Lookout

MTD vs MDM vs MAM

モバイル脅威対策 ｜ モバイル端末管理 ｜ モバイル アプリ管理

多くの組織では、従業員がモバイル端末から機密性の高いビジネス データにアクセスするようになったため、MDM や MAM といったソリューションを採用しています。このようなソリューションが、クラウドにおけるサイバーセキュリティの脅威から企業を保護してくれると考えているからです。

ますます多くの組織が MTD を採用

MTD

200%

「MTD を導入する組織は、2018 年には 10% でしたが 2020 年までに 30% に増える見込みです」[1]
[200% の増加]

MDM

30%

「MDM と EMM を組み合わせて導入しようとする組織は、今後 1 年から 1 年半以内に約 30% 減少する見込みです」

MAM

10%

「MAM と MCM を EMM と組み合わせて採用しようとする組織は、今後 1 年から 1 年半以内に約 10% 減少する見込みです」

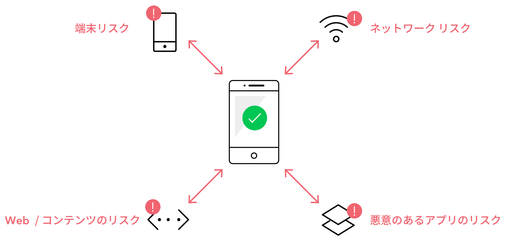
モバイル管理のセキュリティ ギャップを識別するためのガイド

このガイドでは、MTD、MDM、および MAM のサイバーセキュリティ機能をモバイル リスクの全容と比較します。モバイル管理におけるセキュリティ ギャップでは、モバイルのセキュリティ態勢の強化のために組織が取り組む必要のある、システムの潜在的な脆弱性を示します。

リスクの要素	MTD	MDM	MAM
Web およびコンテンツの脅威 メール、SMS、ブラウザー、ソーシャル アプリから開かれた悪意のある URL、公式のログイン ページを装った Web サイトにユーザーを誘導します。 ログイン資格情報を暗号化しなかったり、データを漏洩したりする Web サイトもあります。	要件を満たしている Lookout は、メール、SMS、ブラウザー、アプリにおけるフィッシングから保護します。Lookout は、モバイル端末からのすべてのアウトバウンド接続を、ネットワーク レベルでリアルタイムに検査します。	非対応 MDM ではフィッシングからの保護を行いません。	非対応 MAM ではフィッシングからの保護を行いません。
アプリの脅威 情報の盗用、データの漏洩、他のシステムへの不正なリモート アクセスを行ったり、端末を故障させたりすることが可能な、悪意のあるアプリ。 この中には、連絡先リストを漏洩するなど個別の脆弱性を持つ、悪意のないアプリも含まれます。	要件を満たしている Lookout は、7000 万を超えるアプリケーションのデータ コレクションにより「漏洩しやすい」アプリ (企業データを危険にさらす可能性のあるアプリ) を識別し、レピュテーション スキャンとコード解析により 悪意のあるアプリを識別します。	非対応 MDM では、悪意のあるアプリや脆弱なアプリを検知できません。	非対応 MAM では、悪意のあるアプリや脆弱なアプリを検知できません。
端末の脅威 オペレーティング システムを悪用して権限を強化する脅威。この種の攻撃では特に、OS レベルのアップグレード やパッチの際に生じる脆弱性対応期間が狙われます。 さらに、サイドローディングでインストールされたアプリは端末の脅威を引き起こす可能性があります。	要件を満たしている 端末のジェイルブレイクやルート化、古い OS、および危険な端末設定から保護するために、Lookout は予想される許容可能な使用パターンを追跡することにより、動作異常を検知します。	部分的なソリューション MDM は、ルート化およびジェイルブレイクをリアルタイムで検知できません。代わりに、ソフトウェアの更新をプッシュして脅威を軽減します。このため、攻撃に対して無防備になる時間帯が生じます。	非対応 MAM では、端末の脅威を検知できません。
ネットワークの脅威 Web サイトやアプリケーションが Wi-Fi、セルラー、または他のネットワークを介して TLS/SSL セッションを確立する際の弱みに付け込んだ、ネットワークの脅威。	要件を満たしている Lookout は、危険なネットワークを検知し、中間者攻撃、認証なりすまし、TLS/SSL ストリップ攻撃、TLS/SSL 暗号スイートのダウングレードから保護します。	非対応 MDM には、ネットワークの脅威を検知する機能はありません。	非対応 MAM には、ネットワークの脅威を検知する機能はありません。
脅威修復 モバイル端末の脅威を即座に修復して、モバイル操作の安全性を保ち、企業リソースに引き続きアクセスできるようにします。	要件を満たしている 脅威を検知すると、Lookout は自己修復のための指示をユーザーに送ります。 脅威の 95% はユーザーによって修復されます。	部分的なソリューション 脅威の検知や自己修復は行いません。ただし、MDM は端末をワイプして脅威のリスクを軽減します。 脅威を識別するには MTD からの入力が必要です。	部分的なソリューション 脅威の検知や修復は行いません。MAM では、感染していると識別されたアプリケーションを制限または削除できます。 アプリケーションのリスク レベルを受け取るには、MTD からの入力が必要です。
条件付きアクセス リスクが高いモバイル端末は、企業リソースにアクセスしようとします。一般的に、ウイルス、マルウェア、脆弱性を持つ端末や、ルートや化された端末は、リスクが高いと見なされます。	要件を満たしている Lookout の Continuous Conditional Access は、端末の正常性を監視し、リスクレベルを割り当て、この情報を認証の要素として提供します。	部分的なソリューション MTD からの入力により、MDM はポリシーを制定して認証を防ぎます。 MDM は、古い OS からのアクセスを防止し、端末にパスコードを適用できます。	部分的なソリューション MTD からの入力により、MAM はポリシーを制定し、MAM で保護されているアプリへの認証を防ぎます。 MAM は、古いアプリ バージョンからのアクセスを防ぐこともできます。
ユーザー プライバシー ユーザー プライバシーの保護と、さまざまな業界のプライバシー規制の順守。	要件を満たしている Lookout のセットアップに必要なのはメールアドレスのみです。GPS 位置情報は不要です。 また、Lookout には、ユーザー情報の追加を抑制するための高度なプライバシー モードがあります。	非対応 多くの MDM ツールでは、個人的な通話や Web トラフィックなど、端末のすべてのアクティビティを雇用者がいつでも監視できます。 プライバシー モードは使用できません。	部分的なソリューション 独立型のソリューションである MAM は、雇用主が求めるアプリケーションのみを管理し、ユーザー情報の使用を制限します。 ただし、MAM ソリューションの多くは MDM にも含まれています。
脅威の通知 サイバーセキュリティ イベントの継続的な監視と通知。	要件を満たしている Lookout は、モバイルのサイバーセキュリティ イベントを検知すると、すぐに管理者と指定受信者に通知します。	非対応 モバイルのサイバーセキュリティ イベントは検知できません。	非対応 モバイルのサイバーセキュリティ イベントは検知できません。

MTD はさまざまなサイバーセキュリティ イベントから組織を保護します

MDM および MAM ソリューションは、サイバーセキュリティの脅威やユーザーの行動を検知したり、それらから保護したりすることはしません。これらのソリューションは、組織内で使用されるモバイル端末の管理運営のためのポリシーと手順を適用できる「管理」ツールに過ぎません。組織をモバイルのサイバーセキュリティ攻撃から保護するには、脅威を検知してブロックする MTD ソリューションが必要です。ただし、MTD を既存の MDM や MAM ソリューションと統合することも可能です。統合すると、これらの管理ツールは脅威情報に基づくポリシーを適用できるようになります。



詳細については、lookout.com/jp をご覧ください。

Lookout

1. Hochmuch, Phil.2018 Enterprise Mobility Decision Maker Survey:Software, Management and Security Highlights.IDC.2018 年 (MCM = モバイル コンテンツ管理)

2. Zumerle, Dionisio and Girard, John.2018 Gartner Market Guide for Mobile Threat Defense.IDC.2018 年