Check Point
SOFTWARE TECHNOLOGIES LTD.

2021年5月12日

HARMONY MOBILE PROTECT APP FOR IOS

ユーザ ガイド

[Classification:Protected]

INFINITY VISION QUANTUM CLOUDGUARD HARMONY

Check Point Copyright Notice

© 2021 Check Point Software Technologies Ltd.

All rights reserved.本製品および関連ドキュメントは著作権法によって保護されており、その使用、複写、逆コンパイルを制限するライセンス契約に基づいて配布されています。本製品または関連ドキュメントのいかなる部分も、チェック・ポイントの書面による事前承諾を得ない限り、いかなる形態や方法によっても複製することはできません。本マニュアルを製作するにあたっては細心の注意が払われていますが、チェック・ポイントはいかなる誤りまたは欠落に対しても一切責任を負いません。本マニュアルおよびその記述内容は、予告なく変更される場合があります。

権利の制限

米国政府による本製品の使用、複写、または開示は、DFARS(連邦国防調達規定)252.227-7013およびFAR(連邦調達規定)52.227-19の技術データおよびコンピュータ・ソフトウェアに関する権利条項(c)(1)(ii)により制限されます。

商標

チェック・ポイントの商標の一覧は、コピーライトのページを参照してください。

サードパーティの商標および著作権については、サードパーティについてのページを参照してください。

重要な情報



最新版ソフトウェア

最新版ソフトウェアには、機能や安定性の向上、セキュリティの拡張、新たな脅威や進化する攻撃に対処する最新の保護機能が備えられています。常に最新版をインストールすることをお勧めします。



認証資格

サードパーティによるCheck Pointの認定資格については、Check Point Certificationsページを参照してください。



Check Point

このリリースに関する詳細については、ホームページを参照してください。



最新版ドキュメント(英語版)

Webブラウザでこのドキュメントの最新バージョンを参照してください。
PDF形式のドキュメントの最新バージョンをダウンロードしてください。



ドキュメントに関するご意見

チェック・ポイントは、わかりやすいマニュアルの作成に日々取り組んでいます。
ご意見やご要望がありましたら、ぜひ弊社までお送りください。

改訂履歴

日付	内容
2021年5月12日	SandBlast MobileからHarmony Mobileへ変更
2021年2月2日	初版

目次

このガイドについて *5*

ソリューション アーキテクチャ *6*

事前準備 *8*

インストール方法 *9*

手動ダウンロードとインストール *9*

IT部門によるUEMでの自動ダウンロード *9*

Harmony Mobile Protectアプリのインストール *10*

Apple App Storeからダウンロード *10*

Harmony Mobile Protectアプリのインストール *12*

Harmony Mobile Protectアプリの操作 *21*

状態1 - 脅威/ポリシー違反なし - デバイスは準拠 *21*

マイデバイス *21*

アプリ *22*

マイネットワーク *23*

状態2 - 脅威を検出 - ポリシー違反 *23*

アプリ保護(詳細アプリ分析) *23*

ネットワーク保護 *26*

このガイドについて

Check Point Harmony Mobileは、新たな第5世代のサイバー攻撃を防ぎ、従業員が安全に業務を行えることを実現するために設計された、最も完全な脅威防御ソリューションです。そのテクノロジーは、OS、アプリ、ネットワークに対する脅威から保護し、パフォーマンスやユーザエクスペリエンスに影響を与えることなく、業界で最も高い脅威の検出率を記録しています。

Harmony Mobileでは、次のような脅威防止テクノロジーを用意しています。

- 高度なアプリ分析を実行して、既知および未知の脅威を検出します
- セルラーネットワークとWiFiネットワークの両方に対する中間者攻撃を防止します
- メール、メッセージング、ソーシャルメディアなど、すべてのアプリに対するフィッシング攻撃をブロックします
- 感染したデバイスが機密データをボットネットに送信するのを防ぎます
- 感染したデバイスが企業のアプリケーションやデータにアクセスするのをブロックします
- ユーザのアクションやモバイル管理のプラットフォームに依存することなく脅威を軽減します

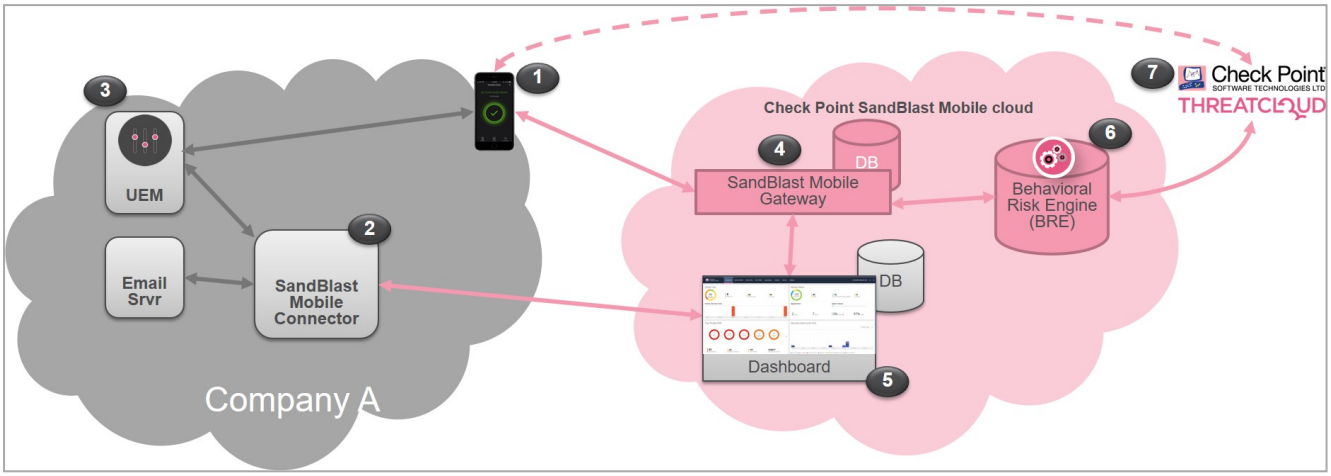
Harmony Mobileは、特許出願中のさまざまなアルゴリズムと検出の手法を使ってモバイルデバイスのリスクを特定し、適切な防御対応を行うことでビジネスデータと個人データを保護します。

Harmony Mobileソリューション(「ソリューション」)には、次のコンポーネントが含まれています。

- Harmony Mobile Behavioral Risk Engine(「エンジン」)
- Harmony Mobileゲートウェイ(「ゲートウェイ」)
- Harmony Mobile管理ダッシュボード(「ダッシュボード」)
- iOSおよびAndroid用のHarmony Mobile Protectアプリ(「アプリ」)

このガイドでは、Harmony Mobile ProtectアプリをiOSデバイスにインストールして使用するための必要な情報が含まれています。

ソリューション アーキテクチャ



#	コンポーネント	内容
1	Harmony Mobile Protect アプリ	Harmony Mobile Protectは、iOS®とAndroid™向けの軽量アプリで、業務環境におけるモバイルの脅威を検出および防御します。オペレーティング システム、アプリの情報、ネットワーク接続をモニタリングして、疑わしい動作や悪質な動作などを識別するクラウド ベース ソリューションへデータを送ります。 ユーザのプライバシーを保護するため、収集するデータは非特定化され、その中に潜むクリティカルなリスク インジケータをチェックします。 一部の分析はデバイス上で行い、詳細な分析はクラウド上で実行されます。これにより、ユーザの操作に影響を与えず、またデバイスのパフォーマンスへの影響とバッテリー消費を最小限に抑えることができます。
2	Harmony Mobile Connector (オプション)	Harmony Mobile ConnectorはWebベースのアプリケーションで、企業のデータ センター内でHarmony Mobile Dashboardとオンプレミス UEM(Unified Endpoint Management) ソリューション間の管理統合インタフェースの役割を果たします。
3	UEM	Unified Endpoint Management (MDM/EMMの一般的表現) デバイス管理とポリシー実施システム
4	Harmony Mobile Gateway	クラウド ベースのHarmony Mobile Gatewayは、モバイル デバイスを登録するマルチテナント アーキテクチャです。 ゲートウェイは、登録されたモバイル デバイスおよびお客様(組織) のダッシュボード インスタンスとのソリューション通信すべてを処理します。
5	Harmony Mobile Dashboard	クラウド ベースのWebGUIであるHarmony Mobile Management Dashboardは、デバイスとポリシーの管理、プロビジョニング、および監視を可能にし、お客様ごとのインスタンスとして構成されます。ダッシュボードは、リスクにさらされているデバイスに対して自動的にポリシーを適用するために、既存のUEMソリューションと統合できます。 この統合を使用すると、UEMは、ダッシュボードが登録済みのデバイスとIDを同期するリポジトリとして機能します。

#	コンポーネント	内容
6	Behavioral Risk Engine	クラウド ベースのHarmony Mobile Behavioral Risk Engineは、アプリから入手したネットワーク、構成、オペレーティング システムの整合性データに関するデータ、およびインストールされているアプリに関する情報を使用して、詳細なモバイル脅威分析を実行します。 エンジンはこのデータを使用して、疑わしいアクティビティを検出および分析し、脅威のタイプと深刻度に基づいてリスク スコアを生成します。 リスク スコアは、デバイスとそのデータを保護するために必要かどうか、そしてどのような自動緩和アクションが必要かを決定します。 エンジンで個人情報を処理したり保存したりすることはありません。
7	ThreatCloud	ThreatCloudにより、アンチフィッシング、セーフブラウジング、アンチボット、URLフィルタリングの技術をHarmony Mobileで実現させます。

事前準備

Harmony Mobile Protectアプリをインストールするには、次の準備を行います。

- iOS モバイル デバイス(iOSバージョン8.x およびそれ以降) 、デバイス上 のネット ワーク保護機能がアクティブな状態、10.xおよびそれ以降)
- モバイル デバイスまたはコンピュータからのエンタープライズEメール アクセス
- Unified Endpoint Management (UEM) Agent (オプション)

インストール方法

手動ダウンロードとインストール

このドキュメントでは、iOSデバイスを手動でインストールする方法とHarmony Mobile Protectアプリの操作について説明します。

IT部門によるUEMでの自動ダウンロード

VMware Workspace ONE UEMやMicrosoft IntuneといったUEMを使用している企業の場合、IT部門から自動的にHarmony Mobile Protectアプリをユーザのデバイスにプッシュすることができます。この場合は、Harmony Mobile Protectアプリの使い方に関するセクションを読んでください。

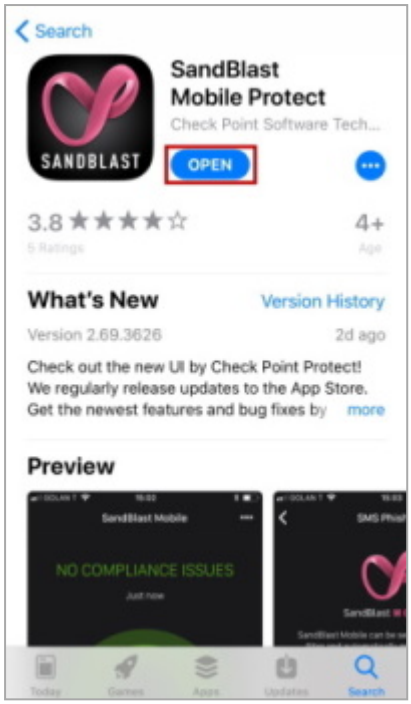
Harmony Mobile Protectアプリのインストール

Apple App Storeからダウンロード

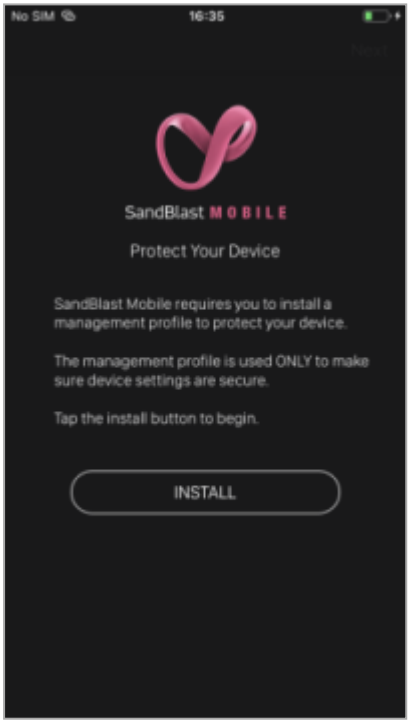
1. 登録Eメールまたは SMSのリンクを受信します。Eメールには、基本的な手順と登録に関する2つの重要な情報(サーバアドレスと登録キー) が記載されています。また、メールにはアプリをダウンロードするリンクと、デバイスでメールが読み取れない場合のQRコードも含まれています。
2. **ここからダウンロード**というリンクをタップするか、QRコードをスキャンすると、Harmony Mobile AppのApple App Storeページが開きます。



3. 確認メッセージが表示されたら、**開く**をタップします(App Storeにリダイレクトされます) 。
4. Harmony Mobile Protect Appをダウンロードして、ダウンロードが完了したら**開く**をクリックします。

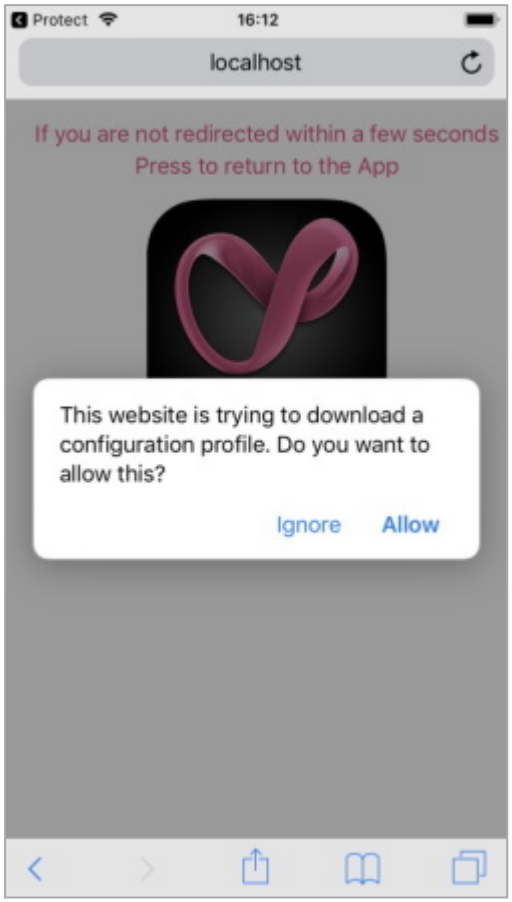


5. **インストール**をタップしてアプリの設定を開始します。

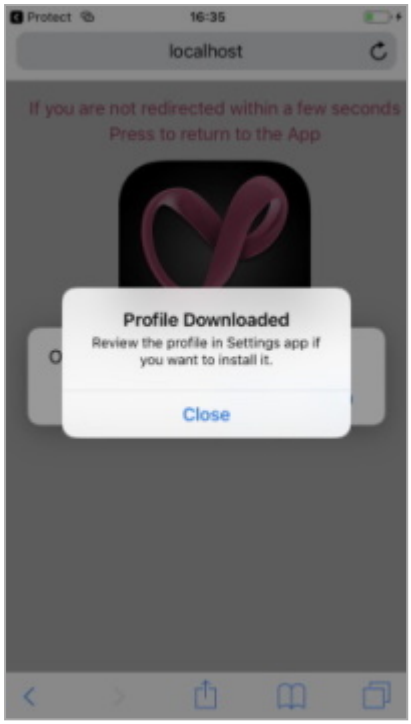


Harmony Mobile Protectアプリのインストール

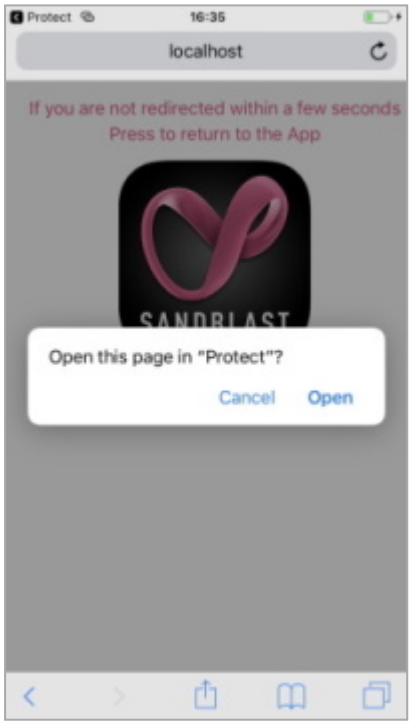
1. 設定プロファイルのインストールを許可します。**許可**をタップします。



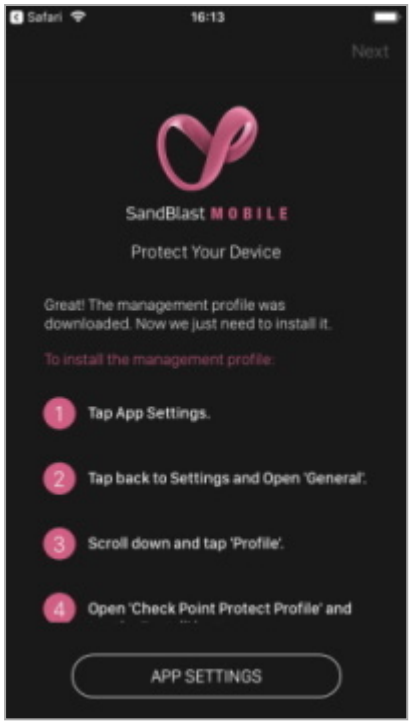
2. プロファイルをダウンロードした後、**閉じる**をタップしてアプリのインストールを続行します。



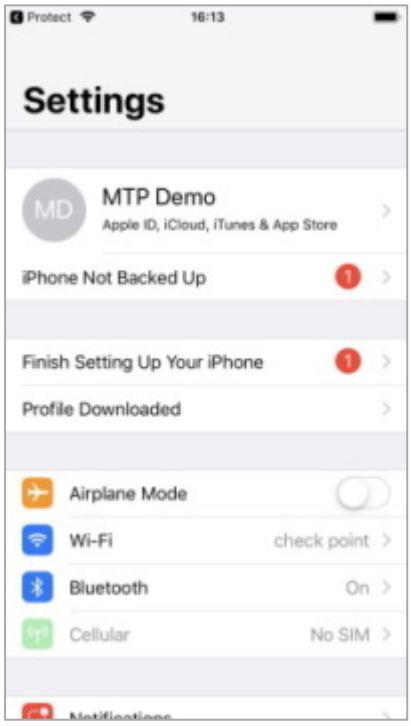
3. **開く**をタップしてHarmony Mobile Protectアプリを続けます。



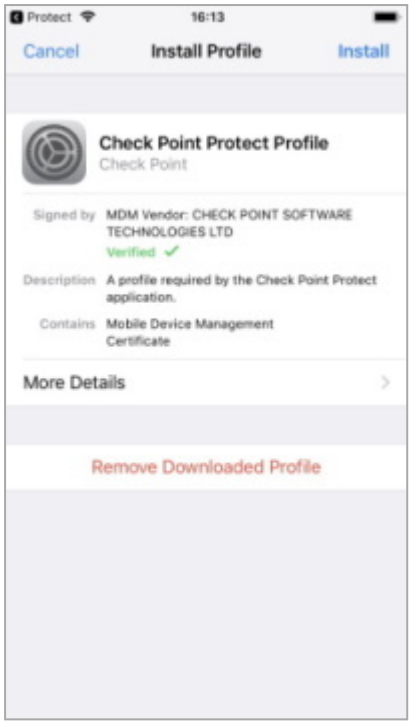
4. 画面の手順に従って設定プロファイルをインストールします。**アプリの設定**をタップしてiPhone設定にアクセスできるようにし、手順に従います。



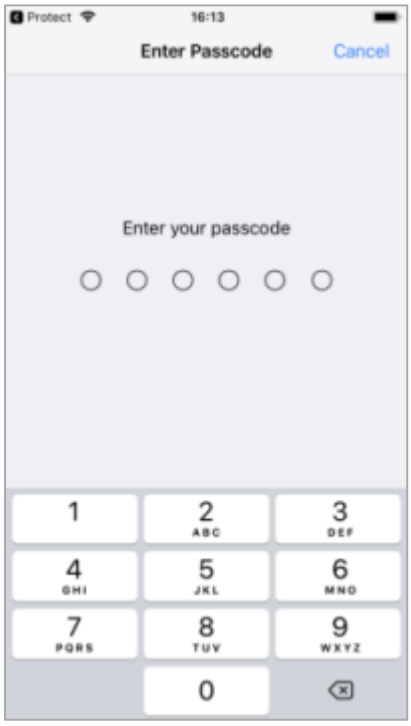
5. **プロファイルのダウンロード**をタップします。



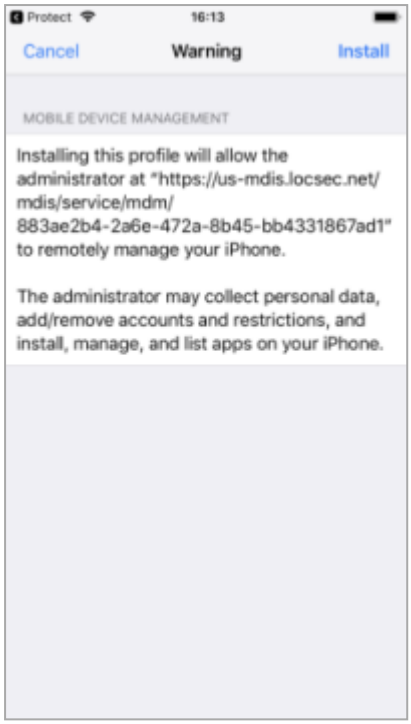
6. **インストール**をタップします。



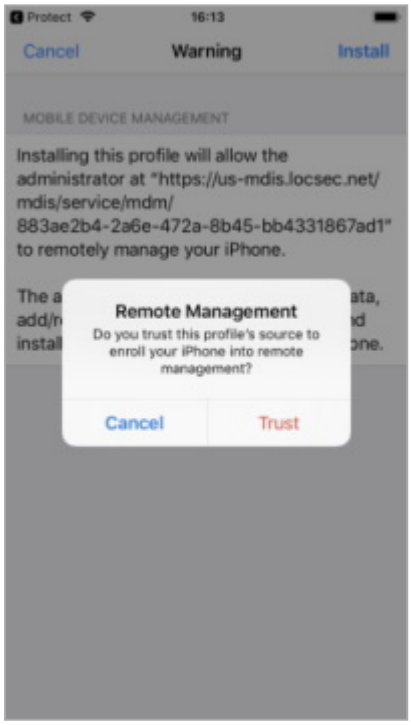
7. パスワードを入力します。



8. **インストール**をタップします。



9. **信頼**をタップします。

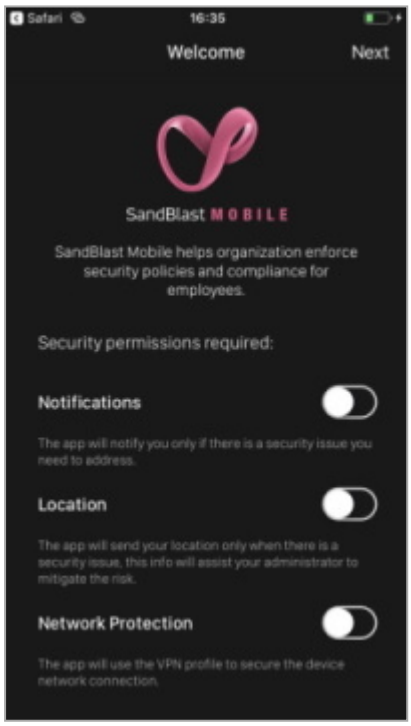


10. 終わったら、**終了**をタップします。



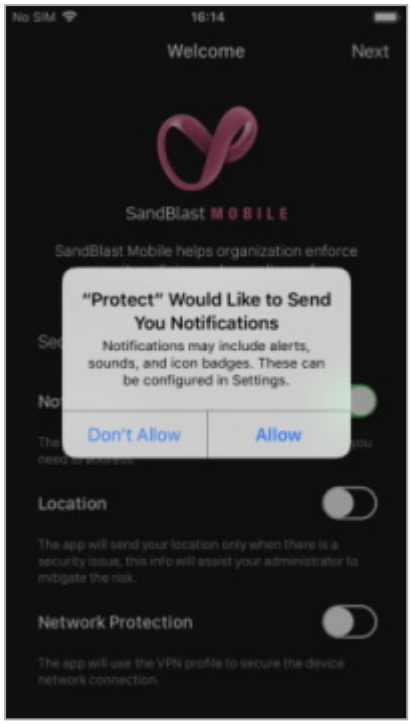
11. 通知、ロケーション、ネットワーク保護(ダッシュボードのポリシー設定に基づく)を有効にするメッセージが表示されます。

    権限を許可します。

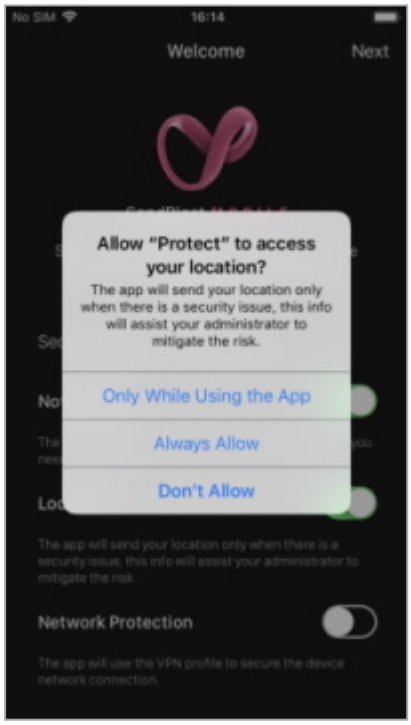


注 - Check Pointでは通知、ロケーション、ネットワーク保護を有効にすることを推奨しています。

12. **通知**をタップして**許可**をタップします。

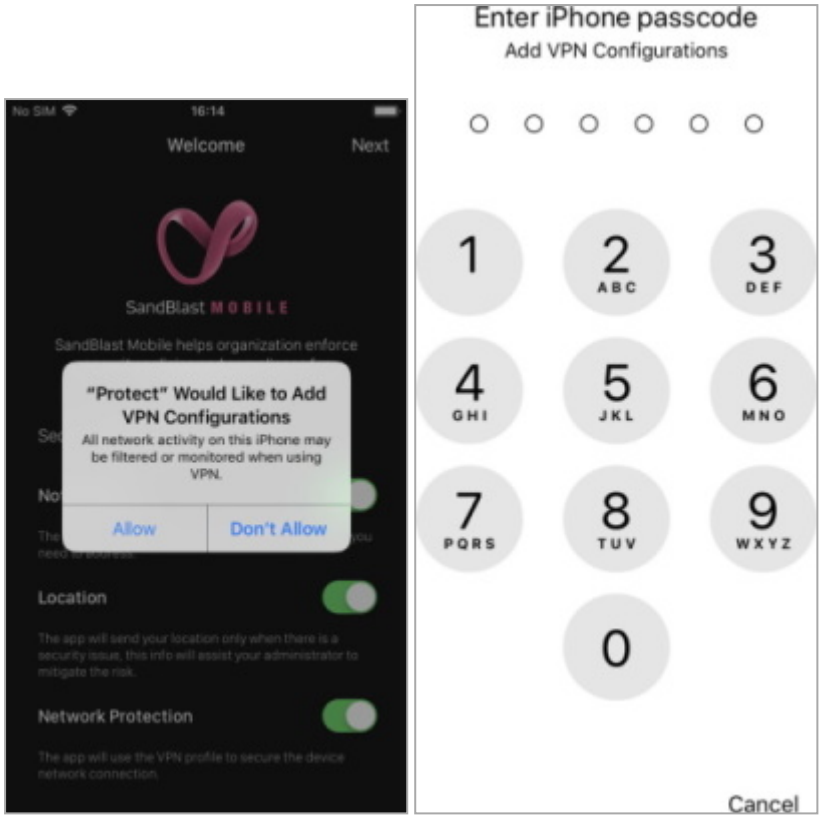


13. **ロケーション**をタップして**常に許可**をタップします。



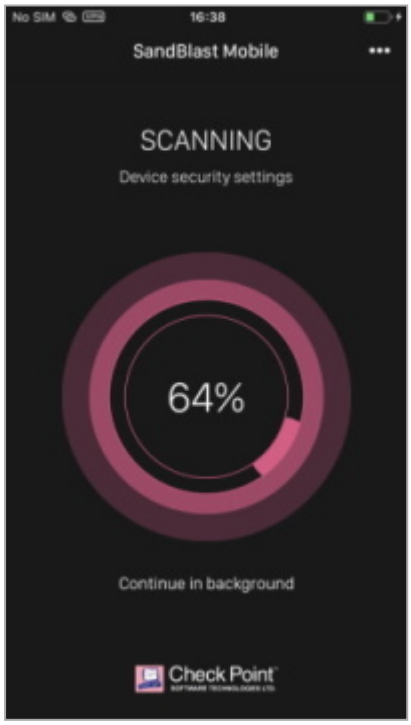
14. VPN設定を追加してデバイス上のネットワーク保護機能を有効にするよう勧めるメッセージが表示されます。

    許可をタップして、デバイスのパスコードを入力します。

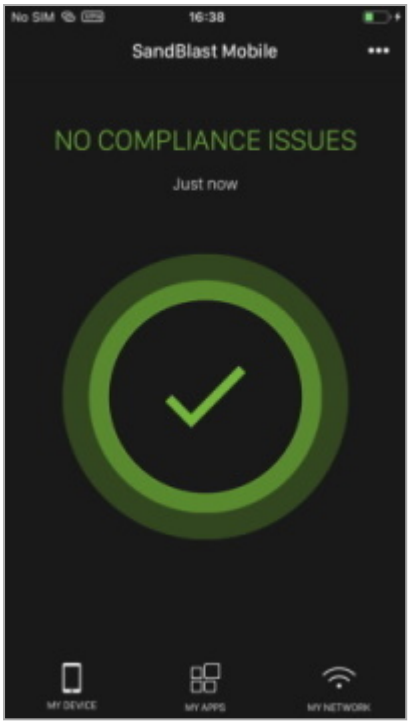


注意 - ユーザのプライバシーを守るため、VPNでトラフィックを外部に出すことはありません。すべてのデータはデバイスに保持され、宛先を確認するためだけにVPN機能を使用します。これにより、悪質な場所や不正な場所へデバイスがアクセスしないよう保護できます。

15. Harmony Mobile Protectでデバイスの初期スキャンを実行します。



Check Point Harmony Mobileによってデバイスが保護されています。


No SIM
16:38
SandBlast Mobile
NO COMPLIANCE ISSUES
Just now
MY DEVICE
MY APPS
MY NETWORK

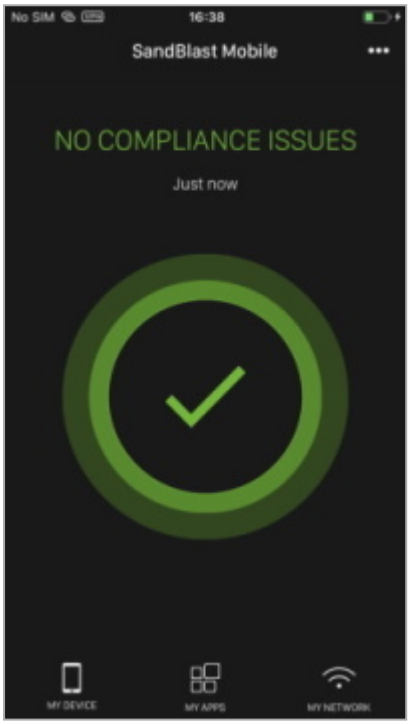
Harmony Mobile Protectアプリの操作

Harmony Mobile Protectアプリはメモリやパフォーマンスに影響することなく、バックグラウンドでシームレスに実行されます。Harmony Mobile Protectアプリを使うことで、モバイルの脅威から完全に保護され、またiOSデバイスの現行ステータスを視覚的に把握することができます。

お使いのiOSデバイスは、2種類の状態になる可能性があります。

状態1 - 脅威/ポリシー違反なし - デバイスは準拠

アプリのメイン画面にこの状態が表示されます。デバイスが保護された状態で脅威がない場合、アプリのメインページは緑色の状態になります。

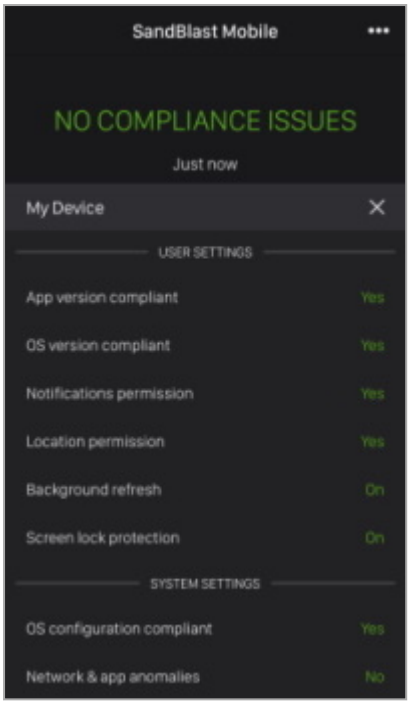


マイ デバイス

Harmony Mobile Protectのメイン画面下の左側にある**マイ デバイス**をタップして、システム設定の画面を確認します。

各設定をタップして、それぞれの設定情報を確認します。

はい/いいえまたは**オン/オフ**インジケータが緑色の場合は、設定が**OK**または**良**であることを示しています。赤色の場合は、設定がセキュリティポリシーに準拠していないことを示しています。設定を調整して、デバイスを可能な限り安全な状態にしてください。

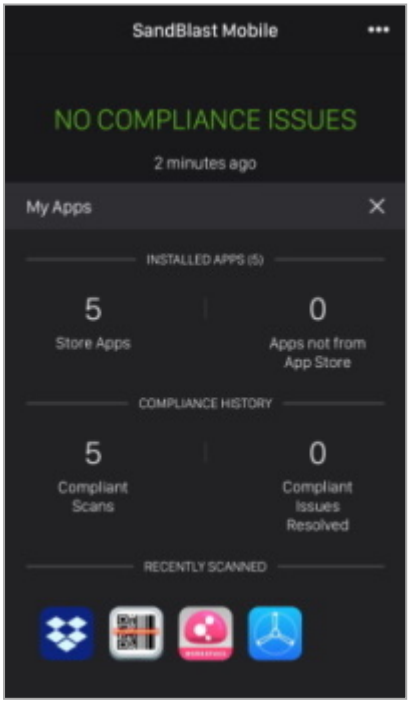


アプリ

Harmony Mobile Protectのメイン画面下の中央にある**アプリ**をタップして、デバイス上のすべてのアプリの概要画面を確認します。

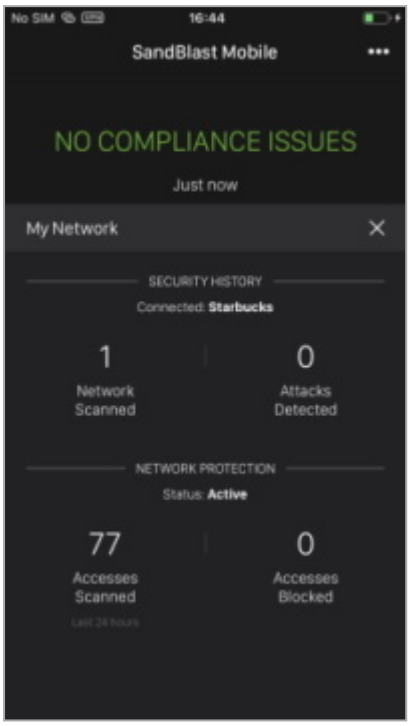
各番号をタップして、選択した並び替えでアプリリストを確認できます(App Store アプリ、システム アプリ、不明なソースなど) 。

Harmony Mobileで検出された悪質なアプリや削除されたアプリなどが確認できます。



マイネットワーク

Harmony Mobile Protectのメイン画面下の右側にある**マイネットワーク**をタップして、現在接続しているWi-Fiネットワークや、過去に接続していたWi-Fiネットワークの一覧を確認します。スキャンしたネットワークの数や、中間者攻撃と思われるような疑わしい動作がみられるネットワークの数の概要も確認できます。



状態2 - 脅威を検出 - ポリシー違反

マルウェアやネットワーク攻撃など、モバイル脅威やポリシー違反を発見すると、Harmony Mobile Protectアプリはその脅威をただちにユーザへ通知し、脅威を除去する処理を行います。

デフォルトでは2つの通知方法があります。

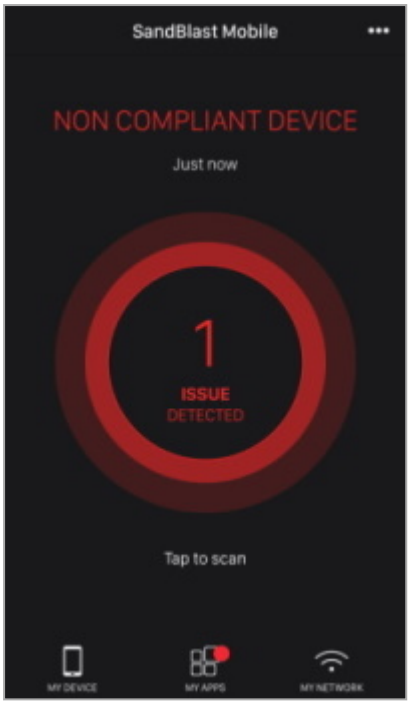
- 画面のポップアップ/バナー
- 通知センターでの通知

アプリ保護(詳細アプリ分析)

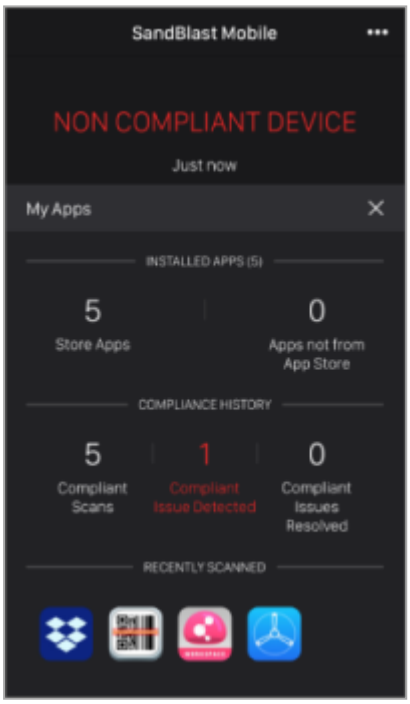
Harmony Mobile Protectアプリを開くと、現状のポリシー違反(脅威)に関する情報が確認できます。以下に赤くハイライトした部分です。ポリシー違反や脅威に基づいて、推奨される必要な対応方法が確認できます。

以下の例では、Harmony Mobile Protectアプリで疑わしいと思われるアプリが発見されています。

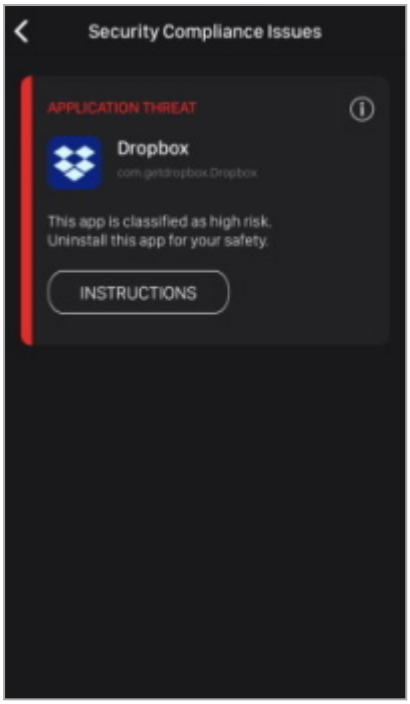
1. **アプリ**をタップすると、Harmony Mobile Protectアプリで1つのマルウェアが検出されているのがわかります。



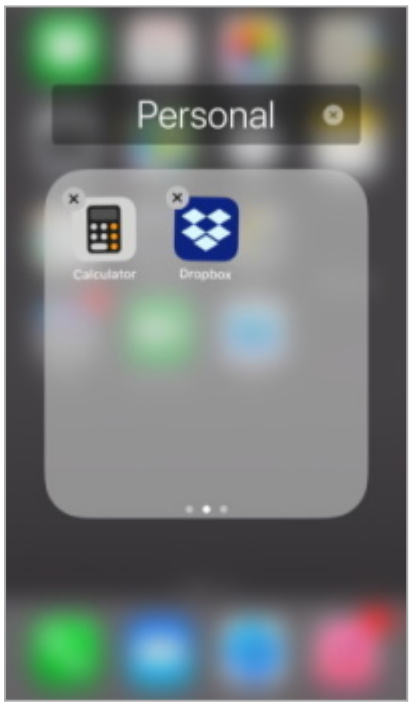
2. メインの検出された脅威をタップするか、**1件のマルウェアを検出**セクションをタップしてThreat Centerビューを開き、現在の脅威のタイトルをすべて確認します。



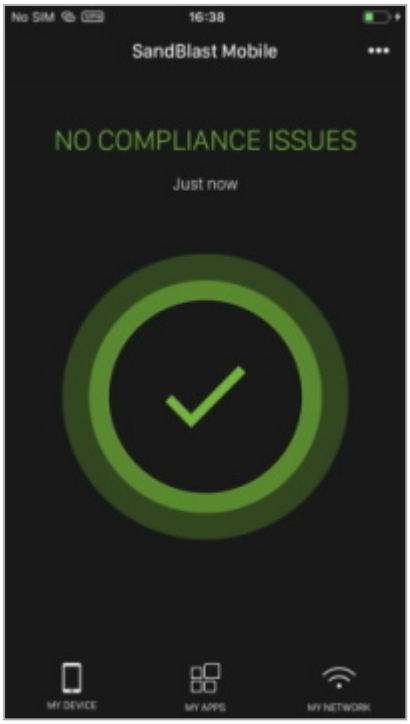
3. **i**をタップして脅威の詳細を確認します。この例では、Dropboxアプリが組織のブラックリストに載り、そのためハイリスクとして警告されています。



4. Dropboxのアプリアイコンを長押しします。アイコンが揺れて、**x**が上部左側に表示されます。**x**をタップして、アプリを削除します。



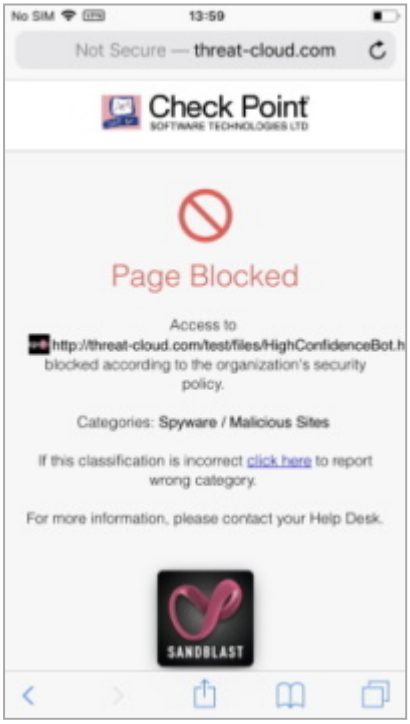
5. アプリを削除すると、ステータスが適切な状態に戻ります。



6. **アプリ**をタップすると、Harmony Mobile Protectアプリで1つの悪質なアプリが削除されているのがわかります。

ネットワーク保護

このセクションは、デバイス上のネットワーク保護機能(ローカルVPN) が有効な場合のみ関連します。以下の手順は、アンチフィッシングが作動しているときの防止メカニズムを表わしています。

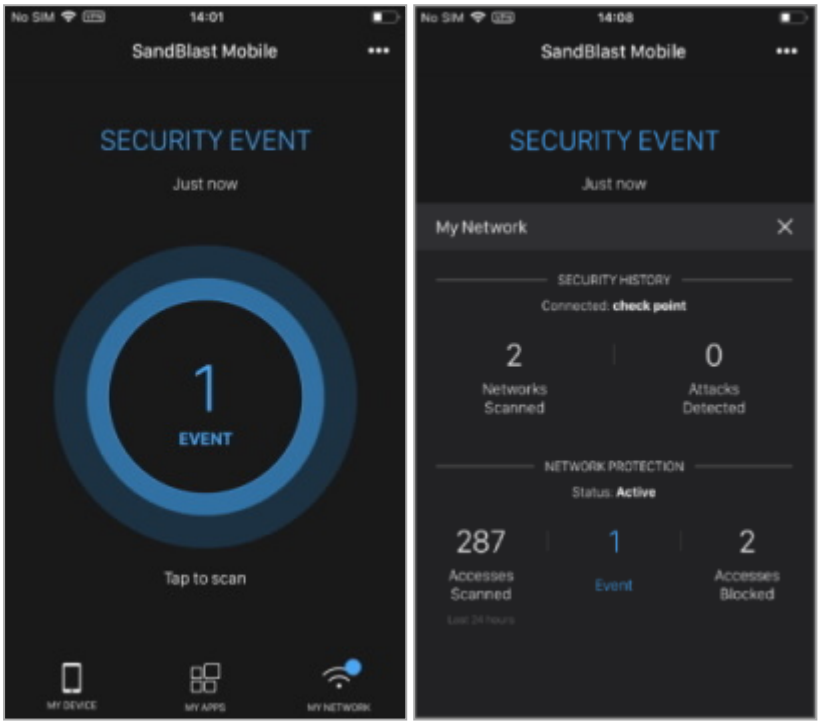


Harmony Mobile Protectアプリを開くと、現状のポリシー違反(脅威) に関する情報が表示されます。ポリシー違反や脅威に基づいて、推奨される必要な対応方法が確認できます。

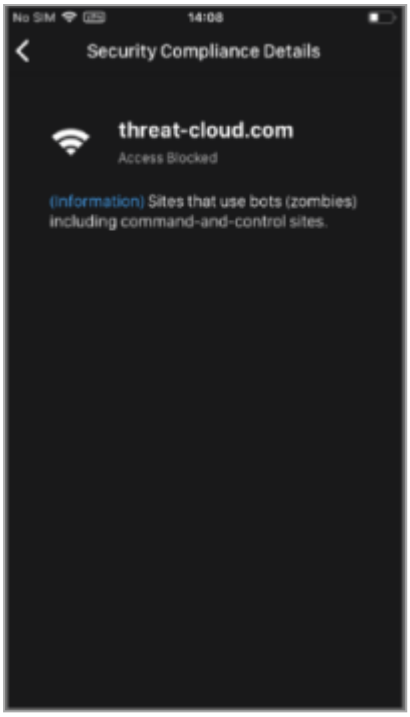
1. この例では、URL:
   http://threat-cloud.com/test/files/HighConfidenceBot.htmlを表示しています。
   Harmony Mobile Protectアプリで、悪質なURLを模倣するこのテスト ページへのアクセスがブロックされるのがわかります。

   重要 - このURLは悪質ページを模倣しています。このURLを通常のコンピュータで開くと、インストールされている保護ソフトウェアがトリガされます。

2. Harmony Mobile Protectアプリのセキュリティ イベントを確認します。
3. **マイネットワーク**をタップして、青色になった1件のイベントを確認します。青色は、情報のアップデート イベントを表わしています。攻撃は防御され、リスクは現在ありません。



4. このイベントをタップすると、脅威に対しどうセキュリティ ポリシーが適用されているか確認できます。



5. タイトル上部の右側にあるiアイコンをタップして、脅威の詳細を確認します。

