Kaspersky Security for Mobile

モバイルエンドポイント向け多層型セキュリティと管理

機能

強力なアンチマルウェア
アンチフィッシングおよびアンチスパム
危険サイトブロック
アプリケーションコントロール
root 化、脱獄（Jailbreak）検知
アプリケーションのコンテナー化
盗難対策
モバイルデバイス管理
セルフサービスポータル
ソリューションの一元管理
Web コンソール

サポートされるプラットフォーム：

- Android
- iOS

セキュリティを妥協することなく、モバイル端末のビジネス上のメリットを実現します。

Kaspersky Security for Mobile は、従業員がモバイル端末を用いて業務を安全かつセキュアにできるようにすることで、企業の生産性と効率の向上を支援する、モバイル脅威防御（MTD）およびモバイル脅威管理（MTM）ソリューションです。

2016 年、カスペルスキーは 850 万件を超えるモバイルマルウェア攻撃を検知しました。従業員 1 人あたり平均 3 台以上モバイル端末を使用していると考えた場合、どのような環境であってもそれらの端末のセキュリティを確保することは、企業にとって重要な事項です。Kaspersky Security for Mobile は管理の手間を最小限に抑えながら、最大限のモバイルセキュリティを実現します。

特長

高度なアンチマルウェア機能

モバイルマルウェアは急増を続けています。モバイルランサムウェアの脅威の数は、2017 年上半期だけで、2016 年年間を通じて検知された脅威の合計数を上回っています。

Kaspersky Security for Mobile は、アンチマルウェア機能をクラウドを利用した脅威インテリジェンスおよび機械学習と組み合わせることで、モバイル端末に保存されたデータを既知および未知の脅威、そして高度な脅威から保護します。

モバイルデバイス管理（MDM）

Android、iOS のパスワード、暗号化、Bluetooth、カメラのルールの設定および有効化をグループポリシーを用いて実行できます。また端末と、インストールされたアプリケーションについてのレポートを実行します。代表的なモバイル端末管理プラットフォームと統合できるため、リモートでの OTA（Over The Air）展開と管理が可能になり、サポートされる端末が使いやすく、また管理しやすくなります。

モバイルアプリケーション管理（MAM）

Android および iOS のアプリケーションコントロールにより、管理者はインストールするアプリケーションを定義し、これらのアプリケーションのブラックリストとホワイトリストを作成できます。

柔軟な展開が可能なオプション

柔軟な端末の登録オプションによって、BYOD（個人所有端末の業務での利用）と COPE（会社所有端末の個人利用）のシナリオの両方がサポートされます。BYOD 環境の場合 Google Play または AppStore からインストールでき、COPE 戦略を採用している場合は、セルフサービスポータルから、またはカスタムインストールによってインストールできます。この柔軟性により、企業は保護機能を利用するために、現行のモバイル戦略を変更する必要はありません。

ソリューションの一元管理

Kaspersky Security for Mobile ではカスペルスキーのほかのエンドポイントセキュリティ製品と同様に、Kaspersky Security Center からモバイル端末を管理できます。端末についての情報の表示、ポリシーの作成と管理、端末へのコマンドの送信、レポートの確認などこれらすべてを一元的に管理コンソールから行うことができます。

モバイルセキュリティ機能と管理機能

強力なアンチマルウェア機能
プロアクティブなクラウドを利用した脅威検知および分析と従来の技術を組み合わせて、既知と未知の脅威、そして高度な脅威から保護します。オンデマンドの定期スキャンと自動アップデートを組み合わせて、保護力を強化します。

Web コントロールと Safe Browser
Kaspersky Security Network（KSN）によって分類された、危険な Web サイトや業務に必要のない Web サイトへのアクセスをブロックすることが可能です。KSN は定期的に脅威情報がアップデートされるため、信頼性が高く、安全な Web フィルタリング機能がリアルタイムでサポートされます。Android 端末では Chrome ベースのブラウザでサポートし、iOS では、Kaspersky Safe Browser にて利用できます。

アプリケーションコントロール
利用可能なアプリケーションを管理者が許可したソフトウェアのみに制限できます。アプリケーションコントロールは、インストールしたソフトウェアに関するデータを提供し、管理者は強制的に特定のアプリケーションを端末にインストールさせることができます。KSN の統合により、ブラックリストとホワイトリストを容易に作成し、管理することができます。

root 化、脱獄（Jailbreak）検知
モバイル端末の約 5 % において、利用者の同意なしに管理タスクが実行可能な状態にあるというデータがあり、Kaspersky Security for Mobile は、そのような root 化された端末、または脱獄（Jailbreak）された端末を検知して管理者に通知することにより、このリスクを排除します。管理者はそうした端末によるアクセスをブロックしたり、リモートでデータを削除することができます。

アプリケーションのコンテナー化
アプリケーションをコンテナーに格納することで、業務データと個人データを分離し、機密データを保護するために、暗号化などの追加のポリシーを適用できます。従業員が退職した際に、個人データに影響を与えることなく、コンテナー化されたデータのみ選択して消去できます。コンテナーへアクセスするには認証が必要です。

盗難対策
端末の盗難が発生した場合でも、端末の位置特定とロック、選択的または完全なデータの消去、不正に取得した人物の顔写真（マグショット）の撮影およびアラームの有効化などのリモート盗難対策機能を使用して、業務データを保護します。Google Firebase Cloud Messaging（FCM）および Apple Push Notification サービス（APNs）との統合により、瞬時にコマンドを送信できます。さらにセルフサービスポータルを利用すれば、管理者が盗難対策を有効化する前でも、コマンド送信が可能です。

モバイルデバイス管理（MDM）
Microsoft Exchange ActiveSync、Samsung KNOX および iOS MDM をサポートしており、強制的な端末の暗号化の適用、強制的なパスワードの設定、カメラ機能の使用制限、APN および VPN の設定など、各プラットフォームに対して統合されたポリシーまたは個別のポリシーを作成・適用できます。Kaspersky Security for Mobile は、iOS MDM をサポートするだけではなく、iOS の端末監視や、システム管理者への包括的な管理権限の付与といった機能の利用が可能で、利用者のセキュリティをさらに強化できます。Android for Work ではビジネスプロファイルの作成、業務アプリケーションおよび端末の管理が可能で、同じ端末上で業務データと個人データを分離することができます。

セルフサービスポータル
定型的なセキュリティ管理を従業員に委譲し、承認された端末に対する管理機能を自分で登録できるようにします。新しい端末の有効化プロセス中に、必要なすべての VPN 設定およびメール証明書がポータルを通じて自動的に配信されます。端末の紛失時には、従業員はすべての盗難対策のアクションを実行できます。

ソリューションの一元管理
すべての機能を、Kaspersky Security Center で管理することができます。モバイル端末用の個別の管理ツールを用意する必要はありません。同じコンソールからモバイル端末や PC、サーバーなどの管理が行えます。

購入方法

- Kaspersky Security for Mobile は以下の製品に含まれています：
- Kaspersky Endpoint Security for Business | Select
- Kaspersky Endpoint Security for Business | Advanced

株式会社カスペルスキー
製品情報：https://www.kaspersky.co.jp/business-security/mobile-device
ご購入相談窓口：jp-sales@kaspersky.com

www.kaspersky.co.jp
#truecybersecurity

PMM-1024-2-201903