Lookout Mobile Endpoint Security

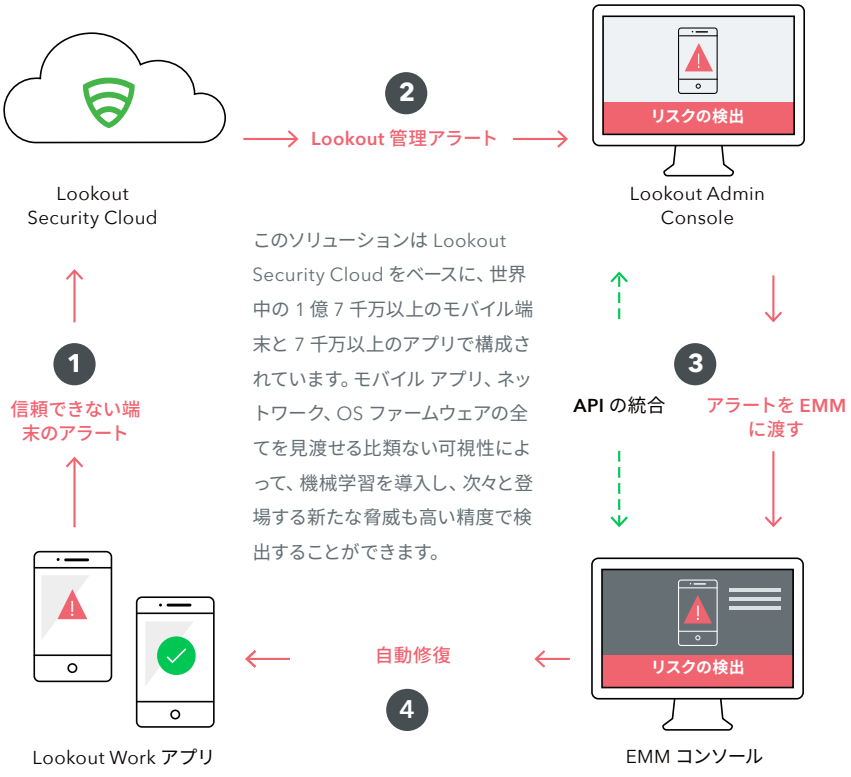
Lookoutでモバイルのセキュリティギャップを解消

概要

現在、さまざまな組織で、現場での生産性を向上させるため、スマートフォンやタブレットの導入が進んでいます。この動きに伴い、モバイル端末上で機密データが操作される機会も増えているので、自社のセキュリティポリシーの適用対象をモバイルのエンドポイント端末にまで拡張する必要があります。Lookout Mobile Endpoint Security は、モバイル リスクの範囲全体を簡単に可視化し、そのリスクをポリシーの適用によってある程度まで低下させ、既存のセキュリティおよびモバイル管理ソリューションに統合することができます。

保護の仕組み

Lookout Mobile Endpoint Security は従業員の端末上で軽量のエンドポイントアプリを使用する、クラウドベースの管理コンソールであり、モバイルリスクをリアルタイムで可視化し、最新の Enterprise Mobility Management（EMM）ソリューションと統合することができます。



メリット

リスクの大幅な減少

Lookout の分析とレポートの機能によって、大規模なセキュリティ ギャップを埋め、リスクを減少させます

シームレスな相互運用性

Lookout は Splunk、Windows Defender ATP、Micro Focus、ArcSight、IBM Security、QRadar など、すべての SIEM システムを Mobile Risk API によって統合します

モバイル インシデントの可視性

モバイル端末上のインシデントにリアルタイムの可視性を持たせ、迅速かつ効率的に対応できるようにします

モバイルセキュリティ対策

BYOD をはじめとする柔軟なモビリティ プログラムをさらに取り入れ、従業員の生産性を高め、競合上の優位を維持します

プライバシー バイ デザイン

プライバシー管理機能を使用して、データの独立性と従業員のプライバシー ポリシーが保たれていることを確認します

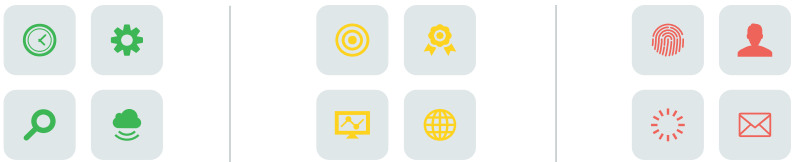
導入/運用が簡単

あらゆる EMM（VMware Workspace ONE® UEM、Microsoft Intune、BlackBerry® UEM、IBM MaaS360®、MobileIron など）と統合が可能なので、導入や運用はシンプルな手順で進められます。

Mobile Endpoint Security で脅威に備える

モバイル端末による機密データへのアクセスが増加するにつれ、機密データが攻撃の対象となることが増えています。Lookout Mobile Endpoint Security では、次のような主な攻撃ベクターを対象としたモバイルの脅威を特定します。

- アプリベースの脅威:マルウェア、ルートキット、スパイウェア
- ネットワークベースの脅威:中間者攻撃
- 端末ベースの脅威:ジェイルブレイク/ルート化端末、古い OS、危険な端末設定



機密に触れる可能性のない振る舞い

機密に触れる可能性のある振る舞い

悪意のある振る舞い

Mobile Endpoint Security でアプリのリスクに備える

一部の iOS および Android アプリは悪意のあるものではありませんが、機密に触れるような振る舞いや脆弱性を含む場合があり、組織のセキュリティポリシーに抵触、またはデータ喪失に関わるような規定違反がある場合があります。Lookout では、このようなアプリのリスクをモバイル端末上で包括的に確認できるため、管理者は社内要件または規定要件違反となるリスクの高いアプリを監視し、これに対処するポリシーを設定することができます。

Lookout の特徴

- Lookout では、グローバルな規模、およびモバイルにフォーカスした世界最大級のモバイル セキュリティデータセットを蓄積しています。Lookout は世界各国の 1 億 7 千万以上の端末と 7 千万以上のアプリからセキュリティデータを収集しており、1 日あたり 9 万のアプリが新たに追加されています。
- このグローバル センサー ネットワークでは、リスクを示す複雑なパターンをマシンインテリジェンスで検知することによって、プラットフォームでの予測を可能にしています。人による分析のみでは、このようなパターンは見落とされてしまうでしょう。
- モバイルはコンピューティングの新しい時代を象徴するものであり、このプラットフォーム専用のセキュリティソリューションも刷新することが求められています。Lookout は 2007 年からモバイルをセキュリティ保護しており、この分野の専門技術を備えています。

Lookout を利用すれば、ITを可視化し、セキュリティチームのニーズを満たしながら、生産性を低下させることなくモバイルのセキュリティ対策をすることが可能になります。モバイル機器を今すぐセキュリティ保護する方法については、lookout.com/jp までお問い合わせください。

Lookout Mobile Endpoint Security
脅威に対抗する Mobile Endpoint Security
アプリベースの脅威からの保護
マルウェア
ルートキット
スパイウェア
ランサムウェア
ネットワークベースの脅威からの保護
中間者攻撃
SSL 攻撃
デバイスベースの脅威からの保護
高度なジェイルブレイク/ルート化の検出
オペレーティング システムの脆弱性
危険な端末設定
Web およびコンテンツベースの脅威からの保護
あらゆるチャネルからのフィッシング攻撃
危険な Web サイトに誘導する悪意のある URL
カスタムの脅威ポリシー
脅威ダッシュボード
アプリのリスクに対抗する Mobile Endpoint Security
次のようなアプリからの情報漏えいの制御:
カレンダーなどの機密データへのアクセス
機密データ(PII)の外部への送信
クラウドサービスとの通信
安全でないデータの保管/転送
危険なアプリ ダッシュボード
危険なアプリに関するカスタム ポリシー
アプリのブラックリスト化
企業向けアプリのレビュー
管理およびサポート
EMM 統合 (VMware Workspace ONE® UEM、Microsoft Intune、Blackberry® UEM、IBM MaaS360®、MobileIron)
Mobile Risk API による SIEM 統合 (Splunk、Windows Defender ATP、Micro Focus、ArcSight、IBM Security、QRadar)
経営層向けにリスクの低下を示すレポート
ロールベースのアクセス制御
データ プライバシー制御
年中無休のサポート