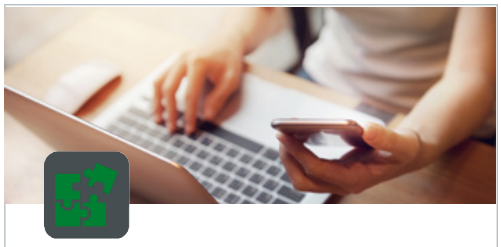
MTD と EMM を同時に導入することが道理にかなっている理由

数回クリックするだけでモバイルの脅威に対する保護を追加可能

モバイル管理におけるサイバーセキュリティの課題

現代のビジネスでは、従業員が頻繁にモバイル端末を使用して働いています。このため、組織はモバイル従業員にクラウドベースの企業データへの安全で柔軟性のあるアクセスを提供する必要に迫られています。従来、モバイル機器を安全に保つために、組織はエンタープライズ モビリティ管理 (EMM) ソリューションをモバイル エンドポイントを保護する解決策として導入してきました。ただし、EMM ソリューションだけでは、モバイル サイバーセキュリティの脅威に対する可視性や保護を提供できません。むしろ、EMM ソリューションは組織が紛失/盗難端末の消去や企業アプリの配信などの端末管理タスクを実行できるようするためのものです。包括的なモバイル セキュリティを実現するため、組織は EMM と同時にモバイル脅威対策 (MTD) を実装する必要があります。



重要なポイント

1. EMM にはモバイル脅威に対する可視性がありません
2. MTD は、モバイル フィッシング、アプリ、端末、およびネットワークの脅威に対する保護を提供します
3. EMM と MTD の統合により、高度なモバイル セキュリティ態勢を提供します

組織内の安全なモバイル活用の実際の使用例

エネルギー管理ソリューションを提供する業界リーダーは、大手の EMM プロバイダーに勧められて、EMM の導入と同時に Lookout Mobile Endpoint Security を統合しました。EMM ベンダーがモバイルの脅威に対する保護として Lookout を推奨し、EMM 実装が最小限の手間でできることが分かると、その組織は Lookout の導入に踏み切りました。その組織は IT リソースの制約に直面していたため、必要なユーザー トレーニングが最小限であることや、iOS および Android 端末へのサイバーセキュリティの導入がシームレスであることに満足しました。Lookout の実装は情報セキュリティ チームが規定した要件を満たすだけでなく、モバイル フィッシング、アプリ、端末、およびネットワークベースの脅威に対する包括的な可視性を提供し、高度なモバイル セキュリティ戦略も可能にしました。

Lookout の重要な機能

Lookout Mobile Endpoint Security は、アプリ、端末、ネットワークベースの脅威に対して安全性を確保するために、iOS および Android 端末全体にわたって包括的かつ継続的なリスク評価を提供します。モバイル端末の健全性を継続的に監視することにより、Lookoutは「高、中、低」のリスクレベルを割り当て、その情報を EMM に渡すことができます。これにより、カスタム ポリシーを実行して、デバイスのリスク許容範囲に基づいて企業リソースへのアクセスを拒否することができます。これにより、許可されたユーザーが正当なデータにアクセスすることだけでなく、それらの端末のリスク レベルが許容範囲内であることも確証します。

Lookout が選ばれる理由

Lookout Mobile Endpoint Security では、世界各国の 1 億 7 千万以上の端末から収集した膨大なデータセットと、7 千万以上のモバイルアプリの分析結果を活用して、端末のセキュリティとコンプライアンスを常に確保することが可能です。また、Lookout Security Cloud を利用すれば、Lookout の導入から、管理対象・非管理対象端末を含めた組織全体へのセキュリティ ポリシー適用までを簡単に行うことができます。ユーザーは、悪意のあるアプリ、ネットワーク接続状況、OS レベルのシステム異常に関するアラートをリアルタイムに受け取ることができ、端末から修復することができます。Lookout は、モバイル リスク全体から機密情報を保護するのに必要な可視性とセキュリティをあらゆる業界の組織に提供します。