jamf

ホワイトペーパー

macOSのセキュリティ機能をJamfで強化

プライバシーやセキュリティの機能をどれだけ搭載していても「完璧なオペレーションシステム」というものは存在しません

セキュリティに対するニーズはあらゆるオペレーティングシステムで高まっており、macOSも例外ではありません。Appleではネイティブのプライバシー機能とセキュリティ機能に多大な投資を行ってきましたが、エンタープライズにおけるMacプラットフォームの採用が拡大するにつれ、マルウェアや侵害、脆弱性利用のターゲットとしてのMacの価値も上昇しています。さらに、多くの企業がこれまでに以上に、従業員選択プログラムを通じて従業員にmacOSの使用を許可しているという現状もあります。このことから、他のプラットフォームと同様に、macOSにもセキュリティの強化や可視性の向上が必要であることが明らかになりつつあります。

Macを保護するためのソリューションは複数のセキュリティベンダーによって提供されていますが、ベンダー固有のものであったり、Windows製品向けに作られたものであったりすることが多く、macOSの最新フレームワークを利用して作られたものではありません。そのため、刻々と変化するオペレーティングシステムに対応することが難しくなっています。このことから、既存のmacOSセキュリティモデルの足りない部分を埋め、効果的に組織を脅威から守るためにセキュリティチームが必要としている、macOS特有の付加価値を追加することが重要になります。

Appleのオペレーティングシステムは、ユーザとユーザのプライバシーの両方を保護するのはもちろん、使いやすさと生産性を第一に考えて設計されています。さらに、Appleはビジネスそのものよりも、そこで活動するユーザを中心に据えたエクスペリエンスを作り出すことに重きを置いています。そして、同じことがmacOSのセキュリティとプライバシー機能の多くにも言えます。

このホワイトペーパーでは、macOSセキュリティの現状について説明するとともに、Appleのセキュリティベースラインを効率的、効果的かつユーザフレンドリーな方法で強化する方法についてご紹介します。

本ホワイトペーパーのトピック

- Macに内蔵されたセキュリティ機能の詳細
- エンタープライズ向けにMac内蔵機能を強化するJamfのソリューション
- 署名や内蔵セキュリティ機能を超えたJamfの脅威検出能力の仕組み
- Appleのセキュリティモデルを拡張して高度なエンタープライズセキュリティを実現する方法

macOSのアプリケーション

Appleは、自社デバイスで実行されるサードパーティ製アプリケーションとそれを使うユーザを保護するためのセキュリティ機能の設計に注力してきました。このセクションではこうした機能の一部を紹介し、それらを戦略的に強化および拡張する方法について説明します。Appleのセキュリティ機能についての詳細は、「Appleプラットフォームのセキュリティ」ガイド（**https://support.apple.com/ja-jp/guide/security/welcome/web**）をご参照ください。

Gatekeeperによる信頼の検証

サードパーティのアプリケーションをインストールするもっとも信頼性の高い方法としてAppleが推奨しているのがApp Storeです。AppleはApp Storeを通してアプリケーションの審査を行い、プライバシー、セキュリティ、ユーザエクスペリエンスの面でAppleの基準を満たさないプログラムをふるいにかけます。しかし、App Storeのアプリケーションには機能に対する制限が課されており、ビジネスに必要なアプリケーションの中にはApp Store経由の配布に適さないものが多くあります。

App Storeからの配布が不可能な場合、開発者はmacOS用アプリケーションをホスト型ダウンロードやその他の従来の方法で直接配布することができます。こうした「アドホック型」の配布をサポートするとともに、macOSデバイスでこういったソフトウェアが蔓延するリスクを軽減するために、Appleはオペレーティングシステムに追加の検証機能を導入しました。これこそがGatekeeperであり、Appleの認証チェックにおいて中心的な役割を果たしています。当初はリスク選好に基づいてプログラムの実行を許可するmacOSの機能としてスタートしたものが、現在は幅広い範囲をカバーし、厳しい要件と対策の両方を提供するものへと進化しています。今でも「AppStore」または「App Storeと確認済みの開発元」からのアプリのみダウンロードを許可するという基本的なオプションは存在しますが、問題やリスクのあるコードを実行するオプションに対しては厳格な対応がなされていない状況が続いています。

さらに、こうした検証はインターネットからダウンロードされたアプリケーションにのみ適用されます。Appleは、ダウンロードされたファイルに「隔離属性」と呼ばれるメタデータを追加することで、このようなアプリケーションを追跡しています。プログラムが実行されると、隔離属性の検証を含む一連のチェックをGatekeeper が行い、プログラムの実行が可能かどうかを判断します。その中でももっとも基本的なチェックの1つが、アプリケーションが正当な開発者によって署名されているか、またはApp Storeを通じて配布されているかを確認するものです。

アプリケーションに開発者の署名がある場合は、失効した署名が登録されているデータベースと照合し、署名者が過去にマルウェアに関係していないことを確認します。こうすることで、必要に応じて証明書を無効化し、マルウェアの蔓延を防ぐことができます。macOS Catalina以降、Gatekeeperのセキュリティチェックを通過するにはAppleのノータリゼーション（公証）が必要になっています。セキュリティチェックを通過するには、ア

プリケーションをAppleにアップロードして分析にかける必要があります。分析に問題がなければ、公証データがアプリケーションと紐付けられ、追加チェックに合格したことが証明されます。

最終的な信頼はユーザが決める

ユーザビリティの観点から、macOSではさまざまな場面でエンドユーザがGatekeeperを無効化することができます。アプリケーションを右クリックして、「開く」または「プログラムから開く」をクリックすると、アプリケーションの起動を頑なに拒否する代わりに、信頼されていないアプリケーションを起動しようとしていることを警告するダイアログが表示されますが、アプリケーションの実行自体をGatekeeperが止めることはありません。ただし、XProtect によってすでに特定されているマルウェアについては実行できません。

アプリケーションが初めて実行されたときに隔離コンポーネントが更新されるので、次にアプリケーションを開いたときにGatekeeperが同じ動作を繰り返すことはありません。

XProtectとMRTによる脅威のブロック

Gatekeeperには、XProtectと呼ばれる署名ベースの検出メカニズムやマルウェア除去ツール（MRT）など、さまざまなテクノロジーが含まれています。こうしたテクノロジーを組み合わせることで、オペレーティングシステム上のファイルをスキャンしたり、既知のマルウェアと関連しているファイルに隠された特徴を探し出すことができます。XProtectがアプリケーションの起動時に作動するのに対して、MRTは定期的にファイルシステムをスキャンします。

XProtectは、Yaraと呼ばれるバイナリ署名スキャンエンジンによって動作します。Yaraは柔軟性が高く強力なバイナリ署名定義と効率的な実行エンジンをサポートしています。アプリケーションの信頼性を検証するために、XProtectは初回起動時のみ、ダウンロードされた実行ファイルをスキャンします。一致する署名が検出されるとプログラムの実行は許可されません。不正な署名のリストは、Appleが提供するmacOSの独立アップデート経由で提供されます。Appleは、Yaraの実行エンジンとは別に、これらの署名を適切な形で定義し、配信しています。Gatekeeperと同様に、このスキャンはアプリケーションが適切な隔離属性を有している場合にのみ実行され、アプリケーションの初回起動が成功した後にアップデートされます。

一方、MRTは、プログラムの実行時ではなく定期的に実行され、ファイルシステムのスキャンで過去に特定されたマルウェアに関連するファイル名やアーティファクトと照らし合わせ、発見された場合はそれらを削除します。この機能は、すでにmacOS全体を狙っている可能性のある既知の脅威を発見し、対策することを主な目的としています。

エンタープライズにおけるGatekeeperの活用

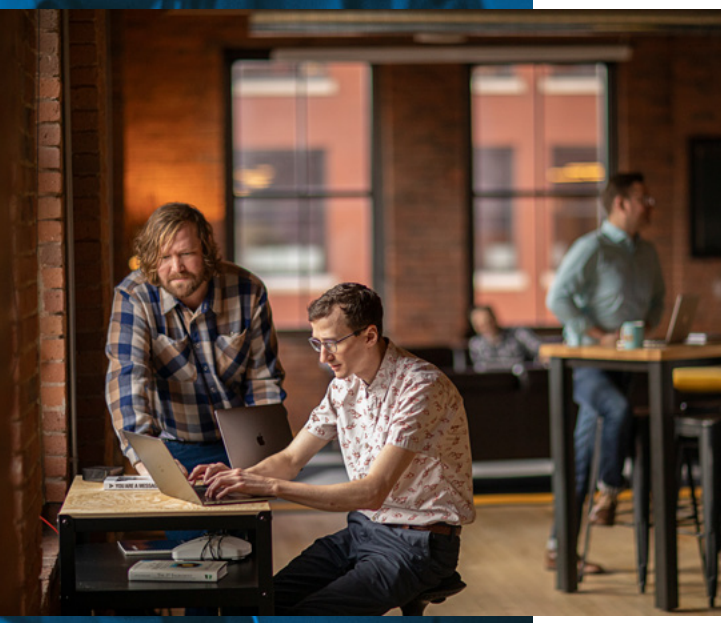
Gatekeeperは、その役割を効果的にこなすことで知られています。信頼性が確認されていないアプリケーションの起動をブロックし、不審あるいは悪意のあるアプリケーションが特定された場合はユーザに通知します。IT管理者やセキュリティ管理者は、企業所有デバイス上で信頼できないソフトウェアを実行する試みを、逐一把握している必要があります。さらに重要なのは、危険なアプリケーションを実際にクリックして実行したのがユーザ自身であり、組織によって用意されたセキュリティ制御をかいくぐって行われたという事実を理解することです。このようなエンタープライズのニーズに応えるために作られたMac専用のエンドポイントセキュリティソリューションであるJamf Protectでは、Gatekeeperのアクションの兆候を監視し、その結果を一箇所にまとめることで、ITチームやセキュリティチームがリスクを正確に評価し、正しい意思決定を行えるよう支援します。

Jamf Protectでは、Gatekeeperのアクティビティの可視化だけでなく、エンタープライズ環境において信頼できないと判断された署名情報を各組織が登録できるため、各組織が信頼できる開発者を決めることが可能です。さらに、Appleの最新のエンドポイントセキュリティAPIを使用しているため、組織固有のブロックリストに含まれるアプリケーションの実行を積極的に拒否することができます。これは、アプリケーション（アプリケーションID）またはベンダー（デベロッパのチームID）ごとに定義できます。

また、迷惑または侵略的な動作をする多くのアドウェアやクリプトマイナーを含む、様々なグレイウェアの署名やブロック機能をmacOSは提供していません。多くの場合、これらのプログ

ラムはAppleの開発者によって合法的に署名されており、ユーザはインストール時に、自分の情報が収集されたりリソースが使用されたりすることに（意図せず）同意しています。したがって多くの場合、Appleはこういったアプリケーションの実行を妨げません。

しかし、エンタープライズでは単純にリスク許容度が異なるため、より厳格で的を射たアプローチが望まれる場合があります。そのため、Jamf Protectは、隔離拡張属性の有無にかかわらず、独自に管理されたYaraルールやバイナリの署名、信頼できない開発者の証明書などを強制適用し、アプリケーション実行時のスキャンに使用しています。これにより、新しい署名が追加され、エンタープライズがセキュリティ態勢をアップデートした場合に、既存のアプリケーションが次回実行時に再びスキャンされるようになります。



Jamfは、macOSを標的とした脅威に関する自社の幅広いリサーチやサードパーティーの研究データに基づいて、Macを狙う既知マルウェアのフィードを作成しています。環境内で使用されているソフトウェアをよりきめ細かく制御したいと考える組織は、Jamf Protectのブロックリストに独自のリスト（バイナリのハッシュ値やチームIDなど）を加えて強化することもできます。macOS 10.15（Catalina）以降が搭載されたMacで、既知のマルウェアの挙動や署名に一致するアプリケーションが実行されそうになった場合、Jamf Protectはそのプロセスを阻止し、問題のファイルを隔離した上でマルウェアが阻止されことを記録します。これら一連のアクションは、GatekeeperまたはXProtectとは別に行われ、セキュリティのさらなる強化につながります。安全でない可能性があるバイナリを識別するための隔離ビットとは関係なく既知のマルウェアを検出することのできるJamf Protectは、より幅広いマルウェアの知識を有しています

App Storeの信頼モデルを拡張するSelf Service

状況によっては、ITの承認を受けたリソースが揃った自社アプリストアを用意して、セルフサービス形式でユーザがインストールできるプログラムを指定しておく方法が適切な場合もあります。

JamfのSelf Serviceは、独自のアプリカタログを作成したいと考えるエンタープライズのIT部門をサポートするためのアプリです。アプリのインストールや構成の変更を行う機能や、よくある問題のトラブルシューティングなどを用意しておくことで、ユーザは安全かつ迅速に必要なリソースにアクセスでき、さらにヘルプデスクへの問い合わせ件数も減らすことができます。

アプリケーションの動作のコントロールと監視

プライバシーコントロールでアプリケーションの動作を検出および制御する

プライバシーに関する環境設定がmacOS Mojaveで登場しました。これによりユーザ（またはエンタープライズ）は、アプリケーションごとに特定のアクションやフォルダへのアクセスを許可することができるようになりました。特定のアクションが一度許可されたら、そのアクションがアプリケーションで検出された際にユーザに通知されることはありません。この機能は、危険を含む可能性のあるOSの要素（ウェブカメラ、マイク、キーストローク、ダウンロード）へのアクセスを特定のアプリに対して明示的に許可するもので、プライベートデータへのアクセスをアプリケーションに許可する前にそのことをしっかりと考えるきっかけをユーザに与えてくれます。

アプリケーションの動作を監査・分析する

ユーザはプライバシー設定を通してアプリケーションに何を許可するのかを決めることができますが、時には判断を誤ったり、権限を乱用したりすることもあるかもしれません。
Jamf Protectが、Appleデバイスに内蔵されたセキュリティ機能や従来のマルウェアやアドウェア防御機能のアクションを可視化することで、エンタープライズに知識と保護を提供することはすでに説明しましたが、エンドポイント保護ソリューションはそれだけに留まるべきではないとJamfは考えています。Jamf Protectは、Appleユーザの求めるプライバシーとセキュリティのスタンダードに目を向けた「Appleファースト」の姿勢を保ちながら、従来エンドポイントの検出と応答（EDR）ソリューションに限られていた監査と監視の機能も併せて提供しています。

Jamf Protectの検出技術

Jamf Protectエージェントの中核を成すのは、Apple独自のロジック実行エンジンであるGameplayKitを活用した、ユーザモードのセンサー（付随テキストなし）です。セキュリティイベントの分析にゲームエンジンを使用していることを意外に思う人もいるかもしれません。しかしこれにより、Appleエコシステムと密接に統合した状態を保ちながらデバイス上のデータを分析し、必要なタイミングでそれを収集またはレポートすることができるのです。
また、ゲームエンジンは膨大な数のイベントをリアルタイムで処理できるように設計されているため、デバイス上で発生するアクティビティの分析に最適です。これは、Windowsプラットフォームにまず焦点を当てて設計され、後付けでmacOSに移植された多くのセキュリティソリューションや、すべてのデータをクラウドで収集し分析することを必要とするソリューションとは対照的です。

GameplayKitのもうひとつのメリットは、Yaraの場合と同じく、実行エンジンと検出定義を分離することで、コアエージェントをアップデートすることなく検出を更新・拡張できることです。検出定義もまたAppleネイティブのものであり、正規表現だけでなく一般的なクエリ構文もサポートする強力なロジッククエリを構築するためのクラスであるNSPredicateを使用しています。Jamf Protectのデータモデルは、ネイティブ機能の呼び出しやデータモデルの連結など、NSPredicateの豊富な機能を活用することを念頭に置いて設計されています。これにより、従来の方法では実現が困難であったり、計算コストが高かったりする機能が利用できるようになります。例えば、Jamf ProtectのデータモデルとNSPredicateを使用すると、以下のようなことが可能になります。

- 自分の痕跡を消すための一般的な手法であるファイルの自己削除があった際にアラートで通知します。これはシンプルなユースケースに見えますが、高価な結合操作やハードコード検出を行うことなく、削除されたファイルと削除プロセスの両方を分析するものです。

- 署名されていない、または不審な署名が認められるバイナリが起動デーモンとして何度も使用された場合にアラートで通知します。そのために、構成ファイルを解析し、埋め込まれたバイナリパスを抽出し、そのバイナリファイルに関するメタデータを解析に使用します。

- Microsoft Officeのマクロ悪用によりアプリケーションが予期せぬ子プロセスを作成した場合にアラートで通知します。これは、親プロセスと子プロセスの関係を理解し、アプリケーション機能が悪用された時に発見できることを意味しています。

- 環境寄生型（LotL）攻撃と思われるアクティビティが検出された場合にアラートを送信します。この種のアクティビティは、通常であれば無害なアクティビティ（curl、ssh、pythonなど）の悪用を発見するために、親のプロセスグループの関係やコマンドラインパラメータなどへのアクセスが必要になります。
- エンタープライズ全体におけるUSBの使用状況を追跡し、リムーバブルメディアに書き込まれているファイルに関するメタデータをレポートします。

Jamf Protectでは、このような検出の影響をより良く理解できるように、特定された攻撃をMITRE ATT&CK™フレームワークにマッピングしています（該当する場合のみ）。現在では、以下のカテゴリに分類されるテクニックの検出を含み、フレームワーク全体のユースケースがカバーされています。

- 永続化
- 初期アクセス
- C&C
- 防衛回避
- 探索
- 権限昇格
- 認証情報アクセス

シンプルな統合ログの収集とレポート

セキュリティアナリストやIT管理者の多くは、コンプライアンス監査の一環として、あるいは他のセキュリティ制御の足りない部分を埋めるために、エンドポイントのログを必要としています。macOSのログがsyslogから統合ログに移行したとき、エンタープライズ全体に関してこのような情報を収集および分析することが難しくなりました。macOS Console.appは、ローカルMac上の統合ログインフラへの優れたアクセスと可視性を提供しますが、そのデータを一元化するのは簡単ではありません。

ところが、Jamf Protectを使えば、統合ログが作成されたタイミングで好きな記録システムにその情報をストリームすることが可能になります。管理者は、Jamf Protectに内蔵されたコマンドラインユーティリティである「log stream」の述語フィルター言語（NSPredicate）を使用することで、対象となるデータのみを収集することができます。そのため、マシン単位で面倒な収集作業を行わずに、Macのログデータを簡単に記録するシステムを構築することが可能になります。収集されるデータには、ログオフ、SSH、AirDropや、各種の認証イベントが含まれます。Jamf Protectは、統合ログに記録されているすべてのデータを収集することができます。

Appleスタンダードとの協調

アップデートの即日サポート

Jamf Protectは、macOSからセキュリティの判断に必要なデータを収集するために、Appleネイティブのテクノロジーを活用しています。これには、AppleのエンドポイントセキュリティAPIやOpenBSMの監査フレームワークのような最新のテクノロジーが含まれています。これらの仕組みを利用することで、Jamf Protectはデバイスへの影響を最小限に抑え、パッチやOSのメジャーリリースで導入されたmacOSの変更に影響されることなく機能することができます。一般的にもっとも推奨されているセキュリティプロトコルとして挙げられるのが、タイムリーかつ定期的なパッチ適用です。リリース即日からのサポートに強くこだわるセキュリティツールは、このようなプロトコルを守る上で中心的な役割を果たし、包括的な深層防御のセキュリティ戦略において不可欠な要素となります。

機能としてのユーザエクスペリエンス

Jamf Protectは、脅威を検出するためにアプリケーションやユーザのアクティビティを継続的に監視しますが、休眠状態のマルウェアやMicrosoft Windows関連のマルウェアのスキャンはあえて行いません。多種多様なマルウェアのシグネチャを検出するためにファイルシステム上に存在するすべてのファイルをスキャンすることは、ユーザエクスペリエンスを低下させる要因になります。Jamf Protectのアプローチは、脅威が実行されそうになったタイミングでそれを検出し、ユーザエクスペリエンスやユーザの生産性への影響を最小限に抑えるという意味で、Gatekeeper/XProtectのアプローチと一致しています。

プライバシー

Jamf Protectでは、例えば悪意のあるアクティビティや関心の高いアクティビティがリアルタイムで検出された時など、適切なタイミングでデバイスのデータを分析して必要な情報のみを収集するよう構成できます。これにより、デバイスから抽出しクラウドに保存するユーザデータが少なくなるため、エンタープライズのニーズとユーザのプライバシーのバランスを取ることができます。悪意のあるアクティビティが確認された場合、そのアクティビティおよび関連データは、Jamf Protectのクラウドコンソールや指定されたSIEM（Sセキュリティ情報イベント管理）システムに転送されます。それ以外のデータの収集があらかじめリクエストされていた場合は、併せてJamf ProtectもしくはSIEMにプッシュされます。このようにして不要なデータの収集を排除することで、インシデントの監視や調査を行うセキュリティアナリストに、高品質なデータを提供することができます。

その他の機能拡張

ベストプラクティス：macOSのハードニング

Appleは世界でもっともセキュアかつ信頼性の高いオペレーティングシステムを提供していますが、macOSを組織の環境における最適解にするためにどのような追加措置を講じることができるのかを考えることも重要です。

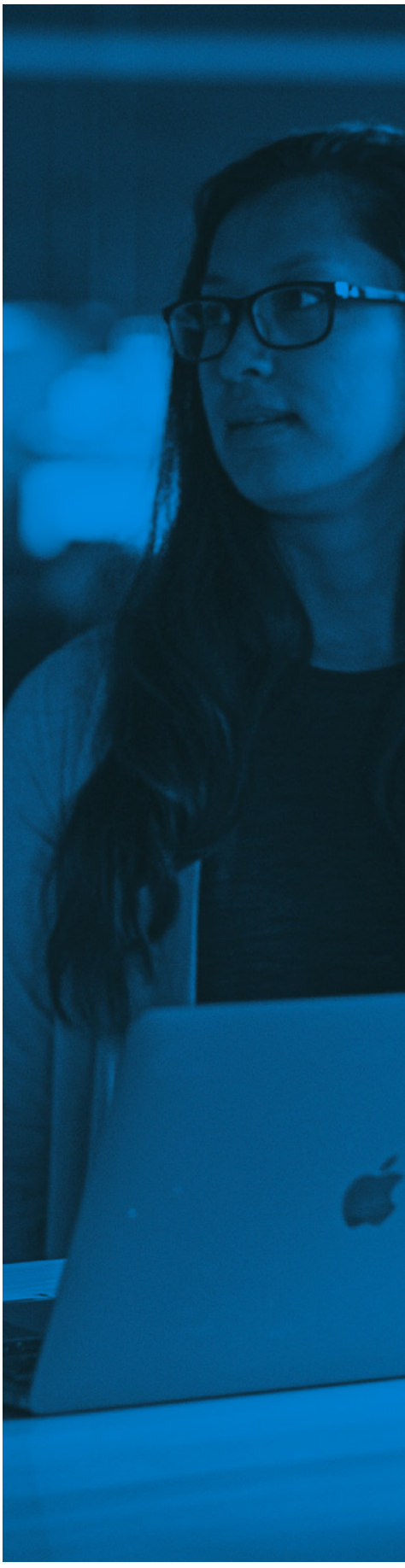
まずは、Appleのモバイルデバイス管理（MDM）フレームワークを活用し、環境の規模に応じた管理の自動化から始めるのがベストでしょう。MDMは組織のセキュリティ担保に役立つだけでなく、大量のデバイスを管理し、セキュアに運用する上でITの負担を軽減してくれます。

OS X 10.7（Lion）で導入されたMDMフレームワークは、組織固有のニーズに合わせてデバイス機能をカスタマイズするための、豊富なワークフローを提供してくれます。構成プロファイルと管理コマンドは、場所を問わず安全に働ける環境を従業員に提供するためのMDMの機能です。
さらに、ハードウェアの調達や管理などを自動化するためのAppleの法人向け無償ソリューション「Apple Business Manager」と組み合わせることで、MDMを使ったセキュリティをさらにレベルアップさせることができます。

まずはAppleから

Appleは長年にわたりセキュリティにフォーカスした企業としての評判を保ってきましたが、この姿勢はmacOSにも表れています。FileVault 2による暗号化、2ファクタ認証、リモートロック/ワイプ機能、パスコードルールの適用といったAppleのネイティブ機能は、組織環境に追加されるすべてのMacで利用可能です。

Jamf Proのような最新の管理プラットフォームを活用することで、これらの機能をさらに進化させ、暗号化に代表される重要なセキュリティツールの実装や適用、レポーティングを組織のニーズに合わせてカスタマイズすることが可能です。



Appleのパワーを Jamfで拡張

MDMはあらゆる組織にとって素晴らしい基礎となりますが、セキュリティ態勢をさらに強化し、従業員のプライバシーを守るために、他に何ができるかを考える組織も少なくありません。Jamfの存在意義はそこにあります。

デバイスの数が一定の規模を超えた時、その管理がITチームの負担になることは周知の事実です。従業員が増えればハードウェアの数も増え、ハードウェアが増えればITにかかるコストも増えます。

少なくとも、Jamf Proのような管理プラットフォームが登場する以前はそうでした。

スマートグループなどの特許技術を活用して組織所有デバイスの状態を把握し、いくつかの管理機能を自動化することで、ITチームはデバイス管理に費やす時間を削減し、他の日常的なIT関連タスクに費やす時間を確保することができます。スマートグループは、インベントリを監視し、デバイスのステータスの変化に応じてあらかじめ設定したグループからデバイスをリアルタイムで削除したり、新たに追加してくれます。

macOSのためのモダンなアイデンティティ管理

現代のセキュリティの中核をなすのは、エンドユーザにセキュアかつカスタマイズされたアクセスを提供するためのアイデンティティ管理です。従来の方法では、ローカルのディレクトリサービスに従業員の名前や部署などの情報が一元的に記録されていました。しかしセキュリティと導入のニーズの進化に伴い、企業はエンタープライズ戦略の一環としてアイデンティティ&アクセス管理に対する新しいアプローチを採用する必要に迫られました。完全にクラウドベースのアイデンティティスタックを採用した企業は、ハードウェアとソフトウェアにおけるアイデンティティ管理を統一することで、機能性や高度なワークフロー、そして最終的にはビジネスの変革を実現しました。

クラウドベースのシングルサインオン（SSO）は、ディレクトリサービスからの情報に基づいて、企業のリソースにアクセスしようとするユーザに認証情報を安全に入力させるための仕組みです。

Jamf Connectはこういった一般的なアイデンティティ管理の仕組みをさらに拡張するものです。

シームレスな認証ワークフローを提供するJamf Connectは、すべての企業アプリへのアクセスとユーザのMacへのログインを同じ認証情報で行えるようにします。エンドユーザは単一のクラウドIDで、必要なリソースに簡単かつ迅速にアクセスして生産的に働くことができます。

Jamf Connectは以下の機能を提供します。

- 効率的なプロビジョニングと認証で、デバイスを開封した瞬間からリモートおよびオンサイトで働く従業員を完全サポート
- ユーザIDとデバイス認証情報の自動同期
- すべてのサービスとデバイスにおける完全なアイデンティティ管理能力をITに提供
- レガシーVPN（仮想プライベートネットワーク）に代わるZTNA（ゼロトラストネットワークアクセス）ソリューションで、ハイブリッドワークを提供するエンタープライズのニーズに対応

Macを狙った脅威への対応と修復

Jamf Proのダッシュボードは、組織のMacデバイスの状態を把握し、注意が必要なハードウェアを監視するのに便利です。特許取得済みのスマートグループ機能により、管理者は対象のデバイスに対してアップデートやパッチを適用し、セキュリティ態勢の向上を図ることができます。この作業はすべてリモートで行われ、自動化も可能なため、ITの担当者がデバイスに物理的に触れる必要はありません。

また、Jamf ProtectとJamf Proを組み合わせることで、脅威の修復をレベルアップさせることができます。スマートグループを活用すると、Jamf Protectからのアクティビティベースのアラートに応じて、すべてのMDMとJamf Proのコマンドを調整することができます。これには、ネットワーク分離の自動化、条件付きアクセスの失敗、ユーザ通知、その他多くのターゲット型修復や対応が含まれます。ユーザまたはデバイスが攻撃された場合、Jamf ProとJamf Connectがあれば、認証情報の使用停止やアクセス権限の変更など、アイデンティティにまつわるさまざまな修復を行うことができます。

デバイス管理を超えたセキュリティ

エンタープライズにおけるAppleデバイスのセキュアな運用について、ITおよび情報セキュリティのプロフェッショナル1,500人を対象に行われた調査レポートを公開しています。組織におけるデバイスの使用状況やアプローチ、デバイスセキュリティの課題、エンドポイントセキュリティの今後のあり方などについてご覧ください。

Trusted Access

デバイス管理を超えたセキュリティを提供するJamfのソリューション「Trusted Access」は、デバイス管理、アイデンティティ管理、エンドポイントセキュリティを統合したJamf独自のワークフローにより、ユーザが好きなデバイスで仕事をし、組織がそのデバイスを信頼できる環境を作り出すための支援します。

Jamf ProとJamf Protectを組み合わせ、さらにJamf Connectを追加することで、コンプライアンスに準拠し信頼性が確認されたデバイスを使う認証されたユーザだけに、企業リソースやアプリケーションへのアクセスを許可することができます。万が一デバイスがウィルスに感染した場合でも、Jamf Proがあれば迅速に修復できるため、ダウンタイムを最小に留めることができます。

これにより、現代の職場環境におけるセキュリティを劇的に向上させるとともに、ユーザがどこにいても業務を効率化することができます。

Appleの管理とセキュアな運用を通じて得られる驚きのメリット

IT および情報セキュリティチームは、適切なツールを使用することで、自信を持って Macの導入を推進し、アイデンティティとアクセスの認証を行い、セキュリティとプライバシーが確保された状態で必要なリソースやアクセスを提供してユーザを全面的に支援することができます。

今すぐにJamfのエンタープライズ向けソリューションを導入し、現代の職場に求められる可視性や修復能力を手に入れてください。

トライアルに申し込む

または、お近くの販売代理店までお問い合わせください。

jamf

www.jamf.com/ja/