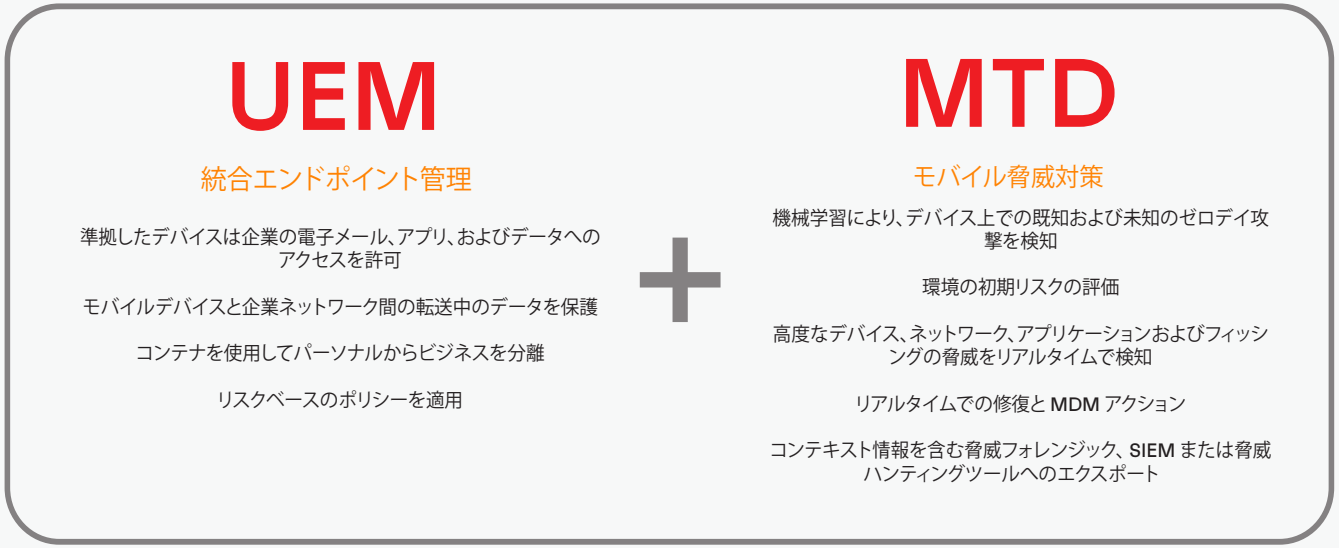
UEM? MTD? 両方必要な理由

完全なエンドツーエンドのモバイル脅威対策を実現



Ivanti と Zimperiumは協業して、Everywhere Workplace（場所にとわられない働き方）の支援のために高度な脅威対策を実現する完全なエンタープライズ・モバイル・セキュリティ・ソリューションを提供します。 このソリューションは、フィッシングから保護し、デバイス、ネットワーク、アプリケーションレベルでの攻撃に対して保護と修正を行います。

Ivanti と Zimperiumを組み合わせることで、企業が幅広い攻撃に対してモバイルデバイスを管理し保護できるようにします。Zimperiumは、継続的に脅威を検知および分析し、リスクベースのポリシーを制定してモバイルデバイスを企業ネットワークとその資産の侵害から保護するための可視性をIvantiに提供します。

この統合されたソリューションは、ITセキュリティ管理者に会社支給デバイスと個人デバイス（BYOD）の両方を安全に管理できる方法を提供します。この方法により、従業員は自分の好みのデバイスを使えるようになり、生産性が向上すると同時に、デバイスと企業を高度な脅威から保護するバランスを取ることができます。

主なメリット

モバイルデバイス向けにゼロから構築された Zimperium のz9モバイル脅威保護エンジンは、インターネットに接続せずにデバイス上で実行するために最適化された機械学習テクノロジーを使用しています。デバイスを保護するための非侵入型アプローチにより、ユーザーエクスペリエンスに影響を与えたり、ユーザーのプライバシーを侵害したりすることなく、24時間保護します。モバイル脅威対策（MTD）はIvantiのUEMクライアントと統合されているため、管理者はユーザー全員に適用させることができます。

ガイドラインの準拠

NIST SP 800.53

NIST SP 800-53 第4版は、情報システムとそれらが動作する環境の根本的な強化のために必要なセキュリティ制御の幅と深さを組織に提供することにより、情報セキュリティとリスク管理に対するより包括的なアプローチを提供するものです。これにより、サイバー攻撃やその他の脅威に対しても、より回復力のあるシステムを作ることができます。Zimperium のz9 MTDエンジンはMTDを強化し、ネットワークのパブリックアクセス攻撃、アプリケーションやOSに対する悪意のあるコード、デバイス上のインシデントレスポンス、モバイルワーカーの脆弱性スキャンを検出します。

NIST 800.124

NIST SP800-124 第 2版 4.2.3項 には、「MTDシステムは、悪意のあるアプリ、ネットワークベースの攻撃、不適切な構成、およびモバイルアプリまたはモバイルOS自体の既知の脆弱性の存在を検知するよう設計される」とあります。Zimperiumのモバイル脅威保護は、継続的なデバイス、OS、ネットワーク、フィッシングおよびアプリケーションのモニタリングをデバイス上でリアルタイムに提供します。 加えて、Zimperiumのz3Aの高度なアプリ分析は、環境内のすべてのアプリに対して20ポイントの検証を実行し、アプリ間の予期しないインタラクション、欠陥または誤ったコードを含むアプリ、対処されていないCVE、またはPII へのアクセスを検知します。

MITRE ATT&CK® フレームワーク

現実の観測に基づく、攻撃者の戦術と技術に関するグローバルでアクセス可能なナレッジベースです。攻撃に対抗するためにMTDプレミアムアプリ分析は攻撃フレームワークの検出と修正に役立ちます。

Zimperium と Ivanti の統合について

導入とアップグレードの容易さ

Zimperium のz9エンジンは、すでにIvanti の UEMエージェントに組み込まれています。 これにより、ソリューションはデバイスに導入されており、必要なのはアクティベートするだけです。 UEMをzConsoleに追加し、UEMからアクティベートしてデバイス保護を開始することにより、設定が行われます。 ユーザーの操作や、新しいアプリケーションの展開は必要ありません。

企業のインフラを保護

デバイスの侵害をMTDが検知すると、素早く修復を行い攻撃を阻止します。 攻撃と設定に基づき、Ivantiはネットワーク接続の終了、特定のIP/ドメインの拒否、特定の検疫アクションの実行など、さまざまな保護アクションを実行できます。 さらに、Ivantiのサーバーは、脅威の重大さに応じてリスクベースのコンプライアンスポリシーを制定することができます。 ポリシーにより、モバイルデバイスから企業サービス（メールまたは他のアプリ、Wi-FiおよびVPN）への接続の一時的に無効にしたり、またはデバイスから企業アプリケーションの削除といった対策ができます これらのアクションにより、感染の広がりを止め企業データのリスクを防ぐことができます。

アラートとレポーティング

Ivanti はあらゆる企業のニーズに合わせ、包括的なモバイル脅威フォレンジックとともに、攻撃タイプ別に設定可能なエンドユーザーへの通知と管理者アラートを提供します。 プライバシーデータ収集ポリシーも地域の規制に準拠して提供されます。

機能	UEM	MTD	MTD Premium
iOS および Android デバイスをサポート	✓	✓	✓
OS/デバイス、ネットワーク、アプリおよびフィッシングの初期脆弱性リスク体制を提供	✓	✓	✓
デバイスで適切な物理的セキュリティが有効になっているか検知（PINコード、デバイスレベルの暗号化）	✓ Basic	✓	✓
デバイスがユーザーによってジェイルブレイク/ルート化されていないか検知（既知のハッシュ値とファイルの場所を使用）		✓	✓
デバイスの侵害または攻撃のツールと手法についての情報分析を提供		✓	✓
OS/カーネルおよび USB の悪用、プロフィール/構成の変更、システムの改ざんを検出		✓	✓
権限昇格攻撃の検出		✓	✓
ネットワーク攻撃（中間者攻撃、不正な Wi-Fi およびセルラーネットワーク）を検出		✓	✓
SSL ストリッピング、偽SSL、SSL トラフィックの妨害の試みの検出		✓	✓
攻撃者による偵察スキャンの実行の検出		✓	✓
フィッシング、スミッシング、URLフィッシング、短縮 URL などの検出		✓	✓
企業アプリの配信と削除	✓		
企業ドキュメント共有の保護	✓		
基幹業務アプリの保護	✓		

機能	UEM	MTD	MTD Premium
悪意のあるアプリ、既知および未知のマルウェア、ダウンロードと実行を使用した動的脅威を検出		✓	✓
許可されていないモバイルデバイスへのアクセスを無効	✓		
モバイル脅威の詳細フォレンジックを提供		✓	✓
侵害されたデバイスのロックまたは選択的ワイプを含む、リスクに基づいたポリシーを適用	✓	✓	✓
攻撃が検知されたら、リアルタイム修正を実行		✓	✓
自社開発のアプリのプライバシーおよびセキュリティ上の懸念・リスクのスキャン			✓
デバイスにインストールされたアプリからのプライバシーおよびセキュリティ情報の受信			✓
脅威の検出	**UEM**	**MTD**	**MTD Premium**
ホスト関連の重大で危険度の高い脅威			
Android デバイス — 改ざんの可能性		✓	✓
異常なプロセス		✓	✓
開発者のオプション		✓	✓
デバイスの暗号化	✓	✓	✓
デバイスの PIN	✓	✓	✓

脅威の検出	UEM	MTD	MTD Premium
ホスト関連の重大で危険度の高い脅威			
デバイスのジェイルブレイク/ルート化 MDMジェイルブレイク/ルート検出はシンプルで簡単にバイパスできます。 また、MDMは攻撃に使われたツールや手法に関する可視的な分析情報を行いません	✓	✓	✓
権限昇格		✓	✓
ファイルシステムの変更		✓	✓
サイドロードアプリ		✓	✓
SE Linux の無効化		✓	✓
システムの改ざん これはデバイスの高度な侵害であり、デバイスのジェイルブレイクまたはルート化の追加手順を使用する場合と使用しない場合があります		✓	✓
疑わしいiOSアプリ		✓	✓
疑わしいAndroidアプリ		✓	✓
信頼できないプロフィール		✓	✓
USB デバッグモード有効		✓	✓
脆弱な Android バージョン		✓	✓
脆弱な iOS バージョン		✓	✓

フィッシング検出と防止			
フィッシング URL の常時検出とブロック		✓	✓
デバイス上のフィッシング検出		✓	✓
リモートサーバーでのフィッシングURL検査の強化		✓	✓
常時フィッシング検出と、ローカルでの修正アクションを含む、すべてのアプリおよびデバイスでの全インターネットトラフィックからのフィッシングURLのブロック		✓	✓
ネットワーク関連の重大で危険度の高い脅威			
MiTM		✓	✓
MiTM - ARP		✓	✓
MiTM – ICMP リダイレクト		✓	✓
MiTM – SSL ストリップ		✓	✓
MiTM – 偽SSLストリップ		✓	✓
SSL/TLS ダウングレード		✓	✓

Ivanti について

Ivanti は Everywhere Workplace（場所にとらわれない働き方）を実現します。 さまざまなデバイスとネットワークを介し、どこからでも社内アプリケーションや社内データにアクセスできるEverywhere Workplaceなら、従業員がどこにいようと、生産性を維持できます。 Ivanti自動化プラットフォームは、業界をリードする統合エンドポイント管理、ゼロトラストセキュリティ、エンタープライズサービス管理ソリューションを一体化することでデバイスの自己修復と自己防御を可能にし、ユーザーのセルフサービス機能を強化する、統合ITプラットフォームです。 アメリカのビジネス誌「Fortune」が選ぶ100社のうち78社を含む、4万社以上の企業がIvantiを導入し、クラウドからエッジまでのIT資産の検出、管理、セキュリティ保護、保守点検を行い、いつでもどこでも従業員に優れたエンドユーザーエクスペリエンスを提供しています。 詳細については、ivanti.co.jp にアクセスしてください。

ivanti

ivanti.co.jp
+81 (0)3-6432-4180
contact@ivanti.co.jp