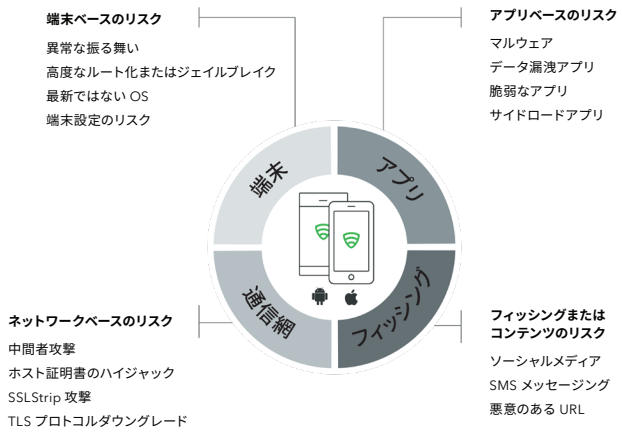
Lookout + Microsoft Partnership

Lookout + Microsoft による企業での安全なモバイル活用

概要

組織はモバイル管理ポリシーを採用してモバイルの生産性を強化していますが、脅威が高度化する現状では、企業データと資産を保護することはかつてなく困難になっています。iOS と Android 端末における Lookout のモバイル保護と Microsoft のモバイルおよびセキュリティソリューションを組み合わせることにより、組織はモバイル端末がアクセスする機密データを保護しつつ、従業員の生産性を高めるためのモバイルファースト、クラウドファーストのアプローチを採用することができます。



包括的なモバイル セキュリティ

Lookout は、自社のクラウドベースの脅威情報を活用して、全てのモバイル リスクから保護します。たとえば、以下のものを検知および保護をします。

- メール、SMS、メッセージング、アプリでのフィッシング
- サイドローディングでインストールされた悪意のあるアプリケーション
- OS、設定、およびルート化/ジェイルブレイクのリスク
- ネットワーク攻撃および中間者攻撃

Lookout + Microsoft Azure Active Directory (AAD) と Intune

リスクベースの条件付きアクセス

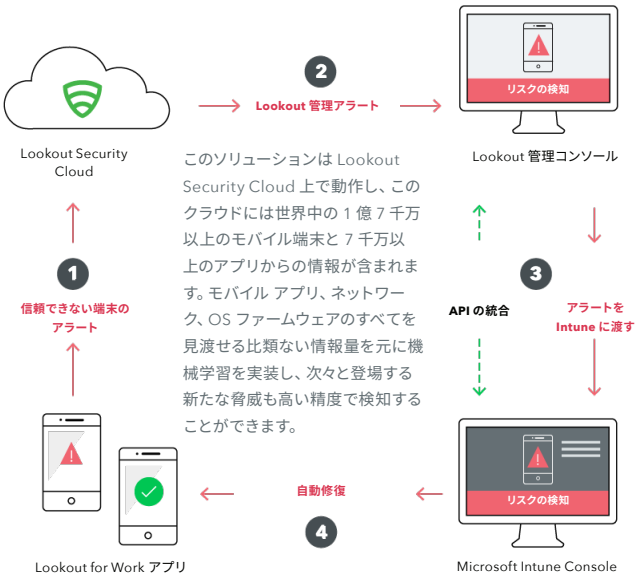
Microsoft EMS と Lookout の連携により、Lookout は、悪意のあるアプリケーション、OS の脆弱性、ネットワーク攻撃、フィッシング攻撃、GDPR ポリシーに違反するアプリケーションなどの端末リスクを Intune に通知できます。これらのアラートは Intune 管理コンソールに統合されており、コンプライアンス違反が修復されるまで危険な端末が企業リソースにアクセスするのを防ぐ条件付きアクセスポリシーを実施するために使用できます。

使いやすさ

Lookout と Azure Active Directory の連携により、Microsoft Intune を介した Lookout クライアントアプリのシームレスな導入と管理が可能になります。これは、ユーザーとグループの統合ポリシー管理と、エンドユーザーと管理者のシングル サインオンを実現する AAD との連携ソリューションです。

セキュリティとコンプライアンス

Lookout アプリケーション コンプライアンス機能により、組織は企業のセキュリティ ポリシー、プライバシー ポリシー、ガバナンス ポリシーに違反するモバイル アプリケーションを発見できます。たとえば、ユーザーの連絡先情報リストや場所を公開するアプリケーションをブラックリストに登録してレポートし、条件付きアクセス ポリシーを施行するために利用状況情報を Intune に送信できます。



Lookout + Microsoft Windows Defender ATP

Windows 端末と連携されたモバイル セキュリティ端末アラート

Lookout の Mobile Endpoint Security ソリューションは、Microsoft の Windows Defender Advanced Threat Protection (ATP) と連携することができます。この連携により、Microsoft のカスタマーは、Windows Defender ATPの管理コンソール内から iOS と Android 端末上の高度なサイバー攻撃やデータ侵害の検知、表示、調査、対応ができます。統合コンソールは、Lookout 端末の脅威と正常性の情報をメイン ダッシュボードとサブセクション全体に公開し、完全に統合された単一の管理画面でシームレスなワークフローを体験できます。

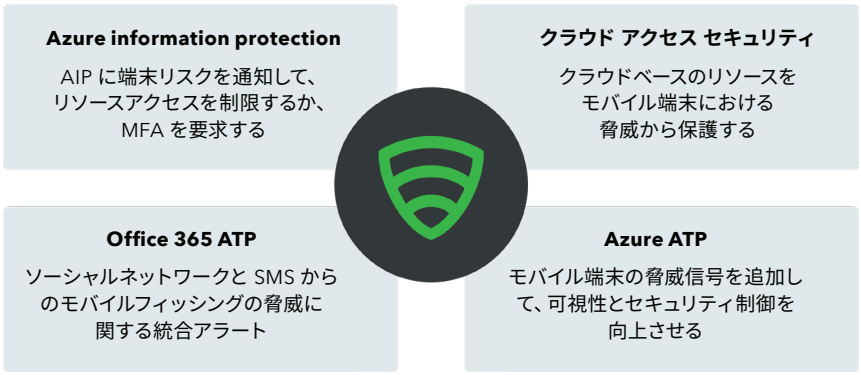
モバイル脅威に対する可視性の強化

- モバイルアラート用の統合コンソール
- 脅威の概要を示すダッシュボード
- ユーザー端末間の相関関係
- 脅威アラートの詳細と修復
- モバイル端末のイベント履歴のタイムライン

Lookout + Microsoft Graph Security API

Microsoft の高度なセキュリティ ワークロードにモバイル端末脅威データを提供

Lookout と Microsoft Graph Security API の統合により、カスタマーは Microsoft Graph に接続されたアプリケーションのエコシステムから Lookout モバイル脅威テレメトリの照会、受信、関連付け、レポートができます。Lookout テレメトリは、Microsoft 製品、サービス、セキュリティ ソリューション全体からの他の脅威情報とセキュリティ シグナルだけでなく、サードパーティの Microsoft Graph プロバイダーからのシグナルも組み合わせて、サイバー脅威の特定と対処ができます。



独自の強力な脅威テレメトリ

- 正常な端末のみが企業リソースにアクセスできるようにする
- 脅威信号を活用して条件付きアクセスを通知する
- フィッシング アラート信号が他の ATP アラートに活用される
- モバイル信号を他の Microsoft に統合する

Lookout が選ばれる理由

Microsoft と Lookout はパートナーシップを結び、企業内利用においてスマートフォンとタブレットを安全に使用できるようにします。Lookout は、新たな脅威を迅速に検知して対応するため、機械学習技術を大規模なセキュリティ データセットに適用するという Microsoft と同じビジョンを持っています。Lookout は世界中の 1 億 7 千万以上の端末からセキュリティ データを収集し、高度な機械学習技術を使用して 7 千万以上の iOS および Android アプリを分析し、これらのプラットフォームのリスクを特定してきました。Lookout は、先駆的な Microsoft Partner として、以下のような、価値ある Microsoft 統合を数多く開拓してきました。

- **Microsoft Intune と Enterprise Mobility + Security** Azure Active Directory を使用したシームレスなアクティベーションにより、Lookout はリアルタイム ネットワークおよび端末ベースのリスクに基づいて Lookout Continuous Conditional Access を実施します。
- **Microsoft Windows Defender ATP** この統合により、Microsoft のカスタマーは、WDATP 管理コンソール内で iOS および Android 端末上のサイバー攻撃やデータ侵害の検知、表示、調査、対応ができます。
- **Microsoft Intelligent Security Graph** Lookout テレメトリ ベースのモバイル脅威イベントを共有するシームレスな統合を実現します。
- **Microsoft Intune MAM** Lookout は、モバイル端末の正常性を評価し、MAM 対応アプリへの Continuous Conditional Access を実施します。

Microsoft EMS + Lookout についての詳細は、 lookout.com/microsoft をご覧ください。