functionality control. MDM enables a single-interface control over all connecting devices such that each device enrolled for corporate use via the MDM service can be monitored, controlled, and managed as per organizational policies.

MDM is often a component of an enterprise mobility management (EMM) solution which includes a collective set of tools to secure and manage mobile apps, company-provided and BYOD devices, content, data, and access. Components within an EMM solution may have overlapping features. For

instance, an MDM solution may also offer features to manage apps and data to complement that may be extensively offered only with mobile applications management solutions.

Key elements of an MDM solution include:

- **Asset management,** which includes multi-platform support for companies to apply custom organizational policies to enterprise mobility and BYO device use in the corporate network. Asset management might monitor and control how the devices can be used as well as enforce company policy across all enrolled devices, multiple platforms, and operating system versions.
- **Configurations management,** which can identify, control, and manage hardware and software settings based on geographic regions, user profiles, and identity.
- **Risk management, audits, and reporting,** which monitors device activity and reports anomalous behavior to limit issues such as unauthorize access of corporate network or data transfers.
- **Software updates and distribution,** which can remotely control applications, software and OS updates, and licenses across multiple devices.
- **Profile management,** which allows management of policies and settings to specific groups of end users based on specific profiles.
- **Identity and access management,** which ensures that the device, data, network connection, and services are provided to appropriate authorized users.
- **Applications management,** which distributes, manages settings, and black- and whitelists apps and software functionality.
- **Enterprise app stores,** which maintain a library of apps and services dedicated for corporate use that are available to authorized end-users.
- **Bandwidth optimization,** which manages bandwidth usage at the device and application level.
- **Data security,** which ensures that data is accessed, transferred, and utilized in accordance with organizational policies. For instance, in event of device theft or loss, data stored on the device can be wiped out remotely.
- **Content management,** which synchronizes and secures business information across multiple devices.
- **Tech support,** which includes dedicated remote technology support can be provided remotely.

Mobile device management: complexity and challenges

Growing interest in BYOD devices and mobility initiatives have fueled mass adoption of smartphones and tablets in the workplace. The promise of employee productivity, however, has not always matched the resulting business value. Potential gains in workforce productivity are often overshadowed by the challenge of managing a scalable pool of less-secure mobile devices, amid growing security threats and the dynamic technology landscape.

While enterprise mobility is a business reality that organizations must embrace, managing endpoint devices is not limited to defining and enforcing static policies. Furthermore, managing mobile devices and the expected enterprise mobility capabilities goes beyond purchasing and deploying MDM solutions.

Consider the case of mobile device fragmentation. As the device market grows, employees can choose devices from multiple brands, platforms, and software versions—which companies must then support and manage. Unforeseen security issues facing a specific platform and software

version must be approached proactively. Yet, risk management must not compromise end-user convenience and preferences in terms of which device they can use and how they can use it for office tasks.

Another complication is that MDM features vary across vendors. A standalone MDM solution from a specific vendor may satisfy the device management needs of the organization today, but the changing technology and business circumstances may necessitate additional investments into changing EMM capabilities. Therefore, device management is not just a technology problem, but a strategic challenge that every company must manage with their own best practices, based on their unique requirements and the future landscape of technology.

MDM solutions are designed to enhance visibility and control into an end user's mobile device activity. But, excessive tracking of mobile device activity could compromise end-user privacy. For example, an MDM may track real-time location, browsing activity, information that reveals personal information, and usage habits of employees beyond the device management and security needs of the employer.

Best practices for mobile device management

With the rapid proliferation of BYOD devices connecting to the corporate network, organizations must enforce device management controls without compromising the security posture of the business or the privacy and convenience of end users. To achieve a balance between both objectives, organizations can adopt the following best practices:

1. **Implement policies before deploying an MDM solution.** The right set of policies should be established to meet the unique technical and business needs of the organization before deploying an MDM solution.
2. **Make device enrollment to MDM solutions easy and convenient.** Ensure that no BYOD device goes under the radar, especially because of difficult or insufficient enrollment procedures or platform support.
3. **Establish self-service capabilities.** End user self-service is crucial in maintaining compliance with MDM solutions. Self-service capabilities can include remote data wipe-out, password reset, and lost device tracking.
4. **Ensure up-to-date MDM versions.** Push configuration changes, patch installations, and install software updates as soon as required and made available. A BYOD device running vulnerable outdated software is a security incident waiting to happen.
5. **Protect end-user privacy.** This will become key to ensuring end users continue compliance. Protect employee privacy by restricting data collection to a bare minimum and establishing procedures to eliminate misuse of personal employee information while still aligning with the company's technical and business needs.
6. **Deploy containment technologies.** These can separate corporate apps, data, and MDM controls from the personal use of a BYO device. With such containment in place, the MDM rules and features will only apply when the BYO device engages in corporate use.
7. **Monitor devices for specific activities or situations.** Monitor devices for anomalous activities or underoptimized data usage.

When choosing an MDM solution, make sure your choice allows you to adopt all these best practices. Adopting enterprise mobility movements and BYO device trends is no longer optional for progressive organizations. Getting MDM solutions to work, however, is critical to gain the maximum

value potential of mobile-drive workforce trends.