jamf

ビジネスの成長を支える Macの管理とセキュリティ

デジタル時代の企業変革において、生産性とセキュリティを両立する、次世代のテクノロジー選択が不可欠です。調査によると、デバイスを自由に選択できる環境では、従業員の満足度、業務効率、そして仕事への意欲 — すべての指標が向上を示しています。そして、ビジネス領域でのMacの利活用がかつてない広がりを見せています。

IT部門にとって、この変化はチャンスとチャレンジの両面をもたらします。ユーザの選択を尊重しながら、円滑な管理と万全なセキュリティをいかにして実現させるか。

macOSには堅牢なセキュリティ機能が標準搭載されていますが、企業で活用するにはさらに一歩進んだ取り組みが不可欠です。管理、コンプライアンス、リスク対策 — これら3つの要素を統合した戦略的アプローチが、ビジネスの安全性を確保します。デバイス管理の規模が数十台から数千台へと拡大する中、IT部門は、セキュリティ対策を強化しながら、いかに生産性の高いユーザ体験を維持するかという課題に直面しています。現在のセキュリティ管理において、大きな課題の一つが、macOS環境に最適化されていないツールに依存せざるを得ない状況です。効果的な監視や迅速な対応を実現する上で、大きな障壁となっています。適切な戦略の導入により、業務の流れを合理化し、生産性を高め、セキュリティリスクの低減を実現できます。セキュリティ部門は、Mac環境全体を正確に把握し、先手を打った効果的な対策を実施できるようになります。

jamf

本ガイドでは、拡大するMac環境の管理とセキュリティ対策において、IT部門が必要とする戦略的フレームワークをご紹介します

Mac管理の基礎 - シスムーズな導入・設定・管理のための重要指針

高度なセキュリティ戦略 - macOSネイティブ機能を補完し、進化するリスクに対処

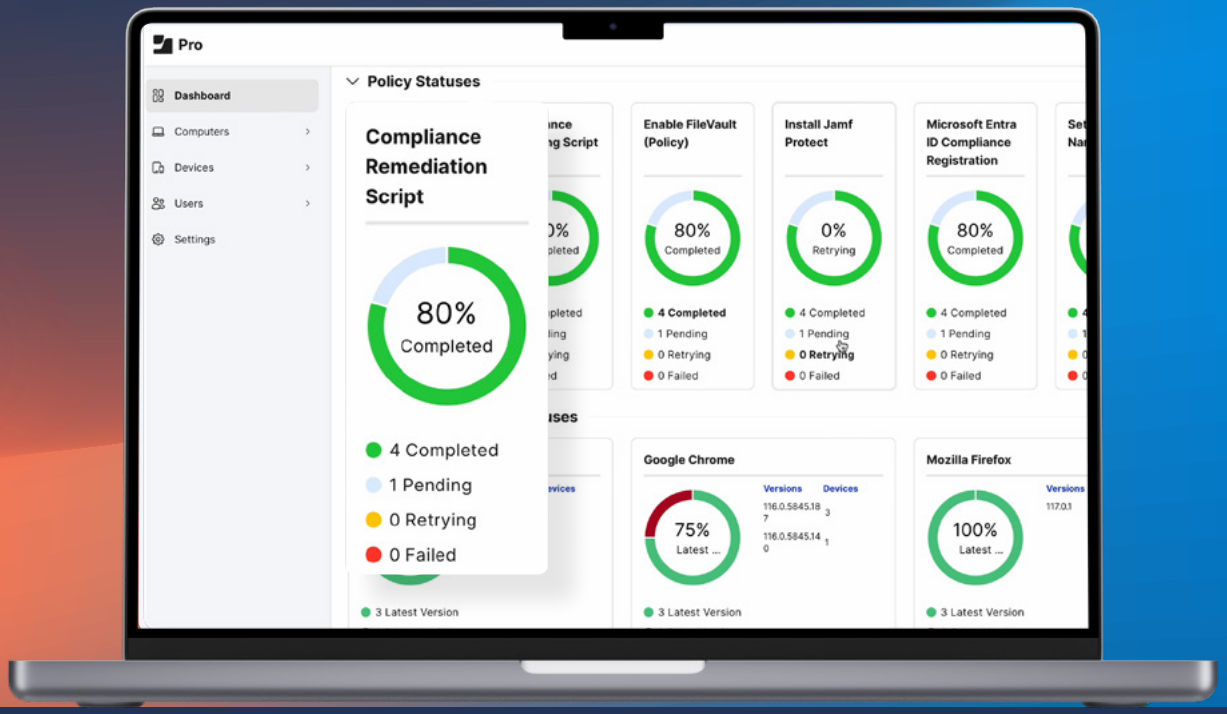
ライフサイクル管理 - ゼロタッチ導入から安全なオフボーディングまで、Macの体験価値を最適化

インフラ統合戦略 - Windows環境と企業ITインフラとの円滑な連携

企業向けセキュリティのベストプラクティス - Macに最適化されたツールで実現する企業のデータ、デバイス、ユーザの保護対策

従来のWindows主体の環境にMacを新規導入する場合でも、既存のApple環境を拡張する場合でも、いずれのケースにおいても本ガイドが成功への道筋をご提案します。運用リスクを抑えながら、IT効率の向上、セキュリティ体制の強化、そしてMac投資価値の最大化を実現するための戦略的アプローチをご説明します。

最新のMac管理：
基本方針とテクノロジー



ビジネス環境で進化するMac管理

現代のビジネス環境において、Macは優れたセキュリティや卓越したパフォーマンス、高く評価されるユーザ体験で、企業の競争力を支えています。かつてクリエイティブ専門職向けのニッチな製品とされていたMacは、現在では企業のITインフラの重要な存在となっています。Macの普及に伴い、企業のIT部門は、統合管理とセキュリティの最適化を目指す、より高度な管理戦略へと舵を切り、Mac管理の効率化と自動化を実現するモバイルデバイス管理（MDM）ソリューションへと移行していきました。

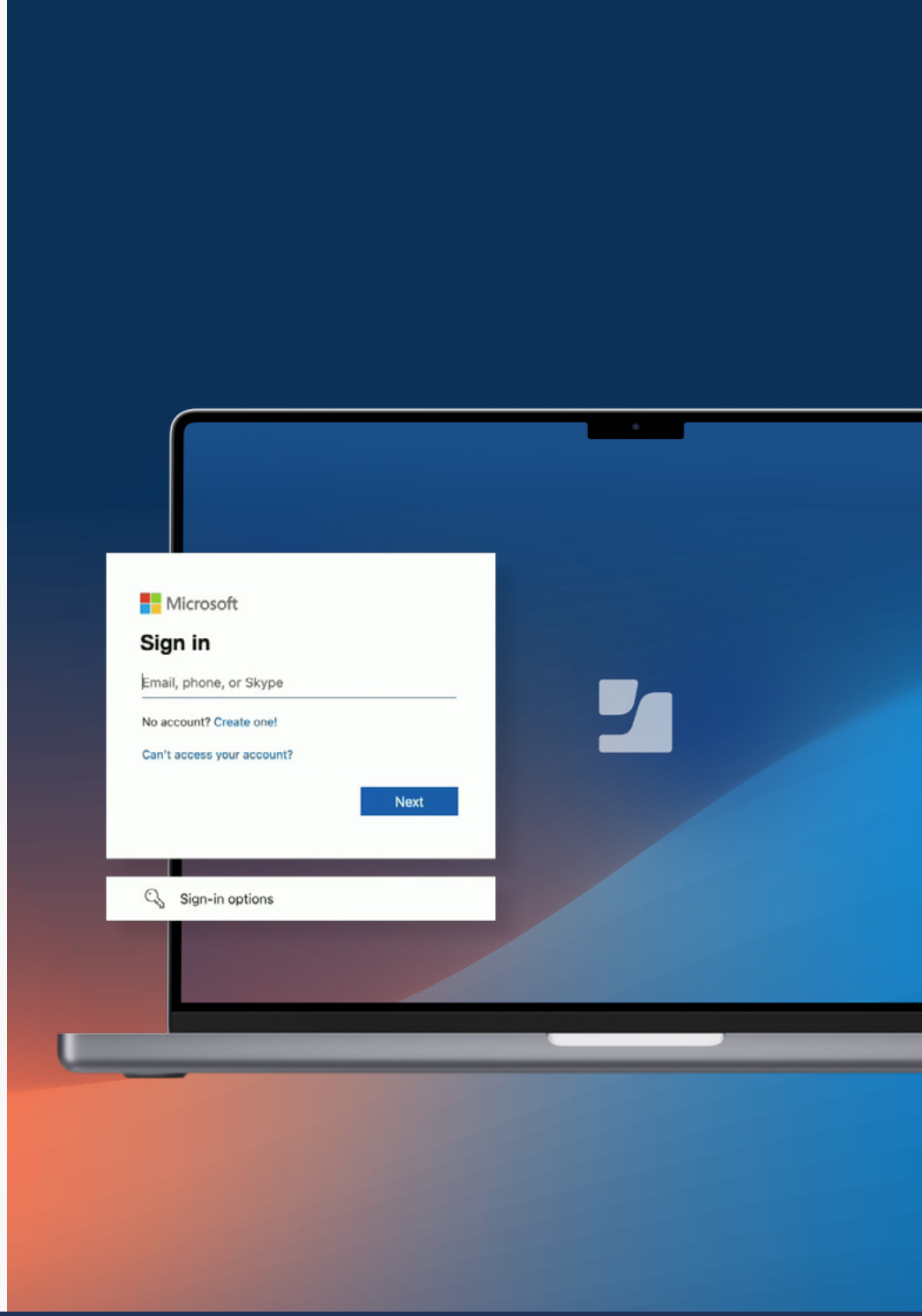
しかし、Mac導入規模の拡大に伴い、従来型MDMソリューションの限界に直面することとなりました。主にWindows環境向けに開発された従来のソリューションでは、進化を続けるAppleエコシステムに完全に適応することは困難です。macOSアップデートへのスムーズな対応、セキュリティ機能や新機能の同日サポート、そしてAppleネイティブなワークフローとの互換性 ー これらを実現するには、Apple環境に特化したソリューションでのみ実現可能な、的確なアプローチが必要となります。

これらの問題点は、IT部門が直面している本質的な課題を浮き彫りにしています。求められているのは、スムーズな統合と効率的なスケーラビリティを実現し、ユーザ体験を妥協することなくセキュリティを強化できる、最新の管理ソリューションへの移行です。IT専門家の多くがMicrosoft環境における従来型PC管理に精通する一方で、macOSエコシステムにおいては、生産性の向上とセキュリティの最適化を両立する、Mac特有のアプローチが効果的です。組織のIT戦略がWindows中心の枠組みを超えて進化する中、業務効率の向上と従業員満足度の改善をもたらす重要な要素として、Macの存在価値が高まっています。しかし、こうしたメリットを十分に引き出すためには、変化するビジネスIT環境に対応できる、プロアクティブかつスケーラブルなApple独自の管理戦略をIT部門が導入することが不可欠です。

IT部門には、以下の重要なビジネス目標に即した、効果的なMac管理の実現が求められます：

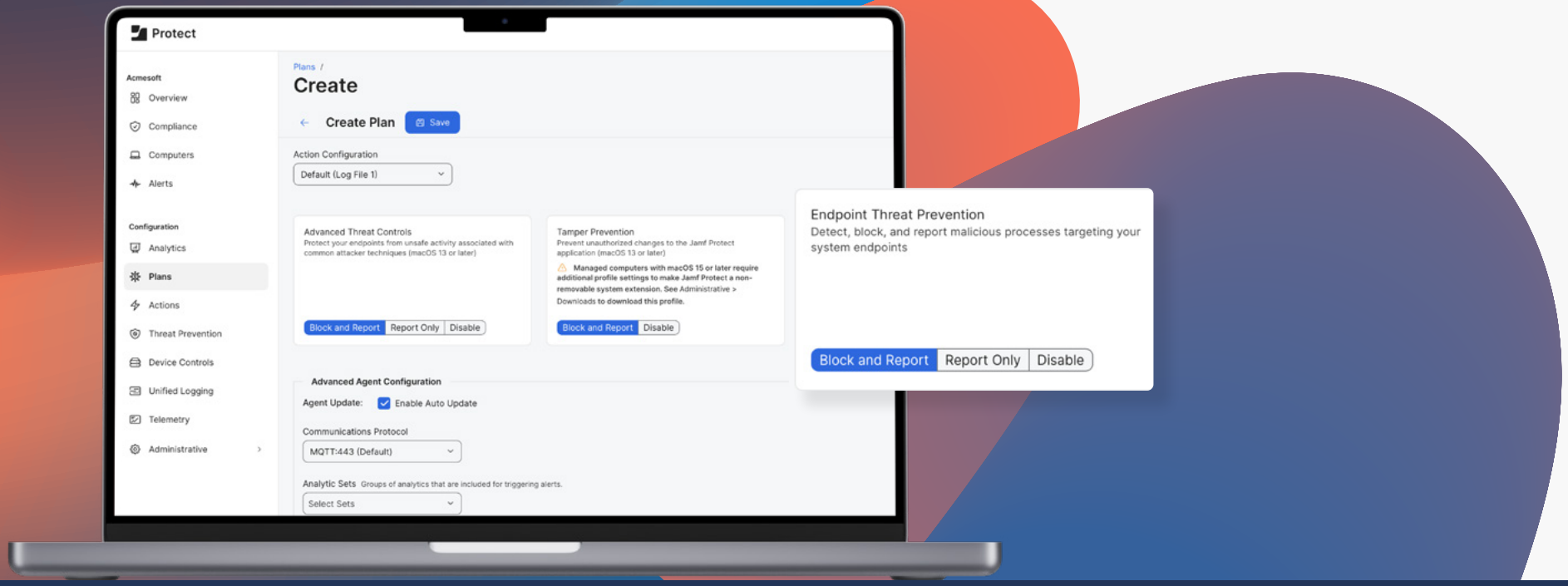
- **生産性の向上：**デバイスのセットアップ、アップデート、サポートの効率化によって、業務中断時間を削減し、従業員の効率的な業務遂行を実現します。
- **リスクの低減：**エンドポイントの常時監視、セキュリティポリシーに基づくコンプライアンスの確保、修復プロセスの自動化を通じて、企業が直面する脅威を最小限に抑制します。

これらの点を考慮した最新のAppleデバイス管理戦略は、AppleのMDMとセキュリティフレームワークを軸に展開し、大規模なMacデバイスの導入、セキュリティ管理、維持のための構造的なアプローチを提供します。



Mac管理の基本：**企業向けの 戦略的アプローチ**

次のような基本原則を指針とすることで、ユーザが期待する操作性を維持し、ユーザのプライバシーを損なうことなく企業に求められる高度なセキュリティ基準を満たすことが可能となり、Macのシームレスな導入・構成・管理を実現できます。



ゼロタッチ導入：
自動化で実現する大規模運用

最適化されたオンボーディングプロセスは、効率性やセキュリティ、ユーザ満足度を高める上で極めて重要です。ゼロタッチ導入により、デバイスの開封前からMacの構成とプロビジョニングを実施でき、手動でのセットアップが不要になるため、IT部門の作業負担を軽減することができます。実現のための主要な要素：

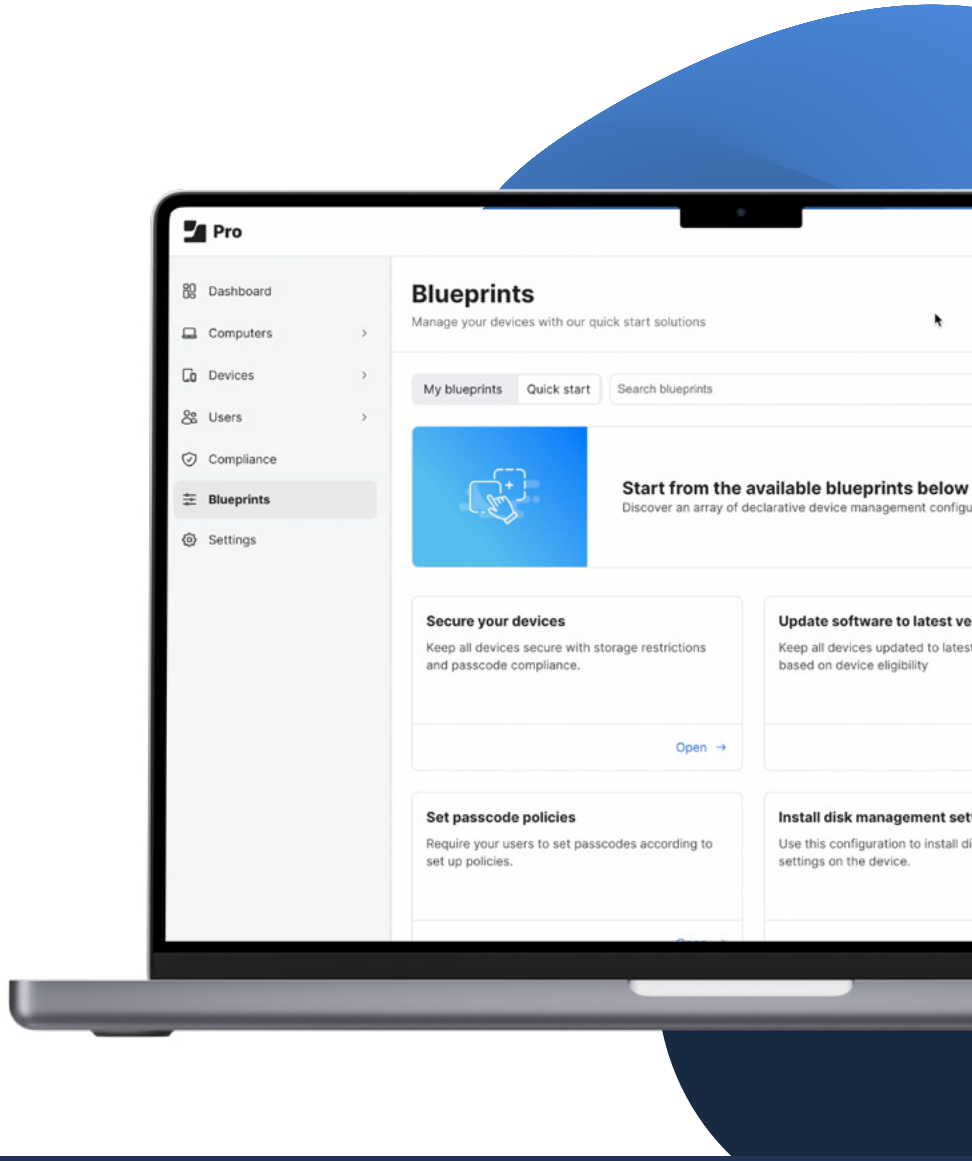
- **登録とカスタマイズの自動化**
- **アカウントプロビジョニングと管理**
- **ジャストインタイムのmacOSオンボーディング**

自動化によって、IT部門は、従業員のオンボーディングプロセスを大幅に効率化し、デバイスの初回起動時からセキュリティを強化することが可能になるため、初日から生産性を最大限に発揮できるスムーズなオンボーディング体験を提供できます。また、運用管理の工数を削減することで、本来注力すべき業務に人的リソースを確保できます。

設定と構成の一元化：
組織全体で一貫性を維持

企業が保有する多数のMacデバイスのセキュリティとコンプライアンスを確保するには、ポリシーに基づいた一元管理の実現が必要不可欠です。IT部門は、ビジネスニーズを担保しながら、一貫性を維持しなければなりません。主要な戦略として：

- **ブループリント**
- **スマートグループ**
- **遠隔セキュリティコマンドと制限機能**
- **Apple Business Manager（ABM）との統合**



アプリ管理とパッチ管理：セキュリティリスクを低減し、業務効率を向上

ソフトウェアの展開とパッチ管理の標準化により、ソフトウェアのセキュリティ脆弱性を減らし、ダウンタイムを最小に抑えたまま、ユーザの生産性を向上させる新機能を提供することができます。アプリの可用性を広げる機能：

- **自動化されたアプリ展開**
- **確実なパッチ適用の実現**
- **App カタログ**
- **オンデマンドのコンテンツおよびデバイスセキュリティ**

企業レベルのセキュリティとコンプライアンス：企業の大切な情報資産を守る

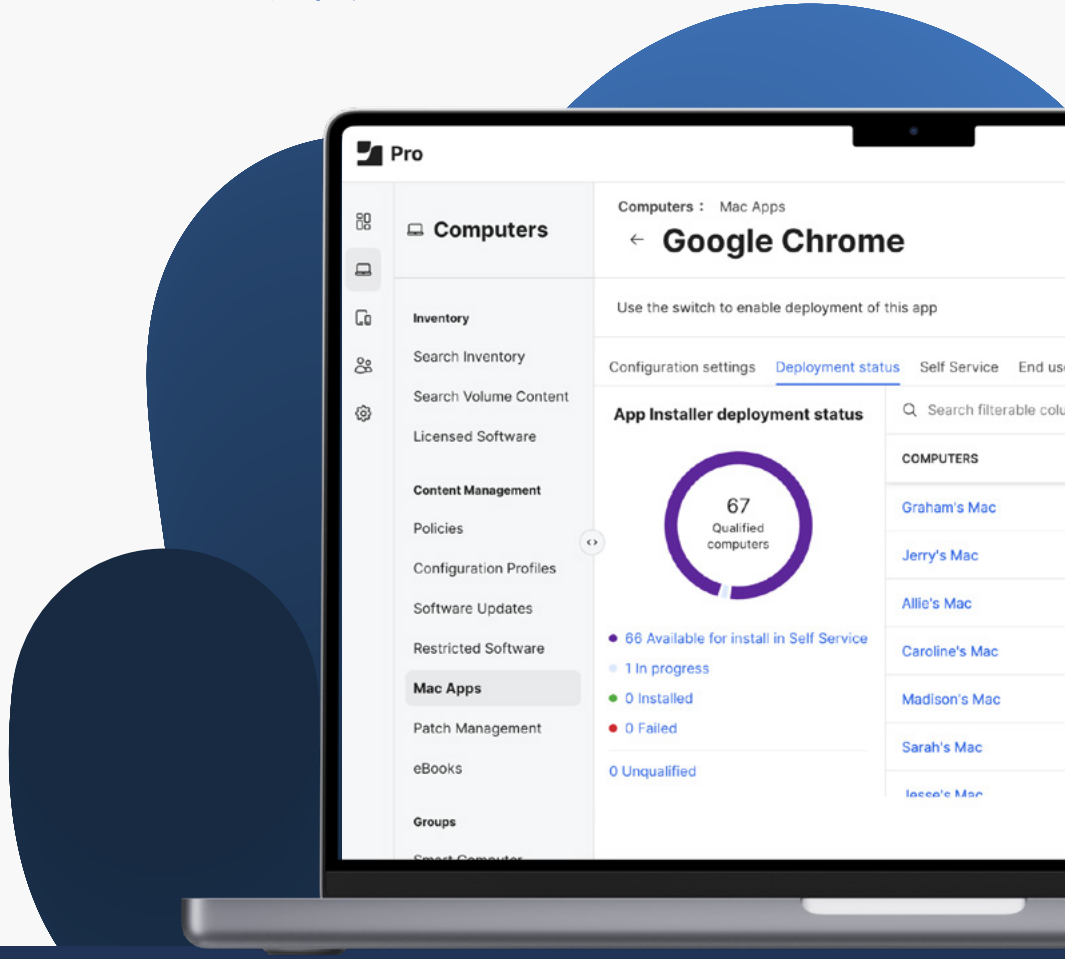
macOSは優れたセキュリティとプライバシー機能を標準搭載していますが、企業のセキュリティ基準や各業界特有のコンプライアンス要件を満たすためには、さらなるセキュリティ対策が不可欠です。最新のMacセキュリティ戦略には以下のような要素が含まれます：

- **エンドポイント保護とコンプライアンス遵守**
- **ID・アクセス管理（IAM）**
- **脅威検知とインシデント対応**
- **ネットワークベースの脅威対策**
- **ゼロトラストネットワークアクセス（ZTNA）**

運用状況の把握とレポーティング

Macの導入から廃棄まで、ライフサイクル全体を一元管理することで、長期的なコスト削減と運用効率の向上を実現します。また、デバイスの紛失・盗難による機密情報漏洩のリスクも最小限に抑制します。実現のための主要な要素としては：

- **インベントリ管理**
- **アプリレポート**
- **スマートターゲティング**



企業の競争力の向上：**IT部門による改革推進の必要性**

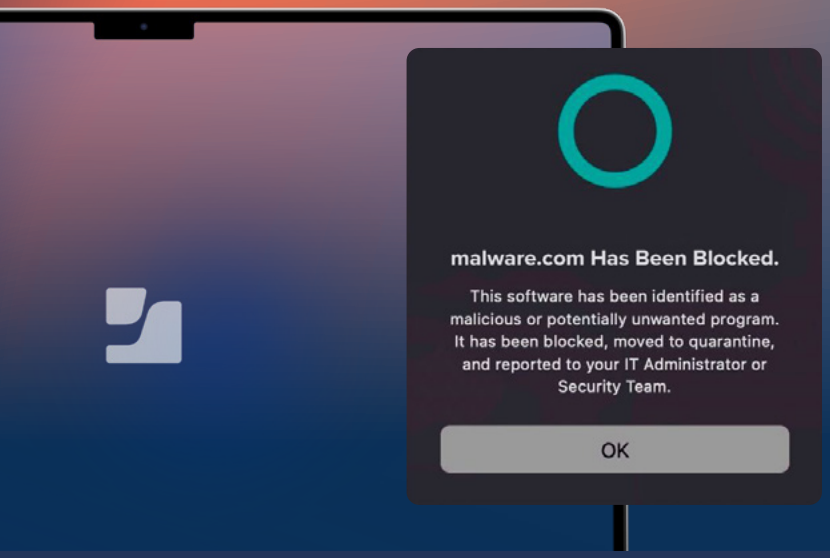
企業でのMac活用が加速する今こそ、IT部門が先導的な役割を担い、次世代のデバイス管理体制を確立する絶好のタイミングです。Appleネイティブな、プロアクティブで自動化されたアプローチを導入することで、IT部門は次のような効果を得られます：

- シンプルな管理でセキュリティとコンプライアンスを強化
- Macならではのパフォーマンスを活かして、ユーザの業務効率を向上
- 運用の自動化と効率化により、IT部門の負担を軽減

こうしたMac管理の基本要素を導入することで、IT部門主導の戦略的なMac活用が可能となり、以下のような効果が期待できます：

- 業務効率とセキュリティを同時に向上し、ビジネス価値を創出
- 従来型の環境と比較して、システム全体の総保有コスト（TCO）を大幅に削減
- 大規模導入におけるスケールメリットを活かし、投資効果（ROI）を最大化

高度なセキュリティ強化戦略：**macOSの基本機能に企業向け対策を追加し、リスクを最小化**



企業のMac管理における セキュリティの重要性

企業におけるMacの普及拡大に伴い、リモートワークや働き方の多様化に起因する新たなセキュリティリスクへの対応が求められています。macOSの堅牢なセキュリティ機能は高く評価されていますが、企業のMacを標的とする攻撃が深刻化する中、基本的なセキュリティ機能だけでは企業データの保護として十分ではありません。効果的なセキュリティ確保のため、以下の対策を総合的に実施する必要があります：

- **エンドポイント保護**
- **ID・アクセス管理**
- **セキュリティベースラインの確立**
- **常時監視とレポーティング**
- **コンプライアンスの徹底**

パッチ適用の自動化、ゼロトラストモデルの採用、リアルタイムの脅威検知を通じて、Macのプロアクティブなセキュリティ対策を実現。これにより、セキュリティリスクの最小化、規制要件への対応、企業データの保護を実現します。適切に定義されたセキュリティ戦略の構築は、もはやIT部門だけの課題ではありません。常に進化するサイバー脅威への対応力を高め、ビジネスの継続性を強化する基盤を構築するために極めて重要な意味を持ちます。

デバイスライフサイクル管理：導入から運用、廃棄まで

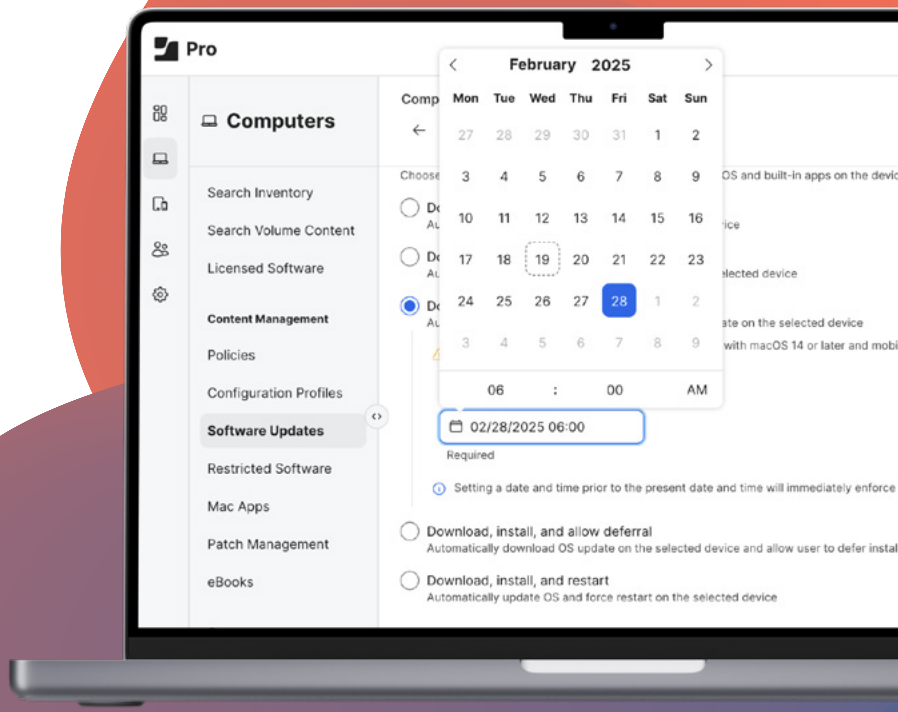
企業の情報セキュリティ対策において、業務に利用され企業リソースに接続する全てのデバイスについて、組織の資産に対するリスクという観点から、同等の扱いが求められます。ここで重要となるのは、デバイスのライフサイクル全体を通じた一貫した管理です。デバイスの調達から初期設定、構成管理、コンプライアンス監視、パッチ管理、そして廃棄処理に至るまで、セキュリティの死角を作らない継続的な管理が不可欠です。一元管理による具体的なメリットとしては以下が挙げられます：

- **組織全体にわたるセキュリティの強化**
- **統一された管理基準の維持**
- **安全な業務フローの確立**
- **デバイスの常時監視と認証**

基準となるセキュリティ状態の確立

企業における適正な運用レベルの範囲を明確に定義することで、信頼できる判断基準を確立できます。さらに、規制要件の厳しい業界のIT部門責任者には、機密データを扱うデバイスとその利用者について、データ保護や業務プロセスに関する法令要件への確実な準拠が求められ、コンプライアンス違反を防ぐための適切な管理が不可欠です。コンプライアンス対応を支える重要機能：

- **業界標準・フレームワークへの適合**
- **監査対応のための文書化**
- **リアルタイム通知**
- **ポリシーの確実な適用**



最新技術による
高度なセキュリティ対策

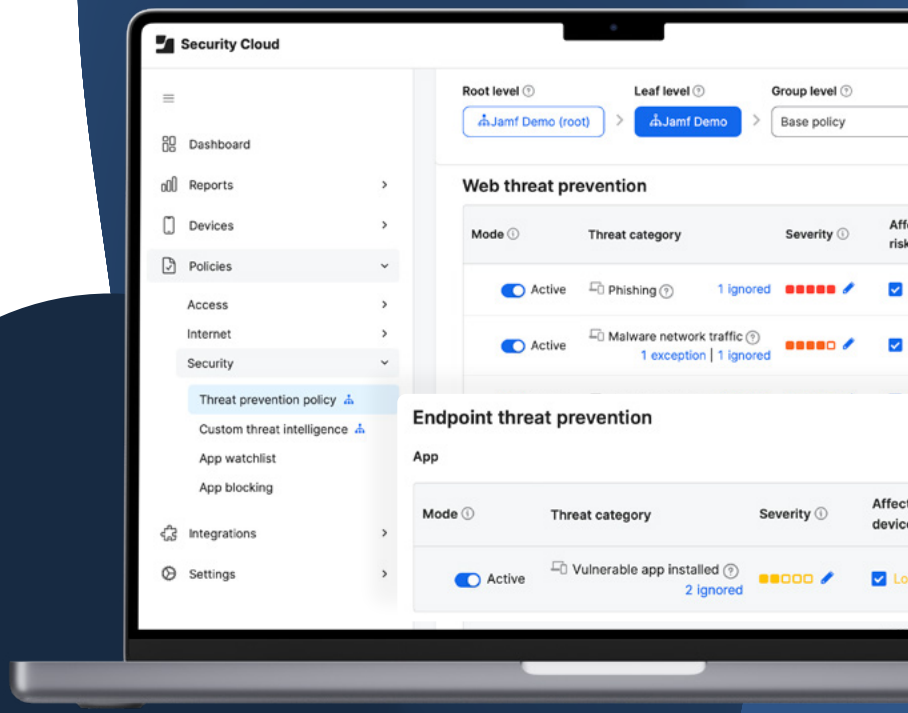
悪意あるサイバー攻撃者はAIを活用して攻撃手法を日々進化させており、従来のエンドポイントセキュリティでは検知や防御が追いつかない新たな脅威が出現しています。最新の脅威に対する予防と対策には、機械学習（ML）などの先進技術の活用が不可欠です。これにより、企業は新たな脅威に対して常に先手を打つことが可能になります。巧妙化する脅威に対して、AI技術を活用することで、IT部門は次のような形で素早く効果的な対策を実現できます：

- **ゼロデイ脅威の早期発見**
- **ネットワーク経由の攻撃をブロック**
- **組織固有のリスク状況に応じてセキュリティ設定を最適化**
- **大規模なテレメトリ分析**

信頼を前提としない対策で
攻撃リスクをゼロに

セキュリティ対策のほんの小さな綻びが、致命的な情報漏洩事故につながりかねないということを、IT部門は認識しています。リスクが高まる状況下では、すべてのアクセス要求において、ユーザ認証情報とデバイスが基準となるセキュリティ水準を満たしているかを、その都度確実に検証することが重要です。ゼロトラストネットワークアクセス（ZTNA）が強固なセキュリティ態勢を維持する主な機能：

- **エンドポイントの健全性を確認**
- **ネットワーク経由の脅威を阻止**
- **通信の分離と暗号化**
- **自動修復ワークフロー**



コンプライアンス遵守の徹底：確かな安全性を、すべてのITインフラへ

業界規制・組織基準への準拠は、企業のセキュリティガバナンスの要となります。デバイス、データ、ユーザ、業務プロセスに至るまで、体系化されたセキュリティフレームワークに基づく統合的な防御を実現することにより、企業は最適化されたセキュリティ体制を確立し、ビジネスの信頼性を確保します。エンドポイントの適切な構成とセキュリティ制御の有効性を実証する機能：

- **構成の堅牢化**
- **セキュリティ分析**
- **ベースラインの設定**
- **監査レポート**

緊密な統合から生まれるソリューションの強化

企業の意思決定には、市場動向や社内の状況など、様々な要因が関係します。セキュリティ対策も同様です。企業が直面する多岐にわたる脅威に対して、単一のソリューションでは、その性能がいかに優れていても十分とは言えません。OSの機能を活用しつつ確かな防御を実現するには、複合的な防御戦略が求められます。その企業特有の要件を満たすために、さらなるソリューションの追加が必要となることもあります。ソリューション統合が企業にもたらす重要なメリット：

- **脅威分析の一元化**
- **脆弱性修復の自動化**
- **条件付きアクセスの実装**
- **運用フローの最適化**

迅速なインシデント対応 + 積極的な脅威ハンティング = リスクの最小化

セキュリティ対策に絶対はありません。どれほど強固な防御でも、脅威が侵入する可能性はあります。このような局面では、対応スピードが、事態の収束となるかデータ漏洩へ発展するかを決定づける重要な分岐点となります。インシデント対応と脅威ハンティングを統合したセキュリティ戦略の展開により、既知・未知双方の脅威に対する包括的な防御体制を確立します。従来型のエンドポイントセキュリティでは対応が困難な脅威に対しても、効果的な検知・対応を実現します。迅速な対応と効果的な探索を実現する戦略的アプローチ：

- **セキュアなベースラインの確立**
- **安全なテレメトリデータ共有**
- **トリアージとレスポンスの自動化**
- **AI/MLによる脅威分析**

セキュリティ意識の向上と実務スキルの強化

個々のセキュリティコントロールやシステム構成、ポリシー設定がパズルのピースのように合わさることで、総合的なセキュリティ体制が構成されます。それがどのようなパズルかは、各企業によって異なり、個々のセキュリティコントロールは、組織特有の要件やリスク評価のニーズに応じてきめ細かくカスタマイズされます。

防御の重層化において不可欠な要素の一つにエンドユーザ トレーニングがあります。これは、技術的なセキュリティ対策ではなく管理的施策に分類されますが、包括的な防御体制の構築において極めて重要な役割を果たします。従来、ユーザは一連のセキュリティ施策における脆弱性として認識される傾向にありましたが、実は組織の強力な防御戦力にもなり得ます。効果的なトレーニングと意識付けによって、ユーザはより強固で回復力の高いセキュリティ環境を実現する重要な担い手となります。従来、ユーザは一連のセキュリティ施策における脆弱性として認識される傾向にありましたが、実は組織の強力な防御戦力にもなり得ます。効果的なトレーニングと意識付けによって、ユーザはより強固で回復力の高いセキュリティ環境を実現する重要な担い手となります。セキュリティ防御を脅威が突破した場合でも、迅速な対応で被害を最小限に抑えることができます。それは、戦略的なセキュリティ計画と効果的な従業員教育により、組織全体の対応力が高められているからです。従業員の適切な判断と行動が、組織の防御力を強化します。

エンドユーザを対象としたセキュリティ意識向上トレーニングによってセキュリティ文化を浸透させることができ、組織全体のセキュリティ耐性が強化されます。このような組織文化が、多くの攻撃を未然に防ぐ重要な鍵となります。ユーザの力を最大限に引き出すために、以下のトレーニングが効果的です：

- **最新の脅威情報の共有**
- **日常的なセキュリティ意識の向上**
- **データ保護の習慣化と定期的なバックアップの励行**
- **ユーザのためのセキュリティポリシーとガイドラインの確立**
- **インシデント対応の改善など、エンドユーザを解決策の一部として積極的に活用することで、セキュリティ体制を強化**

総括と
アクションプラン

Macの管理体制やセキュリティが進化するように、IT部門の在り方もまた、時代とともに変革を遂げています。常に変化し続けるリスクへの深い理解と、macOS向けに最適化されたネイティブテクノロジーの活用、この2つを効果的に融合させることが、企業が保有する多数のMacを効果的に管理・保護するための最適なソリューションを実現する鍵となります。リスクは常に変化していることを理解し、macOSをサポートするために設計されたネイティブテクノロジーとその理解を組み合わせることにより、自社のMacを管理し、セキュアに運用するための最も効果的なソリューションが開発されます。

このアプローチにより実現されるソリューションは、企業固有のニーズや要件に単に対応するだけでなく、それらを大きく超える価値を提供します。そしてその効果は、デバイス、データ、そして関係者すべての安全確保にまで広がっていきます。

Mac管理とセキュリティの重要ポイントのまとめ

総括すると、企業・組織のセキュリティ上の脆弱性を効果的に解消するためには、最新のサイバーセキュリティアプローチが必要です。具体的には、管理機能と保護機能を重層的に展開し、インフラ全体を通じてMac、ユーザ、データの包括的な保護を実現することが求められます。管理、ID、セキュリティを統合した、単一の強力な多層防御ソリューションです。

Macの管理とセキュリティの調和を実現するための重要なポイント：

- デバイスのライフサイクル全体を通じた包括的な戦略の策定
- 管理、ID、およびセキュリティソリューションを統合し、包括的な管理とセキュリティワークフローの自動化
- ゼロタッチ導入により、デバイスの導入を自動化して大規模展開を実現
- 標準規格とフレームワークに適合したセキュリティ基準の設定
- アプリ配布とパッチ管理サイクルの統一
- エンドポイントセキュリティとZTNAでデバイス上およびネットワークベースの脅威を防御
- リアルタイム監視による端末の安全性確保と既知の脅威への対策
- 自動化された管理ポリシーによるコンプライアンスの徹底
- エンドポイントデバイスから収集される特定の情報（テレメトリ）を活用したデータに基づく意思決定を行い、リスクを最小化
- AI/ML基盤の高度なテクノロジーと自動化による未知の脅威の検知と迅速なインシデント対応、および脆弱性の緩和・修復
- 包括的ソリューションの一部として、ユーザのセキュリティ意識向上トレーニングを活用