wandera
a Jamf company

Threat Defense

デバイスやネットワーク上で動作するクラウド配信のセキュリティにより、デバイス、ユーザー、およびアプリケーションをサイバー脅威から保護します。

パワフルなエンドポイントセキュリティ

Threat Defenseは、デバイスの脆弱性、マルウェア、危険なアプリなど、さまざまなエンドポイントにおける脅威を検出し、修復します。包括的なリスク評価を継続的に行い、脅威を特定することで、リアルタイムでセキュリティポリシーを適用することができます。

ユーザーとデータを保護するネットワーク防御

ネットワーク内の防御機能により、攻撃を未然に防ぎます。コンテンツ保護は、企業の認証情報を取得するように設計された、これまでにないゼロデイフィッシングサイトを含む悪質なサイトをブロックします。さらに、Threat Defenseは、危険なサイトとの接続をブロックすることで、コマンド&コントロールを防御し、データの流出を防ぎます。中間者攻撃が検知された場合、接続は自動的に保護されます。

アプリケーションへのアダプティブアクセス

安全で信頼できるデバイスのみがビジネスアプリケーションにアクセスできるようにすることで、Security Postureを強化します。Threat Defenseは、さまざまなテレメトリと状況ごとの入力データを継続的に監視します。これらの情報は、エンドポイントが危険にさらされている場合やリスクが高い場合に、アプリケーションへのアクセスを防ぐために使用されます。アダプティブアクセスポリシーは、ゼロトラストネットワークアクセスソリューションまたはJamfの管理ソリューションであるJamf Proを介してネイティブに適用できます。

包括的な脅威の検知と防止

Threat Defenseは、さまざまなサイバー脅威を特定して阻止します

リアルタイムでのネットワーク保護

Threat Defenseは、ユーザーの認証情報を盗もうとする試みを動的に検出してブロックし、今まで見たことのないようなフィッシング攻撃でも確実に失敗に終わらせます。ブランドの模倣、疑わしいPunycode、サブドメインエントロピーなど、さまざまな要因がスキャンされます。ネットワーク内の保護機能が、メール、ソーシャルメディア、SMSを介して送信される攻撃を拒否します。

詳細なアプリのインサイト

アプリがもたらすリスクを一目で理解し、MI:RIAMのアプリのリスクスコアと推奨される修復アクションとともに、既知の脆弱性がハイライトされます。詳細なフォレンジクスを確認することで、必要な権限、通信されたURL、またはアプリの特定のバージョンで使用されるサードパーティライブラリを把握することができます。

危険な構成の検出

詳細なPosture評価により、昇格された権限から古いOSまで、エンドポイントのリスクを可視化することができます。きめ細かい制御により、エンドユーザーへのプロンプト表示、悪意のある接続のブロック、企業リソースへのアクセス制限などの修復アクションを通じて、セキュリティポリシーを適用できます。

通信傍受の防御

公共のWi-Fi接続は、悪意のある攻撃者にとって攻撃を仕掛けるための理想的なプラットフォームです。Threat Defenseは、フェイルセーフ暗号化により、Wi-Fiに接続されたデバイスを保護します。攻撃が検知されると、Threat Defenseは自動的にユーザーのトラフィックを暗号化し、ユーザーは接続を中断することなく安全に作業を続けることができます。

最先端のセキュリティ機能と性能

さまざまなユースケースに対応する強力な保護とあらゆるシステムとの互換性

常時稼働のエンドポイントディフェンス

ユーザーがどこにいても、場所を問わずユーザやデバイスをサイバー脅威から保護します。Wanderaのエンドポイントアプリケーションは、侵害が発生する前に悪意のあるソフトウェア、脆弱な構成、危険な接続を特定します。潜在的な脅威が見つかると、修復のためのアクションとアラートが自動的に起動して、脅威を軽減します。

Conditional Access ポリシー

Conditional Accessを使用して、危険なユーザやデバイスからビジネスアプリケーションへのアクセスを防ぐことができます。管理対象企業の権限と未管理BYOデバイスの権限は、安全と評価されるまで無効になります。ポリシーは、Threat Defenseネットワーク内でネイティブに適用することも、JamfやIdPとの統合により適用することも可能です。

リアルタイムなレポートとポリシーコントロール

統合されたポリシーエンジンにより、管理者はセキュリティポリシーを迅速に設定して即座に適用できるため、臨機応変にポリシーを調整、カスタマイズできます。詳細な分析結果は、すぐに使える統合機能や一連のAPI、データストリームを利用して、Threat Defenseポータル内またはSIEM／SOARダッシュボードから確認することができます。

統合運用・管理

Threat DefenseをJamfやIdPなどの管理ソリューションと統合することで、組織のユーザグループに関する情報を同期させることができます。これにより、Threat Defenseをデバイスに素早く展開して、ユーザ権限の割り当てを容易にすることができます。また、この統合により、レポートに対して人が読める名前を追加することができるようになるため、ThreatOpsのイベントモニタリングや脅威の検出を簡素化することができます。

MI:RIAM搭載

MI:RIAMは、高度な脅威インテリジェンスエンジンであり、さまざまな既知のゼロデイ脅威を識別するためにリアルタイムで動作します。最大の脅威データに基づいて構築されたMI:RIAMは、世界中の4億2500万のセンサーから情報を収集し、アルゴリズムに入力します。MI:RIAMは、高度なデータサイエンスを利用して、セキュリティリーダーに、最新の脅威インテリジェンスやビジネスに対するアクティブなリスクに関してリアルタイムなインサイトを提供します。

Threat Defenseがユーザー、モバイルデバイス、組織データを悪意から保護する方法の詳細については、jamf.comをご覧ください

wandera
a Jamf company