モバイルデバイスのネットワークセキュリティと デバイス管理を強化する新時代のソリューション

モバイルデバイスに特化した エンドポイントセキュリティ

Jamf Threat Defense

従業員を標的としたフィッシング被害から デバイスをリアルタイムに保護する

データ使用量を取得できる セキュアなウェブゲートウェイ

Jamf Data Policy

一般的なコンテンツフィルタでは難しい 「データ通信量」の可視化と制御を行う

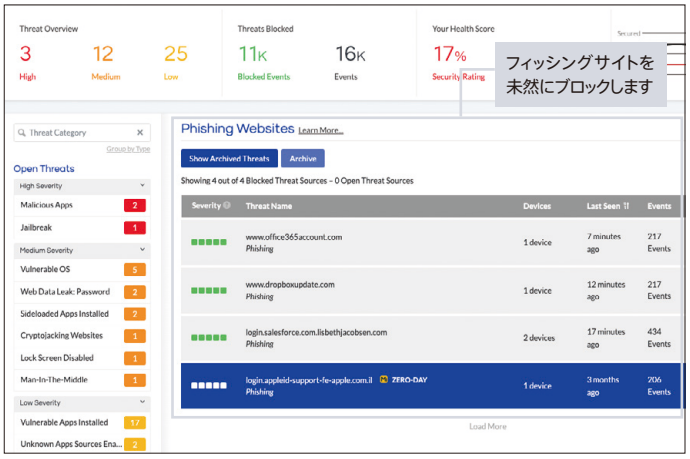
リモートワークが当たり前になった今、
従業員が利用するモバイルデバイスの新しい保護と管理が必要です!

Jamf Threat Defenseの特徴

iPhoneやiPadはシステム標準で強力なセキュリティ機能を搭載しているため、OSの不正改造や不正アプリ混入によるウイルスの危険性は低いものの、サイバー脅威が深刻化する現代は「デバイス自体」のセキュリティを担保しているだけでは安全とはいえません。堅牢なデバイスよりも脆弱性の高い「ユーザ」――つまりは従業員のネットワーク利用時の行動を対象とするフィッシングやデータ漏洩などの脅威にも目を向ける必要があります。Gartnerの調査によると2022年には全マルウェア（悪意あるソフトウェアの総称）の3分の1がモバイルデバイスを対象にすると予測されています。Jamf Threat DefenseではiOSやiPadOS、Android、macOS、Windowsの「デバイス」保護に加えて、これらOSのシステム標準機能では検知しづらいネットの脅威からリアルタイムにデバイスを保護します。

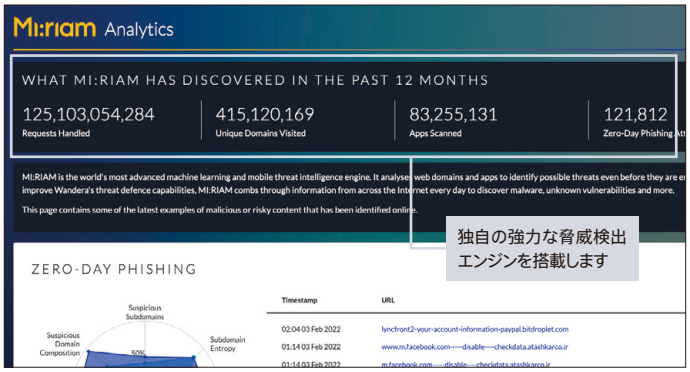
ゼロデイフィッシング対策

電子メールやWEBサイト、SMS、SNSなどを通して偽のURLリンクをクリックさせ、偽サイトに誘導するフィッシング詐欺が増加しています。従業員が被害に遭うと、情報漏洩や不正アクセス、信用喪失など企業にさまざまな影響を及ぼします。Jamf Threat Defense はユーザがアクセスしようとするサイトをリアルタイムに分析し、疑わしいサイトに関しては未然にアクセスをブロックする「ゼロデイフィッシング対策」を実現しています。



脅威検出エンジン「MI:RIAM」

MI:RIAMは、Jamf Threat Defenseに搭載される独自の脅威検出エンジンです。世界中にある4億2500万のセンサ（約9000万のエンドポイントアプリや7500万のドメイン等）を通してネットワーク上の脅威をリアルタイムに検出し、豊富な脅威データベースと高度な機械学習によって既知および未知のネット上の脅威から端末を保護します。

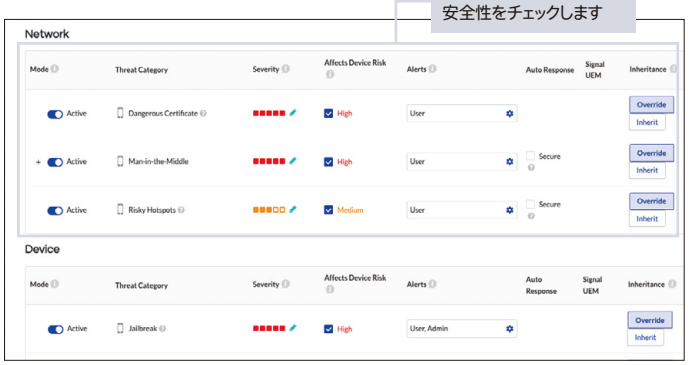


不審なアプリの防御

App Storeをはじめとするサードパーティのアプリストアのリスクアセスメントを行い、不審なアプリをダウンロードするのを防ぐことでマルウェアからの感染を防ぎます。App Storeに登録されるアプリはAppleによって審査されているためマルウェアが紛れ込む可能性は低いもののゼロではありません。Jamf Threat Defense（当時はWandera）は2019年にApp Storeから削除された17本の不正アプリを検出した唯一のMTD（モバイル脅威対策）ソリューションです。

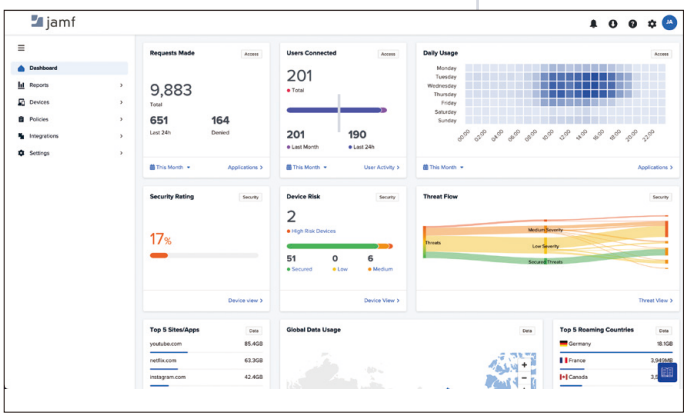
不審なWi-Fiからの保護

リモートワークやテレワークでは在宅やシェアオフィス、カフェなどでWi-Fiを利用するケースが多くあります。しかし、いわゆる「公衆Wi-Fi（フリーWi-Fi）」の中には暗号化に乏しくセキュリティが脆弱なものやアクセスポイントを偽装しているものがあり、こうしたWi-Fiを利用すると情報漏洩や不正アクセスの危険にさらされます。Jamf Threat Defenseでは、Wi-Fiアクセスポイントに不審な証明書などが仕込まれていないかなどを確認し、ユーザの通信を保護します。



グラフィカルな管理コンソール

Jamf Threat Defenseの管理コンソールでは、MI:RIAMによって検出された不審なフィッシングサイトやアプリなどがグラフィカルに一覧で表示され、対処済みの脅威と併せて対処が必要な脅威も容易に確認できます。データベースには登録されていない最新のフィッシングサイトの表示や危険性の理由を確認したり、脅威とみなされる不審なアプリを検出してデバイスにインストールする際に警告を出したりできます。



ポリシーの作成と適用

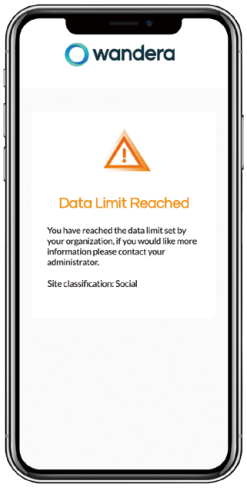
デバイス自体の脆弱性やネットワークの脅威にまつわる各種セキュリティ項目をデバイスが満たしているかどうかを管理コンソールから簡単に確認することが可能です。OSを不正改造していないか、危険性の高いOSをインストールしていないか、画面ロックが無効化されていないか、フィッシングやマルウェア、データ漏洩のリスクはないかといったさまざまなセキュリティ項目に対して企業ごとにアラートレベルを設定したポリシーを作成し、ポリシーに準拠しないデバイスがあった場合は管理者やユーザに対してアラートを出したり、強制的にポリシーを適用させたり、業務用アプリにアクセスさせないなどの対策を施せます。

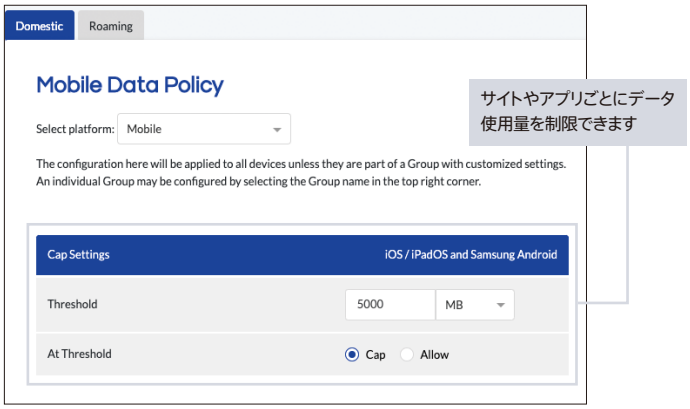
Jamf Data Policyの特徴

リモートワークやテレワーク時代には、業務端末として貸与したiPhoneやiPadなどのモバイルデバイスを従業員がどのように利用しているかを企業側がしっかりと把握する必要があります。WEBブラウザで好ましくないサイトを閲覧していないか、動画アプリで業務に関係のないビデオを視聴していないかを確認したり、場合によっては特定のサイトやアプリをセキュリティ上制限したい場合があるでしょう。さらに、セルラータイプのモバイルデバイスを貸与している場合は、セルラー通信によるOSやアプリのアップデートを禁止したり、従業員が無駄な通信をしていないかのデータ使用量の確認・コントロールも必要になります。Jamf Data Policyを使えば一般的なコンテンツフィルタ製品では難しかった、モバイルデバイス上のアプリの利用や通信の制限、詳細なコンテンツフィルタリング、シャドーITの排除などが可能となります。

データ使用量の制限

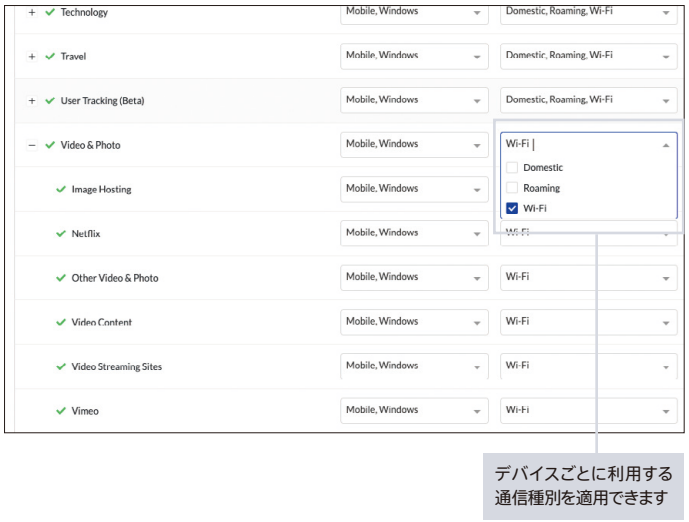
Jamf Data Policyではすべての通信をクラウドプロキシ（Cloud Proxy）経由で行うことで、データ使用量をサイトやアプリごとに細かく分析します。どのデバイスがどのアプリでどのくらいの通信を行っているかをチェックできるため、データ通信制限がかかる前に、データ容量が一定のしきい値に達したら業務アプリのみ通信を許可することなどが可能です。また、データ使用量を元に、あまり使われないアプリを特定しその利用を終了することでコスト削減などにも活用いただけます。





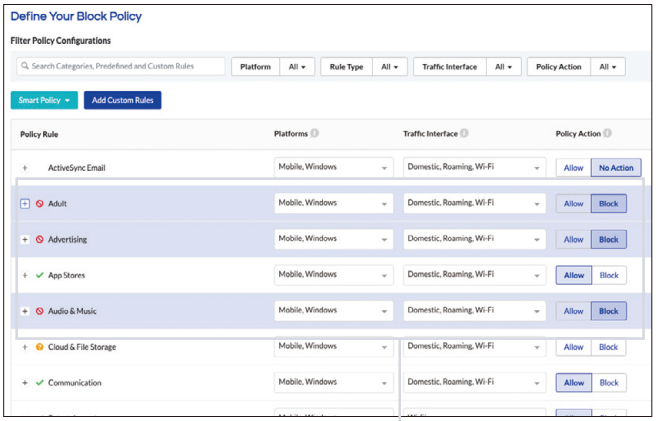
通信種別のコントロール

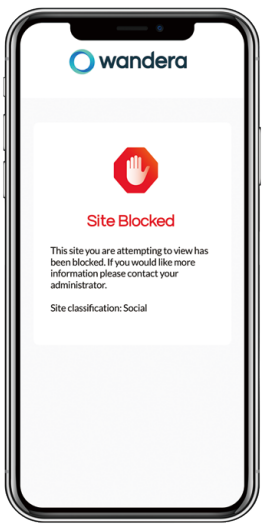
サイトやアプリごとに通信種別（セルラーやWi-Fi、ローミング等）を設定できます。たとえば、動画アプリや動画配信サイトの利用はデータ使用量が多くなるためセルラー通信を使用不可にし、App Storeからのインストールはすべての通信で許可するなどの設定が可能です。また、通信元の国ごとにデータ使用量のポリシーを管理することで海外出張時に予期しないローミング料金が発生することを防げます。



柔軟なコンテンツフィルタリング

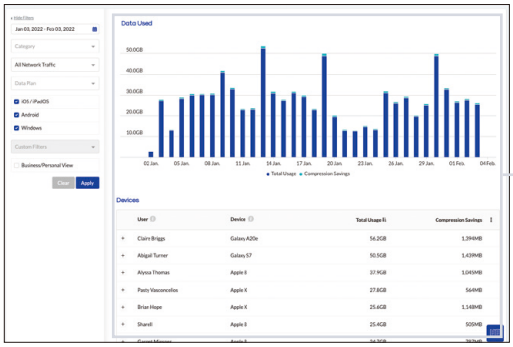
iPhoneやiPadにインストールされているアプリ、またはWEBブラウザやアプリ経由で利用するネットサービスのコンテンツフィルタリングが可能です。アダルトサイトやショッピングサイト、アプリストア等へのアクセスの可否や、動画アプリや動画配信サイト、ゲームアプリなどの利用可否などを、あらかじめ用意された豊富なカテゴリおよび独自にドメイン指定して制御できます。





管理コンソールによる分析

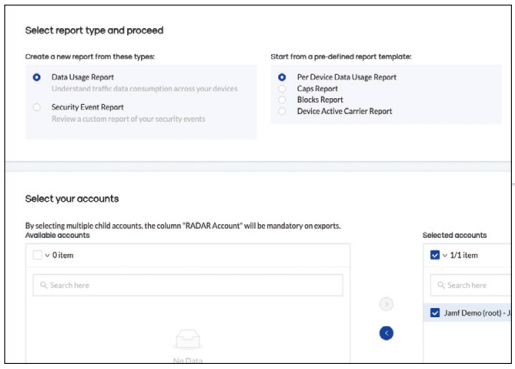
Jamf Data Policyの管理コンソールによって管理者は組織のデータ使用量を詳細に可視化できます。組織全体の一定期間のデータ使用量や通信種別ごとのデータ使用量を確認したり、iOSやiPadOSの場合はユーザや端末を絞り込んでデータ使用量の多いアプリを特定したり、シャドーITを特定したりすることが可能です。また、組織の中でどのようなアプリで通信が発生しているかをカテゴリごとに知れるほか、アプリごとにどのようなドメインに接続しているかを知ることもできます。



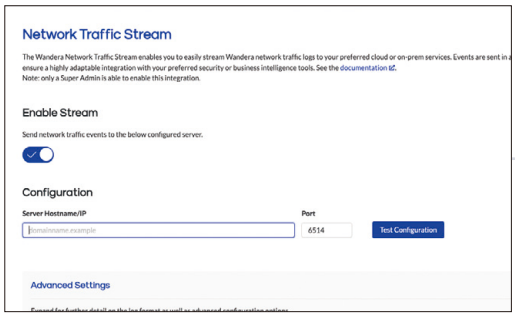
組織全体のデータ使用量を細かく分析できます

レポートの書き出しとSIEM連係

Jamf Data Policyの管理コンソールで取得した各種データは、CSV形式などでレポートとして書き出すことで、業務改善に活用いただけます。また、代表的なSIEMソリューションにエクスポートすることでログを蓄積し、より詳細な分析に役立てることもできます。



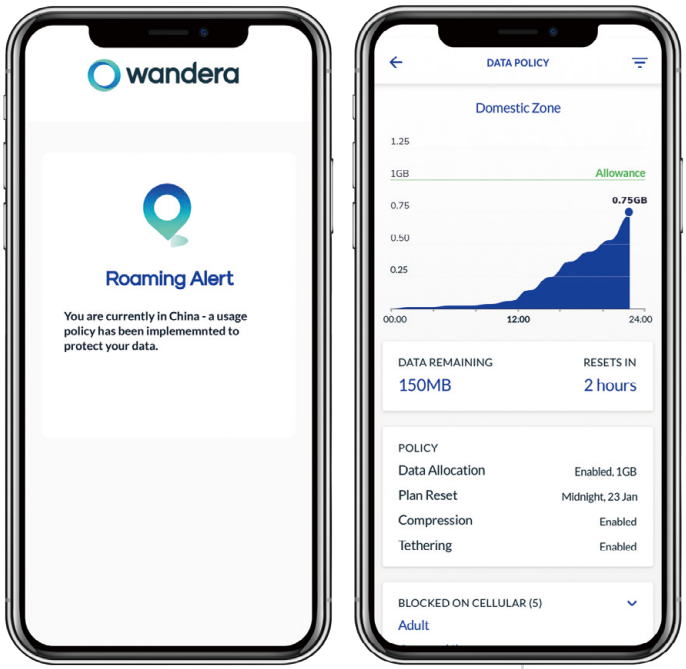
CSV形式などで書き出せます



代表的なSIEMと統合できます

使いやすいクライアントアプリ

Jamf Data Policyのクライアントアプリを使うことで、ユーザは自身のiPhoneやiPadのデータ使用量を確認できます。また、データ使用量のしきい値を超えたり、WEBサイトの閲覧がブロックされたりした際はアラートが即座に通知され、確認することができます。



データ使用量などを従業員が確認できます

MDM経由でリモートでゼロタッチ導入が行える!

Jamf Threat DefenseおよびJamf Data PolicyはJamf ProやJamf Nowのみならず、他社のさまざまなMDMソリューションに対応しているので導入が簡単です。すでに従業員の手元にあるデバイスに対しても、MDMを経由してリモートから強制的に”ゼロタッチ”インストールできます。導入にあたりユーザの操作が必要な場合はユーザが作業を行わないとコントロールできないデバイスが生じてしまいますが、Jamf Threat DefenseおよびJamf Data Policyはそうした心配がありません。

Jamf Threat Defense、Jamf Data Policyのデモは無料でお申し込みいただけます。デモをご希望の場合は右のQRコードを読み取り、弊社WEBサイトから必要事項を記入して申し込みください。

jamf

www.jamf.com/ja/

Jamf Japan 合同会社
東京都港区虎ノ門4-1-1 神谷町トラストタワー25階
Tel：050-1790-2200
E-mail：japan@jamf.com