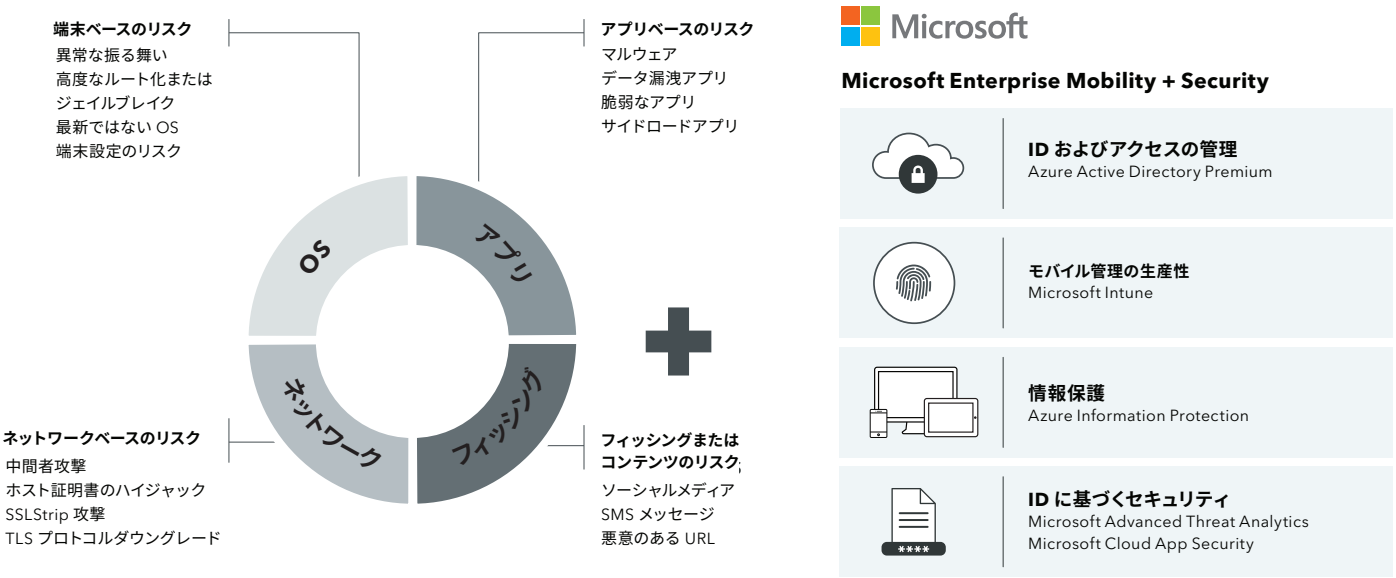
Lookout + Microsoft

企業における安全なモバイル活用を実現するためのパートナーシップ

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する企業が増加していますが、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。Lookout および Microsoft Enterprise Mobility + Security (EMS) を使用すると、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可能にすることができます。



Lookout + Microsoft EMS の主なメリット

生産性を高める包括的なモバイル セキュリティ

Microsoft EMS は、このモバイルファースト、クラウドファースト時代におけるセキュリティの課題に対して総合的なアプローチを取れる、ID に基づくセキュリティ ソリューションを提供します。Lookout は、端末への脅威を継続的に監視し、その情報を EMS に直接渡して条件付きアクセスポリシーが適用されることにより、EMS の ID ベースのセキュリティを、豊富なモバイル脅威情報によって補完します。Lookout は、次の 4 つの攻撃ベクトルの脅威から保護します。

1. アプリベースの脅威: 機密データを漏洩するトロイの木馬、スパイウェア、ルートキット、非準拠アプリ
2. ネットワークベースの脅威: 暗号化された転送中のデータを盗むフィッシング、中間者攻撃、SSL 攻撃
3. OS ベースの脅威: iOS 端末の高度なジェイルブレイクと Android 端末のルート化
4. フィッシングおよびコンテンツの脅威: 個人用および仕事用のメール、メッセージ、SMS、アプリでのフィッシング攻撃

リスクベースの条件付きアクセス

Intune 内で条件付きアクセスポリシーを実施すると、セキュリティとコンプライアンスを確保するカスタマイズ可能な要素 (場所、端末とユーザーの状態、アプリケーションのリスクなど) に基づいて、企業のメール、ファイル、およびその他のリソースを不正アクセスから保護できます。Microsoft EMS と Lookout の統合により、Intune で定義した条件付きアクセスポリシーに Lookout の脅威情報を組み入れて、Office のモバイルアプリなどのアプリへのアクセスを管理および保護し、端末からデータを選択的にワイプする措置を取ることができます。

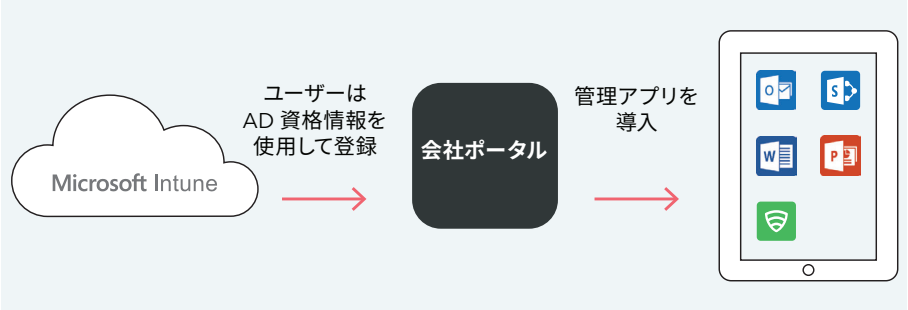
使いやすさ

Lookout と EMS 間の連携により、Microsoft Intune を介した Lookout のクライアントアプリのシームレスな導入と管理、ユーザーとグループの統合ポリシー管理、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 Azure Active Directory との統合 ID が可能になります。

連携の仕組み

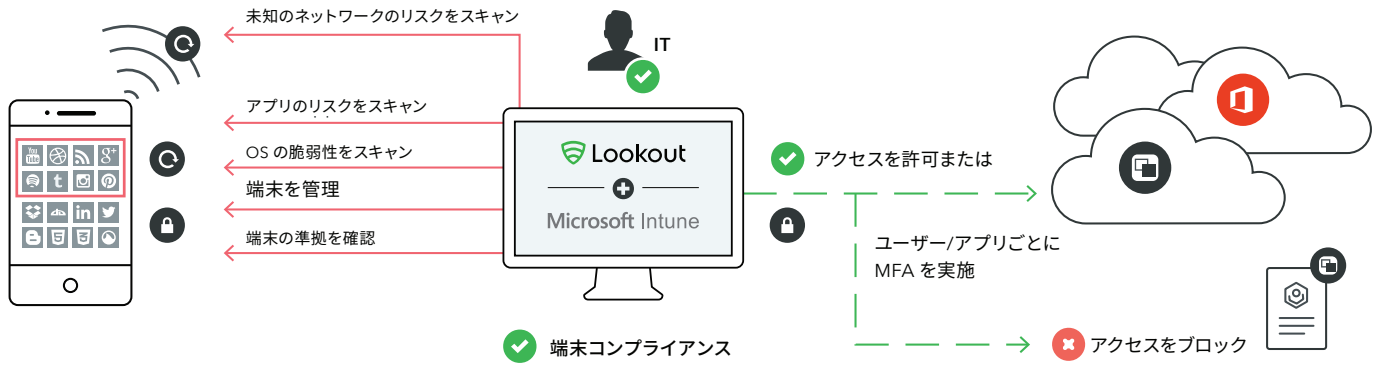
端末プロビジョニング

Microsoft Intune を使うと、Lookout のエンドポイントアプリをモバイル端末に簡単に配信することができます。迅速でスケーラブルな端末プロビジョニングが可能になります。



リスクベースの条件付きアクセス

Lookout では、悪意のある脅威や機密データを漏洩するアプリの存在を可視化し、端末のコンプライアンス状態を Intune の評価で知らせます。たとえば、財務部門の従業員が悪意のあるモバイルアプリケーションをそれと知らずにダウンロードした場合、Lookout はこの脅威を特定し、Intune の条件付きアクセスポリシーをトリガーして、その脅威が修復されるまで企業データへのアクセスを制限します。



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