Detecting Compromised Devices

Isolating Your Mobile Assets at Risk

Table of Contents

Introduction

Mobile devices allow constant communication and access to enterprise content on the go. While mobile devices keep vital business information flowing, malware and corrupted content can just as easily be introduced into your network. Given these potential security threats, your Mobile Device Management (MDM) strategy should be prepared for any challenge. One such security challenge is the presence of a compromised device in your mobile fleet.

Overview

Compromised devices include "jailbroken" iOS and "rooted" Android devices that a user has actively altered from manufacturer presets. These devices strip away integral security settings and may introduce malware in your network and access your enterprise resources. In an MDM environment, the overall chain is only as strong as its weakest link. A single compromised device could leak sensitive information or corrupt your servers. Monitoring and detecting compromised devices becomes even trickier in a Bring Your Own Device (BYOD) environment, with varying versions of devices and operating systems. Compromised devices are a major security concern for an enterprise and should be tackled immediately.

Jailbroken and rooted devices surrender basic safeguards, making them vulnerable entry points for undesired activity, such as:

- **Password & Identity Theft:** Unencrypted usernames and passwords are easily collected and used to go deeper into sensitive areas or assume company identity.
- **Data Interception:** Sent and received communication is in plain view, unprotected by normal security measures.
- **Virus Infiltration:** An unguarded network is a sitting duck for virus and malware intrusion, potentially making your company's data corrupted and unrecoverable.

The Challenge of Detection

Devices running on different platforms respond differently towards compromised detection. For example, iOS devices do not have native background check and thus have to be run through a dedicated app. Android devices, on the other hand, allow for background checks to happen without any restrictions or limitations. AirWatch's solution to this problem ensures detection across multiple devices and operating systems.

AirWatch Approach

To deal with such variations, AirWatch, the leader in MDM, has developed a unique multi-tiered approach to compromised device detection. Refer to the below table to understand the limitation and capabilities of iOS and Android platforms.

Platform Capabilities

Capability	iOS		Android
Agent Enrollment	Compromised status detected during enrollment		Compromised status detected during enrollment
Background Check	Recent Cellular Devices	Wi-Fi Only or older cellular devices	Allows background detection
	Background checks available using AirWatch MDM Agent	Background checks available using AirWatch SDK embedded in internal apps	
On-Demand Checks	Available using scheduled APNs messaging: -On launch of the AirWatch Secure Content Locker -On launch of the AirWatch Secure Web Browser -On launch of the AirWatch MDM Agent		Available using C2DM messaging: -On launch of the AirWatch Secure Content Locker -On launch of the AirWatch Secure Web Browser -On launch of the AirWatch MDM Agent
Compliance Engine	Automated remediation actions when compromised device detected or status is out-of-date.		Automated remediation actions when compromised device detected or status is out-of-date.
Detection built into enterprise apps	AirWatch SDK available to embed compromised detection logic within your enterprise apps.		AirWatch SDK coming soon to embed compromised detection logic within your enterprise apps.

Detecting Compromised Devices with AirWatch

AirWatch's solution spans the entire life of an enrolled device, locking out uninvited devices and severing ties with compromised or non-compliant devices. Our proprietary detection algorithms constantly undergo penetration testing and Research & Development based on new operating systems, ensuring the most advanced detection capabilities possible. This multi-tiered detection approach for compromised devices consists of the following:

Agent Enrollment

AirWatch's first line of defense against unwanted devices starts at enrollment. Configure compliance settings and detect compromised devices before allowing entry to a device. Require all devices to comply with security settings or easily install profiles for the user. Security compliance detection varies based on the type of enrollment:

- **Agent based**: iOS or Android devices can enroll with the **AirWatch MDM Agent** downloaded from the iTunes app store or the Google Play store respectively. Once Agent is installed, the agent checks for the status of the device, the device then sends the information to the server through Beacon as per the time interval set on the Admin Console.
- **Web based:** Currently, iOS devices are the only devices that support web-based enrollment with the default Web browser on the device using the enrollment URL. To detect the status of such devices, any of the AirWatch SDK embedded app should be installed on the device.

- **For more information comparing the various enrollment approaches, see the document titled "iOS Enrollment Capabilities."**

Background Checks

Once the device is enrolled, keep track of its compliance. The AirWatch MDM Agent provides ongoing background checks for compromised status for all Android devices and newer models of iOS devices with access to a cellular network.

For iOS, Apple restricts applications that are submitted to the Apple Store from running in the background on Wi-Fi-only devices and older generation cellular devices (iPhone 3GS and the Original iPad). However, these limitations do not apply to applications that your company builds as enterprise apps. These apps can run in the background based on GPS, VoIP, or Music APIs that Apple provides. Using the compromised detection functionality in the AirWatch SDK, you can tie into this backgrounding logic in your internal application to accomplish background jailbreak detection. Furthermore, AirWatch has battery saving mode capabilities to avoid battery drain when running these functions in the background.

On-Demand Background Checks

Establish detection checkpoints for enterprise information and AirWatch feature usage. When a device launches the AirWatch Secure Content Locker, the AirWatch Secure Web Browser, or the AirWatch MDM Agent, the detection system automatically verifies compliance status, adding an additional wall of protection to your information.

Compliance Engine

Once AirWatch detects compromised or non-compliant devices, the compliance engine quickly takes action on those devices based on the device policy set by the administrator on the console. AirWatch provides flexibility to the administrator to require the initial device status as well as set the time interval frequency of the compliance engine, whether the interval is once a minute or once a month.

Detection Built Into Enterprise Apps

Rather than installing the AirWatch agent to access the SDK, bypass Apple's background restrictions by building AirWatch's SDK into your internal apps. The SDK comes with key features of MDM (*which are outlined in our complete SDK Profile*), including jailbreak and root detection that constantly scans for compliance. Commonly run Enterprise Apps that are pushed down to a device will run detection scans more frequently, so you'll catch compromised devices sooner.

An administrator can then specify the actions to be taken for an app installed on the compromised device in the Admin Console. For example, if a device is found to be compromised, the administrator can apply the following actions:

- Send user warning message
- Lock user out of device
- Wipe application and enterprise data
- Restrict access

Enforcing and Monitoring Compromised Devices

Manage your devices at all times. The AirWatch Admin Console furnishes the administrator with tools to keep the system alert and secured.

Compliance Engine

The Compliance Engine serves as a security checkpoint, automatically locking out or taking additional action on devices or users. Based on the compliance rules set by the administrator for a device, the compliance engine can detect if a device is non-complaint and take defined actions on it. These rules and actions can be defined in the AirWatch Admin Console.

Once the rules and actions are established, the Compliance Engine takes care of the rest. Remediation is automated. If a scan uncovers a compromised device, the system runs through preset warnings and escalated actions. Administrators aren't forced to address each instance as they're found.

However, the Admin Console does enable self-service for compliance protocol. Administrators can wipe a device and send an email or SMS message to the user explaining how and why their device is out of compliance, without the user having to contact the administrator.

With the time saved by the Compliance Engine managing devices, Administrators can review weekly or monthly compliance reports to understand repeat offenders.

Last Compromised Scan compliance

The **Last Compromised Scan** compliance allows the administrator to set the time interval within which the agent should be performing the device scan. This ensures that if AirWatch has not received a compliance status from the device for a certain amount of time, precautionary measures can be taken.

Compromised Status compliance

The **Compromised Status** compliance rule allows the administrator to setup actions for a compromised device.
For the above two compliance rules, the following actions can be applied:

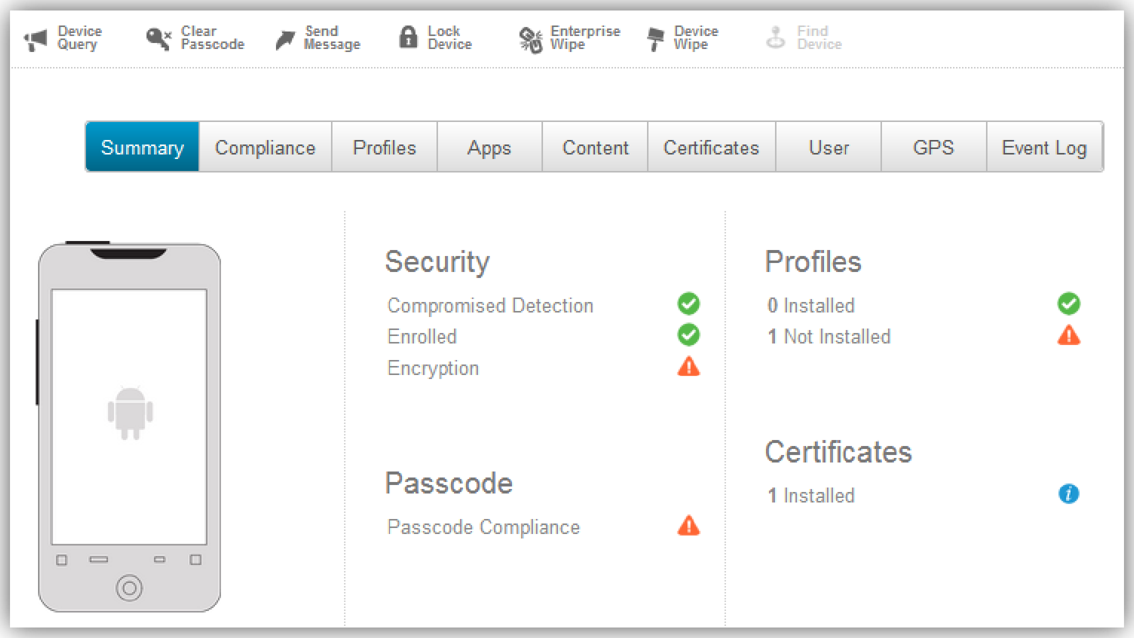
- **Notify**: Notifying the user by sending SMS, Email, and Push Notifications.
- **Application**: Blocking or removing few or all the managed apps.
- **Command**: Performing Enterprise Wipe or requesting for a device check in.
- **Profile**: Blocking or removing all profiles or particular profile type or a particular profile.

Alerts

Automatically alert administrators whenever a device is detected to be compromised. Administrators can also send alerts to the required person or a group of people.

Device Control Panel

Administrators can view the summary of the devices enrolled. The summary includes the security details informing the administrator whether compromised detection has been done on the device or not. If the device is not compromised, green check mark is shown.



Security

Compromised Detection	✓
Enrolled	✓
Encryption	⚠

Passcode

Passcode Compliance	⚠

Profiles

0 Installed	✓
1 Not Installed	⚠

Certificates

1 Installed	ℹ

Figure 1: Device Control Panel displaying the security details of the enrolled device

Visualize Device Compliance

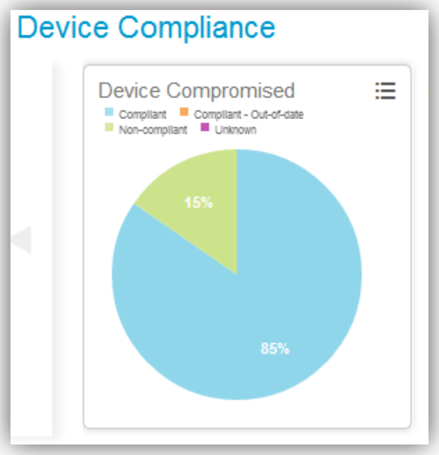
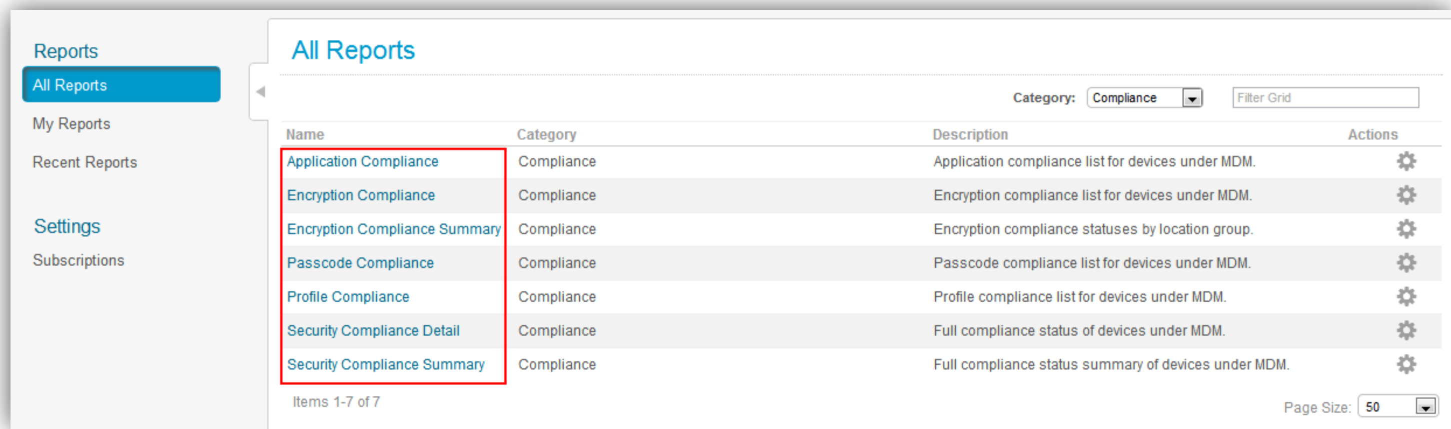


Figure 2: Chart displaying the percentage of compromised devices enrolled in the MDM

Your Dashboard provides a graphical representation of the percentage of compromised devices enrolled in a location group. This gives the administrator a high level view of the compromised devices and helps in keeping track of such devices.

Run Scheduled or On-Demand Compliance Reports

The Admin Console also comes with more than 100 standard reports, including a list of Compliance Reports that can run automatically at scheduled intervals or generated on-demand. Quickly view any non-compliant devices in your entire fleet or in specific location groups. Isolate offending devices for blacklisted apps, weak passcode settings, and overall security compliance. Compliance reports allow a birds-eye view of compromised or non-compliance devices in your system

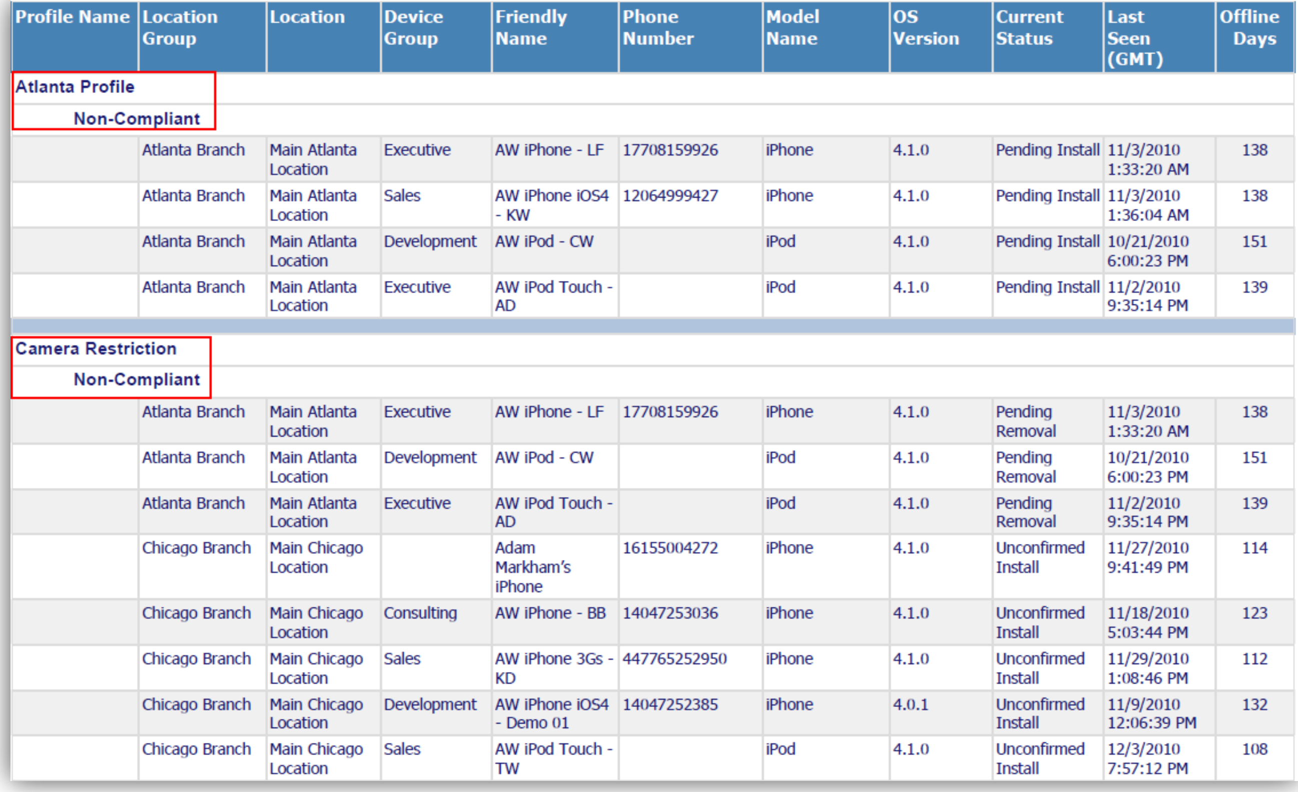


Name	Category	Description	Actions
Application Compliance	Compliance	Application compliance list for devices under MDM.	⚙
Encryption Compliance	Compliance	Encryption compliance list for devices under MDM.	⚙
Encryption Compliance Summary	Compliance	Encryption compliance statuses by location group.	⚙
Passcode Compliance	Compliance	Passcode compliance list for devices under MDM.	⚙
Profile Compliance	Compliance	Profile compliance list for devices under MDM.	⚙
Security Compliance Detail	Compliance	Full compliance status of devices under MDM.	⚙
Security Compliance Summary	Compliance	Full compliance status summary of devices under MDM.	⚙

Items 1-7 of 7

Page Size: 50

Figure 3: Standard Compliance Reports available in Admin Console



Profile Name	Location Group	Location	Device Group	Friendly Name	Phone Number	Model Name	OS Version	Current Status	Last Seen (GMT)	Offline Days
Atlanta Profile										
Non-Compliant										
	Atlanta Branch	Main Atlanta Location	Executive	AW iPhone - LF	17708159926	iPhone	4.1.0	Pending Install	11/3/2010 1:33:20 AM	138
	Atlanta Branch	Main Atlanta Location	Sales	AW iPhone iOS4 - KW	12064999427	iPhone	4.1.0	Pending Install	11/3/2010 1:36:04 AM	138
	Atlanta Branch	Main Atlanta Location	Development	AW iPod - CW		iPod	4.1.0	Pending Install	10/21/2010 6:00:23 PM	151
	Atlanta Branch	Main Atlanta Location	Executive	AW iPod Touch - AD		iPod	4.1.0	Pending Install	11/2/2010 9:35:14 PM	139
Camera Restriction										
Non-Compliant										
	Atlanta Branch	Main Atlanta Location	Executive	AW iPhone - LF	17708159926	iPhone	4.1.0	Pending Removal	11/3/2010 1:33:20 AM	138
	Atlanta Branch	Main Atlanta Location	Development	AW iPod - CW		iPod	4.1.0	Pending Removal	10/21/2010 6:00:23 PM	151
	Atlanta Branch	Main Atlanta Location	Executive	AW iPod Touch - AD		iPod	4.1.0	Pending Removal	11/2/2010 9:35:14 PM	139
	Chicago Branch	Main Chicago Location		Adam Markham's iPhone	16155004272	iPhone	4.1.0	Unconfirmed Install	11/27/2010 9:41:49 PM	114
	Chicago Branch	Main Chicago Location	Consulting	AW iPhone - BB	14047253036	iPhone	4.1.0	Unconfirmed Install	11/18/2010 5:03:44 PM	123
	Chicago Branch	Main Chicago Location	Sales	AW iPhone 3Gs - KD	447765252950	iPhone	4.1.0	Unconfirmed Install	11/29/2010 1:08:46 PM	112
	Chicago Branch	Main Chicago Location	Development	AW iPhone iOS4 - Demo 01	14047252385	iPhone	4.0.1	Unconfirmed Install	11/9/2010 12:06:39 PM	132
	Chicago Branch	Main Chicago Location	Sales	AW iPod Touch - TW		iPod	4.1.0	Unconfirmed Install	12/3/2010 7:57:12 PM	108

Figure 4: Snapshot of Compliance Report showing devices without required Profile and Feature setup.

Conclusion

Secured MDM is an ever growing need and thus, AirWatch takes a step ahead in that direction by offering unparalleled solution that provides and arms you to detect security threats such as compromised devices. AirWatch’s unique multi-tier detection solution has been designed to be effective on all device platforms and also provides flexibility to take required actions on the detected devices. All the above ingredients of the detection solution make AirWatch an effective solution to keep your enterprise secured, smooth, and frictionless.