jamf

モバイル脅威対策

初心者ガイド

Appleの製品は、開封した瞬間から安全に使用できるという点において他のどのプラットフォームよりも優れています。しかし、それ故に攻撃者のターゲットとしての魅力も増しており、組織は現在だけでなく将来の脅威を撃退するための体制を整えておく必要に迫られています。

フィッシング、マルウェア、脆弱性なアプリをはじめとする一般的な攻撃キャンペーンは、以下の目的のためにデバイスを悪用し、企業のリソースや機密データへのアクセスを得ようとします。

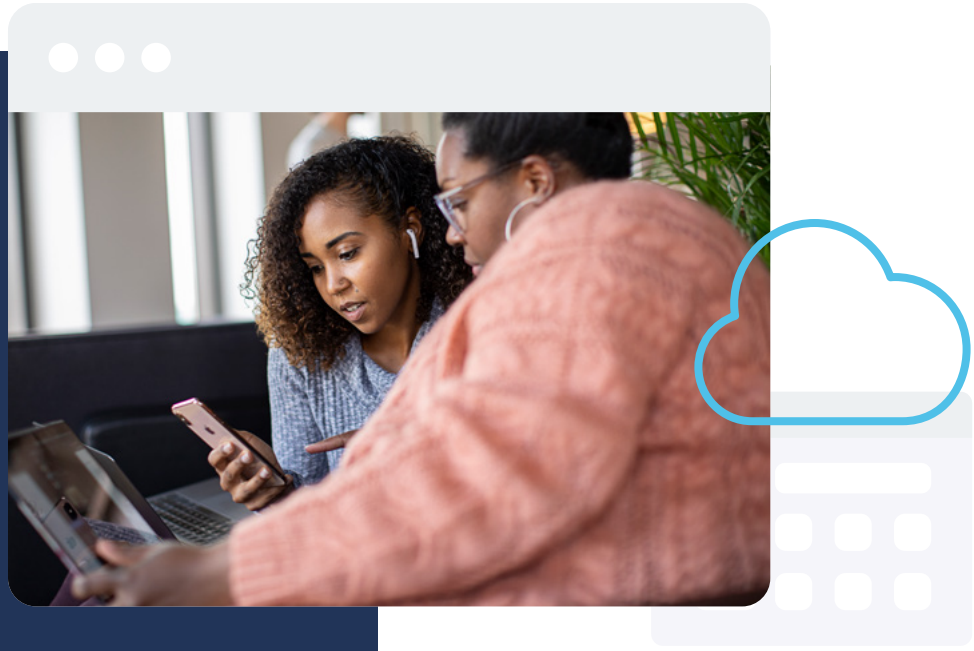
- 機密情報の流出
- 企業サービスへのアクセス取得
- ユーザのプライバシーデータの収集
- ネットワーク通信の傍受

Jamfは、脅威の検出やゼロデイフィッシングおよびマルウェア攻撃の阻止を通じて、モバイルエンドポイントのセキュアな運用を可能にします。モバイルデバイスを狙ったインシデントが増加していることもあり、特にリモートワークやハイブリッドワークを採用している組織にとっては、このような対策は最重要課題のひとつとなっています。

このガイドでは以下の点について説明します。

1. 包括的な脅威の検知と対策
2. あらゆるユースケースに対応する強力な保護
3. リアルタイムのレポート機能
4. ポリシー制御と条件付きアクセス
5. 統合運用管理

APPLEは容赦ない攻撃者の格好のターゲットになりつつありますが...

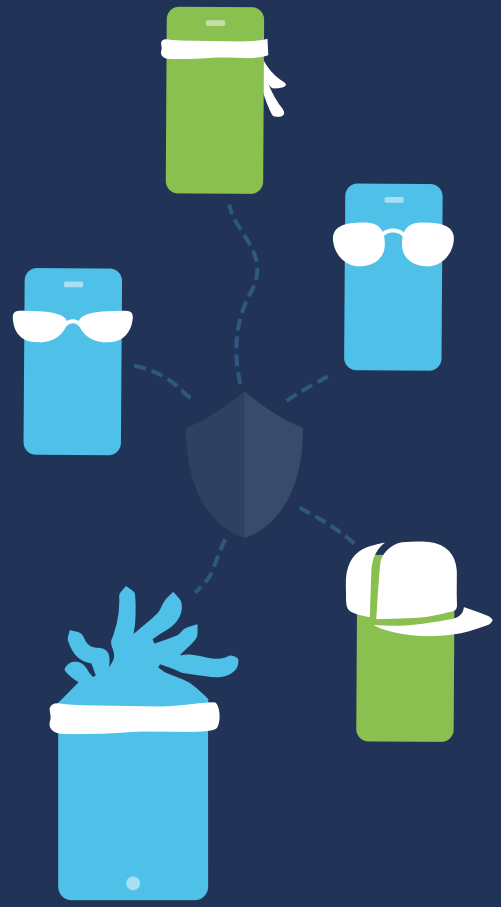


...ご安心ください

Jamf Protectがあります。Jamf Protectは、オーバーヘッド、ネットワークへの負荷、デバイスパフォーマンス、ユーザエクスペリエンスへの影響を最小限に抑えながら、モバイルデバイスとユーザを攻撃から保護することを目的としたソリューションです。

macOSデバイスを使用する従業員を抱える組織は、Jamf Protectを利用することにより、エンドポイントの保護を提供し、セキュリティの脅威からフリートを守るだけでなく、マルウェアの防止やデバイスの健全性の可視化まで手に入れることができます。しかし、iOSやiPadOS、Androidなどを搭載したモバイルデバイスの場合はどうでしょうか。モバイルデバイス特有のニーズに応えるだけでなく、**Jamf Pro**と統合して包括的な管理ソリューションを提供してくれるエンドポイントセキュリティには、どのようなものがあるのでしょうか？

まず最初に守るべきもの



機密性の高いものを守るには、それを含んでいるもの全体を守る必要があります。そして、本ガイドのトピックに関して言えば、それは「モバイルデバイスそのもの」ということになります。なぜなら、攻撃者はモバイルデバイスを足がかりに機密データにアクセスしようとする傾向にあるからです。

「クラウドセキュリティレポート2021」によると、**41%の組織**がリモートデバイスでマルウェア関連のインシデントを経験しており、これは非常に高い割合であるだけでなく、前年から大幅に増加しています。**最新のセキュリティトレンドとリスクについて知ることのできる、「セキュリティ360：最新トレンドレポート」をぜひご覧ください。**

インシデントが急増した原因は、非常にシンプルであると同時に複雑です。まず、リモートワークやハイブリッドワークへの移行に伴ってネットワークの境界が曖昧になりつつあるなか、ユーザはオフィスの外でも生産的に働くためにモバイルデバイスを使うようになっています。ここまでは非常にシンプルです。では何が複雑なのかというと、デバイスやデータの安全性を保つために組織がインフラを進化させている方法です。

Jamfではこの複雑さを少しでもシンプルにするために、高度で強力でありながら、優れた柔軟性と拡張性を持ち合わせたセキュリティ技術をクラウドベースで提供しています。ここには、フリート全体の健全性を監視することができる能力をITおよびセキュリティチームに与えてくれる、リアルタイムの監視や検出・レポート機能が含まれています。

ネットワークの保護

フィッシングは、エンタープライズが直面しているさまざまなセキュリティ脅威のほんの一部に過ぎませんが、セキュリティという鎖のもっとも弱い部分であるユーザを標的としているため、最大の脅威となっています。残念なことに、ユーザをどれだけ教育したとしても、許容誤差があまりにも大きすぎて侵害の成功率が高いため、フィッシングが攻撃の一環として使われることは今後も続きそうです。

ネットワーク内でフィッシングサイトなどに代表されるゼロデイ脅威をリアルタイムで積極的にブロックすることができれば、悪意のある攻撃を引き起こす様々なキャンペーンからデバイスを保護することができます。ユーザとエンドポイントのセキュリティを担保するためには、有線、Wi-Fi、セルラーを含むすべての通信タイプにおいて、デバイスが悪意のあるドメインにアクセスするのを防ぐことが大切になります。

機能の拡張

ベンダーのAPIフレームワークとの統合による機能拡張を念頭に置いて構築されたJamf Protectは、他のセキュリティツールに比べて統合エンドポイント管理（UEM）やセキュリティ情報イベント管理（SIEM）ソリューションとのパートナーシップを多く提供しているのが特徴です。これは、既存のセキュリティツールやデバイス管理ツール、アプリ、サービスなどの価値が最大化されるとともに、脅威の可視化や修復ワークフロー、自動化が活用できることを意味します。

このような統合の良い例として挙げられるのが、Jamf Protectの機能をJamfのRisk APIと組み合わせて、非常に優れたコミュニケーションツールとして利用することです。両システム間でリアルタイムでデータが共有されるため、組織のモバイルデバイスの健全性に基づいたレポートや修復機能のカスタマイズが可能になります。

適応アクセス

Jamf Protectは、増加の一途を辿るサイバーセキュリティ脅威から休むことなくデバイスを保護してくれます。

アクセス関連の脅威が非常に成功しやすい理由の1つに、デバイスが侵害されても明らかな兆候が見られない（例：正常に動作しているように見える）場合、ユーザがリソースにアクセスし続けてしまうという点が挙げられます。デバイスがリクエストを処理してアクセスが許可されてしまえば、リソースを危険にさらすことになります。

Jamfの場合、セキュアなコネクションと信頼できるデバイスのみに組織のリソースへのアクセスを許可することで、この問題に対処し、同時にセキュリティ態勢の強化を図ります。これはどのような仕組みなのでしょうか？

各デバイス固有のテレメトリデータやコンテキスト入力を継続的に監視することで、異常がないかを確認します。

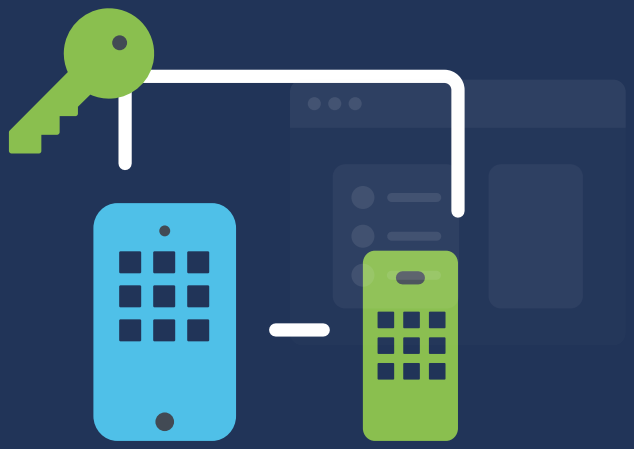
そしてエンドポイントに高いリスクがある、または侵害されていると判断された場合、Jamf Protectはカスタムポリシーを適用してリソースへのアクセスを遮断します。

高度な機械学習

Jamfを活用してエンタープライズやモバイルデバイスを保護する方法についてここまで見てきましたが、次は脅威からデバイスを守るためのソフトウェアの基盤についてもう少し詳しく見ていきましょう。ソフトウェアの機能そのものではなく、前述の機能を支える内蔵の防御テクノロジーであるMI:RIAMをご紹介します。

MI:RIAMは、既知の脅威からゼロデイ脅威までリアルタイムで幅広く特定する高度なインテリジェンスエンジンです。脅威に関する膨大なデータを活用するMI:RIAMは、世界中の4億2500万個のセンサーから収集した情報をベースにしたアルゴリズムと高度なデータ科学を使用し、最新の脅威インテリジェンスやアクティブなリスクに関するインサイトをリアルタイムで提供しています。

あらゆる
デバイスに対応



組織のフリートがiOSおよびiPadOSのデバイスのみで構成されている場合でも心配はいりません。Jamf Protectは、現在および将来の脅威からAppleデバイスとユーザを保護するために必要なセキュリティ機能を備えています。

Apple以外のモバイルデバイスがフリートに含まれている場合でも、まったく問題ありません。Jamfは、AndroidやWindowsのOSについても、他のモバイルデバイスと同様のセキュリティ強化を提供しています。また、Jamfはあらゆる所有モデルに対応しており、企業所有デバイスかBYODデバイスかに関わらず、セキュリティにフルフォーカスしたサポートを提供しています。

ユーザは自分が守られていることを感じたいものです。そしてITやセキュリティチームの担当者は、ユーザがどのような方法で保護されているのかを知りたがるものです。しかし、ネットワークセキュリティや機密情報を保護する上で、攻撃者にはできるだけその詳細を知られないようにするのがベストです。さらに、セキュリティ態勢を維持し、ITおよびセキュリティチームにエンドポイントの最新の健全性データを提供するために、何としても安全を確保しておきたいデータタイプがいくつかあります。

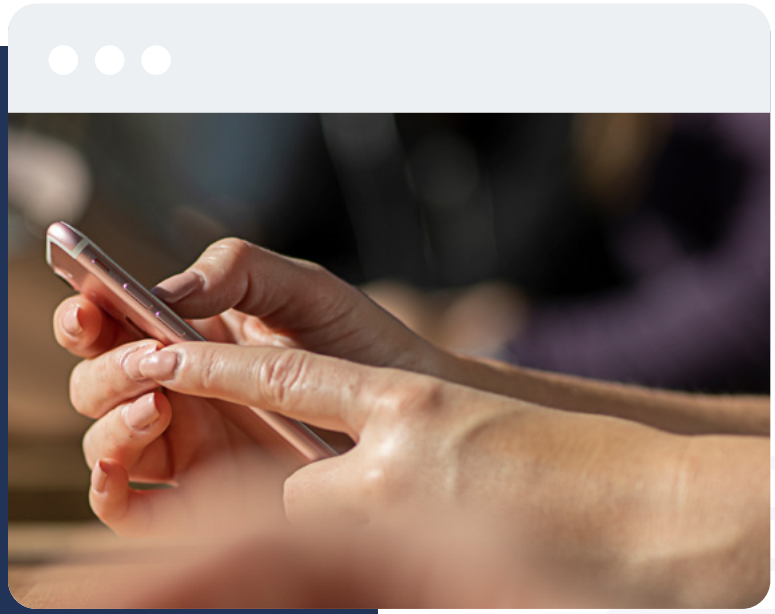
ユーザプライバシー

個人健康情報（PHI）などを含め、個人を特定できる情報（PII）は攻撃者が喉から手が出るほど欲しいデータのひとつです。こういったデータは、集めれば集めるほど今後の攻撃への足がかりとなり、犯罪を達成するための格好の手段となります。

幸いにも、Jamfは通信の暗号化やフィッシング対策を通じてオンラインプライバシー保護を提供しています。これは、ユーザの個人データだけでなく、コンプライアンス遵守のために必要な機密データにも適用されます。また、高度なプライバシー機能とポリシー制御により、リスクのあるユーザやデバイスによる企業リソースやデータへのアクセスをブロックすることができます。

リアルタイムの可視性

ITおよびセキュリティチームは、Jamf Protectに搭載されたレポート機能を利用して、エンドポイントの健全性に関連する詳細を手に入れたり、組織の特定のニーズに合わせてその詳細をカスタマイズしたりすることができます。また、Jamf Protectの活用をさらにレベルアップさせたい場合は、管理者がコンソール内でリアルタイムデータを確認できるようにレポート機能をカスタマイズしたり、内蔵の統合機能を使ってSIEM（セキュリティ情報イベント管理）ツールにエクスポートし、ダッシュボードでデータを可視化したり、APIを活用して統合ポイント管理（UEM）ソリューションと統合させたり、またはJamf Proと組み合わせてソフトウェア間でデータをストリームし、デバイス管理の自動化や検出されたエンドポイントの問題を修復したりすることも可能です。



組織のデータ、デバイス、そしてユーザを保護するためにできることは
無限にあります。このガイドで紹介しきれなかったことも含め、
ぜひJamfでできることを実際に体験してみてください。

Jamfの無料トライアルで、ぜひその可能性をご自身の目でお確かめください。
もしくはお近くの販売代理店にお問い合わせください。

トライアルに申し込む