RSA

RSA Mobile Lock and Mobile Device Management (MDM) Solution Brief

OWN YOUR IDENTITY.

RSA Mobile Lock and MDM Solution Brief

Organizations looking for help securing and managing their mobile devices will likely consider a Mobile Device Management (MDM) solution. It's important to understand the basic uses and capabilities of MDM and how it compares to RSA Mobile Lock. MDM is typically used to manage corporate-owned devices but also works with personal devices that are used to access work resources. RSA Mobile Lock can be used on managed and unmanaged devices, including corporate-owned devices and bring-your-own-device (BYOD) devices.

MDM uses and capabilities:	RSA Mobile Lock uses and capabilities:
Centrally deploy apps over the air and reassign licenses as business needs change.	40+ threats such as device tampering, malware detection, Out of Compliance OS
Configure settings like Wi-Fi and email on devices.	Protects the RSA Authenticator application and has no impact on any other app or device behavior.
Always on and always monitoring mobile devices. This can impact the entire device behavior and is frequently seen as intrusive for BYOD users.	Locks the RSA Authenticator application when critical threats are detected on a device.
Helps to enforce policies such as passcodes and can remotely lock/wipe devices.	Provides detailed information about detected threats to assist with device troubleshooting.

Which solution is right for you? Trick Question! Both!

Organizations can choose to use both MDM and Mobile Lock together. This gives them the capability to manage and control devices with MDM while simultaneously using Mobile Lock to identify critical threats and prevent compromised devices from authenticating into secure environments. If an organization is cost-concerned and has nothing in place for mobile security, Mobile Lock is recommended as it's already built into the RSA Authenticator application and doesn't require a separate installation or a contract with another security vendor. Below are a few scenarios where Mobile Lock can be a valuable addition to an organization regardless of whether they have MDM or not:

- **Organizations that allow BYOD:** Mobile Lock doesn't require a separate installation or application as it's built directly within the RSA Authenticator. This makes it a great option for organizations to protect BYOD devices from critical threats, even if they are not able to manage those devices using an MDM.
- **Zero Trust and security conscious organizations:** Mobile Lock can help organizations enforce zero trust security policies by preventing compromised devices from authenticating and accessing critical resources and/or applications.
- **Limited threat detection with MDM:** Mobile Lock protects against 40+ security threats like man-in-the-middle attacks, out of date operating systems and more. MDM only provides basic security management of mobile devices and can enforce some security policies but when it comes to detecting threats, it generally isn't as robust as Mobile Lock.
- **Protection against unauthorized applications:** MDM solutions cannot prevent users from installing unauthorized apps on their devices. This means users could install malware or other malicious apps without the organization's knowledge. RSA Mobile Lock adds an extra layer of security to help detect these critical threats and prevent the compromised device from authenticating into corporate systems and applications.