jamf

ホワイトペーパー

JamfとMicrosoftの連携が生み出すよい変化

パンデミックによって働き方が変化したように、エンタープライズにおける日々のAppleデバイス管理の現実にも変化が起こっています。リモートワーカーのサポートはかつてないほど重要になり、多くのIT管理者は組織の成功にもっとも貢献してくれる専用のツールを必要としています。例えば、Appleデバイスの管理にはJamfのソリューション、その他のデバイスの管理にはMicrosoftの製品があります。

多くの人は、最適なプラットフォームをひとつ選択するのがベストだと考えるでしょう。しかし、組織で使用するデバイスの種類をひとつに限定したり、すべてのデバイスをひとつの非効率なプラットフォームで管理したりすることは、もはや時代遅れになりつつあります。すべてのデバイスが同じ機能性を持っているわけではないからです。今日の最適な解決策とは、各デバイスに最適なオプションを用意し、MicrosoftやJamfが提供している統合や連携を賢く活用することを意味します。

このホワイトペーパーのトピック

- Macを導入するエンタープライズが増え続けている理由
- JamfとMicrosoftの連携によって生まれる効率性、柔軟性、そして究極の使いやすさ

Macを導入するエンタープライズが増え続けている理由

ユーザにとってテクノロジーが持つ意味は変わりつつあります。誰もが自分にとって一番使いやすいハードウェアを求めており、多くの場合、彼らはMacを選びます。

選択できることのメリット

従業員選択プログラムが一般的になるにつれて、より多くのMacが組織のネットワークに入ってくるようになりました。その規模に関するデータがあります。72%*の人が、PCとMacのどちらかを選ぶとしたらMacを選ぶと答えています。組織やITがエンタープライズにおけるMacの存在について真剣に考えなければならないのは、自分のデバイスに満足し効率的に働くことのできる従業員は高い生産性を生み出すからです。エンタープライズにおけるMacにフォーカスした世界的なリサーチ**によると、Macユーザの：

97%
が生産性がアップしたと報告

95%
が創造力がアップしたと報告

94%
が自立性がアップしたと報告

91%
がコラボレーションが増えたと報告

また、Macは他のどのデバイスメーカーよりも職場で効率性を発揮すると認識されています。調査対象者のうち79%が、Macがなければ仕事を効率的に進められないと回答しています。さらに、IT部門と人事部で働く回答者の83%が、自分の職務においてMacは不可欠であると感じています。

Macで従業員の定着率を上げる

従業員選択プログラムやMacの支給は、従業員が会社に留まるか辞めるかを選択する際の重要な決定要素になります。

95% 業務に使用するデバイスを選択できる企業の方が、就職先として選ぶ、または留まる可能性が高いと感じている人の割合

しかも、Macを提供することで、ユーザが愛用しているMicrosoftの生産性に長けたソフトウェアを活用できなくなるわけではありません。

JamfとMicrosoft：共に歩むパートナー

JamfとAppleが非常に密接な関係にあることは周知の事実ですが、だからこそ、Microsoftとの安全かつ戦略的な統合によりユーザを支援することが重要になります。

2017年、JamfとMicrosoftは、Jamf ProからMicrosoft Intuneへのインベントリデータの共有、条件付きアクセスの適用、修復パスの提供といった機能の提供も含め、macOSにおける条件付きアクセスを可能にするコラボレーションを発表しました。これにより、信頼できるユーザが信頼できるデバイスで信頼できるアプリケーションを使って企業データにアクセスできるようになりました。そして2018年、よりシームレスなログイン体験をエンドユーザに提供するため、JamfはMicrosoftのテクノロジーとの統合を再び拡大し、さらに2020年には、このホワイトペーパーで後ほど詳しく紹介するiOS向けデバイスコンプライアンスへの対応が追加されました。

ワークフローやユーザプロセスがここ数年で変化し、エンタープライズにおける“ニューノーマル”に適応しようとするなか、エンドユーザとITチームの双方にとって合理的な体験を生み出すために、JamfとMicrosoftの関係はより密接なものへと変化しています。

IT管理者にとってのメリット

アップデート、保護、メンテナンスが簡単で、信頼性が高くセキュアなデバイスを組織に浸透させることは、IT管理者の重要な仕事のひとつと言えます。選んだデバイスがMacであってもWindowsであっても、エンドユーザは同等のサービスやセキュリティ、管理性を求めています。

管理者のバックグラウンドがAppleであれWindowsであれ、不慣れなシステムを理解しようとする過程において失敗するのはよくあることです。Macに慣れたIT管理者はJamf Proをよく理解し、使いこなしています。しかし、Apple、Jamf、そしてMicrosoftの新しい統合とパートナーシップが実現した今、IntuneでMacを管理するMicrosoft出身の管理者の多くが、この2つを組み合わせるタイミングについて考えを巡らせています。

Windowsの管理者にとって重要なのは、ゼロトラスト環境におけるセキュリティです。Microsoft Intuneは、Macのためのより良い管理プラットフォームを作るプロセスの一部ではなく、Macからのアプリケーションへのアクセスに対してアイデンティティ保護を提供するために存在しています。

これを実現するために、Windows管理者はAppleのエコシステムの仕組みを理解しなければなりません。暗号化の方法やマルウェア対策の効果性、サインインの方法など、疑問は尽きません。

Jamf ProとMicrosoft Intuneの関係

Jamf Proはデバイスを管理するエンジンの役割を果たし、レポートデータをMicrosoft Intuneに送ります。Microsoft Intuneはそのデータを見て、デバイスがコンプライアンスに準拠しているかどうかを判断する役割を担っています。

コンプライアンスをどのように管理するかは、完全に管理者次第です。特定の設定、複雑なパスワード、暗号化、アクティブでない状態が続いた後のスリープ状態など、必要に応じて要求するか否かを決めることができます。このようなコンプライアンス設定は、Microsoft IntuneとJamf Pro間のコミュニケーションポイントになります。これらのポリシーを適用することで、管理者はデバイスが適切に構成されているか、それとも何らかのアクションを必要としているかについて知ることができます。

異なるのは、このコンプライアンス状況をユーザに関連付ける方法です。そこで登場するのが「条件付きアクセス」です。これはMicrosoft Intune専用の機能で、他の機能との統合も可能ですが、コントロールはIntuneでしか行うことができません。こういったポリシーやコンプライアンス、セキュリティ対策を通して、IntuneとJamf Pro間でコミュニケーションや関係性が生まれ、一定レベルのセキュリティが形成されます。

JamfとMicrosoftパートナーシップの良さはまさにここにあります。Microsoft IntuneとAzure ADを使ってMacからサービスへのアクセスやアイデンティティ保護しながら、Jamf Proが提供する管理能力をフルに活用することができるため、1つのプラットフォームに限定される必要がなくなります。

Microsoftの Enterprise Mobility + SecurityとiOSのデバイスコンプライアンス

リモートワーカーをサポートする必要性から、セキュリティの焦点はこれまでの企業ネットワークの内側から、オフィスの壁を越えたところにまで広がっています。このため、組織はすべてのデバイスを管理しセキュリティを確保するための合理的な方法を求めています。エンタープライズにおけるApple製品管理のスタンダードであるJamfは、組織に最適なサポートを提供するために、Microsoft Enterprise Mobility + Securityとのコラボレーションを拡張し、iOS向けのデバイスコンプライアンスをリリースすると発表しました。

「従業員選択プログラムやITのコンシューマライゼーションなどのトレンドは成長を続けており、組織はハイブリッド環境に適応できる管理ツールを必要としています」Microsoftでコーポレートバイスプレジデントを務めたブラッド・アンダーソンは、そう述べました。「MicrosoftとJamfのパートナーシップにより、IT管理者はエコシステムに特化した重要な機能を提供しつつ、従業員のデバイス管理を一元化することができます」

組織はすでに、Jamfのインベントリデータを Microsoft Endpoint Managerと共有することで、macOSデバイスで条件付きアクセスを利用することができます。iOS向けデバイスコンプライアンスを使用することで、IT管理者は今後、認証されたユーザがセキュリティポリシーに準拠していないiOSデバイスを使えないようにし、さらに修復にJamfのSelf Serviceを活用することができるようになります。

Jamfは、Azure Active Directoryと連携したアプリ（Microsoft 365アプリを含む）にアクセスしようとするユーザにデバイスの登録を義務付けることで、これに対応しています。まず、JamfによってiOSデバイスのコンプライアンス基準が設定および評価されます。次に、Jamfが収集したデバイスの情報がMicrosoft Endpoint Managerに送信されます。最後に、Endpoint Managerがデバイスのコンプライアンス状態をチェックし、Azure Active Directoryを利用して動的にアクセスを許可または却下します。デバイスがコンプライアンスに準拠していない場合は、JamfのSelf Serviceで修復するようユーザに通知が送られます。

この機能により、組織はMicrosoft Endpoint Managerでコンプライアンス状況などの重要なデバイス情報を共有しながら、JamfでiOS管理を行うことができます。IT管理者は、Apple製品のエコシステム管理にJamfの機能を利用しながら、Azure Active DirectoryとMicrosoft Endpoint Managerによる条件付きアクセスを活用することで、コンプライアンスに準拠したデバイスを使用する信頼できるユーザのみに企業データへのアクセスを許可することができるのです。

Jamf ProtectとMicrosoft Azure Sentinelの統合

組織のデバイスやネットワークインフラがより複雑になるにつれ、その環境のセキュリティを確保するために、セキュリティチームはSIEM（セキュリティ情報イベント管理）やSOAR（セキュリティ運用の自動化および効率化）などのツールにますます依存するようになっています。Macの世界に確固たるセキュリティとコントロールをもたらすため、Jamfはエンドポイントセキュリティツールであ るJamf ProtectをMicrosoft Azure Sentinelのデータフローに統合しました。

Mac専用のエンドポイント保護ツールであるJamf Protectは、最小限の構成でMac固有のすべてのセキュリティデータとアラートをAzure Sentinelに直接プッシュすることができます。不審、または悪意のあるアクティビティやマルウェアの通知はすべて、既存のワークフローと簡単に統合できるため、セキュリティ担当者の労力や時間はほとんど必要ありません。Jamf Protectの攻撃検出とログ情報により、Azure Sentinelはその機能を拡張することができます。これにより、組織の環境下にあるすべてのMacデバイスに対する幅広い攻撃を特定・修復しながら、組織全体のセキュリティを向上させます。

MicrosoftとJamfの機能を組み合わせることで、組織は使い慣れたAzure Sentinelのインターフェースから離れることなく、すべてのMacのセキュリティアクティビティに対して完全な可視性を手に入れることができます。

最後に

このような統合やJamfとMicrosoftのパートナーシップが存在する今、組織に積極的にMacを導入すべきでない理由はもはやありません。Windows管理者であっても、MacをWindowsデバイスと同じように保護、管理、統合できる時代になったのです。

今すぐ体験してみたいという方のために、**トライアル**を実施中です。お気軽にお申し込みください。
または、Apple認定販売代理店までお問い合わせください。

出典：

**https://www.jamf.com/resources/e-books/survey-the-impact-of-device-choice-on-the-employee-experience/*
***https://www.jamf.com/resources/e-books/global-survey-mac-in-the-enterprise/*