Check Point SandBlast Mobile

SandBlast Mobile Protect iOS App

Installation & User Guide

V2.70

About This Guide

Only Check Point provides a complete mobile security solution that protects devices from threats on the device (OS), in apps, and in the network, and delivers the industry's highest threat catch rate for iOS and Android. Check Point SandBlast Mobile uses malicious app detection to find known and unknown threats by applying threat emulation, advanced static code analysis, app reputation and machine learning.

- Perform advanced app analysis to detect known and unknown threats
- Monitor network activity for suspicious or malicious behavior
- Assess device-level (OS) vulnerabilities to reduce the attack surface

It uses a variety of patent-pending algorithms and detection techniques to identify mobile device risks, and triggers appropriate defense responses that protect business and personal data.

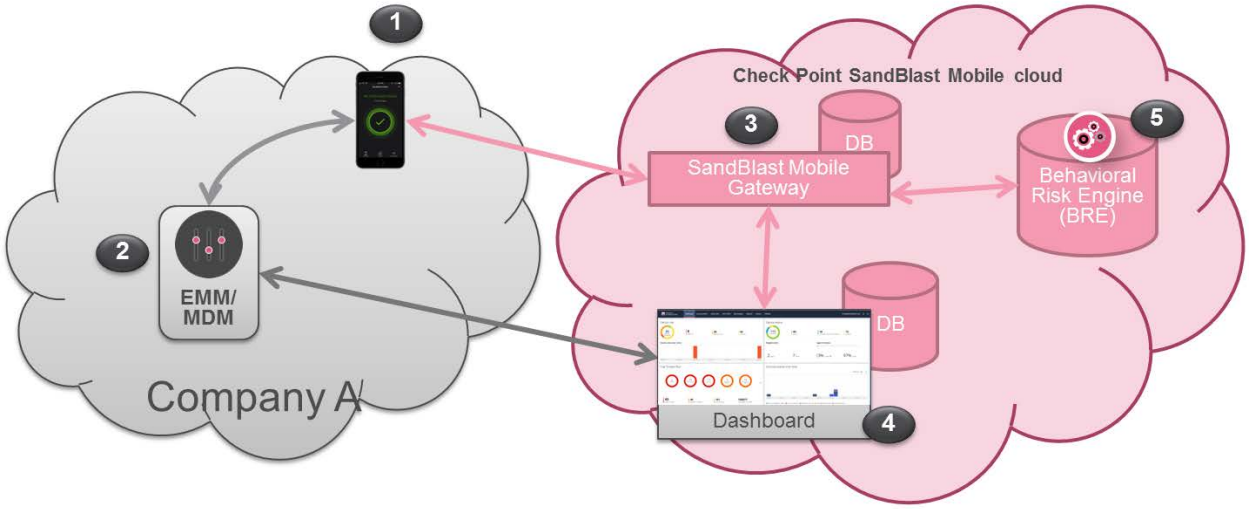
The Check Point SandBlast Mobile solution ("the Solution") includes the following components:

- Check Point SandBlast Mobile Behavioral Risk Engine ("the Engine")
- Check Point SandBlast Mobile Gateway ("the Gateway")
- Check Point SandBlast Mobile Management Dashboard ("the Dashboard")
- SandBlast Mobile Protect app ("the App") for iOS and Android

This guide includes all the instructions the user needs to first install and then use the SandBlast Mobile Protect app on iOS devices.

Contents

1 Check Point SandBlast Mobile Solution Architecture



1.1 Components

	Component	Description
1	SandBlast Mobile Protect app	• The SandBlast Mobile Protect app is a lightweight app for iOS® and Android™ that gathers data and helps analyze threats to devices in an Enterprise environment. It monitors operating systems and information about apps and network connections and provides data to the Solution which it uses to identify suspicious or malicious behavior. • To protect user privacy, the App examines critical risk indicators found in the anonymized data it collects. • The App performs some analysis on the device while resource-intensive analysis is performed in the cloud. This approach minimizes impact on device performance and battery life without changing the end-user experience.
2	EMM/MDM	• Enterprise Mobility Management/Mobile Device Management • Device Management and Policy Enforcement System.
3	SandBlast Mobile Gateway	• The cloud-based Check Point SandBlast Mobile Gateway is a multi-tenant architecture to which mobile devices are registered. • The Gateway handles all Solution communications with enrolled mobile devices and with the customer's ("organization's") Dashboard instance.
4	Dashboard	• The cloud-based web-GUI Check Point SandBlast Mobile Management Dashboard enables administration, provisioning, and monitoring of devices and policies and is configured as a per-customer instance. • The Dashboard can be integrated with an existing Mobile Device Management (MDM)/Enterprise Mobility Management (EMM) solution for automated policy enforcement on devices at risk. • When using this integration, the MDM/EMM serves as a repository with which the Dashboard syncs enrolled devices and identities.
5	Behavioral Risk Engine	• The cloud-based Check Point SandBlast Mobile Behavioral Risk Engine uses data it receives from the App about network, configuration, and operating system integrity data, and information about installed apps to perform in-depth mobile threat analysis. • The Engine uses this data to detect and analyze suspicious activity, and produces a risk score based on the threat type and severity. • The risk score determines if and what automatic mitigation action is needed to keep a device and its data protected. • No Personal Information is processed by or stored in the Engine.

2 Prerequisites

In order to install the SandBlast Mobile Protect app, the user should be prepared with:

1. User's iOS Mobile Device (iOS version 8.x or higher)
2. User's Enterprise Email access from mobile device or computer.
3. User's MDM Agent (optional)

3 Installation Methods

3.1 Manual Download and Installation by the user

The rest of this document discusses the manual installation procedures for iOS devices and the usage of the SandBlast Mobile Protect app.

3.2 Automatic Download by the IT Department using MDM

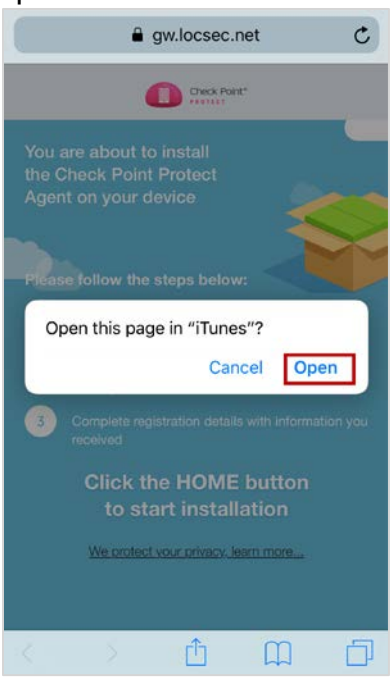
If the organization uses an MDM, such as Airwatch or Microsoft Intune, the SandBlast Mobile Protect app can be automatically pushed to the user's device. If automatically installed and configured using MDM, the user only needs to read the sections describing the usage of the SandBlast Mobile Protect app.

4 Installing SandBlast Mobile Protect App

4.1 SandBlast Mobile Protect App Installation from Apple App Store

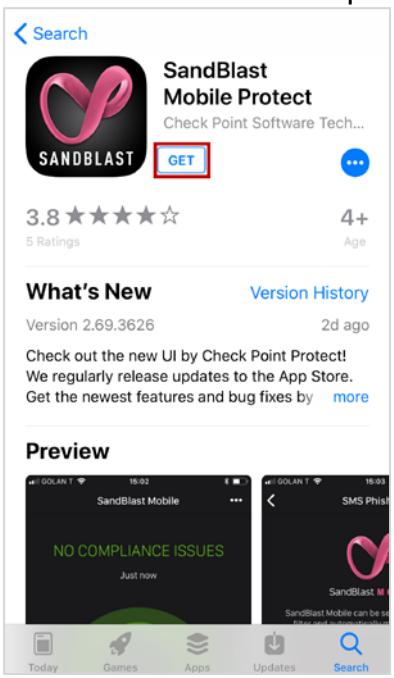
4.1.1. You should receive your email registration. This email contains several basic instructions and two important details for registration, the server address and the registration key. This email will also contain a link to download the App and a QR code, in case the email cannot be read on the device.

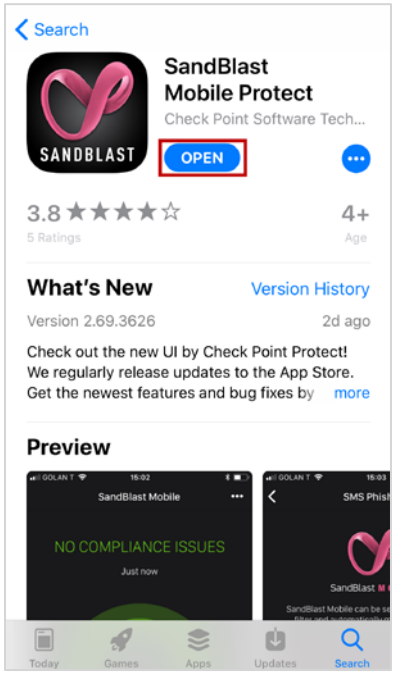
4.1.2. When prompted, tap Open.

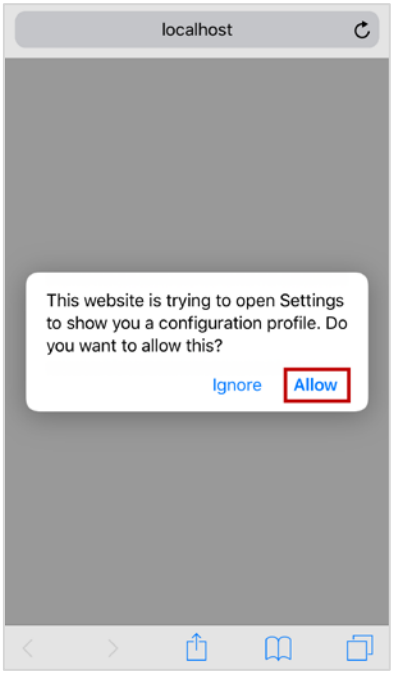


4.1.3. Tap the "Get" button to start the app installing.

4.1.4. Once the app has loaded, open the application, and allow the configuration profile to be installed. Tap "Allow".



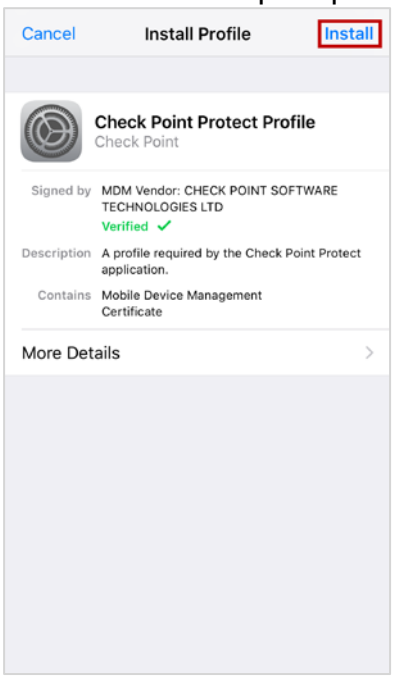


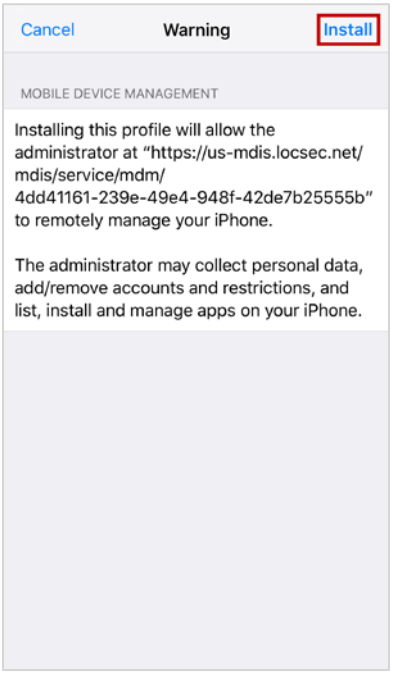


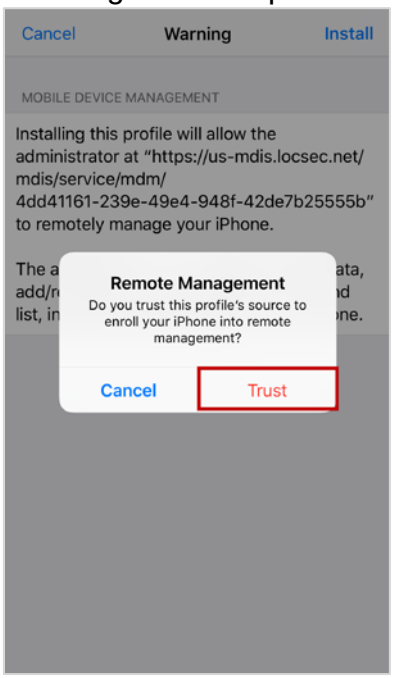
4.1.5. When prompted to install the Check Point Protect Profile, tap “Install” on the top right. This is essential for the App to perform its function.

4.1.6. You will be prompted to install a Mobile Device Management profile from SandBlast Mobile. This is to allow the App to function. Tap “Install” on the top right.

4.1.7. You will be prompted to trust the Profile for Remote Management. Tap “Trust”.



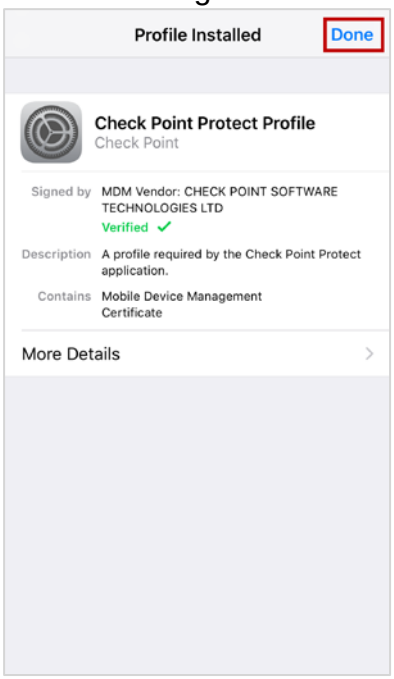


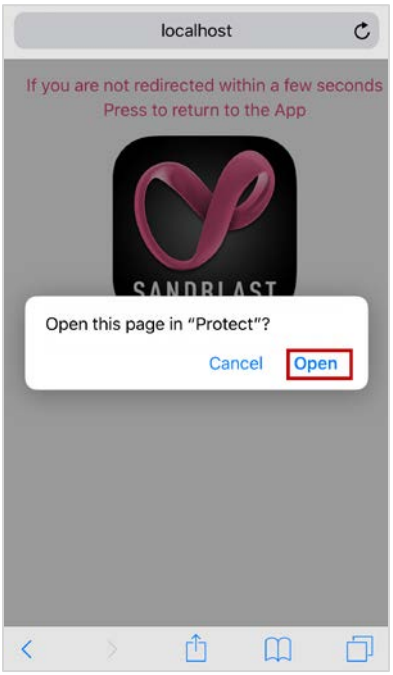


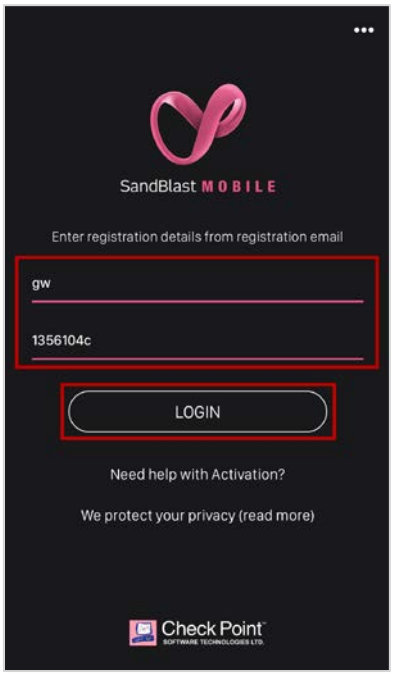
4.1.8. Once the profile, tap “Done” on the top right corner.

4.1.9. Once the process returns to Safari, it will prompt for you to continue to SandBlast Mobile Protect app. Tap “Open”.

4.1.10. Enter the Server Address and Registration Key that is contained in the email, tap the “Login” button.

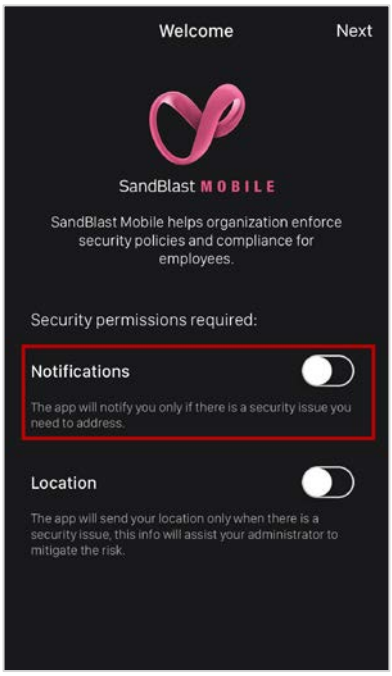


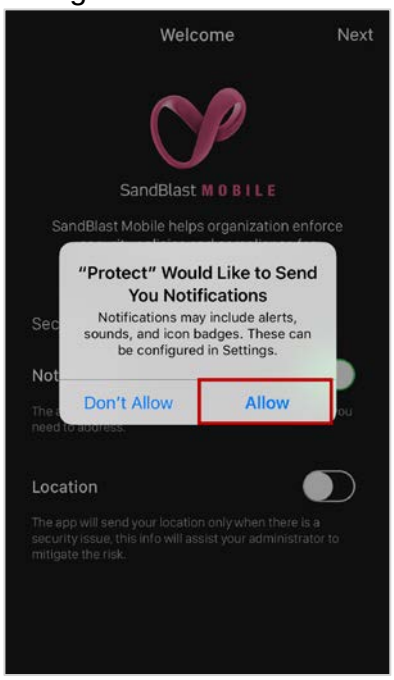


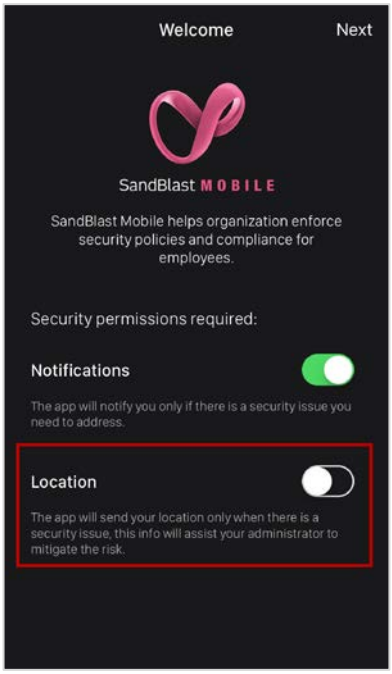


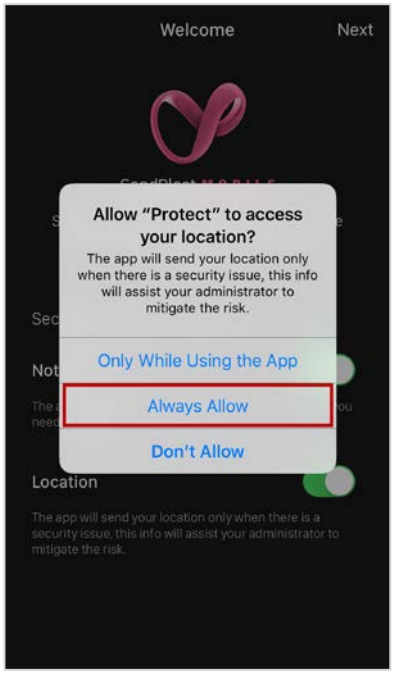
4.1.11. You will now be prompted to enable Notifications, Location, and SMS Phishing Protection.

4.1.12. Enable as appropriate, but it is strongly recommended that you enable Notifications, Location, and SMS Phishing Protection.

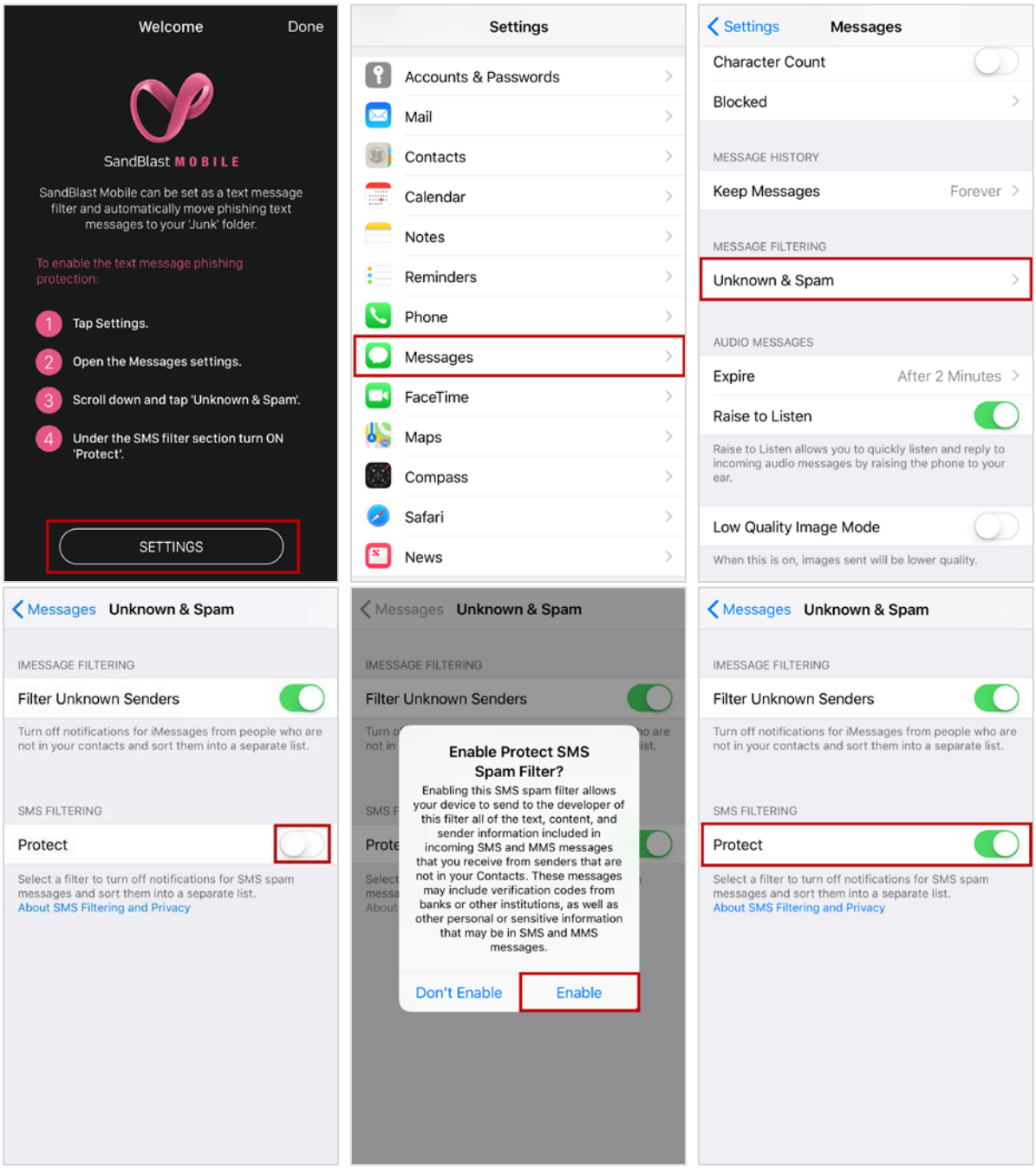




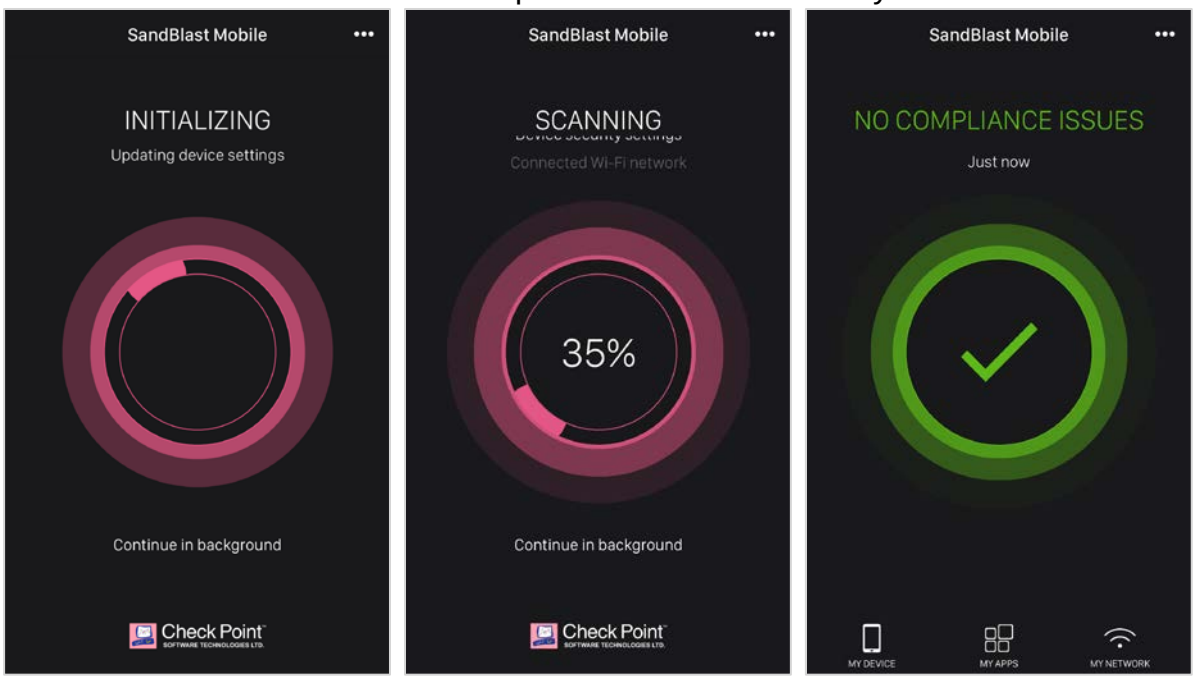




4.1.13. You will now be prompted to enable SMS Phishing Protection.
4.1.14. Follow the instructions to enable SMS Phishing Protection.
4.1.15. Go to **Settings > Messages > Unknown & Spam**, and turn on SMS filtering for Protect.



4.1.16. SandBlast Mobile Protect will perform an initial scan of your device.



4.1.17. Your device is now protected with Check Point SandBlast Mobile.

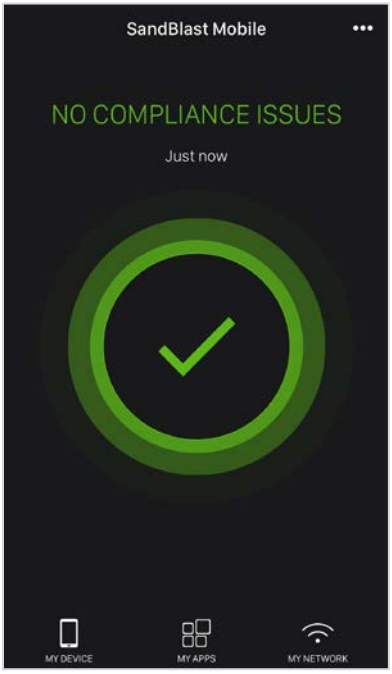
5 Using SandBlast Mobile Protect app

SandBlast Mobile Protect app runs seamlessly in the background without affecting memory or performance. With the SandBlast Mobile Protect app you gain both complete protection from mobile threats and visibility into the current status of your iOS device.

Your iOS device can be in 2 different states:

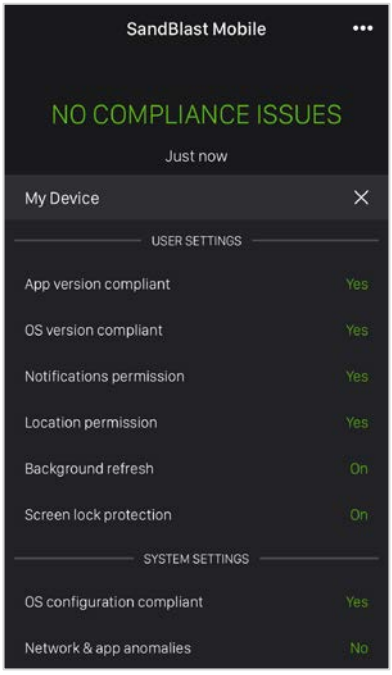
5.1 State 1 – No Threats/Policy Violations Found – Device Compliant

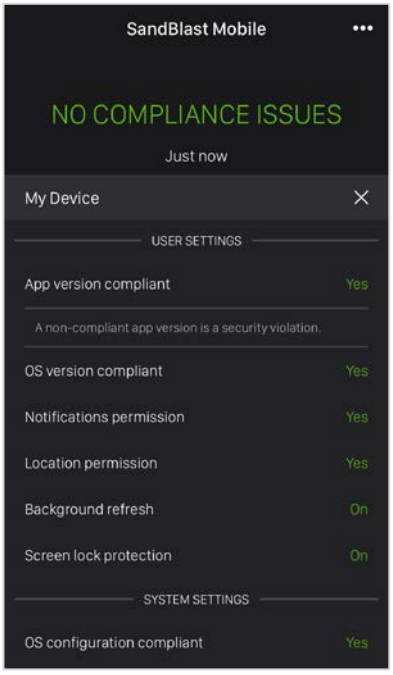
The main screen of the app is based on one main concept: **Green = Good**. As long as your device is protected by the app and is threat free – the app main page remains **Green**.



5.1.1 My Device

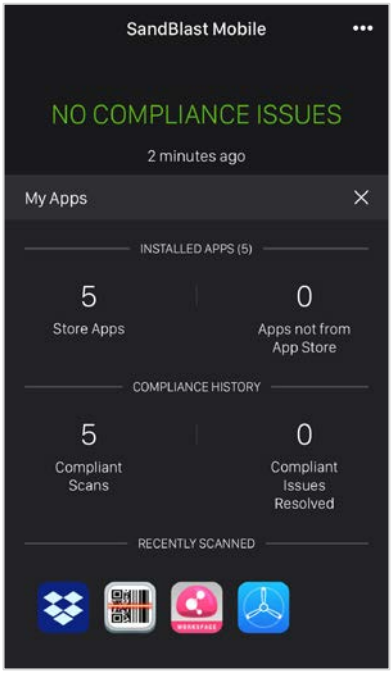
Tapping “My Device” icon on the bottom left of the main SandBlast Mobile Protect screen, you will be brought to a screen of system settings.
Tapping each setting provides additional information regarding the setting.
When the Yes/No or On/Off indicator is in **GREEN**, then the setting is OK or Good; if **RED**, then the setting/configuration should be adjusted in order to make your device as secure as possible.

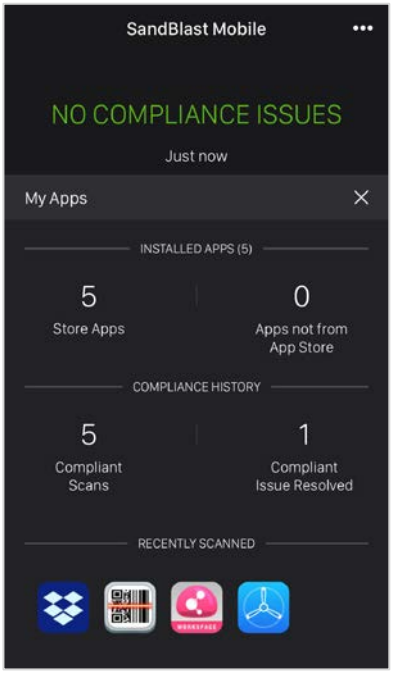




5.1.2 My Apps

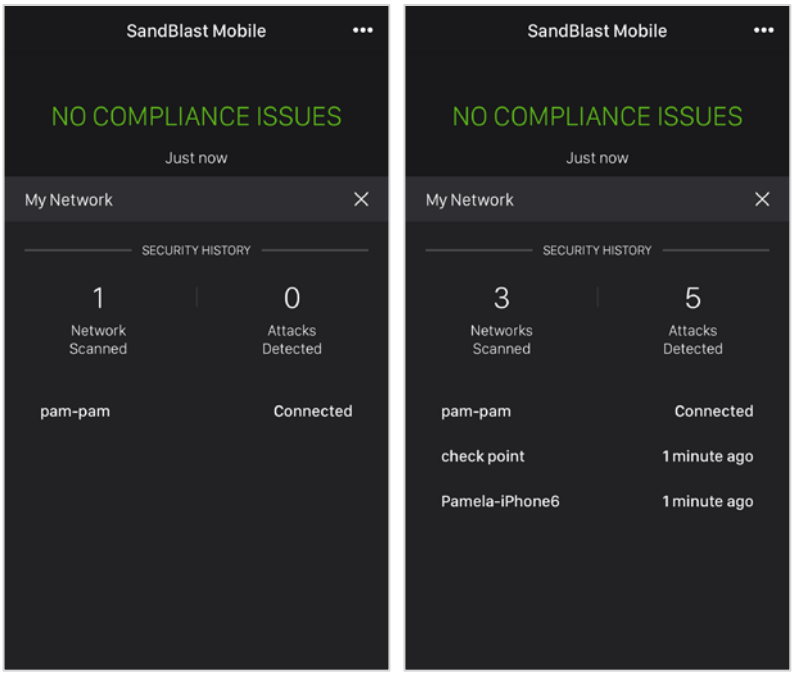
Tapping “My Apps” icon on the bottom center of the main SandBlast Mobile Protect screen, you will be brought to an overview screen for all the apps on your device.
You can also see if any malicious apps were discovered by SandBlast Mobile, and removed by you.





5.1.3 My Network

Tapping “My Network” icon on the bottom right of the main SandBlast Mobile Protect screen, you will be brought to a listing of the Wi-Fi network you are currently connected to and/or Wi-Fi networks you have connected to in the past, as well as an overview of the number networks scanned and the number of networks that exhibited suspicious activity, such as possible Man-in-the-Middle attacks.



5.2 State 2 – Threats Found – Policy Violations

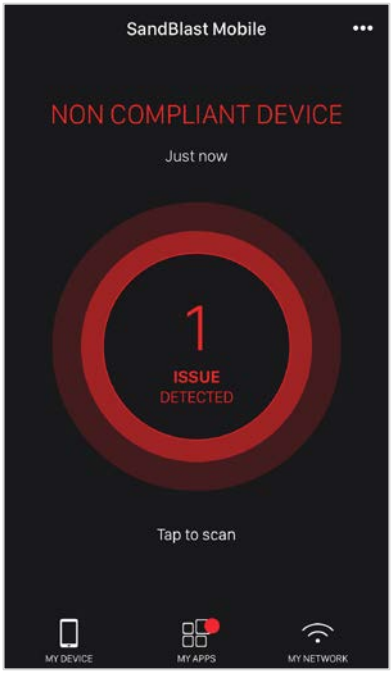
Upon discovery of a mobile threat or policy violation, such as malware, network attack, etc., the SandBlast Mobile Protect app will make sure you're immediately made aware of the threat and take action to remove the threat. There are two notifications methods, if enabled (enabled by default): an on-screen pop-up or banner and/or a notification entry in Notification Center.

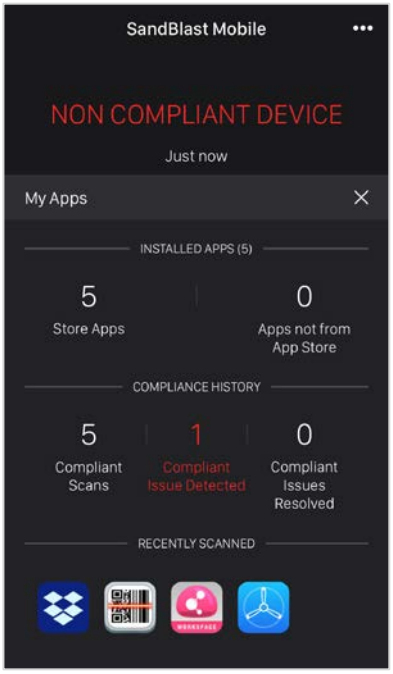
5.2.1 App Protection (Advanced App Analysis)

5.2.1.1. Once you've entered the SandBlast Mobile Protect app, you'll be informed regarding the existing policy violation (threat). The section is highlighted in Red below. Depending on the violation/threat, the app will suggest the required form of mitigation.

5.2.1.2. In our example, a suspicious app has been flagged.

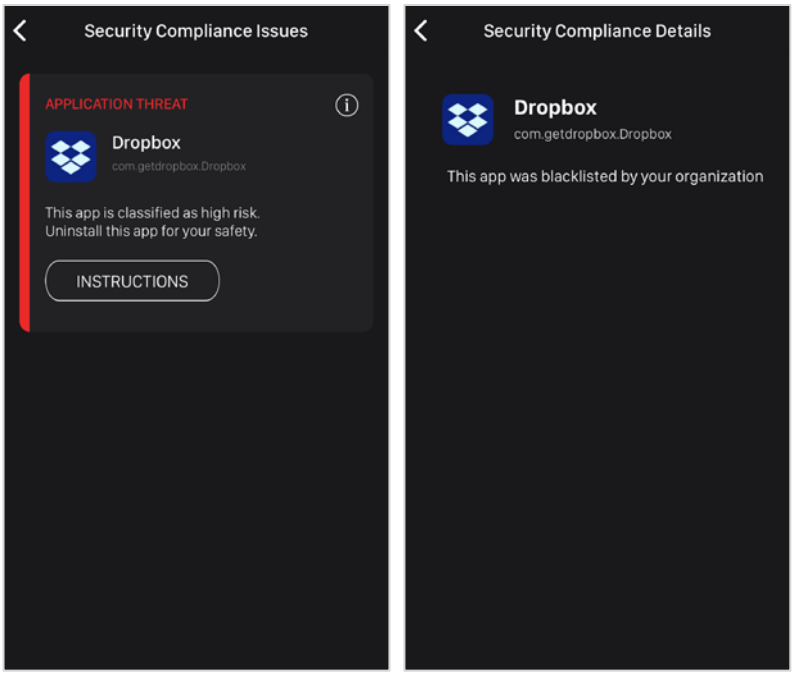
5.2.1.3. Tapping "My Apps" you can see that there is 1 malware detected.



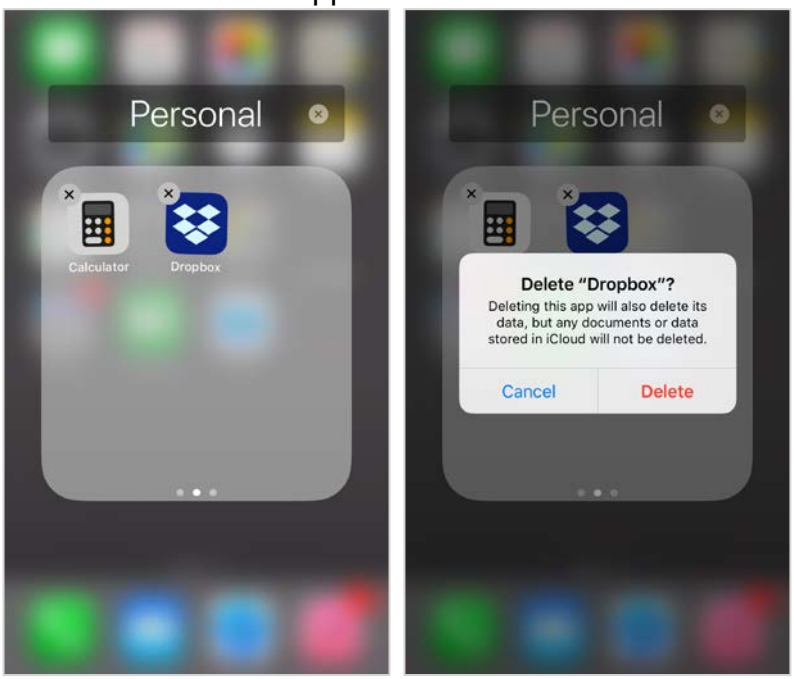


5.2.1.4. Either tapping the main threat detected button or the “1 malware detected” section, you will be taken to the Threat Center view, which will display tiles for all current threats.

5.2.1.5. Tapping the “i” button, you can get treat details. In our example, the Dropbox app has been blacklisted by your organization, and therefore; has been flagged as high risk.

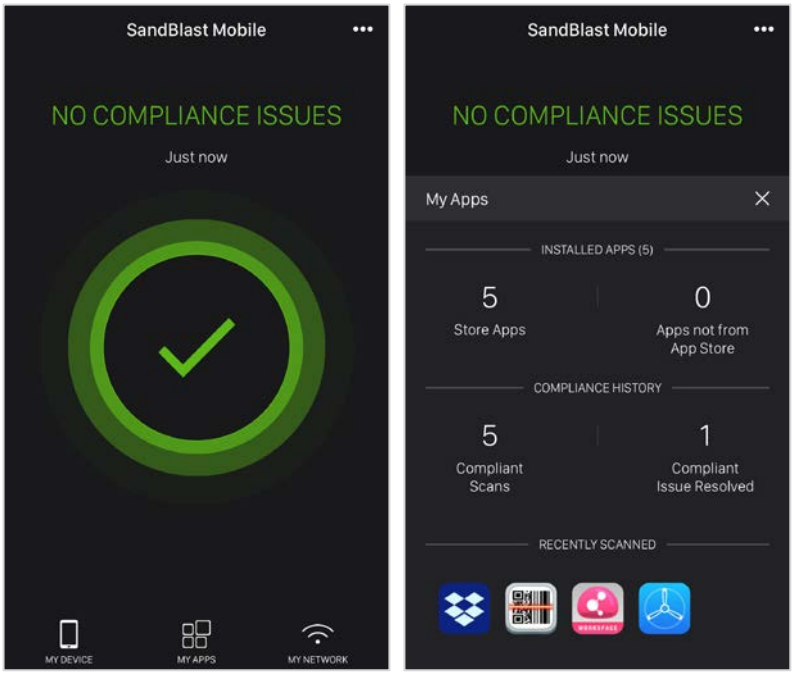


5.2.1.6. Holding down the Dropbox app, will cause it to wiggle and have an “x” appear in the top left corner of the Dropbox icon. Tapping the “x” will prompt the user to confirm the deletion of the app.



5.2.1.7. After the app is removed, the status will return to normal.

5.2.1.8. And tapping “My Apps”, you can see that the history of one malicious app being removed.

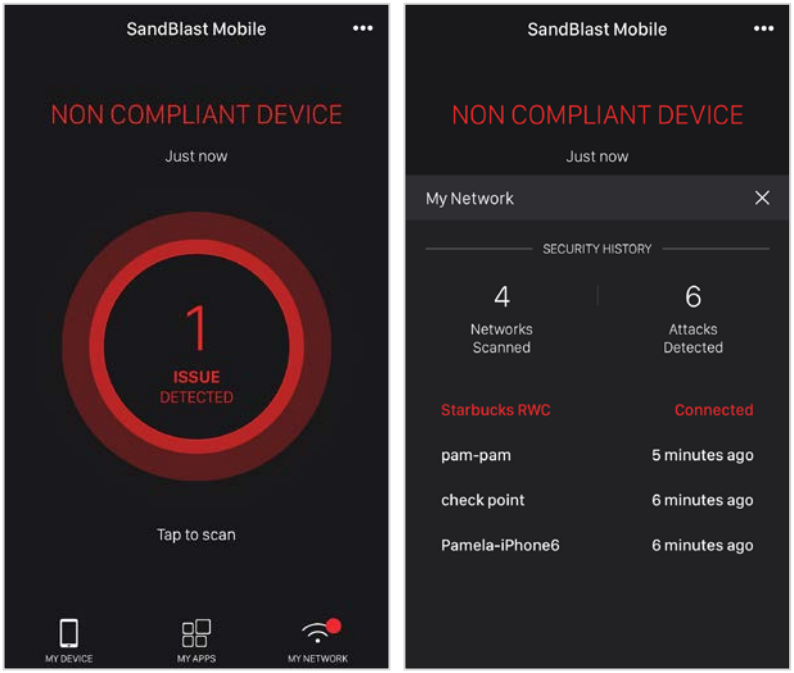


5.2.2 Network Protection (MitM Attacks)

5.2.2.1. Once you’ve entered the SandBlast Mobile Protect app, you’ll be informed regarding the existing policy violation (threat). The section is highlighted in Red below. Depending on the violation/threat, the app will suggest the required form of mitigation.

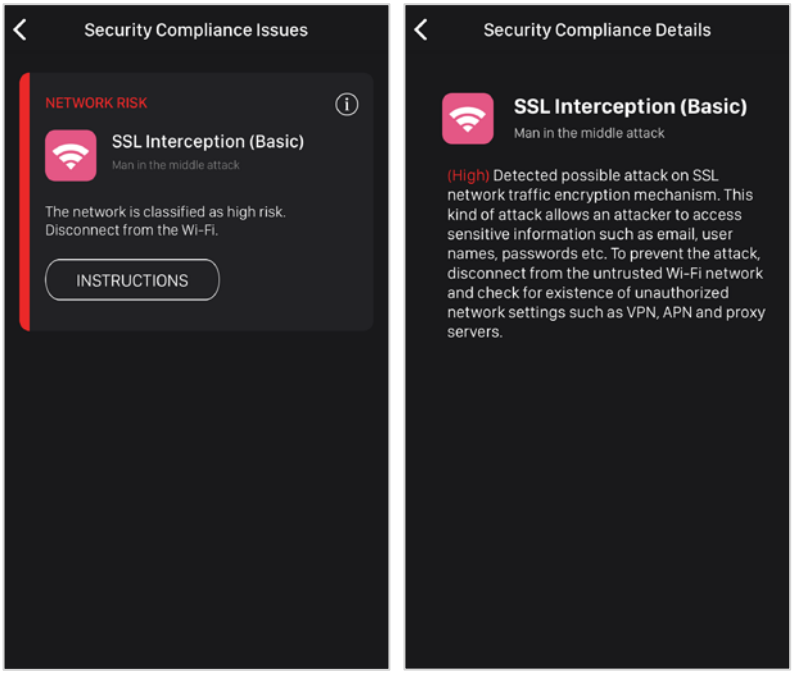
5.2.2.2. In our example, this device is connected to an unsecure Wi-Fi network that is exhibiting a Man-in-the-Middle attack.

5.2.2.3. Tapping on “My Network”, you can see that the currently connected Wi-Fi network is malicious.



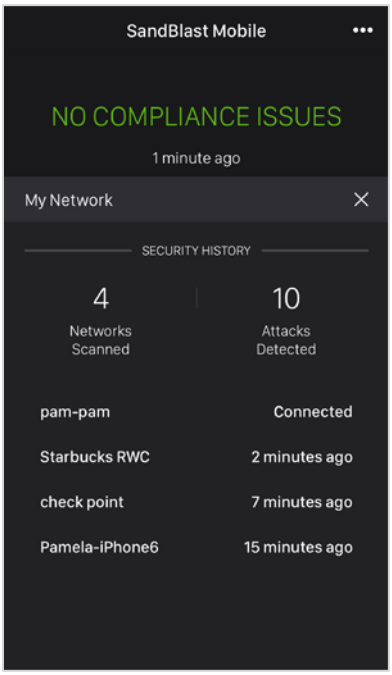
5.2.2.4. Tapping on the Threat Count or the **RED** network name, you will be brought to the Threat Center, which will have tiles for each threat.

5.2.2.5. Tapping the “i” icon on the right top corner of the tile will provide additional threat details.



5.2.2.6. The recommendation is to disconnect from the malicious network immediately by either turning off your Wi-Fi radio or by connecting to a secure network.

5.2.2.7. Once you disconnect from the malicious network, the device state will return to normal, and the “My Network” screen will show the network connection history.



5.2.3 SMS Phishing Protection

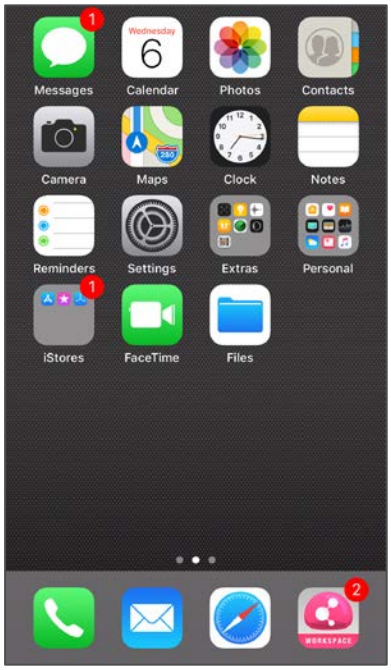
5.2.3.1. This is a new feature as of iOS 11.0. However, due to the limitations Apple imposes for accessing the messaging subsystem, and unlike with other protections that alert the user that a threat has been detected, Malicious Text Messages (URLs) do not alert.

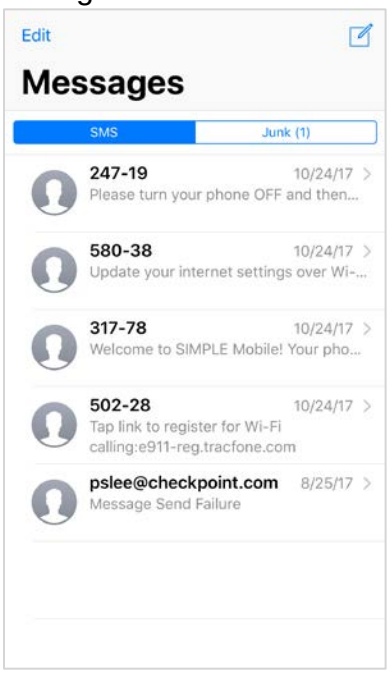
5.2.3.2. Instead they are filtered to the Unknown and/or Junk folder in Messages.

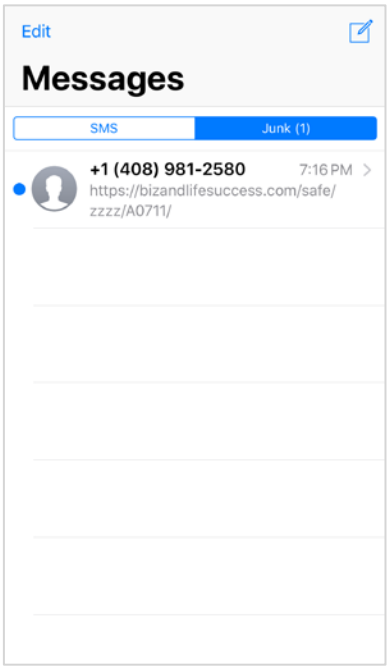
5.2.3.3. In our example, this device received a malicious link (URL) via SMS messaging.

5.2.3.4. Messages shows a badge, but no banner is displayed.

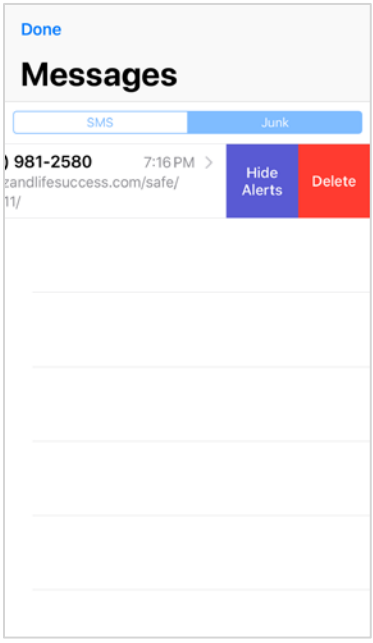
5.2.3.5. The malicious text message was filtered to the Junk folder.







5.2.3.6. Swiping left on the message will allow you to delete this conversation.



For more information, visit checkpoint.com/mobilesecurity

