ZONES

Mobile Device Management (MDM)

WHITE PAPER

Identifying Major Use Cases and Choosing an Ideal Partner

Today, more than 5 billion[i] people around the world own mobile devices. By 2022, nearly 43% of the global workforce will have gone mobile.[ii] In addition to an increase in adoption of workplace devices (smartphones, laptops, tablets, desktops, and other mobile devices), a number of factors are forcing businesses to adopt a mobile-first strategy. These factors include the emergence of cloud technology (which eliminates the need to invest in and own on-premises infrastructure), mounting pressure to cut costs while still delivering seamless access, and a growing millennial workforce that demands a "consumerized" workplace experience. While transitioning to mobile-centric platforms and devices has been shown to enhance employee productivity, it also introduces security and compliance challenges and tradeoffs. Regulations around safe data usage and protection are constantly growing stricter in response to the growing frequency and sophistication of cyberattacks.

These days, businesses need a platform that can help them manage their ever-expanding fleet of mobile devices, ensure robust data protection, track mobile device usage, and offer the capability to remote wipe data from lost/stolen/physically damaged devices. Mobile Device Management (MDM) has emerged as a critical imperative in the modern business landscape and a core component of a fully qualified Unified Endpoint Management (UEM) strategy. The MDM market is growing at an impressive CAGR of over 21% between 2019 and 2023, with a total value that's expected to reach $7.86 billion by 2023.[iii]

In this paper, we'll explore three primary MDM use cases and highlight the best practices enterprises can use to identify the MDM platform that best fits their needs.

While mobile devices are smaller and lighter than desktop computers, they can hold and access the same amount of data as any traditional PC, which means it's crucial to ensure enterprise-grade protection for these devices.

Unleashing the true potential of MDM: Three major use cases

An MDM solution is a core component of UEM, an evolving set of technologies that focus on the business and technological context of workplace device usage in everyday business operations. MDM solutions comprise toolsets and platforms that enable organizations of all sizes (SMB, mid-market, and enterprise) to integrate, manage, and secure workplace devices with a specific focus on mobile. Many have come to conceptualize it as a sort of modernized Active Directory for mobile devices, only with more management features added in. By leveraging MDM solutions, administrators can set rules or control security and application settings on all mobile devices on their network. They have complete visibility into which employees access what company data on their devices (whether company or personally owned), how often, and other critical insights. Administrators can also restrict employees from downloading potentially malicious apps, remotely wipe sensitive data from suspicious devices, push security updates and patches in a centralized manner, and so much more. The greater the level of control an organization has over people's devices, the better it will be at safeguarding its resources, protecting internal and customer data, and maintaining compliance with regulatory standards and guidelines. Here are three major use cases to consider while implementing MDM:

Use case 1: Securing data across devices

One of the most critical reasons to deploy MDM is to secure the data stored on and accessed by mobile devices. While mobile devices are smaller and lighter than desktop computers, they can hold and access the same amount of data as any traditional PC, which means it's crucial to ensure enterprise-grade protection for these devices.

Typically, MDM vendors adopt either a containerized or non-containerized approach to secure the data on mobile devices. A containerized approach adds an extra layer of protection by requiring users to separately log into an MDM solution. The downside is that a containerized approach doesn't necessarily allow users to leverage the apps they are accustomed to using, as not every app is natively compatible. A non-containerized approach, on the other hand, supports a native experience, allowing users to access traditional apps and data from third-party software. While the non-containerized approach is popular due to the flexibility it allows end users, it requires a detailed review by administrators prior to implementation.

Use case 2: Standardizing device protection across the organization

Securing devices is essential to minimizing the threat of network breaches that can result in compromised data. MDM systems alert admins of breach attempts that can increase the risk of exposure of the corporate network. Other ways to protect your mobile devices include enabling password and PIN enforcement with a timeout period, leveraging remote wiping of lost/stolen devices, restricting app usage to whitelisted apps, limiting OS changes by users, and encrypting workplace devices. IT departments can manage all of the above using a centralized MDM solution.

Use case 3: Safeguarding remote connections

Once your devices and your data are protected, an MDM solution can help ensure safe communications by securing the connections between mobile devices and other organizational resources. This can be done by enabling VPN connections, limiting services set identifiers that a wireless device can use, adding an extra layer of authentication, or even by enabling geofencing to ensure that devices work only in certain geographical locations.

MDM has become pivotal to modern organizations in the digital era. But implementing MDM solutions can be challenging, in part because of the wide variety of devices that live in modern organizational environments. While best-in-class MDM offerings such as Microsoft Intune, JAMF (for Apple only), and Workspace ONE (from VMware) are available on the market today, organizations need an attentive and skilled partner to first understand their unique MDM challenges and then implement and manage a customized solution.

Modern businesses put significant time and money into developing sophisticated workplace strategies, and typically, a one-size-fits-all MDM solution won't suffice.

Choosing an ideal MDM partner: Five key considerations

Here are five questions to ask when seeking an ideal MDM partner for your organization.

#1 Can you customize your MDM solution to our organizational needs?

Modern businesses put significant time and money into developing sophisticated workplace strategies, and typically, a one-size-fits-all MDM solution won't suffice. Crafting a customized solution will ensure that your organization makes the most of your investment by allowing your IT and data management teams to effectively control and monitor devices across the organization, scale up or down, and implement security policies, all from a centrally managed console.

Check whether the partner is OEM agnostic and can recommend ideal solutions and best practices that can accelerate adoption and ensure the long-term success of your MDM solution. Also, ask if they offer complimentary services such as Data as a Service (DaaS), OS upgrade and deployment services, or Cloud Solution Provider services for a fully hands-off end user compute and productivity experience.

#2 Do you support BYOD options and environments with diverse device standards?

The BYOD market is on course to reach a total value of $367 billion by 2022.[iv] BYOD is not just an employee preference – organizations stand to gain significantly by enabling BYOD as well. According to Cisco research, companies favoring BYOD realize an annual savings of $350 per employee, per year.[v] As more and more companies embrace BYOD and plan for its adoption, MDM solution providers are starting to include self-enrollment options for quicker onboarding, ensuring smoother adoption.

Ask whether your MDM vendor offers streamlined self-service options and the ability to segregate, control and protect corporate data as opposed to personal information. Also, ask about the specific mobile operating system (MOS) standards supported by the partner to address the challenge of growing device fragmentation.

#3 How do you ensure strong cloud security?

While cloud-based MDM environments enable greater flexibility for businesses, they often present a tradeoff in terms of control, as data is hosted outside the organization's network. On the other hand, on-premises MDM environments require more resources for patching, implementing hardware and software, managing environment uptime, and ensuring around-the-clock monitoring.

Many organizations prefer to go the cloud route, as it offers several advantages over on-prem such as faster deployment, simpler requirements, easier upgrades, and reduced costs by eliminating the need for owned infrastructure. If you are planning on adopting a cloud-based solution, make sure you understand the cloud security protocols of the MDM OEM beforehand.

#4 Does your MDM support seamless integration with commonly used apps?

Modern professionals want to run a variety of apps on their devices. This means organizations must have the ability to seamlessly push policies to manage many different types of devices and apps. Any potential partner's MDM solution should be able to distinguish between and create an inventory of whitelisted and blacklisted apps, giving IT administrators the ability to restrict app installations as required.

Validate if the partner facilitates a cohesive, cost-effective and productive integration with already existing operations and enterprise tools. Can they strategically align to your organization's security and business objectives?

#5 Is your MDM solution future-proofed?

An MDM solution must not only support current devices, but also be scalable enough to handle the growing number of device types in today's corporate environment. Key device management practices to ask about include server and device registration, multi-screen and multi-device access for all users (including remote), removing and blocking devices, and so on.

Ask if the partner takes the time to understand your workforce – how they work, what devices they use currently, and how their device needs are likely to evolve in the future – to create a dynamic solution that grows with your organizational needs. Find out if they are adept at developing personal profiles for the users on your network to make user and device management simpler and more standardized.

Future-proofing your MDM solution

As the connected workplace environment increasingly becomes the norm across all different types of organizations – including public sector, healthcare, education, and more – managing and securing a growing number of devices is critical to both improving employee productivity and tightening up organizational security. Forward-looking organizations that leverage a state-of-the-art MDM platform will be able to secure their devices and their networks while safeguarding employee flexibility and productivity, ensuring sustained success for the organization by balancing employee freedom with simple and effective oversight, all controlled centrally with MDM.

About the Author

Alex Pérez is the Director of Workplace Solutions at Zones and owns the development and success of the portfolio of solutions which fall under End User Compute & Productivity, Collaboration and Store & Branch Modernization.

More Information

Visit our website Zones.com
To speak with a solution specialist in the U.S. call toll-free **1-800-408-9663**.

About Zones, LLC

For over 30 years, Zones has worked with industry-leading partners to offer comprehensive IT solutions to clients around the world. Our Workplace Modernization, Network Optimization, Data Center Transformation, and Security Fortification solutions lead clients through their digital transformations, and our services offer support every step of the way. That's what makes us the First Choice for IT.™

References

i PEW Research Center, Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally, Feb 2019, https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/

ii Human Resources, 42.5% of Global Workforce Set to be Mobile by 2022, Oct 2016, https://www.humanresourcesonline.net/42-5-of-global-workforce-set-to-be-mobile-by-2022/

iii Market Watch, Mobile Device Management Market 2019, June 2019, https://www.marketwatch.com/press-release/mobile-device-management-market-2019-global-industry-trends-statistics-size-share-regional-analysis-by-key-players-industry-forecast-by-product-applications-and-end--user-2019-06-19

iv Forbes, Future of BYOD, Jan 2019, https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/#6511a05f1f30

v Insight, BYOD Statistics Provide Snapshot of the Future, Nov 2017, https://www.insight.com/en_US/content-and-resources/2017/01182017-byod-statistics-provide-snapshot-of-future.html

Corporate Headquarters
Zones, LLC
1102 15th Street SW, Suite 102
Auburn, WA 98001-6524