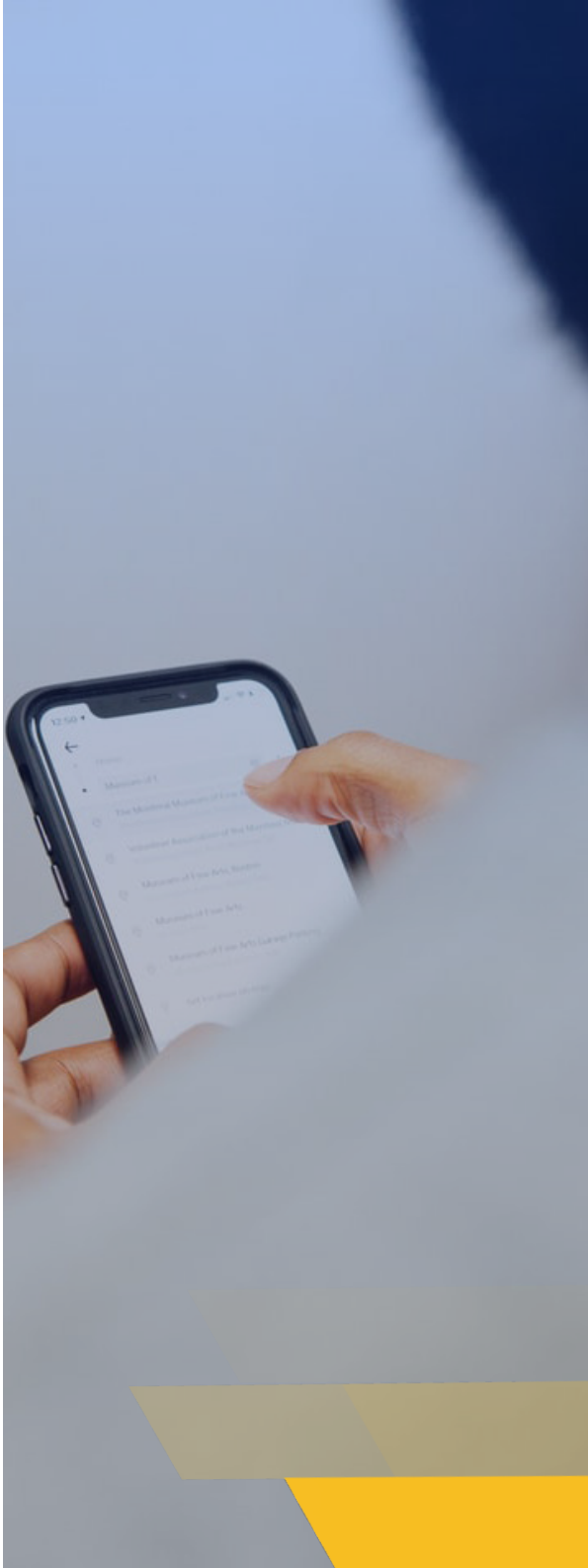
Mobile Device Management Buyer's Guide

Scalefusion

Table of Contents

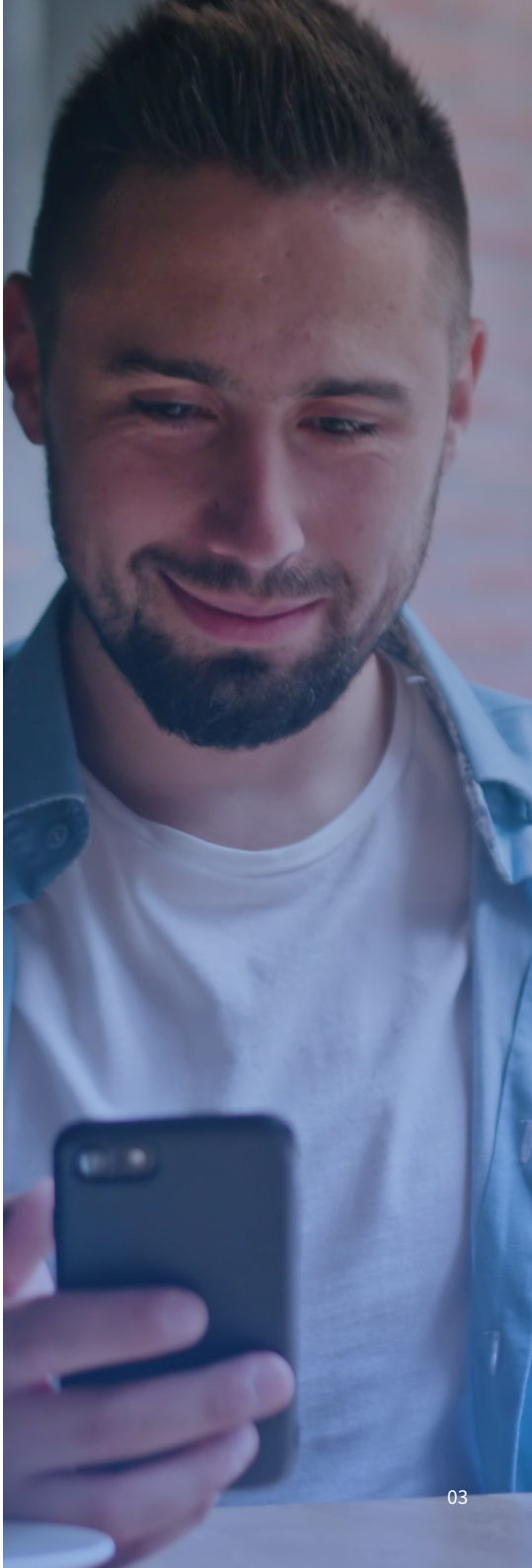


Introduction

The influx of mobile devices into the workplace has changed the entire enterprise ecosystem. Enterprises are competing to leverage new-age mobile technologies to drive multi-dimensional business purposes. Digital transformation driven by enterprise mobility depends heavily on how the employees are using the smart devices at work and the IT team's capability to ensure that the devices and data are judiciously used without being compromised.

Companies with a remote workforce need to provide their field forces with access to relevant and timely data and information to drive easy and effective decision making and accuracy. Hence, it is imperative to empower task and frontline workers with digital devices, applications and real-time information within a secure environment to drive business impact at all levels. Apart from that, in an increasingly divergent enterprise ecosystem, companies also need to support a BYOD (Bring Your Own Device) program to drive employee flexibility and business agility while securing corporate data.

Here's where the major IT pain points lie- enrolling multiple smart devices with different platforms, deploying the correct set of user and security policies and constantly facilitating an environment of data and device security where either of the two would not be misused by any unauthorized access.
A flawless and comprehensive Mobile Device Management can take care of all that more!



Factors to Consider Before Buying an MDM Solution

01 Multi-OS & Diverse Device Fleet Management

Enterprises today are working with heterogeneous devices running on diverse platforms including Android, iOS, macOS and Windows. On top of that, the introduction of BYOD culture at work has taken a forefront. Employees want to use their favorite devices for work and the responsibility to provision these devices of diverse make and model lies with the company IT teams. Furthermore, the IT device management concerns include not only the conventional devices such as mobiles, tablets, laptops and desktops but also comprise special-purpose devices, POS systems, digital TVs, ruggedized devices manufactured to operate in harsh weather conditions and bespoke devices created for a very-particular business need.

Together they create quite a few IT hurdles in streamlining inventory-wide device management. Obviously, having multiple device management setup for different OSs, make and models is not a convenient option at all. So, ensure to go for an MDM solution that extends support for multiple platforms and diverse device models.


Phone


Tablet


Single-Use Device


Interactive Kiosk


Point of Sale


Digital Signage

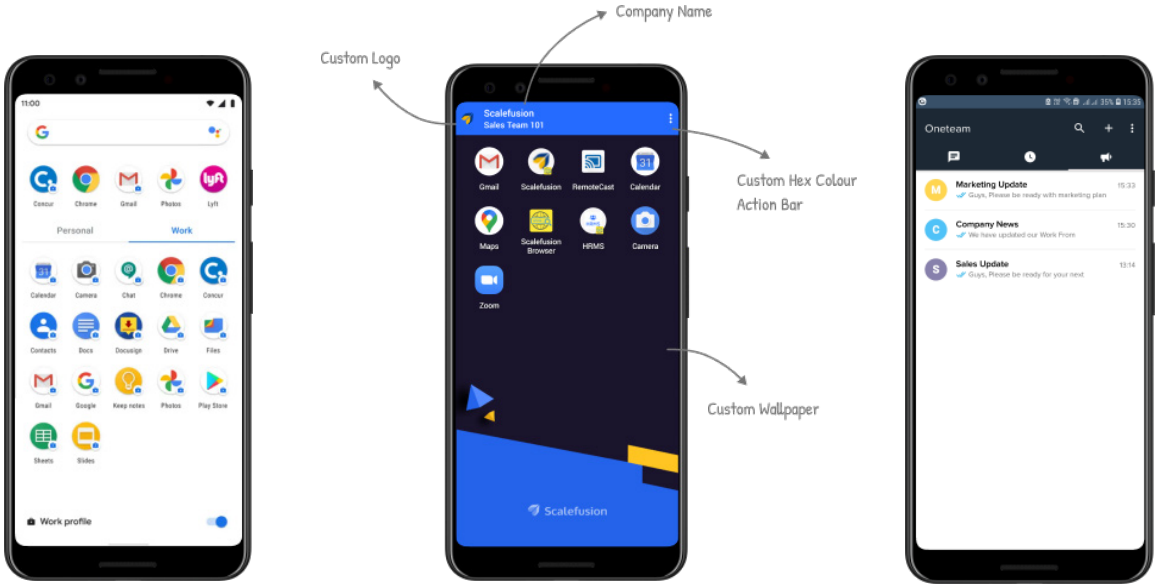

Rugged Device

Custom Device

02 Multiple Management options for business-specific needs

Every business need is different and force-fitting diverse business needs into one MDM solution is counterproductive for businesses. Which is why, opting for an MDM solution that suffices dynamic business needs is essential to ensure the mobility strategy is all-inclusive. Choose an MDM solution that offers multiple management modes to encompass a variety of device ownership models-

- Single-purpose devices owned by the company deployed as kiosks for a dedicated use
- COPE (company-owned personally enabled) used commonly in an enterprise setup
- BYOD (Bring your own devices) owned by employees used for both work and play



03 Faster Deployment and Out of the Box Management

An MDM solution should be designed in a way that would eliminate most of the IT hassles pertaining to challenges around enrollment, onboarding, security, management, tracking and troubleshooting devices. But a competitive MDM solution does more than just simplifying and streamlining the IT operations – it aims to heighten the overall end-user experience.

Individual provisioning of devices involves a tedious and time-consuming manual process wherein the IT teams will have to physically provision each device or train end-users on the setup. An ideal MDM should facilitate the process of bulk device enrollment through a set of automatic enrollment programs like Apple DEP (Device Enrollment Program), Google Zero-Touch enrollment, Samsung Knox Mobile Enrollment and Windows AutoPilot Deployment. Faster device deployment through no-touch enrollment of bulk devices doesn't only lessen the IT admin's burdens and chances of errors but also drives faster go-to-market strategy, simplifies device policy configurations and employee productivity.

04 Device Security, Policy Enforcement & Compliance Checks

Corporate device and data security remain one of the most crucial IT concerns. Additionally, the enterprise IT teams need to work in tandem with strict compliance regulations like PCI DSS, HIPAA, SOC 2, NIST and ISO. Here, the IT teams must ensure that both the employee-owned (BYOD) and corporate-owned devices are updated and adhere to these compliances while accessing business apps and content. Prefer an MDM solution that helps your IT teams to audit the device inventory, assess security threats and extend quick measures.

In an era where cyber attacks and security breaches are costing millions to companies, a dependable MDM solution can go a long way to eliminate IT compliance issues and data security risks. Your chosen MDM solution should facilitate extensive security policy implementation. Considering the ownership diversity in modern enterprises, ensuring data security without compromising on user data privacy is one of the key capabilities of an ideal MDM.

It is advisable to go for an MDM solution that comes with comprehensive security features such as breach detection, automated alerts on unauthorized access. This helps the enterprise IT teams to eliminate data security threats from a remote dashboard

Some of the vital policy configuration capabilities that an MDM should offer include:

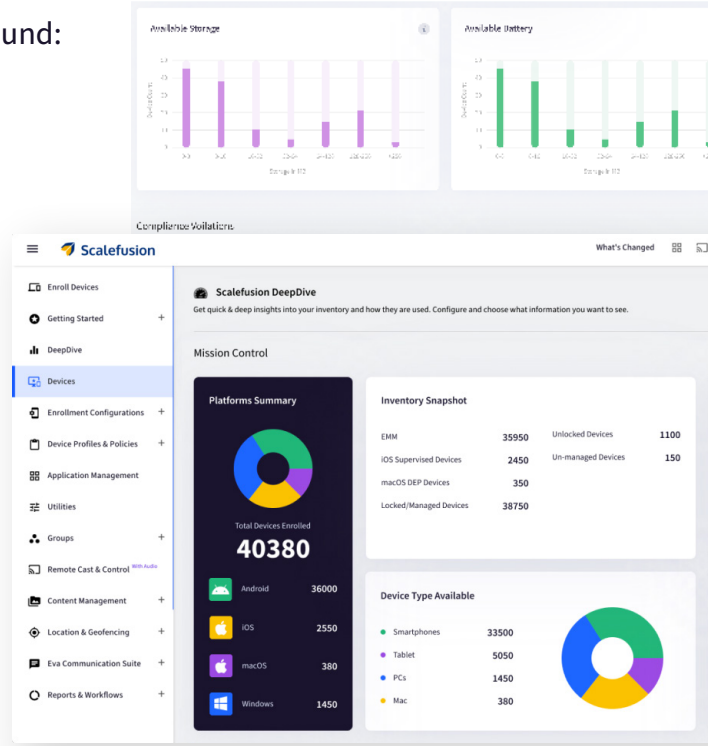
- Application and website whitelisting
- Automated OS and app updates
- Data encryption
- Password policies
- Multi-factor authentication
- Remote wipe and lock
- Real-time notifications for compliance violations
- Location tracking and geo-fencing

05 Unified Endpoint Visibility & Analytics

IT teams often confront day-to-day challenges related to several issues ranging from IT governance, device allocation and management, monitoring of compliance violations, device and network downtime, server management, regulation and security breaches, IT cost reduction, and IT-business synchronization. Selecting a user-friendly MDM can curtail IT efforts. Furthermore, an MDM dashboard offering 360-degree visibility of the entire endpoint inventory can reduce the IT efforts to great lengths.

In a nutshell, the MDM dashboard should offer data points around:

- Number of enrolled, managed, unmanaged devices
- Device platform
- Device health status- data, storage and battery usage
- Device location
- Compliance violations and security alerts

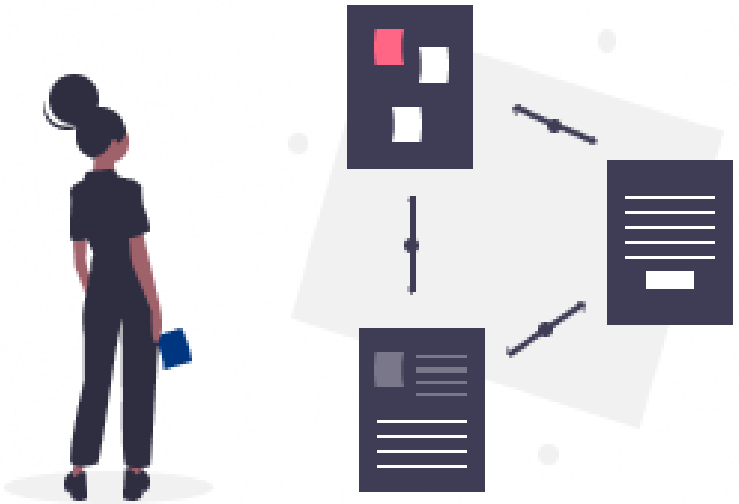


Using these data points, the IT teams should be able to drive device management processes and quick actions right from the dashboard. Automated reports and alerts on security and compliance violations on the managed devices can further ensure that IT teams stay on the top of the device inventory at all times.

06 Automation, Reports & Audit logs

Your IT teams are burdened with the laborious responsibilities to manage large device inventories, provision network and security requirements across the organization amongst others. And while an MDM solution helps in off-loading a bunch of responsibilities in provisioning devices and making them business-ready, keeping an eye on the device activity and impending security concerns. Choosing an MDM solution with automation capabilities is the key to drive IT productivity. Make sure to look for a mobile device management solution that enables your IT teams to schedule and auto-run recurring tasks and obtain detailed reports of device performance and usage over their emails. These automation capabilities could include scheduling tasks like change in policy configuration, remote rebooting of unattended devices, locking/unlocking and compliance checks for geofence breach, security incidents, battery, data and storage usage.

Additionally, in large enterprises with multiple stakeholders managing the MDM dashboard, having a report of MDM operations, activities performed on the MDM platform and tracking detailed audit logs can be immensely helpful in unburdening the enterprise IT teams



07 Remote Support, Communication and Collaboration

In a modern enterprise environment, the devices are deployed at multiple locations and are often unattended, when deployed as kiosk browsers or self-service kiosks and POS systems for instance. These devices need to be monitored closely for security and performance. And while your MDM's visibility and automation capabilities can help track the device performance, there needs to be a provision to resolve the issues upfront to maintain a consistent device uptime. If the IT teams have to physically resolve the device issues, by visiting the device location or fetching the device to a service center, it adds up to the costs. And hence, remote troubleshooting capability is a critical feature to reduce device downtime. This ensures that the unattended devices are always up and running and the employee hand-held devices are always running smoothly ensuring there is no compromise with productivity.

Another hindrance impacting the productivity of field or frontline forces is the lack of engagement and/or information overlapping since they spend most of the time outside the conventional perimeters of an office. And while the collaboration can be solved using a team communication app, it is best to opt for an MDM solution that comes bundled with a communication suite that the IT can have total control over.

08 Integrations

Scalability is one of the most important elements of an MDM solution because it offers the much-needed room for improvement, revising the scope and requirements expected from the mobility exercise. Look for an MDM so offers scalability with the help of integrations a API solutions to build custom solutions for you specific problems.

09 Pre-sales, post-sales, onboarding & customer support

For a successful implementation of an MDM solution, make sure to choose an MDM solution with a time-tested and proven customer support system. A solution with a support team that guides the customers through the entire process of buying, implementing, exploring features, troubleshooting issues and generating results to drive ultimate business value is highly recommended. A reliable and customer-driven MDM will always give importance to customer demands, custom-requirements and solution feedback. Moreso, a considerable aspect of their product development roadmap will be influenced by the market needs driven by the real-world pain points of their existing and prospective customers. Checking the particular MDM solution's customer reviews on authorized online platforms like Capterra, G2 Crowd and Gartner always give a better selection perspective.

Furthermore, it is important to opt for an MDM solution that offers bespoke solutions to enterprises, in guiding them in the end-to-end journey of purchasing and implementing a mobility strategy. Look for an MDM provider that also offers add-on services for staging deployment, on-site onboarding and help in the migration from your existing solution.

Final Thoughts

Keeping these directional guidelines in mind, it is important to select and work with an MDM solution that clearly understands your company's business goals, IT challenges, budgetary restraints, end-user objectives, achievable results and final business benefits. Transitioning to a new MDM solution or starting out with device management, having these pointers in mind can help you make an informed decision that not only mitigates your IT team's effort but also helps in deriving value from your enterprise mobility.

Try it now for free

Register for a free 14-day evaluation at **www.scalefusion.com**

Get a Demo

Request a demonstration and see how Scalefusion can help you in managing your devices and securing your corporate data.

Book a Demo

About Scalefusion

Scalefusion MDM allows organizations to secure & manage endpoints including smartphones, tablets, laptops, rugged devices, mPOS, and digital signages, along with apps and content. It supports the management of Android, iOS, macOS and Windows 10 devices and ensures streamlined device management operations with InterOps.

Enterprise Sales & Partnerships

sales@scalefusion.com

partners@scalefusion.com

Call Us

(US) +1-650-273-5999

(INDIA) +91-8499-835020