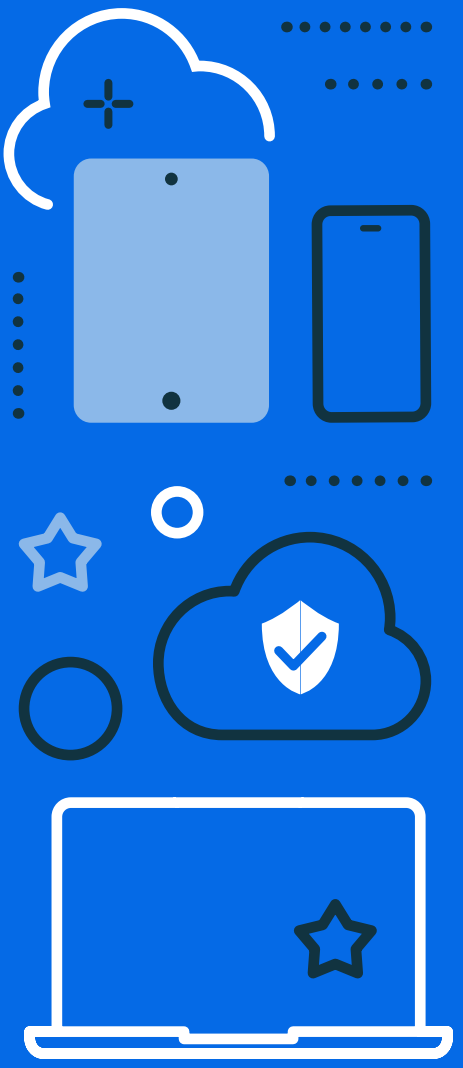


データポリシーと管理

初心者ガイド

jamf

リモートワーカーやハイブリッドワーカーをサポートする組織がこれまで以上に増えるなか、デバイス管理に関して基礎的なもの以上のものが求められるようになっています。企業支給のモバイルデバイスはいつでも好きな場所で働くという自由を叶えてくれますが、そのようなデバイスや、場合によっては通信プランを会社で負担する私的デバイスで、多くのデータを私的使用されるといったケースも珍しくありません。

Jamf Data Policyは、ハイブリッド環境やリモート環境で働くユーザが、物理的なロケーションや使用するデバイスに関わらず生産性を維持できるようにすることで、組織におけるリモートワークの成功を支援するソリューションです。

Jamf Data Policyの活用でできること

- カスタマイズ可能なポリシーの導入でコンプライアンスを維持
- データの使用上限やアラートの設定
- 不適切なコンテンツのフィルタリング
- ポリシーをネットワーク上のすべてのコミュニケーションに拡張
- シャドーITの監視と排除
- 使用状況のリアルタイム管理

このeBookでは、組織やエンドユーザのニーズに応える形で利用規約の策定やデータやデバイスの管理を行う方法についてご紹介します。

デバイス管理は、非常に科学的な取り組みと見なされがちです。デバイスやユーザ、データを確実に保護し、その状態を維持するための最適な管理レベルは、あらゆる種類のデータによって裏付けされてきました。その事実自体に間違いはありませんが、管理者として成功するためには実はちょっとした「魔法」が必要になります。そしてそれは、経験や、組織のネットワークのニーズの完全な理解から生まれるものです。基準やベストプラクティスも重要ですが、結局のところネットワークというものは、その組織の特定のポリシーのもとで運営される独特な存在だからです。

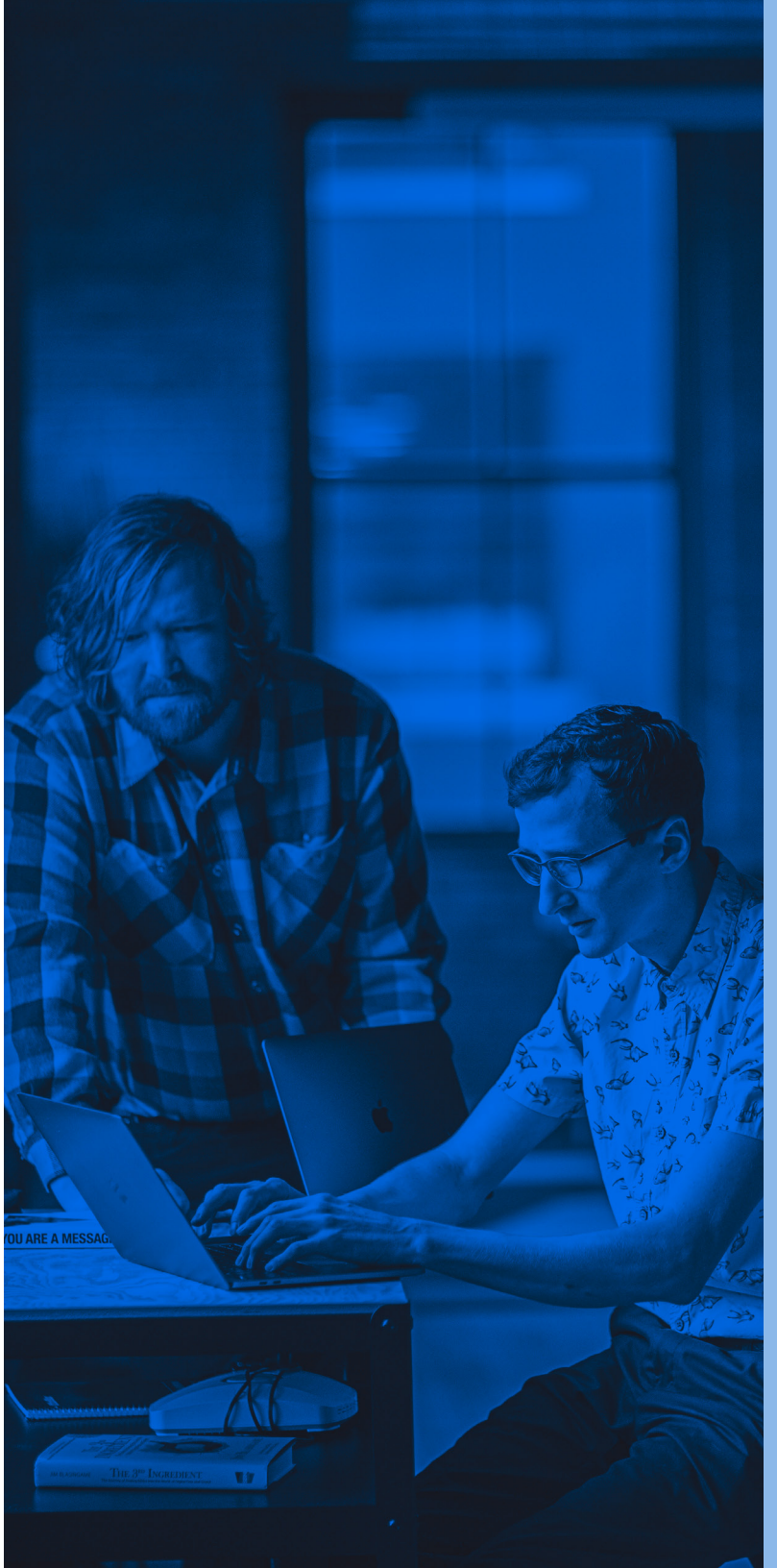
パフォーマンスが最適化されたデバイスを使うと、魔法を手に入れたような気分になりませんか？

データの安全性が確保され、しっかりと保護された企業のアプリケーションやリソースにスムーズにアクセスできます。またセキュリティが保証されたデバイスを使用して仕事や個人のタスクを実行することができ、強引な管理手法によって生産性やプライベートの楽しみが妨げられることがないため、ユーザも大満足です。万が一問題が発生したとしても、IT部門の手を煩わせたりエンドユーザに影響を与えることなく、自動化されたワークフローによりリスクが軽減されます。まるで魔法のようだと思いませんか？

Jamf Data Policyを活用してモバイルデバイス管理を行うと、まさにこのような魔法が生まれます。Jamf Data Policyは、基本にとどまらず、リモートワークやハイブリッドワーク環境での業務をサポートする組織に貢献します。デバイスの種類に関わらず、また、BYOD（私的端末の利用）デバイスか、業務と私的使用の両方が許された企業所有のデバイスかにかかわらず、利用規約を設け、それを管理・適用する手段は組織にとって不可欠です。

まずは、利用規約を作成または評価するために何から始めたらよいのかについて説明します。以下の項目を実行するために何ができるのかを考えてみましょう。

- リアルタイム分析と詳細なレポートによるデータ使用の監視
- 利用規約の徹底
- シャドーITの排除
- コンテンツフィルタリング
- ユーザや組織のニーズに合わせてカスタマイズされた保護ポリシーの導入
- デバイスの種類やオーナーシップタイプを問わない包括的なサポート

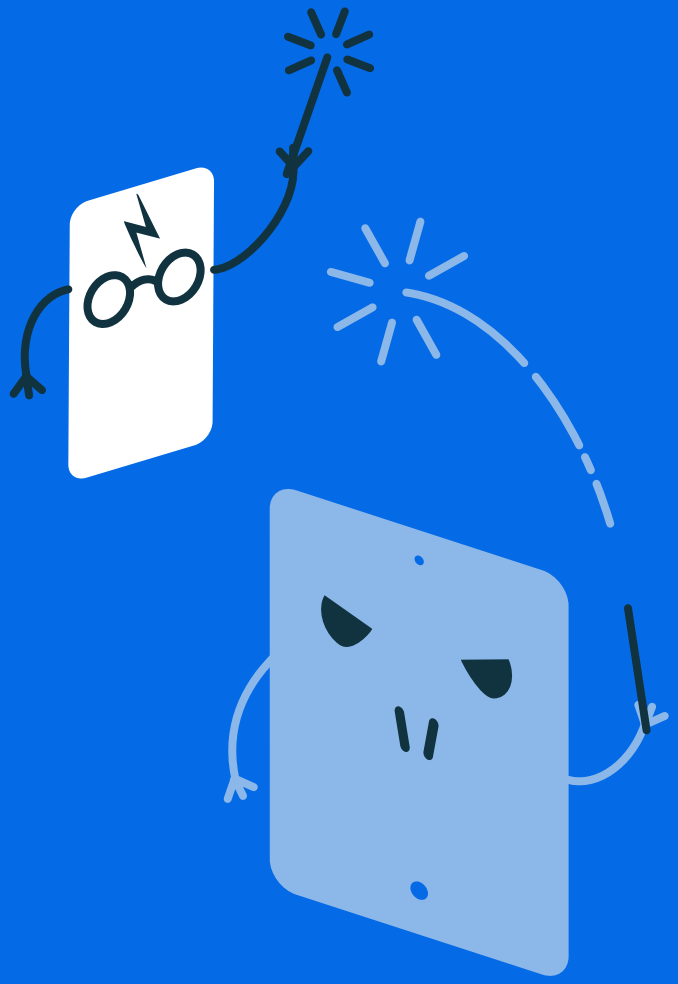


ハリー・ポッター vs ヴォルデモート

Jamf Data Policyの機能を紹介する前に、なぜ組織のネットワーク上にあるモバイルデバイスを管理することが重要なのかについて説明します。この話をする上で、現代のもっとも偉大な魔法使いであるハリー・ポッターに登場してもらいましょう。

J・K・ローリング作の「ハリー・ポッター」シリーズに登場する魔法使いたちは、ヴォルデモートのようになるか、それともハリーのようになるか、選択を迫られます。この点において、彼らはIT管理者と似ています。

もしヴォルデモートのやり方を選んだのなら、その組織は鉄拳でユーザを支配し、彼らのニーズや予期せぬ展開を無視して、ポリシーの準拠を強要するでしょう。



一方、もしハリーのやり方を習うのであれば、組織は公正に運営され、もっと大きな問題を解決するためにユーザと協力し合い、妥協する道を選ぶはずです。

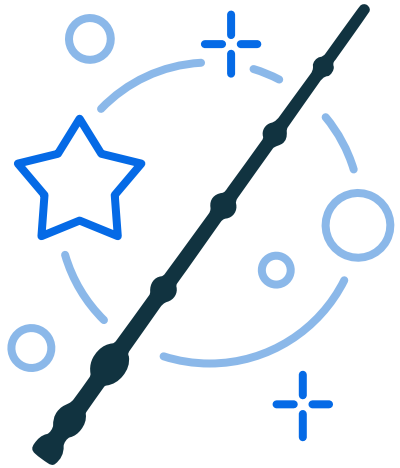
IT部門は、セキュリティとユーザ保護の名の下にヴォルデモートのやり方を選びがちですが、実際は後者の方が、データセキュリティを維持しユーザを保護するための選択肢が多いのです。生産性を抑制し最終的にユーザを遠ざけてしまう恐れのある過剰なコントロールから逃れようとする必要がなく、すべての関係者が同じ目標のために協力し合うことができるからです。

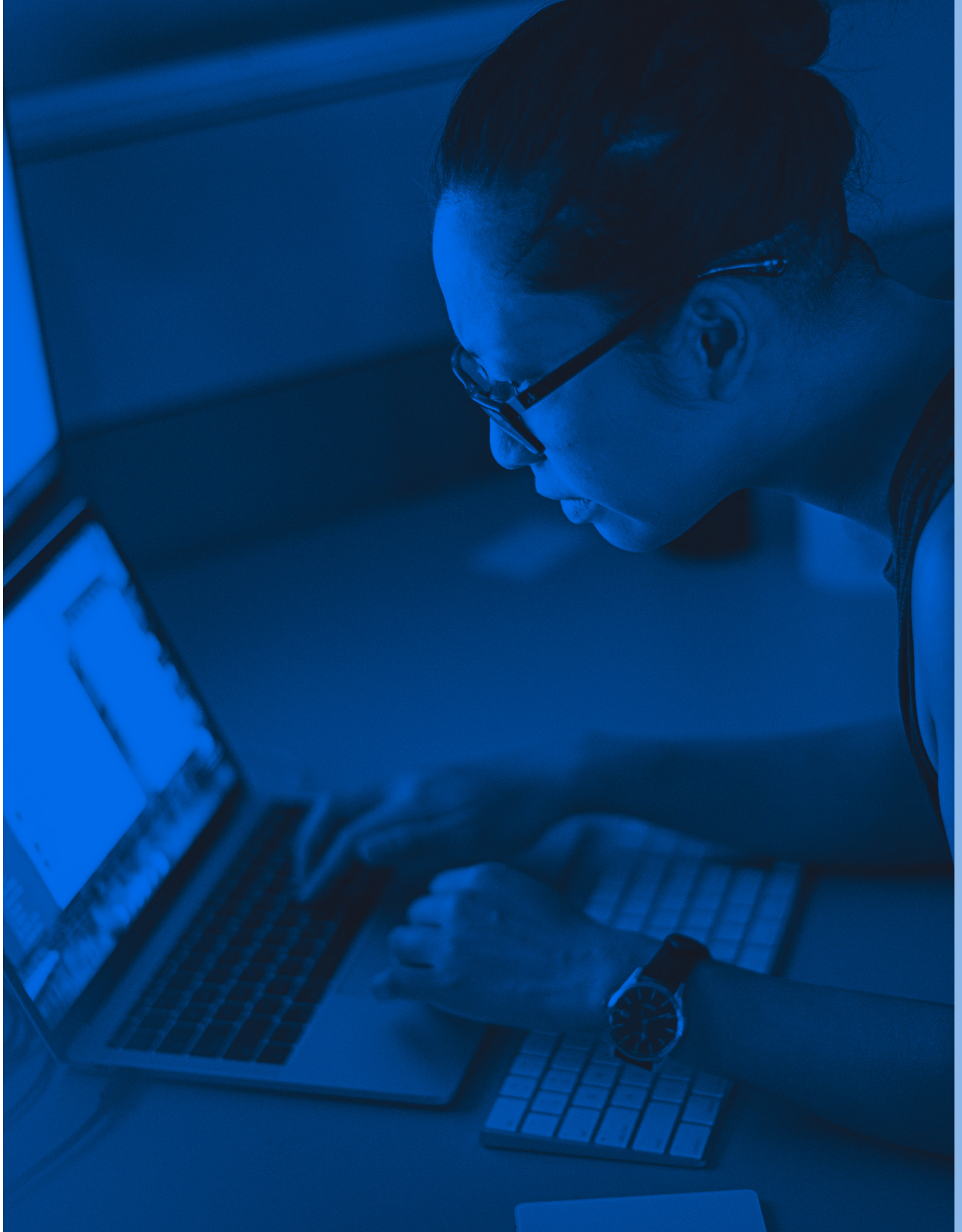
前述したように、ネットワークはそれぞれ異なる規約、ポリシー、法律、規制への遵守を求められます。そのため、データのポリシーと管理においては、すべてのケースに当てはまる回答というものは存在しません。そのことを考え合わせれば、ヴォルデモート方式でデバイスを管理することはIT管理者を囲い込むことに他ならず、動的なITの世界で遭遇するさまざまな問題をモニタリングし、検出、対応、修復するために必要な円滑さを排除してしまうことに他なりません。

ニワトコの杖

ハリー・ポッターと同じように、IT管理者もただの人間です。素晴らしいスキルは持っていても、普通の人がそうであるように、それらを効果的に使う方法が必要です。ハリーにニワトコの杖があるように、ITチームにはJamf Data Policyがあります。

モバイルデバイスを着実かつ効率的な方法で包括的に管理するために必要な能力を組織に提供してくれる2つの機能について、具体的に掘り下げて説明します。





リアルタイムのポリシーコントロール

ビジネスに不必要かつ不適切なコンテンツやアプリへのアクセスを制限するために組織のITポリシーをカスタマイズするには、データ使用量の上限に関するポリシーを構成してそれに達した場合に適用し、アクセス可能なウェブサイト、サービス、アプリを定義した上でカテゴリベースのコントロールで使用状況を可視化し、さらにポリシーが自動的に施行されるようそれをカスタマイズする必要があります。

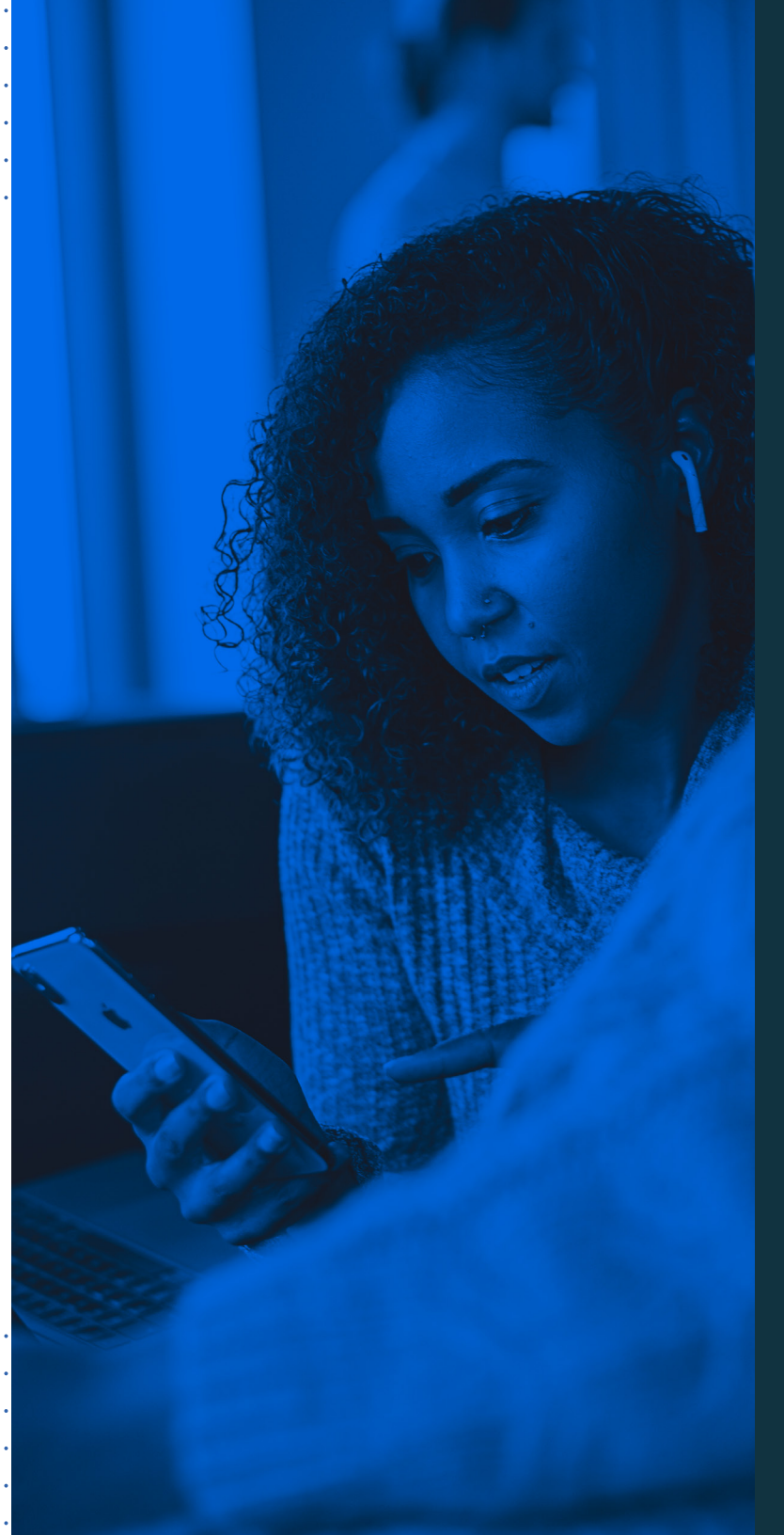
Jamfの調査によると、企業のデータ使用の50%以上がビジネスにとって必要なものではないことがわかっています。データの使用状況をこれまでにないレベルで可視化できるようになった今、組織はデータプールやネットワークベースのトラフィックの使用についてきめ細かく構成することができます。モバイルデバイスを、コントロールの欠如によって悪用が許されるものとしてではなく、有用なツールとして活用できるようになったのです。

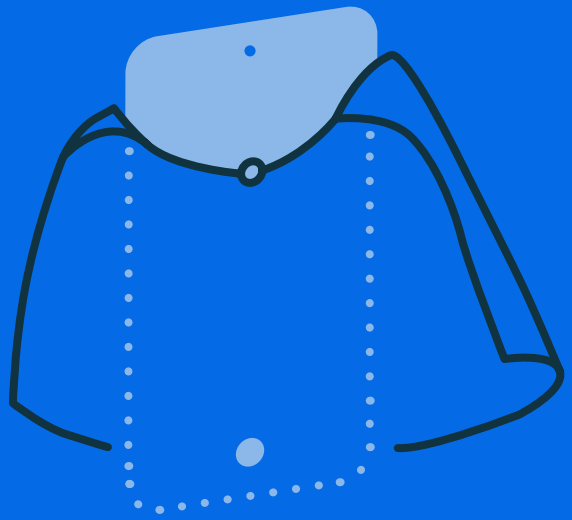
あらゆるモバイルデバイスとあらゆるオーナーシップモデルに対応

BYOD、CYOD、そしてCOPE。モバイルデバイスに関するプログラムを示す略語は色々ありますが、それぞれサポートの度合いが異なります。どのオーナーシップモデルをサポートするかということだけでも十分難しいのに、さまざまなモバイルデバイスの種類、ベンダーや通信業者の存在が問題をさらに複雑にしているのは間違いありません。

それに対し、Jamf Data Policyは非常に単純明快です。

組織がすべきなのは、どのデバイスがビジネスに最適かを選択することだけです。Jamfは、デバイスの種類、オーナーシップモデル、オペレーティングシステムに関係なく、これらの選択肢を幅広くサポートします。これにより、IT部門は、複数のシステムを単一の方法で管理しようとする際に起こる問題について心配することなく、セキュリティとコンプライアンスのポリシーに最大限の注意を払いながらモバイルデバイスの管理に集中することができます。





透明マント

IT管理者の立場に立ってみれば、ヘルプデスクに一度に多くの問い合わせが入った時などは、自分を見えなくするマントが欲しいと感じるかもしれません。次から次へとやってくるメールやメッセージ、電話での問い合わせにひたすら対応し続ける代わりに、問題の根本的な解決に集中できたらどんなにいいかと感じている管理者も多いはずです。

そのように考えているのなら、Jamf Data Policyに用意された機能を活用して、リソースの使用方法を標準化し、コンプライアンスを徹底させ、ユーザの期待値を定めれば、次々とやってくるリクエストを食い止めることが可能です。

フルカスタマイズ可能

2つのまったく同じネットワークが存在しないように、各組織のインフラの管理や事業継続のための要件も異なります。これは、組織のリスクに対する寛容度に大きく左右されます。また、エンタープライズがリスクへの対応としてセキュリティポスチャを調整するのと同様に、Jamf Data Policyも、ポリシーやその施行・管理方法の完全なカスタマイズによりリスクに対応します。

コンテンツフィルタリングのカテゴリーのカスタマイズから、許可リストとブロックリストのカスタマイズまで、ポリシーは組織全体に適用するだけでなく、きめ細かな適用をすることもできます。1人のユーザだけに適用したり、反対にグループに適用することも可能で、組織のニーズに合わせて柔軟に選択することができます。何より重要なのは、選ぶのはあなた自身だということです。

コンテンツフィルタリング

Jamfの調べによると、アダルトやギャンブル関連のアプリやサービスは、暗号化されていない接続に依存する傾向が著しく高く、データ漏洩や規制機関へのコンプライアンスを通じて組織がリスクにさらされる可能性が高いことがわかっています。上記の分野だけでなく、武器やヘイトスピーチ、その他の扇動的な内容を含むコンテンツにアクセスすると、ユーザや組織が民事または刑事上の事件に巻き込まれる可能性もあります。

フィッシングサイトやマルウェアなど、広大なインターネット空間に巣食うウェブコンテンツがもたらすセキュリティ脅威は言うまでもありません。コンテンツフィルタリングは、悪いものを排除することだけが目的ではありません。積極的に活用すれば、安全なウェブサイトやサービス、アプリのみにアクセスを許可し、正当なデータのみを取り込むことができます。

さらに、コンプライアンスに準拠したデータの使用状況を管理・維持し、許可されていないサービスへのアクセスを監視・遮断することで、訴訟のリスクを減らすことも重要な点です。シャドーITなどのサービスは、組織の機密データを不注意に露呈し、デバイスとネットワークのセキュリティ体制を弱体化させます。

賢者の石

このセクションでは、不老不死の薬を作る方法や、何の変哲もない金属を金に変える方法については説明しません。その代わりに、Jamf Data Policyの素晴らしい2つの機能について説明します。リアルタイムでインサイトを収集してくれる魔法のような機能のおかげで、IT管理者はその情報をもとに組織のデバイスやその管理により合った実用的なタスクを作り出すことができます。

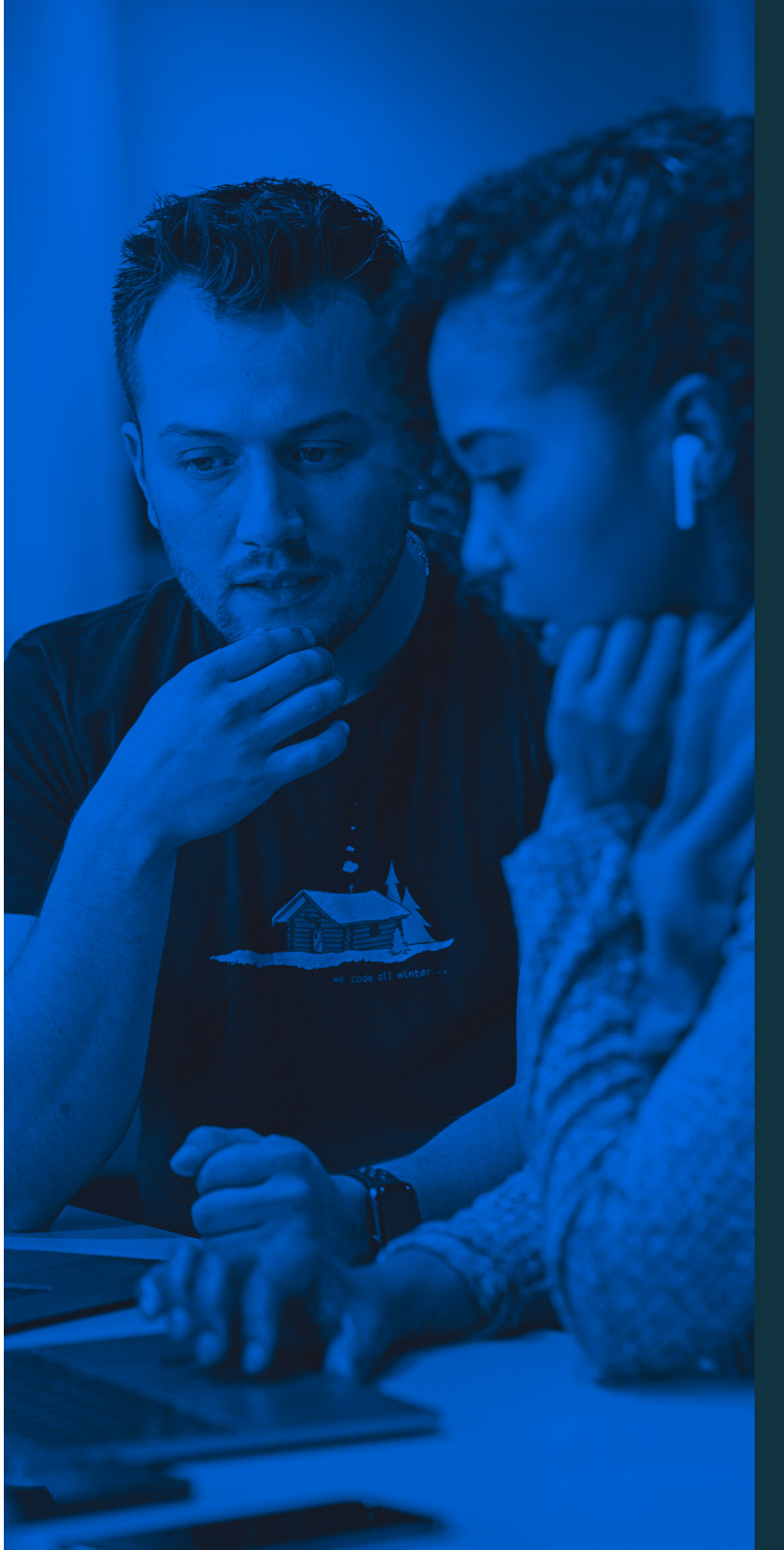
さらにこの機能により、ネットワークを意識した保護が可能になり、新しいセッションが発生した場合や、反対に既存の接続が終了した場合にも、すべてのネットワーク接続タイプにおいてデバイスとユーザを保護し、コンプライアンスを維持することができます。

ネットワークを意識したポリシー

これまで述べてきたように、すべてに対応できるソリューションというものは存在しません。モバイルデバイスのネットワーク接続ほど、このコンセプトを体現しているものはないでしょう。例えば、従量制課金接続を利用する必要がある場合、ローミング料金や超過が発生する可能性があるため、ユーザは使用状況に敏感になります。しかし、公共のWi-Fiホットスポットに接続できる場合は、そのような心配はあまりしないかもしれません。

Jamf Data Policyでは、こういった不透明な状況に対応するために、異なるネットワーク接続タイプとその独自の要素に対するポリシーを作成し適用する機能をIT管理者に提供しています。

例えば、組織がCOPEモデルを採用し、従業員に仕事とプライベートの両方で使えるモバイルデバイスを提供する場合、携帯電話のデータプランは全ユーザーが共有するデータプールに含まれます。この場合、全員が十分なデータを利用できるよう、Wi-Fi接続時の帯域幅は管理せずに、各ユーザのモバイルデータの使用量だけを制限する必要があるかもしれません。Jamf Data Policyは、まさにこのようなポリシーを適用するためのソリューションです。さらに、このポリシーは非常にスマートで、IT部門からのサポートを必要としたりエンドユーザエクスペリエンスに影響を与えたりすることなく、ユーザがどちらの方法で接続しているのかを自動的に検出し、対応することができます。

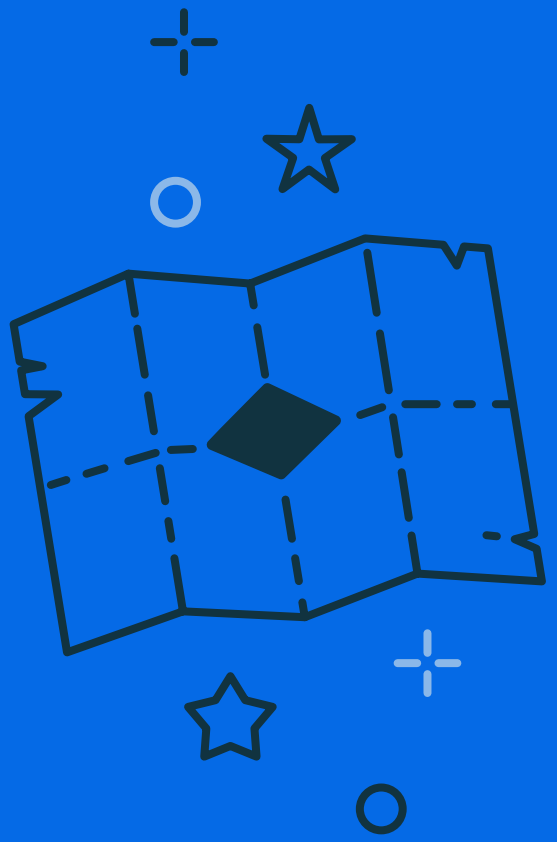


リアルタイムインサイト

何かが壊れたり故障したりしたときに、それが起こる前に知りたいか、それとも起こってから知りたいかをIT管理者に尋ねた場合、恐らくいつも同じ答えが返ってくるはずです。

誰でも、できれば先に知りたいと思うはずです。未然に防ぐとまではいかなくても、少なくともできるだけ早く事態を緩和したいからです。

ご安心ください。そんな時は、Jamf Data Policyのリアルタイムインサイトがあります。デバイスがどのようにデータを使用しているか、どの接続で使用しているかがきめ細かいレポートによって可視化されるため、IT部門は先手を打つことができます。管理者は、状況に応じてポリシーの制限をより厳しくしたり緩和したりできます。また、既存のデータプールを変更したり、特定のアプリやサービスへのアクセスを有効または無効にするためにコンテンツフィルタリングを構成したり、またはシンプルにデバイスのセキュリティポスチャのモニタリングも行うことができます。



9と4分の3番線で搭乗開始

組織のモバイルデバイスフリートやユーザの個人所有のデバイスをJamf Proに登録することは、デバイス管理の優れた基盤になります。しかし、ハイブリッドワークやリモートワークを中心とした現代の労働環境においては、単に物理的なデバイスの管理を行う場合でもより専門的なツールが必要となります。

Jamf Data Policyでできること

- ネットワークを意識したスマートポリシーにより、デバイス上でデータの送受信を行う方法を管理
- ネットワーク接続の種類を問わずコンプライアンスに準拠
- 70種類のインテリジェントなテンプレートでコンテンツをフィルタリングし、未承認のコンテンツに加え、脆弱性、危険性、悪意のあるウェブサイト、アプリ、サービスへのデバイスの接続を防止

Jamf Data Policyは、シャドーITを排除し、オーナーシップモデルに関係なくすべてのデバイスに対して使用ポリシーを適用することで、エンドユーザエクスペリエンスを阻害せずにデータやデバイス、ユーザのセキュリティを確保します。これにより、IT部門の仕事はぐんと楽になります。

トライアルに申し込む

今すぐ体験してみたい方はぜひ無料トライアルにお申し込みください。
または、お近くのApple製品販売代理店までお問い合わせください。