macOSのセキュリティ機能をJamfで強化

セキュリティの必要性は今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は製品にプライバシーとセキュリティの機能を標準搭載することに大きく投資している一方で、Macプラットフォームはエンタープライズ市場でシェアを拡大するのに伴って攻撃者にとっての価値も高まり、マルウェア、侵害、脆弱性発見の標的として魅力的になっています。業務用デバイスの従業員選択制度を通じて従業員にmacOSの使用を許可する企業はますます増えていますが、他のプラットフォームと同様macOSにもセキュリティと可視性の強化が必要であることも多くの企業が認識し始めています。

いくつかのセキュリティベンダーがMac製品を保護するための追加ソリューションを提供していますが、これらのソリューションの多くは、macOSが提供する最新のフレームワークを活用せず、ベンダー製品やWindows製品向けのセキュリティモデルを使用しています。そのため、オペレーティングシステムの継続的な進化に対応することが難しくなっています。代わりとなるベストプラクティスとしては、既存のmacOSセキュリティモデルを拡張し、足りない部分を補完しつつ、セキュリティ部門が脅威から組織を守るために必要とする、macOSに特化した機能を追加することが推奨されます。

Appleのオペレーティングシステムでは、プライバシーとセキュリティがプラットフォームの基盤とされ、ハードウェアとソフトウェアに保護機能が直接組み込まれています。加えて、Appleは使いやすさと生産性を支える直感的な操作性を重視しています。そのため、多くの機能が、組織全体のニーズではなく、主に個々のユーザを見据えて設計されており、可視性とセキュリティ対策の強化に対するニーズが重視されています。

このホワイトペーパーでは、macOSセキュリティの現状を概説し、ユーザが実践しやすいやり方でAppleのセキュリティベースラインを効率的かつ効果的に強化する方法を紹介します。

本書の内容：

- macOS内蔵セキュリティ機能の詳細
- Jamfによる企業向け機能強化のアプローチ
- Jamfがシグネチャや内蔵機能の範囲を超えて脅威検出を拡張する仕組み
- Appleのセキュリティモデルを拡張して高度な企業向けセキュリティを実現するその他の方法

macOS上のアプリケーション

Appleは、ユーザとサードパーティ製アプリケーションを保護するセキュリティ機能の設計に大きな力を注いでいます。このセクションでは、これらの機能のいくつかを紹介し、戦略的に強化・拡張する方法を説明します。Appleのセキュリティ機能の詳しい解説については、**Appleプラットフォームのセキュリティに関する包括的なガイド**をご覧ください。

Gatekeeperで信頼性を検証

サードパーティ製アプリケーションのインストール方法として信頼性が最も高く、Appleも推奨しているのは、App Storeからのインストールです。この方法であれば、Appleがプライバシー、セキュリティ、ユーザエクスペリエンスの基準を満たしているかどうかを審査して承認したアプリだけを取得できます。ただ、AppleはApp Storeで配布されるアプリの機能に制限も設けており、業務上不可欠なアプリの多くはこのタイプの配布には適していません。

App Storeからの配布という手段が使えない場合、Appleではmacos開発者がサーバからのダウンロードといった従来型の配布方法を使ってアプリを直接配布することを許可しています。こうした「臨時的」な配布をサポートするために、Appleではアプリがmacosデバイス全体にむやみに配布されるリスクを軽減するための検証チェックをオペレーティングシステムに導入しています。この検証チェックの中核をなす機能をGatekeeperといいます。Gatekeeperは、当初はmacosでリスク選好度に応じてアプリに実行を許可するためのオプションでしたが、現在は拡張されて厳格な要件と軽減策のセットへと進化しています。「App Store」または「App Storeと確認済みの開発元」からダウンロードしたアプリを許可する基本的な許容レベルは存在する一方で、問題やリスクのあるコードを実行するオプションは引き続き除外されています。

これらのチェックはインターネットからダウンロードされたアプリのみに適用される点に注意が必要です。Appleでは、これらのアプリを追跡するために、ダウンロードされたファイルにquarantine属性と呼ばれるメタデータを付与します。アプリが実行されると、Gatekeeperはquarantine属性を検証して実行の可否を判断するなど一連のチェックを実施します。その中で最も基本的なチェックが、前述した設定に基づいてアプリが正当な開発者によって署名されているか、App Storeによって配布されたものかを判断することです。

アプリが開発者によって署名されていれば、証明書が失効署名データベースと照合され、署名者が過去にマルウェアに関与していないかどうかが確認されます。これにより、Appleは不適切な証明書を速やかに失効させ、マルウェアが広範囲に拡散されるのを阻止することができます。

macOS Catalina以降では、Gatekeeperの検証に合格するには、アプリがAppleのノータリゼーション（公証）を受けることも必須になっています。アプリがこのチェックに合格するには、分析のためにAppleにアプリをアップロードする必要があります。分析で問題が見つからなければ、この追加検査に合格したことを示すノータリゼーションデータがアプリケーションに関連付けられます。

最終的な信頼性の判断はユーザが担う

macOSでは使いやすさを高める目的の下、多くの状況でエンドユーザがGatekeeperを「オーバーライド（迂回）」できるようになっています。オーバーライドするにはアプリを右クリックして［開く］または［このアプリケーションで開く］を選択するだけです。アプリの起動を完全に拒否するのではなく、未知のアプリや害を与えるおそれのあるアプリであることをユーザに警告するプロンプトが表示されますが、起動自体は許可されます。ただし、XProtectによってマルウェアであることが明白であると識別された場合は、そのアプリの実行は許可されません。

quarantine属性はアプリが初めて実行されたときに更新されて、次にアプリを開いたときにはGatekeeperのこのアクションは繰り返されなくなります。

⚠ XProtectとMRTで脅威をブロック

Gatekeeperのテクノロジースイートには、XProtectという名称のAppleのシグネチャベースの検出メカニズムと、マルウェア削除ツール（MRT）も含まれています。これら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、ファイル内で既知のマルウェアに関連付けられている特性を見つけることができます。XProtectはアプリの起動時にトリガーされる一方、MRTは定期的にファイルシステムをスキャンします。

XProtectでは、YARAというバイナリシグネチャスキャンエンジンが使用されます。YARAは柔軟で強力なバイナリシグネチャ定義と効率的な実行エンジンをサポートしています。XProtectではアプリを検証するために、アプリが初めて実行されるときとその後もアップデートされたときに、ダウンロードされた各実行可能ファイルをスキャンします。一致するシグネチャが検出された場合、アプリの実行は許可されません。既知の不正なシグネチャが記載されたファイルは、AppleからmacOSへ独立したアップデートを通じて提供されます。Appleでは、YARA実行エンジン本体とは別に、適切なタイミングでこれらのシグネチャを定義して提供しています。このスキャンは、Gatekeeperと同様、アプリが適切なquarantine拡張属性を保持している場合にのみ実行されます。この属性はアプリが初めて正常に実行された後に更新されます。

一方、MRTはアプリの起動時ではなくスケジュールに基づいて実行され、ファイルシステムをスキャンして過去のマルウェアに関連する特定のファイル名やアーティファクトがないかを探し、見つかった場合には削除します。MRTの目的は主に、macOS搭載デバイスで既に実行されている可能性のある既知の脅威を発見して修復することにあります。

⚙ Gatekeeperは企業環境でも使用可能

Gatekeeperは企業環境でも意図したとおり効果的に機能します。信頼性に欠けるアプリの起動をブロックし、不審なアプリや悪意のあるアプリと識別された場合はユーザに通知します。IT管理者とセキュリティ管理者は、信頼されていないアプリを会社の資産で実行しようとする動きを可視化する必要があります。さらに重要なのは、ユーザが右クリックでアプリを起動し、会社のセキュリティ対策をくぐり抜けようとしたことに気づけることです。Macのために設計されたエンドポイントセキュリティソリューションを搭載したJamf for Macでは、こうした企業のニーズに対応するために、Gatekeeperのアクションの兆候を常に監視し、その結果を一元化して報告します。IT部門やセキュリティ部門はこれを活用して、リスクを正確に評価し、十分な情報に基づいて意思決定を行うことができます。

Jamf for Macではさらに、Gatekeeperのアクティビティを可視化するだけでなく、企業環境内で信頼されていない署名情報を独自で追加登録することができ、企業は自社の状況に合わせて開発者信頼モデルを実践できます。Jamf for Macでは、Appleの最新のEndpoint Security APIを使用して、企業独自のブロックリストに登録されたアプリの実行を未然に拒否します。これは、アプリレベル（アプリケーションID単位）でもベンダーレベル（開発者チームID単位）でも定義できます。

これに加えて、macOSでは、望ましくない挙動や侵害の可能性のある挙動に関わる多くのアドウェアや暗号通貨マイニングアプリを含む、さまざまなグレイウェア（迷惑ソフトウェアや未承認のソフトウェア）については、シグネチャやブロックを提供していません。これらのソフトウェアは、Apple開発者によって正当に署名されていて、ユーザがインストール時に情報の収集やリソースの使用に知らず知らず同意しているケースが少なくありません。多くの場合、このようなソフトウェアの動作にAppleは干渉しません。

一方、企業ではリスクの算出方法が異なるため、より厳格で精度の高いアプローチが望ましい場合があります。これを受けて、Jamf for Macでは、quarantine拡張属性の有無にかかわらず、管理されているYARAルール、バイナリシグネチャ、信頼されていない開発者証明書の独自のセットを適用してアプリの実行時にプロセスをスキャンします。これにより、新しいシグネチャが追加され、企業がセキュリティ状態を更新したときも、初回の実行時だけでなく、既存のアプリの次回の実行時にも再スキャンが行われます。

Jamf for Macでは、macOSを標的とした脅威に関するJamfの広範囲の調査と外部のMac脅威データに基づいて、既知のMac標的マルウェアのフィードを選別しています。自社の環境で実行されているアプリをより細かく制御したい場合は、バイナリハッシュやTeamIDなどのリストを独自に作成して、Jamf for Macによってブロックされるアプリのリストを拡張できます。10.15（Catalina）以降のmacOSで既知のマルウェアの挙動やシグネチャと一致するアプリが実行されると、Jamf for Macはそのプロセスの実行を阻止し、有害なファイルを隔離して、マルウェアが阻止されたことを示すアラートを登録します。この処理は、Gatekeeper/XProtectのアクションの外部で行われ、それらの機能のスーパーセットとなるように設計されています。Jamf for Macでは、安全性が疑われるバイナリを識別するために、より幅広いマルウェア知識を維持しており、quarantine属性にかかわらず既知のマルウェアを特定します。

セルフサービス方式でアプリストアの信頼モデルを拡張

状況によっては、IT部門が承認したリソースが事前設定されているセルフサービス方式のアプリストアを使用して、ユーザがインストールできるアプリを指定することが実情に適する場合があります。

Jamf Self Service+では、IT部門が自社用のアプリカタログを作成して、リソースへのセキュアかつスピーディなアクセスを実現できます。ユーザはITヘルプチケットを作成しなくても、アプリのインストール、構成の更新、よくある問題のトラブルシューティングを自分で行うことができます。

アプリの挙動の制御と監視

プライバシー制御でアプリの挙動を認識・制限

システムのプライバシー制御はmacOS Mojaveで導入されました。この制御では、ユーザ（または会社）がアプリ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必要があります。アプリに特定のアクションへのアクセスをいったん許可すると、その後は同じアプリからそのアクションが実行される際にアクセス許可は求められなくなります。この機能を使用することで、アプリがOSの機密になりうる要素（Webカメラ、マイク、キー入力、ダウンロード）にアクセスすることに対して明示的に許可を与えられ、ユーザは個人データへのアクセスをアプリに許可することを把握して安心できるようになります。

制御の範囲を超えて、アプリの挙動を監査・分析

プライバシー制御でアプリの権限を制限できる一方で、ユーザがミスしたり権限が悪用されたりする可能性もあります。Jamf for MacがAppleのセキュリティ機能と従来のマルウェア/アドウェア防御機能のアクションを可視化し、企業に情報を提供して環境を保護する方法は既に説明したとおりです。しかし、Jamfではエンドポイント保護はそれで終わりとするべきではないと考えます。Jamf for Macは、これまでエンドポイント検出・対応（EDR）製品にしか搭載されていなかった監査・監視機能も備えていますが、それにとどまらずAppleファーストのアプローチを採用し、macOSユーザが期待するレベルのプライバシーとセキュリティにも気を配っています。

Jamf for Macが備える検出エンジニアリング

Jamf for Macのエンドポイント保護の中核を成しているのはエージェントです。その実体は、Apple独自のロジック実行エンジンの1つであるGameplayKitを活用する（付随テキストが不要な）軽量のユーザモードセンサーです。ゲームエンジンを使用してセキュリティイベントを分析するのは従来とは異なる手法ですが、これによってJamf for MacはAppleエコシステムと緊密に統合した状態を維持し、収集やレポートで必要になったときのためにデバイス上のデータを分析できます。また、ゲームエンジンは大量のイベントが発生したときにリアルタイムで処理するよう設計されているので、デバイス上で行われるアクティビティを分析するのにうってつけです。この設計は、最初はWindowsプラットフォームを対象として作られて後から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て分析しなければならないソリューションとは対照的です。

GameplayKitのもう一つの利点は、YARAと同じく実行エンジンを検出の定義から分離しているため、コアエージェントを更新せずに検出を更新・拡張できる点にあります。検出の定義もAppleネイティブであり、NSPredicateを使用します。NSPredicateは、一般的なクエリ構文と正規表現をサポートする強力なロジッククエリメカニズムです。Jamfのデータモデルは、ネイティブ関数の呼び出しやデータモデルの連結など、NSPredicateが備える豊富な機能を活用できるように設計されています。これにより、従来の手法では実装が面倒だったり、コンピューティングコストが高かったりした機能が活用できます。

JamfのデータモデルとNSPredicateを使用して実現できる例には、次のようなものがあります。

- ファイルが自己削除された場合にアラートで通知します。ファイルの自己削除は痕跡を隠すためによく使われる手法です。シンプルに思えるこのユースケースでは、削除されたファイルと削除プロセスの両方を、高コストな結合演算やハードコーディングされた検出を使わずに分析します。
- 未署名のバイナリや署名が疑わしいバイナリが起動デーモンとして永続化されている場合にアラートで通知します。このケースでは、構成ファイルを解析し、コンテンツに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使用して分析を行います。
- Microsoft Officeアプリが予期しない子プロセスを作成した場合にアラートで通知し、Officeマクロの悪用を特定します。このケースは、子プロセスと親プロセスの関連を理解し、アプリの機能の悪用を検出できることを示す好例です。
- その他の「環境寄生型」アクティビティが攻撃を示唆する方法で使用されている場合にアラートで通知します。この種のアクティビティでは、子プロセス/親プロセスと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となり、通常であれば無害であるアクティビティ（curl、ssh、pythonなど）の悪用を検出します。
- 企業全体で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報告します。

こういった種類の検出の影響を理解しやすくするために、Jamfでは特定された攻撃を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）。現在は、以下のカテゴリに属する手法の検出を含め、このフレームワーク全体のユースケースが対応範囲に含まれています。

- 永続化
- 初期アクセス
- コマンド&コントロール（遠隔操作）
- 防衛回避
- 探索
- 権限昇格
- 認証情報アクセス

Macネイティブテレメトリを活用した可視性の向上

組織がmacOSのセキュリティ体制を強化すればするほど、システムとユーザのアクティビティを詳細に可視化することがますます重要になります。Appleネイティブのフレームワークは強力な基盤となる一方で、セキュリティ部門は多くの場合、異常な動作の検出、インシデントの調査、一元的なコンプライアンス維持のために、相関性の高い豊富なシグナルが必要になります。

Jamfのテレメトリ機能は、AppleのEndpoint Security APIを基盤として、macOS固有の詳細なシグナルを各デバイスから収集します。組織はmacOSの動作内容が反映されたデータを活用して、システム、ユーザ、アプリ、ネットワークのアクティビティを高い精度で分析できます。Jamfのテレメトリは軽量でありながら高性能なので、ユーザエクスペリエンスに影響が及ぶことはありません。また、改ざん防止機能を備えているため、調査やコンプライアンスでログとセキュリティイベントの信頼性が損なわれません。

Jamfのテレメトリは、プロセス、アプリ、認証、構成変更、ユーザアクションにわたってイベントを相関付けることで、セキュリティ部門が詳細な時系列を復元し、悪用や新たな脅威を示している可能性のある挙動を特定するのに役立ちます。

組織がJamfのテレメトリを活用することで得られるメリットには、次のようなものがあります。

- 精度と品質の高いイベントデータを活用して、規制や社内のコンプライアンス要件を満たす
- 構成の齟齬、シャドーIT、ポリシーの逸脱を検出する
- 相関付けられたイベントと攻撃経路を分析することで、インシデント対応をスピードアップする
- macOSに特化した豊富なインサイトを活用して、予防型の脅威ハンティングをサポートする
- SIEMプラットフォームとシームレスに統合し、一元的に可視化する

この機能によって、Macデバイスの一元的な管理とセキュアな運用を実現するために必要となる詳細情報や背景情報を得ることができ、高度な検出と分析のための強固な基盤を構築できます。また、JamfのテレメトリはmacOSの Unified Logging（ユニファイドロギング）システムと連携するため、組織は豊富なセキュリティシグナルと対象を絞ったログデータの両方を収集して、監査、調査、コンプライアンスに役立てることができます。

シンプルな Unified Log（ユニファイドログ）収集とレポート

多くのセキュリティアナリストやIT管理者が、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対策のギャップを埋めるために、エンドポイントログの必要を強く感じています。macOSでsyslogファイルが Unified Logging（ユニファイドロギング）に移行されたことで、企業環境でのこの情報の収集、インベントリ、検査が難しくなりました。macOSのコンソールアプリは、ローカルのMacの Unified Logging（ユニファイドロギング）インフラにアクセスして閲覧するには優れたツールですが、組織がデータを簡単に一元管理するのには向いていません。

Jamf for Macなら、クライアントログが Unified Log（ユニファイドログ）に書き込まれたら即座に記録システムにストリーミングできます。Jamf管理者が対象とするデータのみが収集されるようにしたい場合は、内蔵の「log stream」コマンドラインユーティリティで同じ述語フィルタリング言語（NSPredicate）を利用できます。これによって、シンプルな構成でMacのログデータ用の記録システムを構築でき、デバイスごとに面倒な収集を行わなくて済みます。例えば、ログインとログオフ、SSH、AirDrop、認証イベントなどを収集できます。Unified Log（ユニファイドログ）に記録されているデータであれば、Jamf for Macで収集が可能です。

Appleの標準と連動。

リリース同日サポート

Jamf for Macは、macOSと連携してセキュリティの意思決定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。具体的には、AppleのEndpoint Security APIや（デバイス管理フレームワークの進化形である）宣言型デバイス管理プロトコルといった、新しいフレームワークなどです。Jamf for Macでは、これらのメカニズムを使用して、デバイスへの影響を最小限に抑え、パッチやメジャーOSリリースで導入されるmacOSの変更点との競合を回避しています。パッチを早期に、また頻繁に適用することは、セキュリティ対策として最も広く推奨される手段です。リリース当日からのサポートを厳守するセキュリティツールは、この対策を実践する心臓部であり、包括的な多層防御セキュリティ戦略に欠かせない要素です。

機能としてのユーザエクスペリエンス

Jamf for Macは、潜在的な脅威がないかアプリとユーザのアクティビティを継続的に監視する一方で、活動していないマルウェアやMicrosoft Windows関連のマルウェアはあえてスキャンしません。単にファイルシステムにあるファイルをさまざまなマルウェアシグネチャでスキャンすることが、ユーザエクスペリエンスを低下させる主な要因となっているケースは少なくありません。上記の方針は、脅威が実行されている可能性があるときにそれを特定するという点でGatekeeper/XProtectと合致しており、ユーザエクスペリエンスと生産性への影響を最小限に抑える効果があります。

宣言型デバイス管理フレームワーク

WWDC 21で発表された宣言型デバイス管理（DDM）は、デバイス管理プロトコルを進化・アップデートさせたものです。DDMを使用すると、デバイスは管理設定を予防措置的に適用し、状態の変化を自律的に報告して、MDMサーバと非同期に通信できるようになります。DDMの導入は、従来のコマンド&レスポンスモデルから、より効率的で自律的なアプローチへの飛躍的な転換だと言えます。

プライバシー

Jamf for Macは、デバイス上のデータを分析しますが、関連情報の収集は設定されている場合にのみ行います。通常は、害を与えるおそれのあるアクティビティや要注意のアクティビティがリアルタイムで検出された場合です。この方針によって、デバイスから取得されてクラウドに保存されるユーザデータを抑えられ、企業のニーズとユーザのプライバシーのバランスを保つことができます。悪意のあるアクティビティが特定された場合は、そのアクティビティのデータおよび関連情報がJamfのクラウドコンソールまたは設定されたセキュリティ情報およびイベント管理（SIEM）システムに渡されます。具体的に要求されたデータがある場合は、それもJamfまたはSIEMにプッシュされます。不要なデータはすべてフィルタリングされるため、インシデントの監視と調査を担うセキュリティアナリストには、関連性の高い高品質なデータだけが提示されます。

その他のAppleセキュリティモデルの拡張

ベストプラクティス：macOSの堅牢化

Appleは市場でも屈指のセキュアで信頼性の高いオペレーティングシステムを提供・サポートしていますが、macOSを企業環境でもっとうまく活用するにはどのような追加措置を講じればよいかという声もよく耳にします。

最初に講じる措置として最善なのは、Appleのモバイルデバイス管理（MDM）フレームワークを活用して一括管理を自動化することです。MDMは組織の保護強化に役立つだけでなく、デバイスの管理とセキュアな運用におけるIT部門の負担も大幅に軽減します。

OS X 10.7（「Lion」）で導入されたMDMフレームワークでは、非常に豊富なワークフローを活用して、組織固有のニーズに合わせてデバイスの機能を調整できます。従業員の働く場所を問わずセキュリティを維持するためのMDMの活用法としては、構成プロファイルと管理コマンドの使用が最も一般的です。

MDMを活用したセキュリティは、Apple Business Managerの機能と組み合わせることでさらに強化できます。Apple Business Managerは、ハードウェアの調達や管理などを自動化するのに役立つAppleのビジネス向け無料ソリューションです。

Appleの機能からスタート

Appleは長年にわたってセキュリティ最優先の企業として評判を築いてきており、そのことはmacOSにも表れています。FileVault 2 暗号化、二要素認証、リモートロック/ワイプ機能、パスコード基準の強制といったネイティブ機能は、組織の環境に追加されるすべての新しいMacで利用できます。

Jamf for Macのような最新の管理・セキュリティプラットフォームを導入すれば、Appleの最新テクノロジーを活用してこれらの機能をレベルアップさせて、暗号化などの重要なセキュリティツールの実装、適用、レポートをカスタマイズできます。

Jamfで強化

MDMはどの組織にとっても優れた基盤になりますが、セキュリティ体制をさらに強化し、従業員のプライバシーを保護するために、他に何ができるかを考える組織は少なくありません。Jamfの存在意義はそこにあります。

ある程度の規模になると、デバイス管理が担当部署のリソースを大きく奪ってしまうことはよく知られるところでしょう。人が増えればハードウェアも増え、ハードウェアが増えればIT部門の負担も増えます。

少なくとも、Jamfのようなプラットフォームが登場する以前はそうでした。

IT部門は、ブループリントやスマートグループといったJamfの特許取得済みテクノロジーを活用することで、業務用デバイスの統括がしやすくなり、管理機能の実行を自動でき、こまごましたデバイス管理に要する時間を減らして、IT関連の日常業務に投じる時間を増やすことができます。スマートグループは、デバイスインベントリを常時監視し、デバイスの状態が変化すると、事前に定義されたグループに対してデバイスをリアルタイムで追加または削除する機能です。

macOSにおける最先端のアイデンティティ管理

最新セキュリティの中核を成すのは、エンドユーザ向けにカスタマイズされたセキュアなアクセス権であるアイデンティティです。従来のITシステムでは、氏名や部署などの従業員情報の一元的な記録場所として、ローカルディレクトリサービスが使用されてきました。セキュリティと導入に関するニーズが刻々と進化する現在、企業はエンタープライズ戦略の一環として、アイデンティティベースの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ています。クラウドベースの包括的なアイデンティティソリューションを活用すれば、ハードウェアとソフトウェア全体でアイデンティティを統合し、実用的かつ高度なワークフローを実現して、究極的にはビジネスの変革につなげることができます。

クラウドベースのシングルサインオン（SSO）では、ディレクトリサービスの情報に基づいて、エンドユーザがセキュアな認証情報を入力して社内リソースにアクセスできます。

Jamfは、このような一般的なアイデンティティ管理手法を拡張します。

Jamf for Macでは、シームレスな認証ワークフローですべての業務アプリとユーザのMacでアイデンティティを統合します。エンドユーザは1つのクラウドアイデンティティで生産性向上に必要なリソースに素早く簡単にアクセスできます。

Jamf for Macの導入により、次のようなメリットが得られます。

- プロビジョニングと認証を合理化し、デバイスを開封した瞬間からリモートワーカーとオフィスワーカーを完全サポート
- ユーザのアイデンティティとデバイス認証情報を自動的に同期
- IT部門にサービスとデバイス全体にわたるアイデンティティ管理機能をフルに提供
- 従来のVPN（仮想プライベートネットワーク）に代わるゼロトラストネットワークアクセス（ZTNA）ソリューションで、現代のハイブリッド企業のニーズに対応

Macの脅威に対応して修復

Jamf for Macは、組織がMacデバイスの状態を継続的に評価するのに役立つダッシュボードや、注意が必要なハードウェアにフラグを設定する機能を備えています。特許取得済みのスマートグループ機能では、IT管理者がセキュリティ体制を強化するためにアップデートやパッチの適用が必要なデバイスを特定できます。アップデートやパッチの適用はすべてリモートで自動的に行われるため、IT部門がデバイスに直接触れる必要はありません。

Jamf ProtectとJamf Proを組み合わせることで、脅威からの修復をさらに強化しています。このスマートグループテクノロジーを活用することで、アクティビティベースのアラートが発行されたときに、すべてのMDMコマンドとJamfコマンドを調整して実行できます。これには、ネットワーク分離の自動化、失敗した条件付きアクセス、ユーザ通知など、対象を絞ったさまざまな形式の修復や対応が含まれます。

デバイス管理の枠を超えたセキュリティ

1,500人のITおよび情報セキュリティ担当者にアンケート調査を実施して作成された、企業におけるAppleセキュリティの現状に関するこちらのレポートをぜひご覧ください。このレポートには、現在のデバイスの使用状況とアプローチ、デバイスセキュリティの課題に加えて、エンドポイントセキュリティの将来像についても解説しています。

Jamf for Mac

現代の組織には、macOSデバイスを一元的に管理してセキュアに運用するための統一されたアプローチが必要です。Jamf for Macは、Appleの標準搭載のセキュリティ機能と、アイデンティティと権限の管理、リムーバブルストレージ制御、脅威防止といった高度な機能を統合することで、これを実現します。これにより、ユーザが求めるmacOSの使い慣れた操作性を損なうことなく、デバイスをリアルタイムで保護する、Apple連動の多層型セキュリティ体制が実現します。

Jamf for Macを利用することで、組織はデバイスアクティビティの詳細な可視化、コンプライアンスベースラインへの適合の強化、最小権限の適用、リムーバブルメディアの制御、Webベース脅威の防御といったことができるようになります。これらの機能を駆使して、シームレスなAppleエクスペリエンスを損なうことなく、ユーザの生産性を維持しながらMacデバイス全体のリスクを軽減できます。

管理、アイデンティティ、エンドポイントセキュリティがAppleに特化した単一のソリューションとして統合されているJamf for Macを採用することで、組織はmacOSデバイスを包括的に保護し、Macの導入が拡大しても確実に運用を維持できます。

jamf

トライアルに申し込む
または、販売代理店までお問い合わせください。

www.jamf.com/ja/