jamf

もっとも脆弱なエンドポイントであるモバイルデバイスの管理とセキュアな運用

モバイルデバイスといえば、ノートパソコンやタブレット、スマートフォンを思い浮かべる人が多いのではないでしょうか。いずれもモバイルデバイスのカテゴリーに分類されますが、本ガイドは主にスマートフォンとタブレットに焦点を当てた内容となっています。世界中の何百万人ものユーザが、毎日の仕事や学習、個人的なタスクをこなすためにこれらのデバイスを利用しています。しかし、このようなデバイスへの依存により、モバイルデバイスのセキュリティに対する重大な懸念が浮き彫りになりつつあります。

しかし、既存のMacフリートに加えて、モバイルエンドポイントのセキュリティやコンプライアンスを維持することは不可能ではありません。このガイドでは、組織のフリート全体（Macとモバイル）の安全を守りデータを保護してくれる業界トップクラスのエンドポイントセキュリティソリューションを、モバイルデバイスの保護に効果的かつ効率的に役立てる方法をご紹介します。

このガイドのトピック

モビリティセキュリティの現状

テクノロジーの進歩に伴い、モバイルデバイスの使用がますます増えています。モバイルデバイスはデスクトップコンピュータ並みの機能を備えながら、スリムで軽量、エネルギー効率の高い設計になっています。また、あらゆる用途に対応し、ネットワークへの高速接続が可能で、いつでもどこからでもさまざまなアプリやサービスにアクセスすることができます。

ビジネスの観点から見れば、場所を問わずに働けることや、クラウドベースのサービスへのリアルタイムアクセスも含め、ネットワークへの接続を通じて特定のプラットフォームに縛られずに働くことができるという利点があります。各従業員に会社所有のモバイルデバイスを提供するにはコストがかかりますが、モバイルデバイスのプライベート使用が普及したことで、多くの組織で幅広いオーナーシップモデル（会社所有、COPE、従業員選択プログラム、BYOD）が採用されるようになりました。BYOD（私用デバイスの業務利用）は、ユーザが個人所有のデバイスを仕事に利用できるようにするもので、企業にとってはコスト削減というメリットがあります。そしてユーザにとっても、使い慣れたプラットフォームやデバイスを使って仕事を行えるというメリットがあります。

しかし、モバイルデバイスの採用や依存度が高まったことで、セキュリティに関する懸念点が増加したのも事実です。エンタープライズに影響を与える一般的な懸念点には以下のものが含まれます。

- データ漏洩リスクの増大
- ユーザの個人情報への不正アクセス
- モバイルデバイスとMacのエンドポイントセキュリティの差異
- コンプライアンスの評価や維持の難しさ
- デバイスを通じたデータへの不正アクセス

組織はしばしば誤った安全意識を抱いています。コンピュータを保護するために設計されたセキュリティポリシーはモバイルデバイスを十分に保護するようにはできておらず、これによってモバイルデバイスのセキュリティ態勢に空いた穴が、組織全体のセキュリティ態勢の弱体化につながる可能性があります。もうひとつ考慮しなければならないのは、複数のプラットフォームをサポートする際に生じる複雑さです。これにより、会社所有デバイスのプロビジョニングや、BYODデバイス上の企業データの保護など、モバイルデバイスの導入スピードにかかる時間が増大します。しかもこれら全てを、ユーザのプライバシーや使い勝手の良さに影響を与えることなく実現しなければなりません。

もう1つの重要なのが、BYODプログラム対象外のモバイルデバイスの使用を制限するポリシーが組織にあるかどうかです。自分の組織にはモバイル脅威は及ばないと考えているのなら、考え直す必要があります。あなたの組織では、個人所有のモバイルデバイスを業務に利用することを許していますか？

この問いにNoと答えた組織は、追加の質問についても考えてみてください。例えば、CEOが出張中にタブレットを使うようなケースについてはどうでしょうか？CEOの子供たちも宿題などに使っているこのタブレットは、仕事用のメールをチェックするためにも使われている可能性があります。あるいは、役員や取締役がミーティングのスケジュール調整や機密性の高いビジネス運営事項について話し合うために使っているスマートフォンについてはどうでしょう？こういったデバイスはしばしば組織内でのコミュニケーションに使用され、ホエーリング攻撃をはじめとする企業の幹部を狙った攻撃のベクトルとして使用される可能性があります。

モビリティの促進

働き方の進化に深く関係する「エンタープライズモビリティ」という従来の概念は近年大きな課題に直面しており、組織モデルの迅速な転換が必要となっています。この変革は、以下を含むさまざまな要因によってもたらされています。

> 業務のクラウドサービスへの移行

> 分散型ワークフォースの採用

> ネイティブのモバイルアプリの普及

モバイルビジネスアプリの開発と利用は、変化し続ける職場環境にシームレスに対応しています。また、その利便性、適応性、エンゲージメント、費用対効果により、モバイルデバイスは不可欠なツールとしての地位を確立しています。

ここでの焦点は、現代のグローバルな職場におけるモバイルデバイスとビジネスアプリケーションの重要性です。

仕事の効率化

スマートフォンなどのモバイルデバイスは、今や仕事に欠かせないツールとなっています。どこからでもビジネスアプリケーションにアクセスし、ネットワークに接続できるため、よりスマートで効率的な働き方ができます。

モバイル向けビジネスアプリの人気

モバイル向けのビジネスアプリケーションは、ダイナミックな職場環境にシームレスに適応することから人気を集めています。利便性、パーソナライズ能力、エンゲージメント、そして費用対効果の高さから、多くの人にとって不可欠なツールとなっています。

多彩なワークフロー

モバイルデバイスは、さまざまなタスクに対応する効果的なワークフローの作成に役立ちます。Web会議、ビジネスチャット、ドキュメントの共同編集、ビジネスメールの処理など、モバイルデバイスを使って様々なタスクを簡単に行うことが可能です。

モバイルのパフォーマンスに対する期待

従来のコンピュータに追加して業務に使用されるようになったモバイルデバイスは、効率的かつ迅速に仕事能力を強化してくれる存在としてシームレスに機能することが求められています。

職場におけるイノベーション

モバイルデバイスは職場におけるイノベーションにおいて重要な役割を果たし、従業員の満足度、生産性、定着率の向上に貢献します。モバイルデバイスのおかげで、組織はよりシンプルで効率的な仕事の進め方を見つけ、変化する職場環境に適応できるようになっています。

モバイルデバイスの継続的な成長

モバイルデバイスは引き続き市場を支配しており、ほとんどのユーザがモバイルデバイスでインターネットにアクセスしたり、仕事に関連するタスクを行ったりしています。このことは、モバイルデバイスの市場シェアが前年比で増加し続けていることに現れており、Statcounter GlobalStatsによれば、モバイル、デスクトップ、タブレットを使用するユーザの世界的な割合はそれぞれ58.72%、39.18%、2.1%となっています。

リモートワーク&ハイブリッドワークのトレンド

2020年のリモートワーク採用によって加速した柔軟なワークスペースへの需要は、モバイルデバイスの普及と足並みを揃えています。従業員がリモートワークを強く希望していることからもわかるように、モバイルデバイスの導入はリモート&ハイブリッドワーク環境を実現する上で鍵となります。FlexJobsによると、従業員の97%が何らかの形（フルリモートまたはハイブリッド）でのリモートワークを望んでいることがわかりました。

世界におけるモバイルデバイスの普及

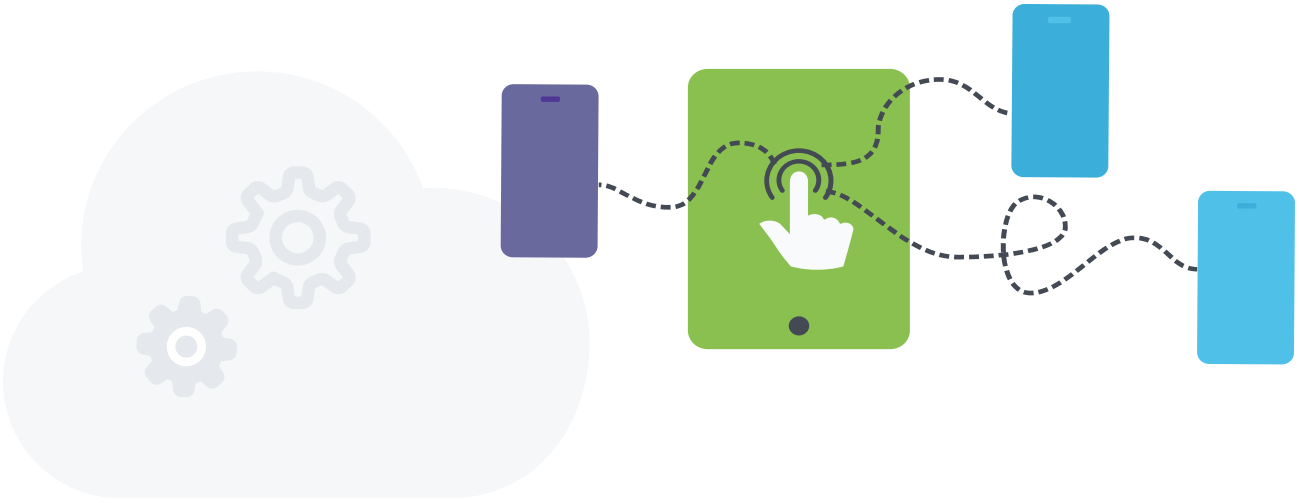
モバイルデバイスの普及は、世界人口の大多数が携帯電話を所有し、スマートフォンがその大部分を占めているという事実によって浮き彫りにされています。Statistaが行った調査によると、2023年には世界人口の90.97%が携帯電話を所有し、そのうち85.88%をスマートフォンが占めていました。

エンタープライズにおけるモバイルデバイスの導入

従来、多くの組織はビジネスニーズに単一のプラットフォーム（多くの場合はMicrosoft Windows）で対応する傾向にあり、選択したオペレーティングシステム（OS）と互換性のあるコンピュータを導入する必要がありました。さらに、Microsoft社とのエンタープライズ契約により、組織は移行の準備が整うまでWindowsの最新バージョンの導入を遅らせることができました。さらに、古いOSバージョンには、組織のニーズに対応するため長期にわたってサポートが継続されるという利点がありました。

しかし、これには問題があります。歴史的にコンシューマー向けと考えられてきたモバイルデバイスの世界においては、OSアップデートは利用可能になったらすぐに導入すべきものとして扱われてきました。リリース後どれくらいの期間でアップデートをインストールするかをユーザ自身が決めることができるという点は、以下の理由からエンタープライズにおけるモバイルデバイスの導入における障害として捉えられてきました。

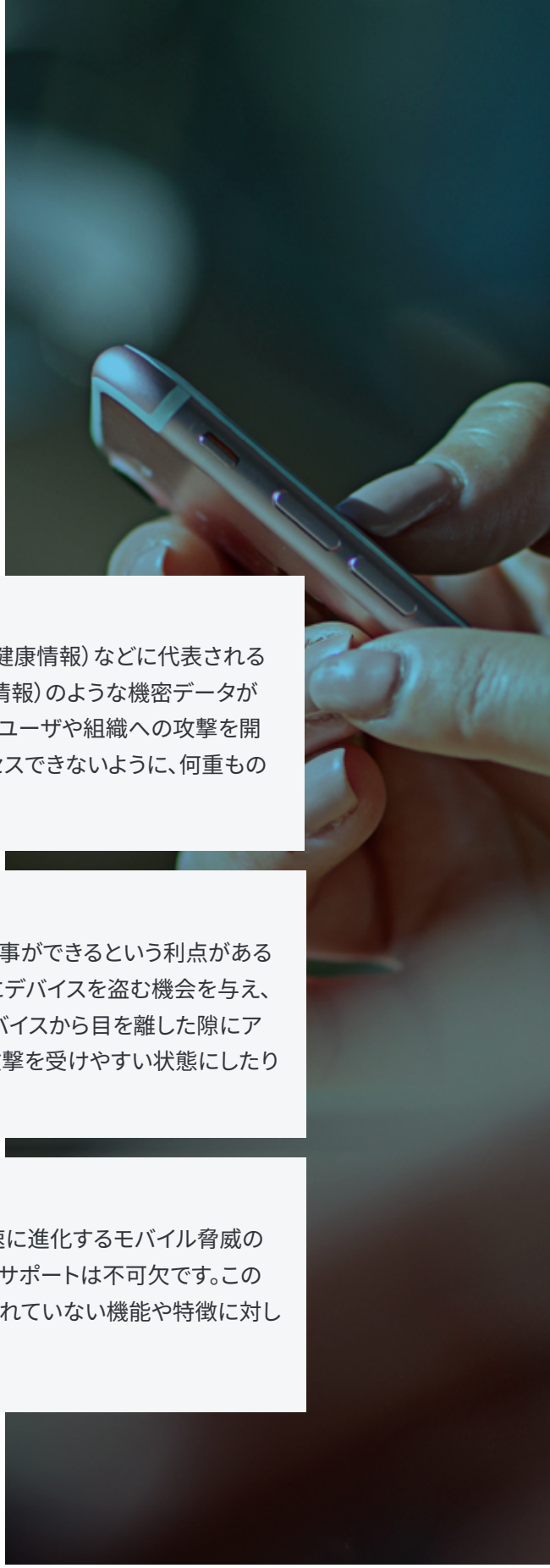
- **モバイル向けOSの多様性**
- **各OSでサポートされているバージョンの断片化**
- **さまざまなタイプのOSにおける導入方法の進化**
- **異なるサポートを必要とすることから生じるアップグレードの遅れ**
- **OSバージョンによって異なるビジネスアプリのサポート**
- **開発者によって異なるアップデートスケジュールや機能サポート**
- **オーナーシップモデル（例：BYOD、COPEなど）によって異なる管理方法**
- **MDMソリューションによって異なる機能サポート（ネイティブおよび非ネイティブのフレームワーク）**
- **OSタイプによって異なるセキュリティレベル**
- **コンプライアンス条件を満たすためのポリシーベース適用の不足**



高まる懸念

ここまで、組織におけるモバイルデバイス採用の急増に関連するセキュリティ上の懸念について触れてきました。ここからは、モバイルデバイスを標的とする脅威と、その使用に関連するリスクについて掘り下げていきます。また、職場におけるモバイルデバイスのセキュアな運用に関する一般的な誤解についても取り上げます。

最初の問題は、これらのデバイスが持ち運び可能であるという性質に起因するもので、以下の理由から攻撃者にとって魅力的な標的となっています。



1

貴重なデータの宝庫

モバイルデバイスには、個人やビジネスのデータに加え、PHI（個人健康情報）などに代表される規制対象のプライバシーデータや、さらにはPII（個人を特定できる情報）のような機密データが豊富に含まれています。脅威者は様々な目的でこの情報を悪用し、ユーザや組織への攻撃を開始します。そのため、このようなデータに正規のユーザ以外がアクセスできないように、何重ものレイヤーで保護することが極めて重要となります。

2

紛失や盗難の危険性

モバイルデバイスは携帯性に優れていることから、様々な場所で仕事ができるという利点がある反面、盗難や置き忘れのリスクも高まります。これは脅威アクターにデバイスを盗む機会を与え、データセキュリティに直接的な危険をもたらします。ほんの一瞬デバイスから目を離した隙にアクセスを許すだけで、そのデバイスを危険にさらしたり、将来的に攻撃を受けやすい状態にしたりする可能性があります。

3

セキュリティに関する誤解

セキュリティに多様性以上のものを求める人もいます。しかし、急速に進化するモバイル脅威の状況を考えれば、エンドポイントフレームワークに対するネイティブサポートは不可欠です。このサポートが欠如しているソリューションを使用する場合、サポートされていない機能や特徴に対して攻撃ベクトルが向くことになりかねません。

過保護 VS 管理不足：適度なバランスを見つけることの重要性

モバイルテクノロジー、そしてセキュリティと管理というさらに広い領域において、バランスは非常に重要な概念となります。これは、ITチームとセキュリティチームの綱引きとして捉えられがちですが、実際のところMDMソリューションだけに頼っていては不十分です。真に効果的なモバイルセキュリティソリューションを確立するためには、その不可欠な構成要素として管理とセキュリティへのアプローチを考える必要があります。

適切なバランスを見つけるのは、口で言うほど容易なことではありません。モバイルセキュリティをおろそかにすると、貴重な資産を危険にさらす可能性がある一方で、多数のソリューションを使ってデバイスを過剰に保護すると、劣悪なユーザエクスペリエンスにつながる可能性があります。どちらか一方を選ぶのではなく、効果的で適応性のあるモバイルセキュリティの指針として、管理とセキュリティのバランスを追求することが重要です。

問題	過剰な保護	管理不足
パフォーマンスの低下		✔
使いやすさ		✔
シャドーIT（プライバシーへの懸念から従業員が個人所有のデバイスを使用するケース）		✔
企業のセキュリティ対策の回避		✔
モバイルワークスペースの可能性の損失		✔
規制要件へのコンプライアンス	✔	
進化するモバイル脅威への対策	✔	
ビジネスデータを個人データとは別の暗号化されたフォルダに分離	✔	
パッチ適用の定期的な実施	✔	
モバイルエンドポイント導入の効率化	✔	
非認可デバイスによる企業リソースへのアクセス阻止	✔	
ビジネスリソースを保護しながらプライバシーも適切に保護		✔

包括的なアプローチ：Macパラダイムから得られる教訓

すでにMacのセキュリティ対策が講じられているのなら、同じようにモバイルデバイスを保護しない理由はありません。

業界や地域に関係なく、世界中の組織でAppleデバイスの採用が進んでいます。Appleの統計データによると、2年前のApple社の年間売上高は3658億ドルという莫大な数字となっており、そのうちの60.7%をiPhone（51.9%）とiPad（8.8%）が占めていました。また、Apple Watchの売上はiPadやMac（9.8%）を上回り、総売上の10.4%を占めました。

iOS、iPadOS、Windows、Android、ChromeOSなど、異なるオペレーティングシステムを搭載したさまざまなモバイルデバイスに対する需要が高まっているのは明確な事実です。

注目すべきなのは、これらのオペレーティングシステムを保護するために採用されている戦略に、相違点よりも共通点の方が多いことです。まったく同じではないものの、類似する点が見られるのです。例えば、高く評価されているAppleのユーザエクスペリエンスや、セキュリティ、管理、プライバシーのバランスを重視する姿勢は、そのままモバイルセキュリティに有意義な形で応用されています。このアプローチにより、フリート内のすべてのエンドポイントを潜在的脅威から保護する包括的な戦略が可能になります。

効果的なMac向けのセキュリティ戦略はAppleそのものから始まります。Appleのセキュリティ戦略はハードウェアやソフトウェアの開発段階から考慮に入れられており、セキュリティやプライバシーの保護は後付けや追加的要素としてではなく、すべての構成要素に最初から組み込まれています。この基盤をさらに強化する上で重要なのが、Appleネイティブのフレームワークです。ユーザがデバイスを使用するたびにデータの機密性、整合性、および可用性が確保されている状態を作るために、開発者はこういったフレームワークを利用しなければなりません。

これらのフレームワークは、ユーザにとっての使いやすさやシンプルさといったAppleの基本原則に沿うよう、相当な注意を払って作られています。興味深いことに、Appleのフレームワークは、厳しいセキュリティ対策が効率的かつ快適に仕事をする上で妨げになるというよくある批判をも退けます。先ほども触れたように、一番大切なのは「バランス」なのです。

セキュリティ対策を強化しながらユーザのプライバシーに配慮するセキュリティアプローチを採用したい組織は、以下のような戦略を立てることができます。

1. ユーザフレンドリーなワークフローの優先的な採用

使いやすさとシンプルさを考えたセキュリティプロセスの構築は、ユーザだけでなくモバイルデバイスの管理とセキュアな運用を任されているチームにもメリットを提供します。

2. データを中心に据えたセキュリティへのシフト

デバイスのセキュリティだけに注目するのではなく、データセキュリティの考えを持つことが重要です。デバイスは何かあれば交換できますが、機密データは一度失われたらそれきりです。確実に守られなければなりません。

3. 多様なオーナーシップモデルの受容

異なるオーナーシップモデルを受け入れ、それぞれのニーズに合ったセキュリティ対策を準備することで、様々なデバイスから企業リソースに安全なアクセスが行われるようになります。特定のオーナーシップモデルのデバイスを無視すると、全体的なセキュリティ戦略に脆弱性が生じる可能性があります。

4. 包括的なデータ保護

あらゆる形態のデータを確実に保護することが大切です。これには、ボリュームの暗号化、ビジネスデータと個人データの分離、あらゆるネットワーク接続を介して送信されるデータの保護が含まれます。

5. 最新のモバイルテクノロジーの採用

最新のモバイルデバイスのニーズを満たすように設計されたテクノロジーを採用することが重要です。従来のセキュリティツールを過信しすぎると、新たに出現したモバイル脅威に対処できないことがあります。

6. スプリットトンネルの導入

モバイルデバイスを使う上で不可欠なのが効率性です。スプリットトンネル技術は、保護が必要な業務データを安全にルーティングしながら、個人情報のように業務に無関係なデータには会社のセキュリティプロトコルをバイパスさせることができるもので、BYODユーザのプライバシーを尊重しながらデータの安全を守ることができます。

モバイルデバイスをMacと同様に扱うことの意味

macOSとiOSの統合が進むことは、モバイルとエンドポイントセキュリティの将来にとってどのような意味を持つのでしょうか？

デスクトップコンピュータであるMacとモバイルデバイスを比較することは、リンゴとオレンジを比較するようなものかもしれませんが、macOSとiOSがバージョンアップするたびにその距離を縮めていくのは紛れもない事実です。新たなバージョンがリリースされるたびに、この2つのOSの統合はますますその重要性を高めていくはずです。

しかし、もっとも重要なのは組織がいかにしてこの深い統合を活用できるかということです。この統合がさまざまなデバイスタイプに及ぼす影響には以下のようなものがあります。

- セキュリティギャップの迅速な解消
- 生産性のシームレスな回復
- ユーザエクスペリエンスの向上
- 従業員の信頼の獲得
- インフラ全体で一貫したコンプライアンス
- 組織のポリシーの確実な遵守
- 包括的で多層的なセキュリティプロセス
- 一貫性のあるアプリ管理
- オーナーシップを問わない深層防護戦略
- 柔軟かつ堅牢なセキュリティと管理ソリューションの連携による包括的サポート

モバイルデバイスのコンプライアンス

コンプライアンスは規制のある業界だけのものではありません。コンプライアンスは金融、ヘルスケア、教育といった業界の組織にとって不可欠なものですが、ルールやポリシーに準拠することは、ビジネスの継続に対するリスクを最小限に抑えながら特有のニーズを満たしたいと考えるその他の組織にとっても非常に重要です。このことから、Macの場合と同様に、組織全体をカバーするモバイルポリシーを適用することは、デバイスフリート全体に対する包括的なセキュリティ戦略を構築する上で重要な役割を果たします。

例えば、ハイブリッドワークやリモートワークの普及によりモバイルデバイスの盗難、紛失、悪用のリスクが高まり、機密データが危険に晒されている事実を例にとってみましょう。この場合IT部門は、MDMワークフローを活用してセキュリティ構成をすべてのデバイスに導入することで、暗号化ポリシーや安全な認証プロトコルを適用させることができます。さらに、リモートワイプ機能により、必要に応じて侵害を受けたデバイスからデータを安全に消去することもできます。

また、既存のMac向けのコンプライアンス計画を参考に、モバイルユーザ向けのコンプライアンス計画を策定することも可能です。このアプローチは、固有のリスクに対処すると同時に、基盤となる堅牢なベースラインを提供してくれます。これは、カリフォルニア州消費者プライバシー法（CCPA）のような規制にすでに準拠している成熟したウェブサイトとはまったく異なる形で設計されたモバイルアプリケーションなど、新たな枠組みに関連するリスクを軽減する上で特にメリットがあります。

さらに、コンプライアンスには、深刻な脆弱性や規則違反に発展する前に問題を特定し、それに対処することも含まれます。この場合、セキュリティ（監視）と管理（強敵適用）の組み合わせが連携して脅威を検出・対処し、モバイルデバイスがコンプライアンスを維持できるようにします。

モバイルデバイスの汎用性により、ユーザが誤って業務用の承認済みアプリをプライベートで使用したり、反対に承認されていないアプリを業務関連のタスクに使用したりしてしまう可能性があります。どちらのケースも、データの混在、プライバシーの侵害、データ漏洩、もしくは規制違反など、組織にリスクを及ぼす可能性を含んでいます。

モバイルデバイスのコンプライアンスをMacのコンプライアンスと同様に真剣に扱うことで、企業は最新の脅威からモバイルエンドポイントを保護し、デバイスのインベントリ、使用状況、支給デバイス、企業データにアクセスする従業員、導入されたセキュリティ対策などの正確な記録を、Macと同じように管理することができます。

モバイルデバイスのコンプライアンスについて考えるべき最後の事項は、ユーザの継続的なセキュリティトレーニングです。これは、しばしば見落とされがちな点ですが、セキュリティのベストプラクティスや、セキュリティを脅かす脅威に遭遇した際に従うべき手順やワークフローに関する知識をユーザに授けるという意味で、包括的なモバイルセキュリティ計画において非常に重要です。このようなトレーニングは重要なセーフガードとして機能し、管理およびセキュリティ対策を補完する重要な役割を果たします。

簡単に言えば、サイバーセキュリティはIT部門や企業だけの責任ではなく、すべての人の責任でもあるのです。

モバイルおよびMacの管理とセキュリティを一体化させるためのポイント

ここまでの内容を一言でまとめると、「セキュリティの鍵はフリート全体における管理とセキュリティを一体化させることにある」ということになります。

1. コンバージェンス
これは、モバイル中心の現代の職場において、デバイス管理とセキュリティがシームレスに一体化し、堅牢なセキュリティプロトコルが存在していることを指します。

2. 問題の克服
モバイルセキュリティの問題克服に必要なのは、たいした効果もない複数のツールが積み重ねられている従来の断片的なアプローチではなく、包括的なソリューションです。

3. 一貫性
一貫性を確保するためには、異なるデバイスのセキュリティベースラインを確認し、エンドポイントに問題があることを示す変化がないか、またはセキュリティ脅威、脆弱性、異常の有無について調査が必要かどうかを、積極的に監視する必要があります。

4. 使いやすさ
ユーザエクスペリエンスを優先しつつ、保護とのバランスを取ることは、包括的な戦略にとって不可欠であり、IT、セキュリティチーム、エンドユーザにとっての有効性とシンプルさの微妙なバランスを達成する上で非常に重要です。

5. 対応
すべてのデバイスタイプ、プラットフォーム、そしてインフラ全体において、適切な優先順位付けや調査、解決に重点をおいてセキュリティ脅威に迅速に対応することが重要です。

6. バランス
適切なバランスを達成するには、ユーザエクスペリエンスを損なうことなくセキュリティを達成することや、安全性とユーザ満足度をシームレスに融合させる可能性について常に意識することが重要になります。

Jamfでは、すべてのデバイスが妥協のない保護を得られる未来を目指しています。これは、素晴らしいユーザエクスペリエンスと組織にとっての安心・安全を届けることのできるセキュアでシンプルなテクノロジーを提供するというJamfの最終目標に基づくビジョンです。私たちは、あらゆる状況においてシームレスなデバイス管理と保護を届けたいと考えています。Jamfではこのコンセプトを「**Trusted Access**」と呼んでいます。

組織のセキュリティニーズや、すべてのエンドポイントを管理・保護する方法を再評価したいとお考えなら、ぜひJamfまでお問い合わせください。

jamf

www.jamf.com/ja/

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気軽にお問い合わせください。