MobileIron

MobileIron Threat Defense データシート

概要

MobileIron Threat Defenseは、卓越したモバイルセキュリティで、企業のデバイス、ネットワーク、アプリケーションのレベルでサイバー攻撃を検出し、防御します。単一のインテリジェントなエージェントが、機械学習アルゴリズムで、既知の脅威からもゼロデイのモバイル脅威からも企業資産を守ります。

MobileIron Threat Defenseは、マネージドデバイスと非マネージドデバイスに対してサイレントに導入し、有効化できるため、ユーザー側の操作なしに全員に確実に装備させることができます。脅威修復は、インターネット接続がなくてもオンデバイスで実行されます。

ユーザーの生産性は阻害されず、侵害を受けたモバイルデバイスが企業ネットワークに影響したり情報漏洩のリスクをもたらしたりすることもありません。デバイス上で有効化された後は、ユーザーが脅威保護機能を削除したり無効化したりすることはできません。

主な利点

モバイルデバイス向けに開発されたMobileIron Threat Defenseは、デバイス上での継続的動作に最適化した機械学習アルゴリズムを使用し、デバイスがオフラインでも脅威を検出します。

簡単

MobileIron Clientに保護機能が組み込まれているため、1つのアプリだけで済み、ユーザーが何もしなくてもクライアントが有効化されるので簡単です。

有用な情報

あらゆるモバイルデバイスに対する危険や脅威をリアルタイムで継続的に可視化し、リスクの高いアプリを分析します。

オンデバイス

オンデバイスの機械学習アルゴリズムで、既知の攻撃とゼロデイ攻撃を検出し、脆弱性を修復。インターネット接続は不要です。

MobileIronについて

MobileIronは、新しい働き方に必要なセキュリティの基盤を提供します。詳しい情報については www.mobileiron.com/jaをご覧ください。

〒106-0041 東京都港区麻布台1-11-10 日総第22ビル3階 • japan@mobileiron.com • www.mobileiron.com/ja • Tel: 03-6426-5301 • Fax: 03-6426-5302

機能	詳細	利点	オペレーティングシステム	
			iOS	
UEM統合	統合エンドポイント管理（UEM）に脅威防御を統合したソリューション。	IT部門が1つのアプリで管理とメンテナンスを実行できるため、運用コストを軽減。	あり	あり
自動導入	管理者がクライアントの導入を自動化し、選択したデバイスでThreat Defenseを有効化可能。	100%のユーザー普及率。	あり	あり
脅威検出	**デバイスの脆弱性** • ジェイルブレイク • ルート化検出 • 脆弱なOSバージョン • 最小OSバージョン • 暗号化が無効 • パスワード削除済み/無効 • ファイルシステムの改ざん • 信頼できない/疑わしいプロファイル • 権限の昇格 **ネットワークの脆弱性** • 中間者（MitM）攻撃 • 悪意あるホットスポット • セキュアでないWi-Fi • 悪意あるBluetooth • 不正アクセスポイント • キャプティブポータル **アプリケーションの脆弱性** • プライバシーリスクが高い • セキュリティリスクが高い • 疑わしいアプリ挙動 • サイドロードしたアプリ	機械学習アルゴリズムで既知の脅威やゼロデイ脅威をオンデバイスで検出。 デバイス、OS、ネットワーク、アプリケーションの脆弱性や脅威を認識し、可視性を強化。	あり	あり

アプリ分析	• **アプリの可視化：**デバイスにインストールされているアプリケーションの構成可能インベントリ
	  • すべてのアプリケーション（iOS）
	  • マネージドアプリケーション
	
	• **アプリ分析：**アプリケーションをオフラインで分析するオプション。アプリのリスクとデバイス分析を自動的に相関させ、次の情報を提供：
	  • コンテンツ：マルウェア
	  • 意図：アプリの挙動
	  • コンテキスト：ドメイン、証明書、共有コード、ネットワーク通信
	
	• **アプリ情報：**セキュリティポリシーを設定してリスクを軽減
	
	• **レポート：**アプリのセキュリティとプライバシーリスクの概要レポートを印刷
	
	• **アプリケーションのアップロード：**分析とリスク評価に対応
		デバイスにインストールされているアプリを把握。
		
		オプションのの分析機能で、脅威評価スコア、リスクの説明、影響に関する詳細なレポートを作成。
			あり	あり

脅威通知	サーバーで脅威が検出された場合にデバイスユーザーに通知したい脅威を管理者が選択。メッセージはカスタマイズや複数言語での作成が可能。	デバイス上で検出された脅威のオンデバイス通知を構成可能。	あり	あり
ローカル脅威通知	自動的にインポートされた最新の脅威リストを使用し、複数のローカルアクション構成を作成。 新しい脅威リストが提供されるとシステムが管理者に通知し、リストから削除された脅威を特定。	検出された脅威に関してデバイスユーザーに表示する情報量と内容を管理者が制御。デバイス上の選択言語で脅威を通知。	あり	あり

修復アクション	• 自動インポートされた最新の脅威リストを使用して、複数のローカル修復アクション構成を作成。
	
	• インポートされたリスト上の脅威ごとにプラットフォームが実行するアクションを管理者が選択。
	
	• **サーバー起動型のコンプライアンスアクション**
	  • 監視
	  • アラート送信
	  • AppConnectとメールをブロック
	  • 検疫
	  • セレクティブワイプ
	  • 階層型コンプライアンス（自動で段階的に反応）
	
	• **Android上のローカルアクション：**
	  • 検疫 – すべての構成を削除
	  • 検疫 –「Wi-Fiのみ」の場合はWi-Fiを除くすべての構成を削除
	  • Wi-Fiを除くすべての構成を削除
	  • マネージドアプリを削除し、ダウンロードをブロック
	  • Bluetoothを無効化
	  • Wi-Fiを切断
	  • 撤去とワイプ
	
	• **iOS上のローカルアクション：**
	  • AppConnectアプリをブロック
	  • ネットワークトラフィックをシンクホール化
	
	• **新しい脅威リストが提供されるとシステムが管理者に通知**
		インターネット接続のあるときもないときも、コンプライアンスアクションと脅威通知を実行。
		
		モバイルデバイス上でポリシーを適用し、脅威や攻撃の検出時間を短縮するとともに、モバイルデバイスに起因する攻撃への対応時間を大幅に短縮。
		
		デバイス上で検出された脅威の最新リストでローカルコンプライアンスポリシーを常に更新し、時間と人的ミスを削減。
		
		複数のローカル修復アクション構成を作成し、異なるユーザーグループに適用可能。
			あり	あり

デバイスの脅威をスキャン	継続的なスキャンで脅威を検出。	モバイル脅威の検出と修復の間の時間を短縮。	あり	あり
	デバイスのチェックイン時にスキャンを実行。	保護とバッテリー寿命を最適化。	あり	あり
管理コンソール	クラウドベースのzConsoleと統合エンドポイント管理サーバーを統合。	企業所有および従業員所有デバイスを簡単に管理。	あり	あり
導入形態オプション	オンプレミス、SaaS。	ビジネスニーズに応じて導入形態を選択。	あり	あり

ホスティングロケーション	サーバーは世界中の主要地域に配置。	データのプライバシー要件を満たし、レイテンシを最小化するロケーションを選択可能。	あり	あり
データプライバシーポリシー制御	個人情報（PII）開示を制御するデータプライバシーポリシーを柔軟に構成可能。	GDPR、業界のベストプラクティス、デバイスOEM条件への企業コンプライアンスを促進。	あり	あり
企業規模の導入を実証済み	250,000デバイス規模での導入実績。	小規模から大企業にもにわたる広い導入実績。	あり	あり
対応言語	14言語に翻訳済み。	使いやすさ。	あり	あり

プライバシー
UEMのセキュリティやロックダウンポリシー設定とMobileIron Threat Defenseを組み合わせることで、多層型のセキュリティ戦略を実行し、自動化された脅威対策でモバイルユーザーの個人情報を含む保存データおよび通信中データを保護します。

サポート
その他の製品仕様についてはMobileIronのリリースノートをご覧ください。

ライセンス
MobileIron Threat Defenseの利用契約は、統合エンドポイント管理ライセンスのアドオンとして、ユーザーあたりまたはデバイスあたりのライセンスとして提供しています。御社に最適なプランについては、最寄りの営業担当者または販売代理店にお問い合わせください。