jamf

PCが主流の環境で

MacとiOSを徹底活用する

はじめに

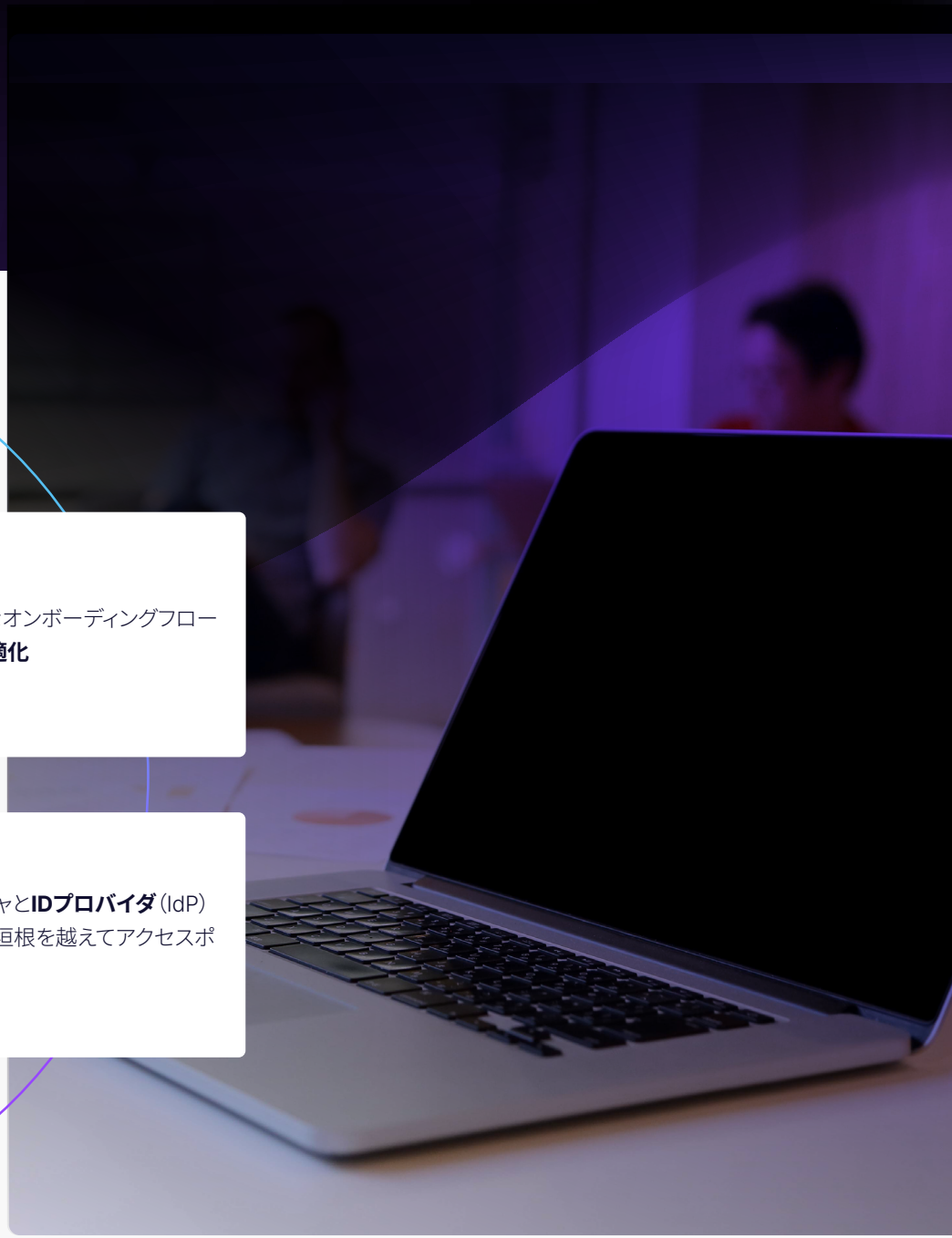
Windowsデバイスが中心の大企業がAppleデバイスを導入する際は、何よりも効率性が重要です。IT部門がその後も円滑に業務を続けられるか、余分な作業に追われることになるかを左右するのは効率性であり、人員を増やしたところで根本的な解決にはなりません。

このガイドは、「Jamfが選ばれる理由」シリーズの第1段です。今回は、IT管理者からエグゼクティブ職までさまざまなスキルレベルの方々を対象に、ID管理、セキュリティ、自動化、オブザーバビリティなどに関する既存のIT資産を活かしてコンプライアンスを確保しつつ、面倒な手作業を減らしていくためのヒントをお届けします。究極的には、業務負担を増やすことなく、AppleデバイスとWindowsデバイスのどちらにも一貫したエクスペリエンスを実現することが鍵となります。

概要

Windowsが中心の環境にAppleデバイスの導入を進める場合、その成否を左右するのは運用効率です。このeBookでは、プロセスやワークフローに影響を与える重大な課題に対処することで、人員や総保有コスト、複雑さを増やすことなくAppleデバイスを導入・運用する方法を解説します。本資料で紹介する方法を活用することで、従来よりも短時間で導入を完了できるほか、可視性が向上したり、組織の規模が拡大しても変わらない安全で一貫したAppleデバイスのエクスペリエンスを実現したりする効果が期待できます。

Jamfなら、Appleデバイスの導入に関する課題を解決



ID管理システム、セキュリティツール、既存のITソリューションを統合し、データサイロと非効率な作業フローを解消。包括的戦略に基づく業務運営を実現

ゼロタッチのシームレスなオンボーディングフローで、従業員の**生産性を最適化**

エコシステムの統合により、調達からパッチ適用、安全な廃棄・再利用に至るまで、Appleデバイスのライフサイクル管理全般を**自動化**

ゼロトラストアーキテクチャと**IDプロバイダ**（IdP）により、プラットフォームの垣根を越えてアクセスポリシーを統合

豊富なテレメトリデータを絶えず評価し、セキュリティ状態のベースラインを標準化して維持。それにより、**インシデント対応**を迅速化

今ある技術スタックとの密な統合が重要

デバイス管理が既存のセキュリティツールやID管理ツールと連携していないと、データサイロが生まれ、業務フローが非効率になったり、コンプライアンスの問題が発生したりする原因になります。

Appleデバイスと従来のWindows中心のネットワークは相互に互換性がないという思い込みが、いまだに根強く残っています。何十年も続くこの迷信をよそに、世界各地で事業継続が求められる現代の大企業では、クロスプラットフォーム対応のテクノロジーがもはや当たり前となっています。この点が非常に重要なのは、現代の組織が価値の創出や生産性維持を目的としてクラウドベースのアーキテクチャ、アプリケーション、サービスに依存する度合いをますます強めているからです。従業員が使用するデバイスの種類、プラットフォーム、バージョンも多種多様なうえに、勤務地も各地に分散しているなかで、全体として一貫したセキュリティやガバナンスを確保しなければなりません。

そして、クロスプラットフォーム対応と並んで重要なのが、大規模に導入するAppleデバイスと既存の技術スタックとの密な統合です。

Jamfのソリューションには、企業のAppleデバイスの統合プロセスを円滑に進めるための仕組みが備わっています。

それが、**プラットフォーム アプリケーション プログラミング インターフェース**（プラットフォーム API）です。

Appleエンドポイントと既存のテクノロジースタックをスムーズに連携させる鍵は、管理・ID・セキュリティのワークフローに紐づく、セキュアで標準ベースのソリューション間連携にあります。

では、企業が現代の脅威に対応し、コンプライアンスを確保していくという観点では、上に挙げた状態を実現するメリットは何でしょうか。それは、ソリューションも業務も、複雑さを削ぎ落としたシンプルな形に変えることができるということにほかなりません。

既存の技術スタックにAppleデバイスをシームレスに統合できれば、プラットフォームの垣根を越えて以下が実現します。

自動化により均質で一貫したワークフローを推進

ID中心のセキュリティで脅威対策を一元化

既にあるソリューションを駆使してコンプライアンス状態を維持

IT部門のサイロ化を軽減し、応答時間を最適化

Jamfが選ばれる理由

Jamf Marketplaceでは、300以上（随時追加中）のあらかじめ構築された統合機能を提供しており、企業の既存環境へのApple導入における複雑さを解消します。

デバイス導入を効率化し、従業員のダウンタイムを削減

従業員がデバイスの初期設定を待つ時間は、生産性が失われる時間でもあります。この待ち時間は、PCの場合には1台あたり平均2〜4時間にものぼります。

PCが中心の環境にAppleデバイスを統合するプロジェクトにおいて、計画に続いて最も重要なのが、導入の段階です。導入段階では、デバイスが新品であるか再利用品であるかを問わず、従業員がIT部門による初期設定を待つ時間が発生するのが普通です。また、適用する設定、インストールするアプリの数、従業員が担当する業務に必要な構成によっては、従業員にデバイスが支給されてからデバイスが実際の業務に利用できる状態になるまでの待ち時間も、直接的に生産性が失われています。

では、こうした時間を、Macは1台あたり約15分、iPadやiPhoneにいたっては1台わずか5〜7分にまで短縮できるとしたら、どうでしょうか？

このような早さで導入が完了する秘密は、初期設定をゼロタッチで完了できる点にあります。Apple Business Manager（ABM）をApple製品の管理に特化したソリューションに接続すれば、Windows環境ではとても真似できない自動化フレームワークが実現します。ABMは、Windows AutopilotのApple版のようなものですが、シリコンから登録サービスまでAppleが管理しているため、ハードウェアとの統合が密である点が大きく異なります。ABMとJamfを連携させ、管理コンソール上でデバイスの準備状態（アプリ、構成、セキュリティポリシー、ID設定）を定義します。その後、Appleからデバイスを調達すると、ABMがデバイス情報をJamfと同期し、事前登録グループに追加します。

ここまで完了すれば、IT部門の作業はほぼ終わりです。

その後は、会社所有のデバイスがユーザの手元に届きます。デバイスを受け取ったユーザに必要なことは、オフィス勤務であるかリモート勤務であるかを問わず変わりません。開封して電源を入れるだけです。電源を入れると、デバイスがJamfに自動で登録され、登録前のワークフローが実行されます。デバイスの初期設定はこれで完了です。ゼロタッチなのですべてが自動で完結し、エンドユーザは何もする必要がありません。当然、ヘルプデスクに問い合わせるようなこともせずに済みます。

Jamfが選ばれる理由

Jamfのブループリントを使えば、デバイスが宣言型デバイス管理を使用して自律的にポリシーを適用できるため、設定作業に要する時間をMacの場合には約15分、モバイルデバイスの場合には7分未満にまで、それぞれ削減できます。また、管理対象デバイス認証では、ハードウェアをベースにコンプライアンスを確認できるため、正規のデバイスのみ企業リソースにアクセスできる状態が実現します。

Appleは、シリコンからソフトウェアに至るまでの認証・ID・管理を単一のフレームワークに統合

宣言型デバイス管理（DDM）は、デバイスが非同期的に設定を適用し、デバイス管理サービスに自らの状態を報告できるようにする仕組みです。インターネットに接続していなくてもデバイスが自律的かつスピーディーに構成を完了できるようになるので、常にコンプライアンスが保たれます。また、Appleサポートに何度も問い合わせる必要もなくなります。

管理対象デバイス認証は、信頼評価の一環としてデバイス情報の正当性を示す強力な証拠を提供する仕組みです。Secure EnclaveとAppleの認証サーバーを駆使して暗号技術に基づく宣言を作成し、企業リソースにアクセスするデバイスの正当性を事前に確認できます。

プラットフォームSSOは、タッチIDを使ったパスワードレスの認証機能です。使用する認証情報は、Secure Enclaveに格納されているハードウェアに紐付いた鍵をベースとしており、フィッシング耐性に優れています。従業員は、一度ログインするだけで様々な企業アプリにスムーズにアクセスできるため、パスワードを逐一入力する煩雑さから解放されます。

IT部門の業務とプロセスの多くを自動化

Forrester社によると、単純なパスワードリセットの作業には1件あたり70ドルものコストが発生しており、平均的な大企業の場合、パスワード関連の手作業のコストは年間100万ドル超にのぼるといいます。

自動化という概念は非常に大きなものです。巨大な袋に次々とモノを詰め込んでいくように、その気になれば何でも自動化の対象にできてしまいます。そこで、自動化と時間がどのような関係にあるかを把握することが非常に重要です。自動化と時間というと、「作業を自動化した場合にIT部門の時間をどれだけ節約できるか」という論点が思い浮かぶかもしれません。これも非常に重要ではありますが、「自動化を成し遂げるために必要な知識を習得するまでにどれほどの時間がかかるか」も忘れてはなりません。

大企業では膨大な量のデバイス、テクノロジー、ソリューションを運用しているため、ITチームの時間は非常に貴重です。自動化の効用は、単に業務効率が高まるだけではありません。むしろ、IT部門が目先の問題に対応する事態が少なくなり、戦略的な業務に取り組める時間が増えるという点が重要なのです。ここで、自動化の具体的な効用をいくつか見てみましょう。

一貫したポリシー適用を実現

Mac、iPhone、iPadのいずれにも一貫してポリシーを適用できます。適用漏れの心配もありません。

ヒューマンエラーを削減

業務フローを標準化し、手作業によるリスクを排除します。

人員を増やさずに拡張性を確保

会社の規模が拡大し、管理やセキュリティの需要が高まっても対応できます。

優れた自動化フレームワークでは、デバイスの導入、ポリシーの適用、ソフトウェアのパッチ、パスワードのリセットなど、何度も繰り返し発生する作業を自動化できます。しかし、そのさらに先を行くのがAppleです。Appleの宣言型デバイス管理を使うと、デバイスがサーバーの命令を待つことなく自律的にポリシーを適用したり、自らの状態の変化をリアルタイムで報告したりできるようになります。そのため、サポートチケットが少なくなる、迅速にコンプライアンスを確保できる、Appleデバイスが増えても手作業による介入が少なくなるなどの効果が期待できます。

Jamfが選ばれる理由

Jamfの高度な自動化ワークフローは、ポリシーベースの管理、スマートグループ、APIを使ったプロセスにより手作業による構成を根絶し、ミスのない一貫した導入とコンプライアンス監視を実現します。

ゼロトラストによりアクセスポリシーを強化

現代の脅威は日々進化を続けています。攻撃者の間では、脅威の巧妙化、ペイロードの最大化、検出の回避などを目的としてAIをはじめとする高度なテクノロジーの利用が進んでいます。

正しく認識しておきたいのは、攻撃者はあらゆるプラットフォームを標的とするという点です。あらゆる攻撃に耐えうるOSなど存在しません。そこで、現代のデバイス管理では、エンドポイントを最新の状態に保ち、多層防御戦略を実践することが非常に重要になります。そのために必要なのが、あらゆるデバイス、ユーザ、要求を、信頼できることが証明されるまでは信頼できないものとして扱うというアプローチです。これがゼロトラストです。ゼロトラストは、製品ではなくフレームワークであり、Appleのアーキテクチャには、ゼロトラストがあらかじめ組み込まれています。

管理対象デバイス認証は、デバイスが企業リソースにアクセスする前に、暗号化技術を使ってデバイスの正当性を証明する仕組みです。プラットフォームSSOは、ユーザIDをSecure Enclaveに格納されているハードウェアに紐付いた鍵と結びつけるもので、認証情報の窃取防止に大きな効果を発揮します。宣言型デバイス管理は、デバイスがオンラインであるかどうかを問わず、セキュリティポリシーを自律的に適用できる状態を実現します。ここに挙げた3つのすべてが、デバイスを当然には信頼せず、信頼できるかどうかを常に検証していくための基盤となります。

大企業がインシデント対応のスピードを上げつつアジリティを高めていくためには、**以下に従って自社のデバイスの管理、ID、セキュリティを一元化する必要があります。**

Jamfが選ばれる理由

アリング対策の負担は今や非常に大きくなっています。また、AI生成のマルウェアも、これまでにないほど検知が困難です。

AppleのSecure Enclaveと管理対象デバイス認証では、ハードウェアレベルでデバイスのIDを検証できます。さらに、Jamfのソリューションを使えばリスクベースのアクセスポリシー、デバイス コンプライアンス検証、条件付きアクセスによりゼロトラストのネットワーク制御が実現し、エンドポイントの機密データを保護できます。

ゼロトラストネットワークアクセス（ZTNA）の導入

- コンテキストを加味したアクセスポリシーを適用し、要求ごとにデバイスの状態や認証情報の健全性を検証しましょう。
- 頻度の高いデバイス内攻撃やネットワーク内攻撃を予防できるよう、
  マイクロトンネルを使ってセッションを分離しましょう。
- macOS、iOS、iPadOS、Android、Windowsのすべてを保護しましょう。

ベースラインの適用とベンチマークに対するコンプライアンスの確保

- 各種規制や独自のコンプライアンス要件に応じて、**ベースラインとなるセキュリティ構成を自動で導入しましょう。**
- コンプライアンス検証のためのベンチマークを活用し、**会社やデバイスの状態を監査**しましょう。
- **脅威ハンティング、インシデント対応、ITサポートにAI/MLを活用しましょう。**
- 既知の脅威を先回りして検出しつつ、未知の脅威を**早期に発見し、抑止できるようにしましょう。**
- セキュリティギャップの解消を進めながら、**応答時間の短縮と修復のスピードアップに取り組みましょう。**
- 各種テクノロジーの検討、構成案の検証、修復の迅速化には、**Jamf AIアシスタント**を利用しましょう。

デバイスのライフサイクル全体を可視化し、対応の質を高める

セキュリティに関する議論は、アクティブ脅威の話が中心になることが少なくありません。しかし、インベントリへの掲載漏れ、未使用ソフトウェアライセンスの放置、適切なデータワイプを実施していないデバイスなども、多額の損失につながるおそれがあります。最大のリスクは細部に潜んでいるのです。

IT部門もセキュリティ部門も、攻撃者に関する問題に集中するあまり、デバイスの他の側面に対する可視性を確保する重要性を忘れてしまいがちです。

可視性とは、単にネットワークで何が起こっているかを把握すれば良いわけではありません。組織内のデバイスに何がインストールされているか、ライセンスやコンプライアンス状況がどうなっているか、どのデバイスが廃棄できる状態にあるかなど、様々な要素を一覧できる必要があります。そのために重要なのが、エンドポイントのコンテキストデータです。最新のデバイスインベントリやソフトウェアのスプロール状況などのデータがあれば、エンドポイントの健全性の全容をライフサイクル全体にわたって把握できるからです。Appleデバイスの場合、自らの状態の変化を自律的に報告する「宣言型デバイス管理」が使えます。そのため、OSのバージョンは何か、セキュリティ状態はどうなっているか、何のアプリがインストールされているかといった事項をわざわざIT部門に問い合わせなくても、インベントリを常に最新の状態に保つことができます。

可視性が十分でない場合の影響は以下のとおりです。

未使用のソフトウェアライセンス

ソフトウェアライセンスの使用状況を正確に把握していないと、ソフトウェアライセンスの50%が未使用のまま放置され、**1か月あたり約4,500万ドルもの無駄な支出**が発生するおそれがあります。

デバイスの廃棄の問題

近年発生したデータ侵害の10～20%は、電子機器やデバイスを適切に廃棄しなかったことが原因で発生しています。現在使用中のエンドポイントに比べると、対策がおろそかになりがちな盲点です。

コンプライアンス関連のギャップ

組織が使わなくなったデバイスを回収して別の従業員に再支給している場合には、デバイスを正しく管理していないと、データが他人に漏えいするおそれがあります（内部関係者による脅威が代表例です）。例えば、人事担当役員が使っていたノートPCを、営業部門で新たに採用した人員に再利用したとします。そのデバイスに個人識別情報が残っていると、新しいユーザが閲覧できる事態も起こりかねません。これは、業界の規制の状況によっては、GDPRをはじめとするプライバシー関連の法規に違反する結果となります。

Apple製品には、このような管理業務を簡単に進められる機能が備わっています。例えば、デバイスは自らの状態を自律的に報告したり、ポリシーを適用したりすることができます。さらに、Apple Business Managerと組織内の管理ソリューションを統合しておけば、データをワイプして再利用する際に再登録を自動で実行することもできます。これなら手作業がないため、セキュリティギャップも発生しません。

Jamfが選ばれる理由

Jamfのソリューションでは、Apple シリコン搭載のMacデバイスを廃棄に先立って「完全なセキュリティ」モードで運用しておくことができます。そのため、デバイスを紛失したり、適切でない方法で廃棄したりした場合でも、FileVaultで暗号化されているデータが確実に保護されます。近年のデータ侵害の10～20%が電子機器廃棄物を原因として発生していることを考えると、ハードウェアに基づいてセキュアブートの状態を確認できるようにしておくことが、セキュリティギャップを解消し、事態が手遅れになる前に対応するうえで役立ちます。

様々な業界で効果を発揮

デバイス管理の成否を測る指標は、ITバックエンドの数値ではありません。従業員やお客様が改善を実感できたかどうかです。以下では、デバイスの導入によって作業フローの効率化に成功した事例をいくつかご紹介します。

医療業界

患者の医療記録が「退院」に変わった時点で、ベッドの横に置かれたiPadが患者データを自動的に全消去し、次の患者が使っても問題ない状態を整えられます。その間、スタッフがデバイスを操作する必要は一切ありません。また、複数名でiPhoneを共有することもできます。シフトを終え、次のスタッフがiPhoneを使うときには、役割や認証情報に基づいてアプリにそのスタッフの設定が自動で適用されます。

航空業界

iPadを電子フライトバッグとして使えば、パイロットが重たいチェックリストや航空図、マニュアルを持ち運ばなくて済むようになります。また、メカニックや搭乗口係員、キャビンアテンダントが日々どのデバイスを割り当てられても、必要なアプリが自動で揃います。

小売業界

iPadをシングルAppモードに固定して、セルフサービスキオスクとして運用すれば、不適切なコンテンツが表示されることもなければ、トラブルシューティングも、日々の終わりのリセット操作も必要ありません。また、ログインしたユーザに基づいて必要な構成を自動で適用できるので、共有デバイスを使ってPOSシステム、在庫管理システム、顧客情報システムをシームレスに行き来できます。

製造業界

現場作業員は、ネットワークの認証情報を支給されていなかったり、モバイルテクノロジーに慣れていなかったりすることが少なくありません。そこで、セキュア充電ロッカーでティア0サポートを提供します。iPadが使用中に動かなくなったら、充電ロッカーに戻すだけでデバイスが自動的にリセットされ、必要な設定が完了します。これで、問題を修復したのと同じ効果を発揮します。従業員は代わりのiPadを取って作業に戻れば良いので、IT部門に問い合わせたり、実地のサポートを依頼したりする必要がありません。

金融業界

アジャスター、融資担当者、フィールドアドバイザーなど、金融業界で働く人にとっては、共有デバイスであっても機密データに即座にアクセスできることが必須の条件です。さらに、そのようなアクセスが必要になるのは、コンプライアンス要件の厳しい予期せぬ場所であることも多々あります。iPadなら、その日に手に取ったデバイスがどれであれ、認証情報を1回入力するだけで、請求アプリ、写真ツール、顧客記録のすべてに即座にアクセスできます。勤務を終えた後の認証情報の削除もわずか数秒で完了し、次のユーザがすぐに使える状態になります。もちろん、コンプライアンス目的の監査証跡はしっかり残ります。

終わりに

Windowsデバイスが中心の環境にAppleデバイスを統合しても、必ずしも大きな変化や追加の業務負担を強いられるわけではありません。必要なのは、業務フローの効率化・自動化・標準化です。既存のツールと統合できるAppleネイティブのソリューションを採用し、そこにデバイスのライフサイクル管理、ID、セキュリティのすべてを一元化していけば、IT部門の運用習熟度は確実に高まっていきます。また、このようなアプローチでは、手作業の削減、一貫性の向上、プロアクティブな運用の実現といった効果も期待できます。それがひいては、デスクトップPC、モバイルデバイスを問わずクロスプラットフォームの可用性、コンプライアンス、制御を維持しつつ、自社のペースで最新テクノロジーの導入を進めていくことにつながっていきます。

まとめ

- Apple製品の統合で重要なのは効率性であり、人員の頭数ではありません。
- ゼロタッチ導入を使うと、何時間もかかる設定作業がわずか数秒で完了できるので、ダウンタイムの削減につながります。
- 管理、ID、セキュリティを一元化すれば、サイロ化を解消できます。
- 自動化は、ポリシーの適用を標準化できるため、広くヒューマンエラーを減らす効果があります。
- ゼロトラストネットワークアクセスは、複雑さを増すことなくセキュリティを強化できます。
- ライフサイクル全体にわたる可視化を実現すれば、アップタイム維持、コンプライアンス確保、無駄なソフトウェア支出の削減に役立ちます。
- 宣言型デバイス管理を使えば、オフラインであってもデバイスのコンプライアンス状態を維持できます。

トライアルはこちらから

トライアルに申し込む