mobileiron

MobileIron Threat Defense (MTD) Risk Assessment & Deployment Best Practices

Updated: September 2019

MobileIron Strategy & Advisory Services
490 E. Middlefield Road
Mountain View, CA 94043
www.mobileiron.com

MKT EN-US v2

mobileiron

Version History

Version	Version Date	Summary of Changes
1.0	12/19/2018	Document Creation
1.1	09/06/2019	New MobileIron branding and general updates.

Table of Contents

Overview

This document provides MobileIron administrators a best practices approach to configure and deploy the MobileIron Threat Defense (MTD) product based on device use case and risk tolerance.

Audience

This document is for experienced MobileIron administrators and information security officers who understand the nature of mobile threats and are interested in further enhancing their organization's security posture with MTD.

Definitions

The General Data Protection Regulation (GDPR) is a regulation in European Union (EU) law about data protection and privacy for all individuals within the EU and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

Introduction

With one app, enterprises can protect company data by detecting and remediating known and zero-day threats on the mobile device without internet connectivity required, and no need for users to take any action. MobileIron Threat Defense provides the secure foundation for modern work to companies of all sizes around the world.

To take full advantage of MTD, the MobileIron administrator must understand the overall organizational impact when deploying the solution. Different organizations with different security postures, device ownerships, and user experience can significantly influence how the solution is deployed.

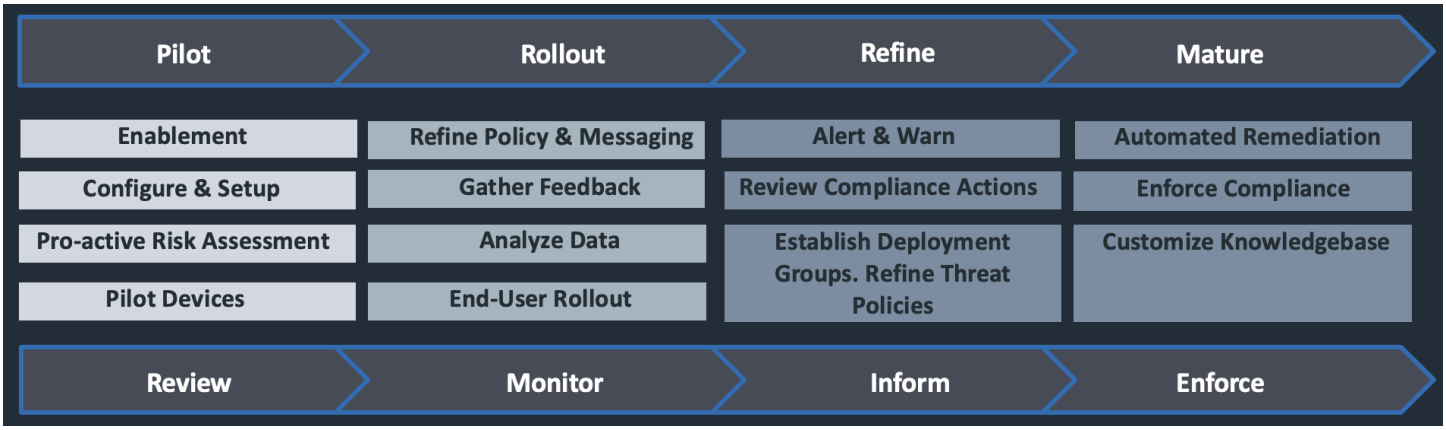
Lastly, privacy policies can affect how effective the organization can combat mobile security threats, especially in countries with more stringent privacy laws such as the EU.

MobileIron provides the recommendations in this document as a baseline. Each customer must determine their risk tolerance level, user experience, and corresponding policies that best meet the business requirements and the security postures of their organization.

MTD Risk Assessment & Deployment Best Practices

There are many methodologies when deploying MTD. Some organizations simply turn on all the MTD features and deploy them to their users while others will take a more conservative approach by first observing what the mobile threat landscape looks like but somehow never fully deploy MTD. The best methodology, however, is to deploy MTD with a phased approach consisting of the following:

- Pilot & Review
- Rollout & Monitor
- Refine & Inform
- Mature & Enforce



I. Pilot & Review

The Pilot & Review phase consists of four steps:

- Enablement
- Configure & Setup
- Pro-active Risk Assessment
- Pilot Devices

Depending on the organization's risk tolerance level, device ownerships, and familiarity with mobile devices, the amount of time required to complete each step may vary.

Enablement

In the simplest sense, Enablement means turning on MTD to observe the mobile threat landscape of your organization. Through Enablement, the organization will have a better understanding about where mobile threats originate, how they threaten the organization, and start to formulate a strategy to mitigate those threats using the data collected.

For example, a law firm may give all their lawyers the same access to their internal network on their bring-your-own (BYO) device. After turning on MTD, they may realize that their senior partners are constantly being targeted with Man-In-The-Middle (MITM) attacks so rogue agents can gain access to those high-profile cases on which they are working. With this type of data being collected from the devices, the security team is now armed with the proper tools to help mitigate any associated risk from this attack vector.

Configure & Setup

Once the organization has a better understanding of their mobile threat landscape and has collected enough data from MTD, they can start formulating a strategy to mitigate those threats. Before the organization starts configuring and setting up MTD to combat those threats, it is important that the organization reviews their "risk tolerance level" and privacy policies, as both will play important parts in determining how configurations are set.

Typically, the risk tolerance level is divided into four categories:

- **Defensive** - An organization is classified as defensive if it maintains the highest level of security with the lowest risk tolerance. Typically, a defensive organization values security over user experience and prioritizes securing data and access to corporate resources. With regards to mobile threats, a defensive organization tends to block and/or quarantine the device and alert the user and the MobileIron administrator if mobile threats are detected to mitigate the threat. An example of a defensive organization is a government department/ministry/agency.

- **Reluctant** - An organization is classified as reluctant if it maintains a high level of security with a low risk tolerance. Typically, a reluctant organization values security over user experience, but compromises some security for an improved user experience. With regards to mobile threats, a reluctant organization tends to block a device and alert the user and the MobileIron administrator if mobile threats are detected to mitigate the threat. For certain high-level threats, the organization will quarantine the device. Examples of reluctant organizations are financial institutions and healthcare organizations.

- **Opportunistic** - An organization is classified as opportunistic if it maintains a medium level of security with a medium risk tolerance. Typically, an opportunistic organization strives to maintain a balance between security and user experience. With regards to mobile threats, an opportunistic organization tends to alert the MobileIron Administrator and the user if mobile threats are detected. For certain high-level threats, the organization will block the device from accessing internal resources to mitigate the threat. Examples of opportunistic organizations are manufacturing and transportation companies.

- **Aggressive** - An organization is classified as aggressive if it maintains a low level of security with a high-risk tolerance. Typically, an aggressive organization sacrifices security for user experience. With regards to mobile threats, an aggressive organization tends to alert the MobileIron Administrator and the user of the threat. Examples of aggressive organizations are hi-tech companies or other businesses that are not highly regulated.

As far as privacy policies are concerned, depending on the organization's corporate culture and their view on privacy, the organization may choose to limit their app inventory to only those managed by MobileIron. However, for MTD to be an effective deterrent of mobile threats, the organization may need to modify their privacy policies so MobileIron can inventory all apps on a managed device. Without the ability to inventory all apps, MTD may not be able to detect all the malware, trojan, or rogue apps that potentially reside on the device in addition to privacy risks that may reside within the apps. Without inventory and analyzation of the Apps, threats will only be detected when the App triggers a threat policy such as elevated privileges on the device.

For organizations that must abide by GDPR, a privacy policy is available on the management console specifically for this requirement. It maintains privacy of user information while still allowing for some forensic data to be collected if a threat is detected on the device.

Pro-active Risk Assessment

Pro-active Risk Assessment consists of reviewing the different use cases brought on by the different device ownerships. Typically, an organization may have any or all of these device ownership types:

- COSU - Corporate-Owned, Single Use device. Organization purchased device that are distributed to employees as dedicated work tools. Examples of a COSU device are hospital clinical devices, devices mounted on a delivery truck, and tablets for taking inventory inside a warehouse.
- COPE - Corporate-Owned, Personally Enabled device. Organization purchased device that employee uses as their own, but organization maintains complete management of the device.
- BYOD - Bring Your Own Device. Personally-owned device an employee voluntarily uses to connect to corporate resources, while the organization manages certain aspects of it to secure access to corporate resources.

Each device ownership use case will carry its own set of risks for which the organization will mitigate depending on their risk tolerance level. Understanding device use case plays an important role in determining how an organization will form policy based on the threat type.

COSU Recommendations

COSU device behavior is rather predictable. Once MTD has been deployed to those devices, a monitoring period will allow enough data to be collected to determine what threats, if any, are currently known to the devices. These threats can then be whitelisted by the security admin. This will create a baseline from which any other type of threat detected in the future likely indicates an actual attack on the device.

For example, an in-house app deployed to the devices may carry some potential security or privacy risks, even though the app itself is legitimate and is not acting maliciously. Since this app is a known app, it can be whitelisted in order to prevent the app from causing false positive alerts.

For threats that are detected, an organization will need to determine their strategy for how they wish to mitigate that risk, and we have some suggestions. For COSU devices that are deployed within a defensive organization, any threats that are considered critical would usually be mitigated with a quarantine action in order to remove company data. Threats that are classified as elevated would be mitigated by blocking the device from connecting to internal resources. For aggressive organizations, critical threats may be mitigated by blocking access to resources and elevated threats may be configured to notify the security team.

COPE Recommendations

COPE devices are typically locked down, while still allowing a certain level of freedom to enable personal usage of the device. Using the device for personal consumption will put the device at greater risks compared to COSU devices. Similar to BYO devices, there is a greater amount of unknown threats as users will be connecting to various networks that are out of the control of IT. It will be up to the organization as to how they mitigate these risks.

For example, many defensive organizations may decide not to allow devices to connect to unsecure Wi-Fi networks, and if the device does, they would choose to block access to internal resources, or take a local action and send all device traffic to a network sinkhole. On the other hand, aggressive organizations would likely allow users to connect to unsecure Wi-Fi networks and perhaps only monitor such activities in order to collect the forensic data if a network-based attack were to occur.

These devices present the challenge for organizations as the device is still fully under corporate control, but the personal side will present greater risk. It becomes a balancing act as organizations want to secure the device while still providing a "functional" device to the user. Much like with BYO devices, privacy must also be considered, which depending on the organizations policy may impact the level of forensic data that can be collected.

BYOD Recommendations

BYOD devices generally carry the greatest level of risk to an organization. Users are able to fully control their device which allows them to connect to unsecure networks, install any apps, and even modify system settings.

In many cases, defensive organizations will not allow these types of devices to be used in the environment, as the level of risk is far too high. Aggressive organizations may mitigate the increased risk by choosing to quarantine or block access to internal resources for any critical threats. For elevated threats, notifications may be sent to the security team for further analysis while also notifying the end user so possible remediation action can be taken without IT involvement. For example, if a user installs a potentially malicious app, the security team may need to further review the app to determine if the app presents a true threat or just has associated risk. The user may also be notified of the potential threat, which may persuade them to remove the app until further analysis has been conducted by the security team.

Pilot Devices

Once the organization has configured MTD, it is time to start the deployment process. It is recommended that the organization starts the initial deployment with their IT department. This will allow savvy users to provide initial feedback and familiarize the mobility team with the deployment process.

This phase may last for only a short period before a larger pilot group is chosen. This larger pilot group would encompass all the use cases an organization will have. This will ensure that enough data is being captured for further threat analysis. It will also give the organization the feedback it needs with regards to the deployment process and the user experience, so it can be readied for the larger, company-wide rollout in the next phase.

II. Rollout & Monitor

The Rollout & Monitor phase consists of threat analysis and policy creation based on device use cases, as well as data that was collected during the pilot phase. The mobility team will work with security to begin laying the groundwork as to what threats are relevant in their environment after analyzing the data. After receiving feedback from end users, the mobility team should be looking to extend the deployment to a larger group of devices. Most organizations who fall into the defensive or reluctant risk categories may decide to begin enforcement at this stage, while opportunistic and aggressive will continue to monitor for further data collection.

Refine policy and messaging

Full review of policies should be conducted by the security team and/or MTD administrators. Based on threat types that have been detected during the Pilot phase may require some additional modifications to the severity classifications of these threats. This in turn may also impact how the organization chooses to mitigate the associated risk.

Gathering feedback

Allow users time to provide feedback that were part of the larger pilot rollout. The information gathered will be fed back into the messaging refinement. This may be due to some of the notifications being sent causing confusion to the user.

Analyze Data

Security and mobility team work together to analyze all the threat data that has been collected from devices during the pilot phase. The data gathered will be used to refine policy and messaging.

End-User Rollout

Now that the mobility team understands the deployment process, a plan will be put in place to deploy to the entire organization. There are a couple of different approaches that can be taken:

1. Deploy to the entire organization all at once. This approach can work well when a limited number of devices are going to be deployed.
2. Phased approach. This is generally the recommended approach when the organization has a large number of devices. This will prevent the help desk / mobility admin from being overwhelmed with too many issues simultaneously. In addition, it will give the organization time to fine-tune their MTD configurations and policies.

III. Refine & Inform

During the Refine and Inform phase organizations will continue to analyze threats that are being detected as part of larger device deployment rollout that occurred in the rollout and monitor phase. It is also possible that the previous phase blends into this phase and is still ongoing as the rollout may be for a very large number of devices. This may require some modifications to existing policies that were set in the previous stage. A complete review of potential compliance actions should also be done at this time. This will help the security team determine what actions will be taken on specific threats in order to mitigate risk based on the organizations internal risk threshold. Opportunistic and aggressive type organizations will also begin alerting devices of potential threats while defensive and reluctant type organizations will continue to refine their mitigation process.

Alert and inform

At this stage MTD is fully deployed. With the data collected from the full deployment, the MobileIron Administrator will start to fine-tune the alerts so only certain high-level threats will be alerted to avoid alert-fatigue. For defensive organizations, they may continue to deliver alerts for low severity threats to both the admin as well as the device user. However, aggressive organizations may choose to notify the admin only of any critical alerts as they prefer MTD to be much more transparent to the end user. In either case, security team would be informed of threats, so they can conduct the proper investigation in order to determine if further actions must be taken. For example, once the security team has been informed of a critical threat, such as a jailbroken/rooted device, depending on the device use case, it will inform the user as to what corrective actions must be taken in order to remediate the issue.

Review compliance actions

The security team may conduct a review of current compliance actions to ensure there is alignment with the organizations risk tolerance and the severity of threats. Some tweaks may be made to allow end users some additional time to remediate the issue before additional actions are taken against their device.

For example, as the organization gets more comfortable with MTD and becomes more aware of the types of threats that are present, it may decide that detection of certain threats should not initially cutoff access to resources, as this is more disruptive to the end user. It may in some cases make more sense to provide a warning to the user and allow them a period of time to correct the issue before taking action and blocking access or even quarantining the device. An aggressive organization may opt to use tiered compliance whereas they are willing to accept a certain level of risk for a short period of time. For example, the user installs an app that is flagged as malicious by the Management Console. If immediate access to resources is blocked this could potentially be very disruptive to the end user resulting in loss of productivity. Notifying the user that a malicious app has been installed will allow the user time to remove the app, and also allow the admin time to investigate the app to determine if it is indeed malicious, and if not whitelist it. If the app is determined to be malicious the app could remain on the device for a certain period of time before the next staged action occurs, which may result in blocked access to internal resources.

In addition, organizations may wish to start looking into using both local action in addition to the Management Console to mitigate risks associated with threats. With local action, risks can be mitigated even in the event the device doesn't have a network connection. Defensive organizations may opt to choose local enforcement, which can block access to resources or even send traffic to a network sinkhole in order to force a user to disconnect from an unsecured Wi-Fi network. Aggressive organizations may simply choose to use local notifications to continue to allow offline threat notifications to be presented to the device user.

Establish Deployment Groups

By now, the security team will have enough data to further segment their users or device use cases into groups, each with a finely-tuned set of policies specific for that group.

For example, a transportation company may start grouping all their truck drivers together and finetune the MTD policies on those devices to just alert the MobileIron Administrator and the user instead of blocking or quarantining the device when a threat is detected, knowing that truck drivers tend not to have access to much company sensitive data. At the same time, the MobileIron Administrator may further lockdown those devices to prevent data loss. On the other hand, the organization may employ more stringent MTD policies on their executives because they do have access to sensitive corporate information and tend to be targets of more sophisticated threats such as Man-In-The-Middle attacks.

Typically, for defensive organizations, they may only have a few deployment groups as they tend to see threats from everywhere and treat them as equal, whether it comes from a low-level clerk or a high-level executive. For aggressive organizations, they may have many groups based on geographical locations and/or business functions, each group having its own unique configurations.

IV. Mature & Enforce

By the time most organizations reach this phase, automated mitigation is going to be configured in the system. This will automatically enforce policies that were defined in previous phases. Also, all compliance rules will be strictly enforced. The type of mitigation used to enforce the policies will vary depending on the risk tolerance of the organization. For example, a defensive organization may wish to quarantine or block access to internal resources for any threat that is considered critical or elevated, whereas an aggressive organization may choose to mitigate some of those same risks with simply an alert.

Also, at this phase, the organization will start to develop a knowledgebase about the threats they encounter and how to remediate them based on the organization's security posture. As additional Device, network, or app related threats become known, the organization will return to the refine phase and modify compliance actions accordingly to mitigate the risk associated with the everchanging threat landscape.

Additional information can be found in the community portal or on mobileiron.com. You can also reach out to MobileIron Professional Services if assistance with implementation is required.