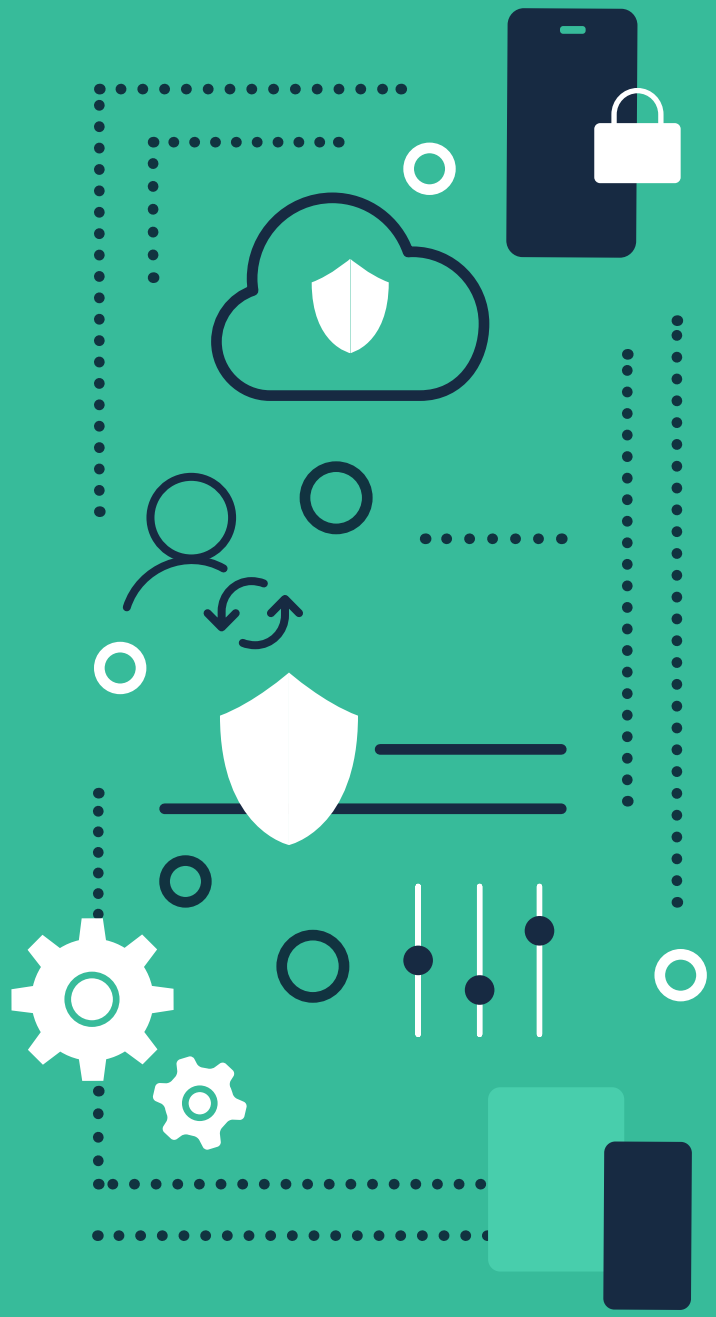


jamf

Macのための エンドポイント保護

初心者ガイド

ネイティブセキュリティだけでは十分でない理由

Macが開封した瞬間からもっとも安全に使用できるデバイスであることに疑いの余地はありません。その事実は10年前も、今も変わりません。組織が業務に使用するフリートの構成を考えるとき、データやデバイス、ユーザを保護するセキュリティソリューションは非常に重要な要素となります。

このことを軽く考えていれば、組織にとって有害、または経済的損失につながるセキュリティ侵害を許してしまう可能性もあります。Mac向けに作られたエンドポイント保護ソリューションを利用することで、ITチームやセキュリティチームは、既知の脅威からの保護はもちろんのこと、組織の将来的なセキュリティニーズを予測し、それに適応し続けることができます。

Appleフリートを保有する企業であっても、少数のMacデバイスを管理する小規模ビジネスであっても、JamfならAppleがネイティブ機能として提供するエンドポイント保護機能を拡張し、組織のmacOSデバイスやデータ、エンドユーザを保護することが可能です。

このガイドのトピック：

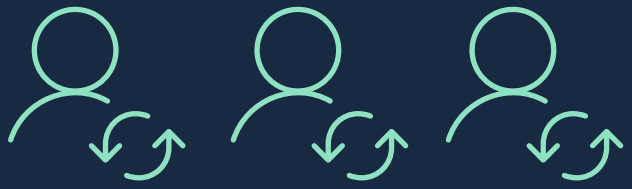
- Macのためのエンドポイント保護とは
- 複数のオペレーティングシステム向けに設計されたエンドポイント保護がMacにとって不十分である理由

Macのための
エンドポイント保護

Appleネイティブのセキュリティ機能のメリットを拡大し、未知の脅威に備えましょう。

Macを使用するエンタープライズや小規模のビジネス、学校、ヘルスケア組織などが増えるなか、デバイスやデータが認証されたユーザによって正しい目的のために使われていることを確認する重要性が高まっています。そこで必要となるのが、Macのために作られたエンドポイント保護機能です。

これを実現するためには、アイデンティティ管理、パッチ適用、アンチウィルス（AV）、構成、エンドポイント検出応答など、いくつもの要素を組み合わせてITやセキュリティチームのニーズに応える必要があります。



企業のリソース、データ、ユーザを管理する方法について説明した当社のeBook「アイデンティティ管理 初心者ガイド」も併せてご覧ください。

アイデンティティ&アクセス管理

アイデンティティ管理を通して実行されるセキュリティ対策は、オフィス勤務かリモート勤務かに関わらず、従業員のライフサイクル全般を通じてエンドユーザとITの双方に影響を及ぼします。ゼロトラストネットワークアクセス（ZTNA）、仮想プライベートネットワーク（VPN）、SaaSアプリケーションなど、従業員を企業リソースにつなげるためのこれらのソリューションはすべて、エンドポイント保護を強化する機会を提供します。

ワークフォースのモバイル化が進み、従業員がさまざまな場所であらゆるタイプのデバイスを使って仕事をするようになりつつある今、組織はオンプレミスのActive Directoryへの紐付けという課題から自らを解放し、デバイスや企業データを管理・保護する方法を求めています。Jamf Connectは、ユーザが入社してから退社するまで継続的にサポートします。Jamf Connectを使うことで、ユーザはMacを開封し、電源を入れて、単一のクラウド認証情報でサインインするだけで企業のすべてのアプリケーションにアクセスできるようになります。さらに組織は、エンドユーザへの影響を最小限に抑えながらアイデンティティとアクセスを監視し、デバイスとデータのセキュリティを一貫して優先させることができます。

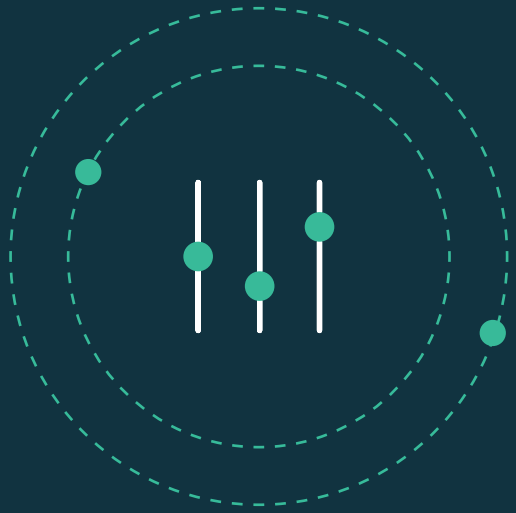
アプリ管理

アプリ管理の自動化は、作業の簡素化に加え、ユーザのセキュリティや生産性を強化します。

ユーザがJamfのSelf ServiceアプリやMac App Storeのような安全な場所から適切なアプリを入手できる環境を作ることで、以下のことが可能になります。

- 正しいユーザとデバイスに対してアプリを導入
- ユーザが必要な時に入手できるカスタムタイトルやアプリ
- IT側でアップデートをプッシュ、または組織とユーザのセキュリティを確保するための要件を設定

組織のアプリケーションやソフトウェアのライセンスを割り当てる、または管理するには、Jamf ProとApple Business Manager を統合するのがベストです。Jamf Proはパッチ適用やソフトウェアアップデートに対するサポートに加えて、脆弱性のあるソフトウェアのバージョンアップデートや管理、組織のMacフリート全体の状況の可視化なども提供しています。既知の脆弱性に対する対策を確実に行うためにも、セキュリティパッチは頻繁にかつ簡単に適用されなければなりません。Jamfを使用することで、macOS上のアプリケーションのメンテナンスやアップデートに必要な作業を効率化し、コンプライアンスと互換性に対する可視性をさらに高め、質の高いエンドユーザエクスペリエンスを提供することができます。また、アップグレードの遅れによってセキュリティに穴が開く事態を避けるために、常に最新バージョンのmacOSがデバイスに搭載されていることも大切です。



セキュリティや管理ツールが原因でOSのアップデートやアップグレードに遅れが出てしまっては、元も子もありません。Jamfはこのような遅延の原因となるソリューションではありません。それどころか、新しいmacOSのバージョンがリリースされたその日からサポートを提供します。それぞれの組織にとって都合の良いタイミングでデバイスのアップグレードを行うことが可能なのです。

アンチウィルス（AV）

アンチウィルスはこれまで、Macにとって必要のないものだと考えられてきました。ですが、現実は変わりつつあります。エンタープライズにおける普及が進むにつれて、MacとmacOSへの注目度が高まっています。

ほとんどの組織にとって、AVはデバイスにベースラインのセキュリティを提供するために必要なものです。macOSには、XProtect、Gatekeeper、MRTといった基本的なAV機能が搭載されています。しかし、これらのツールはあまり定期的にアップデートされておらず、そのアクションに対してもあまり可視性がありません。Macを狙ったマルウェアの阻止と検疫のための高度なAV機能を追加するJamf Protectは、WindowsベースのソリューションがmacOSに提供できる範囲をはるかに超えています。

マルウェア、アドウェア、その他の迷惑なソフトウェアの問題が発生してから対策を打ったり、またWindowsを狙った脅威をMac上で探すのではなく、Macを狙った攻撃を効果的に検出し、修復してくれるAVを導入するのが賢明です。デバイスのセキュリティやユーザエクスペリエンスの点においても、効果的かつ効率的、そして包括的なMac向けのAV機能は不可欠です。ただし、エンドユーザの生産性を阻害するようなAVソリューションは、誰にとっても迷惑な存在でしかありません。Jamf Protectは、エンドユーザがMacに求めるエクスペリエンスを変えることなく、マルウェアからmacOSを保護するために設計されています。

Mac向けのAVはもはや「あったらいいな」ではなく、「なければならない」ものです。AVが必要なのはもちろんですが、複数のシステム用に設計されたAVがもたらす制限に縛られないために、Mac用に構築されたAVが必要なのです。

構成

Macに内蔵されたセキュリティ機能は非常に優れていますが、日々進化し続けるサイバーセキュリティの脅威に対抗するには十分ではありません。デバイスとデータを確実に保護するためには、セキュリティポスチャを評価し、進化させる必要があります。セキュリティの堅牢化を簡単に行える方法があるのなら、積極的に使用したいものです。

セキュリティコミュニティは、すでにこの件に関して豊富な知識を持っており、それを実行するためのスクリプトもすでに存在しています。

Jamfを使えばこれらを簡単に実行でき、基準から逸脱しようとするユーザをモニタリングすることも可能です。組織の全デバイスのベースラインセキュリティを設定する上で、妨げとなっていた可能性のある障害を取り除くことができるのです。

FileVault、ファイアウォールやパスワード要件の適用、スクリーンセーバーやロック条件の設定など、すべてを組み合わせてセキュリティ要件やベンチマークの位置づけを行うことが可能になります。

どこから始めて良いかわからない場合は、まずはJamfを試してみることをお勧めします。Jamfは、Center for Information Security（CIS）が提供している業界ベンチマークの認定を受けており、豊富なサポート資料もご利用いただけます。

CISのセキュリティベンチマークとJamfに興味のある方は、ぜひ「macOSのセキュリティチェックリスト」も併せてご覧ください。

Macに特化した検出と対応

従来のエンドポイント検出対応（EDR）ツールはかなり前からMac用に存在していましたが、そのほとんどは、Macだけを標的とする攻撃を効果的に検出するようにはできていません。どちらかというと、Windows向けのソリューションを無理やりMacに当てはめようとしたものでした。MacとmacOSにフォーカスしたツールであるJamf Protectは、誤検知を最小限に抑えながら、Macにおける検出率を最大限まで高めてくれます。

Jamf Proと組み合わせることで、エンドユーザへの影響を極限まで抑えながら、一般的なEDRの能力をはるかに超える修復能力を提供することができます。また、シームレスなインシデント対応プランを用意することで、ITやセキュリティチームはより優れた協力体制を築くことができます。

JAMF = エンドポイントセキュリティ

Jamf ProtectによるMacのエンドポイント保護は、エンドポイントのコンプライアンスをサポートし、macOSを狙ったマルウェアを阻止することでアンチウイルスのニーズに対応します。また、組織で使用されているMacアプリケーションのコントロールや保護を提供し、エンドユーザへの影響を最小に抑えながら、Macを狙った脅威を検知し、修復することができます。

また、Jamf Proと組み合わせると、さらに幅広い自動化や調査、修復機能を利用できるため、エンドポイントにおける大小さまざまなセキュリティリスクを軽減することが可能になります。

無料トライアルに申し込む

またはお近くの販売代理店までご連絡ください。セキュリティの堅牢化のお手伝いをさせていただきます。

Jamfが提供するエンドポイント保護機能に関する詳細はこちらからご覧いただけます。