MTD: モバイル脅威対策
モバイルセキュリティのためのソリューション

MTD（モバイル脅威対策）の重要なメリット

常時保護を実現

MTD（モバイル脅威対策）は、デバイス上で継続的に動作するように最適化された機械学習アルゴリズムを使用しており、たとえデバイスがオフラインの状態のときでも、既知の脅威やゼロデイ脅威を検知し、対処することができます。

脅威の可視性を向上

すべてのモバイルデバイスの悪意のある脅威を即時かつ継続的に可視化し、危険なアプリに関する詳細な分析を提供します。

ユーザー導入率100%を実現

Ivanti UEMに登録されたモバイルデバイスのMTD（モバイル脅威対策）を有効にするのに、ユーザーと対話したり、新しいアプリを導入したりする必要はありません。

モバイルの脅威から保護

今日のEverywhere Workplace（場所にとらわれない働き方）の環境下で、モバイルデバイスは、企業の重要なリソースとなっています。従業員は、実質的にすべてのものにアクセスするためにそれらを使用しています。そして、ほとんどの従業員は、モバイルセキュリティに関して十分な知識を持っていないため、ハッカーに狙われてしまいます。

Ivanti Mobile Threat Defense (Ivanti MTD) は、企業や従業員が所有するAndroidやiOSデバイスを、高度な脅威から保護します。これによって、企業は、デバイス、ネットワーク、アプリケーションの各レベルで発生する攻撃に対してデバイスを監視、管理、保護でき、さらにモバイルを狙うフィッシング攻撃を阻止することができます。

他のソリューションとは異なり、Ivanti MTDは、デバイスがWi-Fiまたはセルラーネットワークに接続されていない場合でも、デバイス上の既知のモバイル脅威とゼロデイモバイル脅威の両方を検出して、修復するローカルコンプライアンスアクションをプッシュします。さらに、Ivanti UEMに登録されているモバイルデバイスでMTD（モバイル脅威対策）を有効にするのにユーザーと対話する必要ありません。これによって、企業は、ユーザー導入率100%を達成し、モバイル脅威からの保護を確かなものにすることができます。

MTD の機能

デバイス上での検出と修復

デバイス上の機械学習ベースの保護機能は、たとえネットワークに接続されていないときでも、デバイス、ネットワーク、アプリケーションの各レベルにおける攻撃やフィッシング攻撃からモバイルデバイスを安全に保ちます。

マルチベクタのフィッシング対策

デバイスにおけるMTD（モバイル脅威対策）の機械学習とフィッシングURL探索機能（ルックアップ）は、効果を強化するためにクラウドベースの探索機能（ルックアップ）を含めるように拡張することが可能です。このソリューションのフィッシング対策機能は、電子メール、テキスト、SMSメッセージ、インスタントメッセージ、ソーシャルメディアなど、すべてのモバイル脅威ベクトルにおいてフィッシング攻撃を検出して修復することができます。

プロアクティブな修復アプローチ

ポリシーベースのコンプライアンスアクションは、危険な行動のアラートを提供し、デバイス上の攻撃を事前にシャットダウンして侵害されたデバイスをネットワークから分離し、悪意あるアプリとそのコンテンツを削除するため、悪用の可能性のある露出時間を限定してゼロデイ攻撃を阻止します。

詳細なレポート

ダッシュボードとレポートによって、企業は、デバイス、OS、ネットワーク、アプリのリスクを可視化して認識し、脅威のベクトルに対して迅速かつ効果的に対応できるよう、迅速に実行できる情報を得ることができます。

UEM 統合

Ivanti UEMに登録されたモバイルデバイスのMTD（モバイル脅威対策）を有効にするのに、ユーザーと対話したり、新しいアプリを導入したりする必要はないので、ユーザー導入率100%の実現が容易になります。さらに、ユーザーがMTD（モバイル脅威対策）を無効にしたり、デバイスから削除できないようにコンプライアンスポリシーを制定することができます。

攻撃の実例

MTD（モバイル脅威対策）は、デバイス、ネットワーク、アプリケーションの各レベルの攻撃、およびフィッシング攻撃から保護します。

デバイスの乗っ取り

MMSメッセージが標的となるユーザーに送信されると、ユーザーが操作しなくても、ゼロクリックの連鎖エクスプロイトが発動され、悪意のある攻撃者の権限を高めて、ネットワークへの横移動（ラテラルムーブメント）を可能にするリモートコードを実行しました。

ネットワーク攻撃

オフィスの近くの喫茶店で、Wi-Fiを使った中間者（MITM）は、ある企業に対して攻撃を仕掛け、スピアフィッシングのページに誘導して企業データを盗みました。

悪意あるアプリ

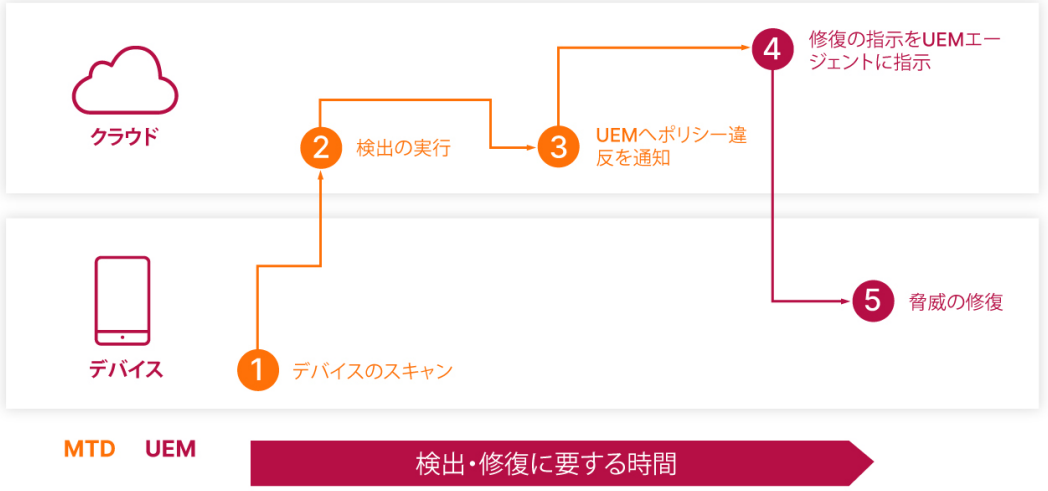
疑いを持たないユーザーは、第三者のアプリストアからアプリをインストールしました。MMSメッセージが、標的となるユーザーに送信されると、ユーザーが操作しなくてもゼロクリックの連鎖エクスプロイトが発動され、悪意のある攻撃者の権限を高めてネットワークへの横移動（ラテラルムーブメント）を可能にするリモートコードを実行しました。

フィッシング攻撃

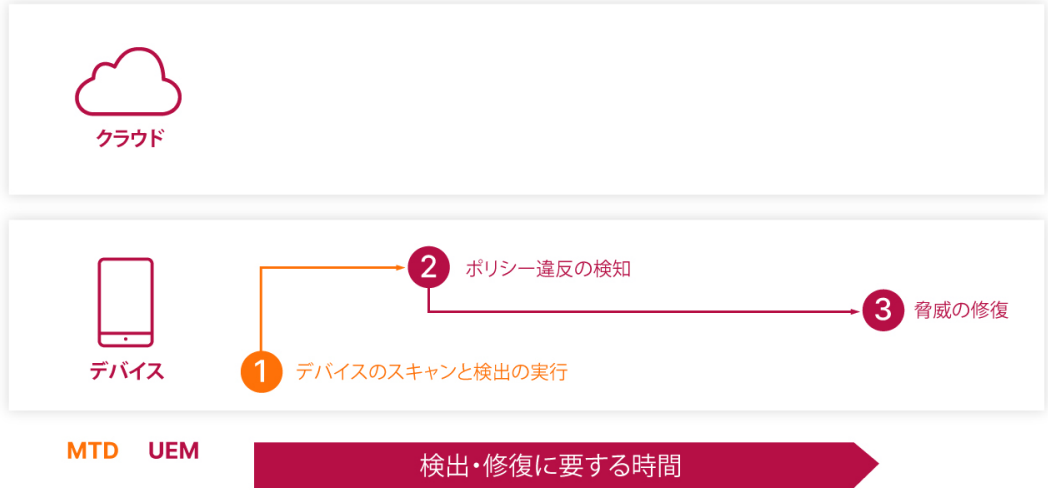
悪意のある攻撃者は、ソーシャルエンジニアリングを利用して、疑いを持たないユーザーを騙してリンクをクリックさせ、企業のログイン資格情報を提供させました。そして、攻撃者は、そのユーザーになりすましてログインし、企業のリソースにアクセスしました。

検出と修復

その他の脅威対策ソリューション



Ivanti MTDソリューション



Ivanti について

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。場所にとらわれない 働き方により、従業員は多種多様なデバイスでさまざまなネットワークから IT アプリケーションやデータにアクセスし、高い生産性を保つことができます。Ivanti Neurons 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と、エンタープライズサービス管理のソリューションをつなぎ、デバイスの 自己修復および自己保護、またエンドユーザーのセルフサービスを可能にする統合 IT プラットフォームを提供し ます。Fortune 100の96社を含む 40,000社以上の顧客が、クラウドからエッジまで IT 資産の管理、検 出、保護、サービスのために Ivanti を選択し、従業員があらゆる場所にいても作業できる優れたユーザー体験 を提供しています。詳細については、www.ivanti.co.jp をご参照ください。

ivanti

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