Mobile Device Management

Everything you need to know

Electric

Overview

How It Works

MDM software has two core components: a server-based management console and a lightweight MDM agent that is installed on each endpoint (endpoints are most commonly identified as laptops, tablets and devices connected to an organization's network). The central management console enables IT administrators to configure policies and push those policies to the MDM agent on the endpoint; applications can be managed and deployed in a similar manner. Meanwhile, MDM gives you constant visibility into your organization's fleet of devices.

MDM Features Overview

Productivity

- Device provisioning
- Application distribution and management
- Application configuration
- Device and app management from a central console

Inventory

- Automatic, real-time visibility into a device inventory
- Device health (including OS version, battery health and warranty information)
- Device reporting
- Asset management (only from premier MDM solutions)

Security and Compliance

- Enforce device data encryption
- Manage device settings and configurations
- Remotely wipe a device when it is lost or stolen
- Organization-wide policy enforcement

Device provisioning and onboarding

Employee onboarding is not only important for security and standardization but also for employee retention. By empowering employees with choice and supporting them with simple configurations and the software they need to meet your business's security needs, they can and will be productive from day one.

A study conducted by JAMF found that:

68% of enterprise workers say that technology choice makes them more productive

77% of enterprise workers say they're more likely to choose to work and stay at a company that offers device choice

Application distribution and management

Improve user productivity by specifying who gets which applications.

MDM software helps you confront the core challenge of managing your organization's inventory of applications and devices.

Inventory: Device and App Management with MDM

Inventory

- Central console management of all devices and apps
- Automatic, real-time inventory visibility
- Unparalleled device reporting

Hardware

- Device type/model
- Serial number/UDID
- Processor, RAM, storage
- Battery health
- Warranty expiration date

Software

- OS version
- App installation
- App versions
- Certificates and profiles

Security

- Encryption status
- System configurations
- Software restrictions
- Audit reporting

MDM helps you manage your IT investment by providing comprehensive visibility into devices and user details. This visibility is often displayed in a dashboard that can show device type and health, OS version, encryption status, and system configurations, among other details.

MDM software also helps you manage all the applications on devices within your organization. You can use MDM to install, update and remove/restrict any application on a device remotely. Moreover, you can proactively install a specific set of apps on a device so that your employees have all the mobile tools they need, starting on day one.

While MDM centralizes the management of your devices, someone still has to oversee all of the applications and devices in your mobile fleet. They also have to think about device security, adding another layer of complexity.

Security and Compliance: MDM and Security

Section Overview:

- Enforce device data encryption
- Manage device settings and configurations
- Remotely wipe a lost or stolen device
- Enforce policies

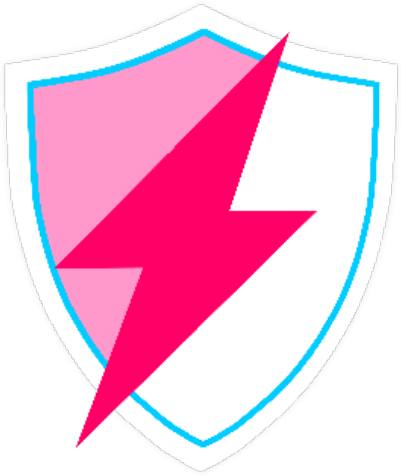
IT security is increasingly difficult to navigate. New threats are emerging rapidly and ransomware costs businesses billions annually. Securing and standardizing endpoints with MDM is your first, and often most robust, protection.

Whether it is employee negligence, malware or data loss, installing MDM on your organization's devices can substantially reduce risk. **Here's how:**

- Enforcing strict login rules (e.g., two-factor authentication)
- Encrypting all data on devices, making devices inaccessible without an encryption key
- Remotely securing or wiping all the data on a device
- Automatically pushing patch and OS updates
- Standardizing policies company wide
- Restricting applications by user

When it comes to making the decision to install MDM on your organization's devices, other things to consider include the legal and reputational ramifications. The portability of mobile devices makes them attractive targets for criminals. If one of your devices is stolen and valuable data is compromised, you could be sued for negligence.

While at its core, MDM delivers security through simplicity, it requires expertise to manage effectively. To leverage MDM to its full potential, SMBs and small in-house IT teams should consider working with a provider who has specialized experience.



Compliance: Premier MDM solutions will help your business comply with multiple frameworks, such as GDPR, HIPAA and SOC 2.

Assess: By creating a detailed view of your devices, software and security settings, MDM solutions can be used to assess your current environment and help inform which actions need to be taken.

Manage: If vulnerabilities are identified, patches can be deployed automatically to ensure security and compliance are up to date.

Report: Premier MDM solutions allow per-device reporting on settings or policies and track what changes are made. This reporting is used to demonstrate compliance, minimize compliance risks and make audits effortless.

Common MDM limitations

While MDM solves an immense challenge, it can be bottlenecked by poor implementation and lack of expertise.

Customization: Because every company is different, every implementation of MDM must be tailored to a business's specific set of challenges.

Implementation: MDM typically costs upwards of $5,000 for implementation + $3-9/device/month — Electric absorbs these costs.

Complexity/ongoing management: Things get complicated quickly when you're dealing with multiple employees, devices, operating systems, applications and tools. There's a reason MDM is chiefly a component of enterprise mobile management. It takes an IT staff with specialized knowledge and an extensive track record to get it right. That's more than many smaller businesses can handle on an ongoing basis.

SMBs and MDM Partnerships

Mobile technologies aren't going away. In fact, the technologies are only getting more varied and specialized.

Small businesses that cannot afford a dedicated IT professional/team often pile technology tasks on de facto IT people. Usually, it's the person most adept with technology and least intimidated by everyday tech challenges.

Your de facto IT person might be able to manage a few mobile devices, but every additional employee makes that expectation more unrealistic. After all, your de facto IT person has other work to do. Who's left to do their work when they lack MDM expertise from the start?

The challenges of inventory control and application management are daunting enough. When you add in the security risks and reputation risks, the value of mobile device management becomes readily apparent.

At Electric, we give smaller companies the opportunity to tackle their mobile challenges head-on and confront the potential risks. We partner with the best technology providers to help you keep your mind on your business, removing any worries about mobile devices or inventory.

That's the kind of mobility every small business needs.