jamf

ホワイトペーパーパー

企業内でのAppleのセキュリティー懸念

この白書は、Appleデバイスが環境に導入される前に、社内チームがセキュリティーベストプラクティスに関して十分に教育を受けられるよう、一般的なセキュリティー議論に着目し、Appleプラットフォームに対して組織は何をする必要があるのか説明しています。

含まれるトピック：

- デバイス管理へのAppleのアプロ―チ
- Apple特有のセキュリティー特徴
- 新たなAppleデバイスを追加する時に考慮すべき点
- すでに持っているものを活用するために利用可能なApple統合とは何か

Apple エコシステムの構造

Appleデバイス管理にどのようにアプローチすべきか

Appleは、設計によりセキュリティーを提供し、ITチームが設定、デプロイ、管理を簡単に行うことのできるハードウェア、ソフトウェア、サービスへのアプローチが統合されたiOSとmacOSプラットフォームをデザインしました。仕事上でiPhone、iPad、Macを使う時に、従業員は一貫性のある経験を期待するのと同じように、ITはプラットフォームと従業員の両方の管理を行う時に同じような経験を期待できるべきです。

Appleにはエンタープライズプログラムがあり、展開とセキュリティーを合理化し、ユーザーに優れた 「OOBE」 (「箱から出したばかり」の状態で提供される) 体験をもたらしています。AppleのDevice Enrollment Program (DEP) と Volume Purchase Program (VPP)をモバイルデバイス管理 (MDM) と組み合わせることで、Mac、iPad、iPhone、Apple TV デバイスを一貫してまた保護下で管理できます。

多くの組織は、Apple、Microsoft、Googleデバイス全てのニーズに対応できる一つのツールを求めています。組織にとって、管理、ユーザエクスペリエンス、セキュリティーのギャップが残ります。単一の管理ツールが複数のプラットフォーム管理に利用される時、セキュリティー特徴は正しく活用されず、Apple専用の能力のマジックが失われます。

Apple構想

セキュリティーに対するAppleのアプローチをはっきりさせるには、基礎的なAppleの構想をまず理解する必要があります。

Apple管理がMicrosoftとどのように異なるか

Appleは従来のMicrosoftのエンドポイント管理とどのように異なるか

Appleを簡単に使うための鍵は、モバイルデバイス管理（MDM）として知られるビルトイン管理フレームワークにあります。MDMはITが、OS内で様々な設定を定義する設定プロファイルを構築するのを可能にします。これらのプロファイルは、Appleプッシュ通知サービス（APN）を通して送られます。APNはAppleデバイスに安定したコネクションを保つため、ITがそれを行う必要はありません。MDMは、従来のWindows管理者ならバインディングかGroup Policy Object (GPO)でなければできないと信じているような管理機能をやってのけます。

APNはセキュリティー姿勢に影響を与えるか？

APNは、iOS、watchOS、tvOS、macOSデバイスに情報を伝達するのに安全で高い効果性を持つサービスです。APNは、Appleデプロイプログラムと、リモートロックやリモートワイプといった、その他のセキュリティー特徴に重要な階層です。実際、プログラムはプロキシ接続を通して利用されることはないため、DEP、VPP、MDMといったAppleのプログラムはAPNがあるべき場所にないと作用しません。APNsなど、Appleで直接的なチャンネルを通してアクセスしなければなりません。

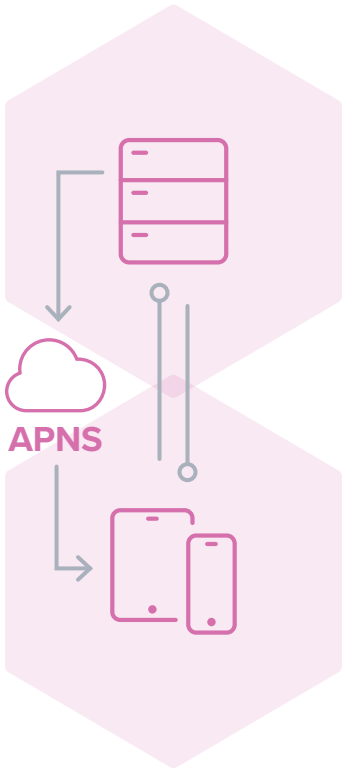
APNの補足的な利点には以下が含まれます:

- 企業が所有するAppleアセットを管理するための強化されたセキュリティー姿勢
  APNで、紛失/盗難/感染済みデバイスを通信的に遠隔でロック/ワイプすることが可能になります。.
- MDMは、ソフトウェアインストールやインベントリアップデートなど重要なコマンドの送信に関してAPNに依存しています。
- MDMの設定プロファイペイロードはmacOS「オフライン」に送信可能な一方で、この方法には、通信で管理を行うよりも、かなりの作業コストが必要です。
- APNは、MDMサーバーで自動チェックインするよう各デバイスをトリガーします。

セキュリティー課題に見える特有のテクノロジーには、多くの利点があります。
多くのGoogleまたMicrosoftサービスは同じレベルの信用を必要とし始めており、APNのような直接接続が必要です。iOS用のCiscoが提供するVOIPソリューションは、プッシュメッセージやCallkitでAPNに依存しています。APNsはセキュリティーとユーザエクスペリエンスに不可欠です。App Store、iCloud Authentication、Internet Recoveryのようなサービスは、APNなしでは十分に（全く）機能しません。お使いのポートをAppleの仕様に開けると、全てが正しく収まります。

さらに情報をお求めの場合は、Appleのウェブサイトをご覧ください：https://help.apple.com/deployment/macos/#/ior9d28751c0.

Appleプッシュ通知サーバアーキテクチャ



Appleはサードパーティーセキュリティーソフトウェアを必要とするか
WindowsやAndroidとは異なり、付随的なセキュリティー階層やビルトオンサードパーティーツールは、Appleデバイスには通常あまり使われません。

従来のWindowsに焦点を置いたセキュリティー会社は、Appleの開発サイクルに遅れを取りがちであり、新しいオペレーションシステムとセキュリティー特徴の採用が遅くなると考えられます。実際、Appleを他のプラットフォームのように扱うと、従業員は往々にして最高の生産性を維持できなくなり、Appleが知られているユーザーフレンドリーエクスペリエンスを妨げます。加えて、Appleデバイス上にWindowsのソフトウェアバージョンを採用すると、終わりのないITとセキュリティーの悩みの種となる、コード実行の衰え、パニックによるメモリー消費とカーネル拡張（KEXT）を全て引き起こしてしまいます。

Appleのビルトイン暗号化とアンチウイルスは多くの組織がサードパーティーなしで稼働するのを可能にするにもかかわらず、未だに企業データ漏れへのソリューションを探している組織があります。しかしながら、Cisco Security Connectorなどのツールを活用して、ネットワークサイド上で追加保護を加えれば、企業データ漏れはMDMを通して監視できます。

2018年2月、Cisco、Apple、Aon、Allianzはその類で初めてのビジネス用サイバーリスク管理ソリューションを紹介しました。これは、Aonのサイバー復元評価サービス、CiscoとAppleからの最も高い安全性を誇るテクノロジー、Allianzからの強化されたサイバー保険適用オプションから成っています。このパートナーシップに関する詳細は、Appleウェブサイトの全声明をご覧ください。

Appleデバイスを管理する時の経験はどのようなものか
従来、ITの考え方は「Windowsデバイスを管理する時と同じようなクオリティーのツールはApple管理用にない」というものでした。この認識は、他のプラットフォームよりAppleの管理は難しいという誤解に輪をかけてしまい、多くの組織がAppleを提供したりサポートしたりするのを躊躇しました。

調査によれば、Appleは他のプラットフォームより管理が簡単です。Dimensional Research 調査は、回答者の66%がMacはPCより保護が簡単であると答えており、90パーセントがiOSは他のプラットフォームより保護が簡単であると答えています。Appleデバイスのデプロイ、設定、サポートの簡易性に関しても同じような回答が報告されています。

Appleプラットフォームで、従業員が選択できるプログラムを提供することに決めた多数の組織の内の一つは、業界大手のIBMです。実際、今のIBMの最高経営責任者Fletcher Previnは、PC以上に選ばれたMacがIBMで利益を生み出し、コストを削減していると証明しています。

これは、企業が一貫したデプロイとユーザエクスペリエンスを強く望んでいるということを示しています。Appleは一貫性とセキュリティーを細かい設定なしで提供します。

66%
組織の66パーセントは、Macのほうが PCより保護が簡単であると答えています

90%
組織の90パーセントは、iOSのほうが他のプラットフォームより保護が簡単であると答えています

Appleエコシステム特有のセキュリティー特徴

macOSにビルトインされているセキュリティー特徴は何か
macOSの基礎は、安全なソフトウェアにより形成され統合されています。

ビルトインmacOSシステムセキュリティー特徴には以下が含まれます：

- FileVaultは、デバイスが紛失または盗難にあった場合に、ユーザデータを保護するためのmacOSにビルトインされた暗号化の追加階層です。
- ソフトウェアアップデートはAppleから直接送られ、Appleは電子的にサインするので、組織とITは信頼されていることがわかります。
- System Integrity Protection (SIP)は、ユーザやアプリケーションアクセスからセキュリティー上の弱点として標的にされかねない、コアオペレーションシステムファイルを保護します。
- Gatekeeperにより、ユーザーがアプリケーションフォームをどこからダウンロードできるか、ITが定義できます。割り当てられていないアプリ（またはマルウェア）が稼働するのを防ぎ、XProtectと一緒に働いてマルウェアの拡散を速やかに阻止します。
- XProtectは自動化されたアンチマルウェアユーティリティで、Appleが随時更新します。これは悪意のあるソフトウェアや、JavaやFlashなどの時代遅れとなった脆弱なプラグインがMac上で稼働するのを防ぎます。
- マルウェア除去ツールAppleはシステムに入り込んだマルウェアを除去できます。
- p Storeで入手可能なApp StoreのアプリはAppleにより十分に調査されており、Appleが承認するリソースのみがストアにあります。Appleはアプリの入手可能性を止め、直ちにデベロッパーの証明を取り消すことができます。
- App Sandboxingは、システムやその他からデータを共有（または盗難）しないアプリであることを確認します。
- ユーザとITにはプライバシー制御 - ロケーションサービスがいつ使われたか、どのアプリが連絡先やカレンダーにアクセスできるか、どの情報がAppleや他のアプリデベロッパーと共有されたかをユーザに知らせる透過的なプロセスが利用可能です。

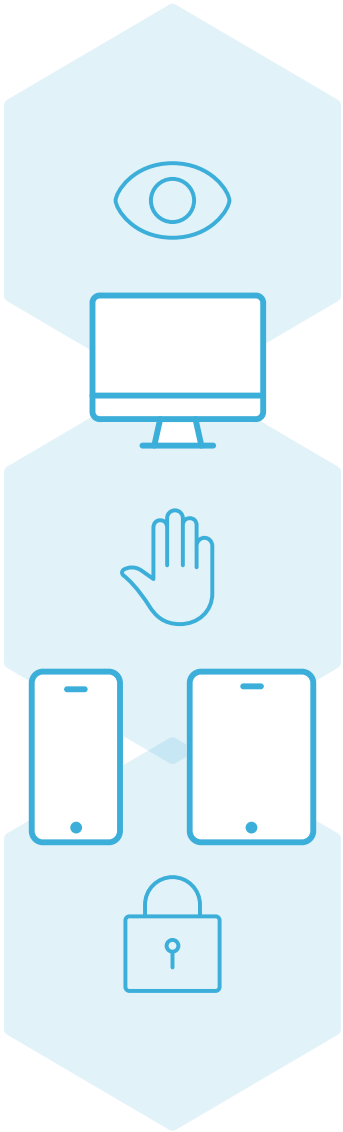
Macセキュリティー機能の全様を見るには以下にアクセスしてください：https://www.apple.com/macos/security/.

ディスク暗号化にFileVaultを活用すべき理由とは
FileVault とは、macOS用のビルトインディスク暗号化で、ITは、ドライブを暗号化するために追加のソフトウェアを加える必要がないという意味です。手動でも使用可能で、もしくは、ITが全てのMacコンピュータを遠隔で使用可能です。暗号化キーは中心的に管理され、従業員が組織を離れた後や、パスワードを忘れてログインするのにヘルプが必要な場合、ITは必要なデータにアクセスできます。暗号化キーはセキュリティーの増加に合わせて簡単に交代できます。

iOSにビルトインされているセキュリティー特徴は何か
Macの同じコアセキュリティー性能は、iPadやiPhoneでも利用可能で、Appleエコシステム全体で一貫して安全なエクスペリエンスを提供しています。

- システムセキュリティーには、Secure Boot、Software Authorization、Secure Enclaveなどのテクノロジーが含まれ、OSがウイルスに感染していないことを確かめます。ITもiOSオペレーションシステム全体を消去し、再度スタートする権限を持っています。
- Touch ID / Face IDは、ログインプロセスを合理化し、権限のあるユーザのみがデバイスにアクセスすることを確認するため、指紋認証と顔認識を利用します。
- 暗号化とデータ保護は、盗難や紛失によりデバイスがワイプされたとしても、個人また企業データが感染しないよう確実に保護します。
- 監視は、より制御された環境で付加的な管理能力を得るために、ITが活用できる追加的なフィーチャーのセットです。

iOSセキュリティー機能の全様を見るには以下にアクセスしてください：https://www.apple.com/business/docs/iOS_Security_Guide.pdf.



新たなAppleデバイスを追加する時に考慮すべき点

Appleデバイスの安全性を証明する方法とは
Appleデバイス管理の基本とは、設定プロファイルを作成する能力のことです。Jamf Proのようなモバイルデバイス管理ソリューションで設定プロファイルを構築して、ITはパスコードの強化、設定の制限、ネットワークプロトコルの定義、VPN設定やメールアカウントを設定したり、その他にも様々なことができます。それから、ITはそれらの設定を管理したデバイスにデプロイします。

アプリコンテナが必要でない理由とは
Jamf Proのように、Appleに焦点を当てた管理ツールは、デバイスに承認されたアプリを展開し、承認されていないアプリにもデバイス上で対応します。iOS はすでに、Jamf Proのようなソリューションが付帯したネイティブアプリ管理を利用して企業アプリを管理する機能のサポートしています。この管理方法は、パフォーマンスが遅くなったり、OSのリリース毎に廃棄されるコンテナアプリを使わずに企業データを個人のデータや管理データから分けることができます。

MDMフレームワーク外でMac用にはどんなセキュリティー制御がありますか
macOSにとって、Jamf Proのようなソリューションは、Jamf Agentでの基礎的なデバイス管理以上の事を成し遂げます。Jamf Agentは、Macが管理に登録された後インストールされる二次的なものです。これによりITは、全てのMacコンピュータに遠隔ルート

アクセスする権限を与える、隠れた管理者アカウントを作成することが可能です。

Jamf Agentのインストールで、ITはより進んだポリシーとスクリプトを実行でき、AdobeのようなApp Store外でのソフトウェアをインストールしたり、さらに多くのことができます。MDMができる以上に、カスタマイズを拡大し管理能力を拡大します。

自分の環境内でAppleデバイスのコンプライアンスを有効化、強化、レポートするにはどうすれば良いか

高度に統制された業界では、監査は一貫しており飽きのくる作業です。そのため、コンプライアンスを示すのに、デバイスは絶対的に管理化にあり安全であることを証明するのは大切です。

規制の企業セキュリティー要項を満たすにはインベントリを収集することが鍵です。組織環境に何台のデバイスがあり、だれがどのデバイスを持っていて、ソフトウェアアップデートのステータス、どのプロファイルと設定が各デバイスに割り当てられているか、現在の暗号化ステータス、適用される規制と設定は何かを知ることは、どんな健全で安全な環境にとって鍵となります。

Jamf Proのようなソリューションは、ITが実質上終わりのないインベントリカテゴリの容量のレポートを実行することが可能になり、より良いビジネス決定とコンプライアンスの遵守ができるよう組織を助けます。一台のデバイスがコンプライアンスに満たない場合、正しいデバイスフォースに設定プロファイルをデプロイしてコンプライアンスに戻します。

コンプライアンスを満たしていないデバイスが複数ある場合、環境全体のチャックを実行しなければならない場合、Jamf Proを活用してデバイスのダイナミックスマートグループを作成します。スマートグループは、ITが定義した高度なインベントリクライテリアに基づいており、インベントリレポートに基づいて、自動管理アクションをトリガーできます。

サードパーティーmacOSソフトウェアの補修を扱う方法
ソフトウェアはすぐに時代遅れになることがあり、そうなると、デバイス、データ、ネットワークは、内部脅威また外部脅威に対して脆弱になりかねません。これらの脆弱性には、すぐに補修管理を活用して効果的に対応できます。

更新されたサードパーティーソフトウェアバージョンが利用可能になった時に、MDM補修管理機能はITが補修アラートを受け取り、適切なパッチ（更新済みソフトウェアバージョン）でソフトウェアパッケージを作成し、そのパッチを適切なデバイスに配信して、パッチが正しくインストールされたことを確認するためインベントリ管理を経由してパッチレポートを受け取ることが可能にします。

即座にどのアプリとソフトウェアが古いかを知り、最新で安全なバージョンが確実にインストールされるように素早く行動を取り、組織はセキュリティワークフローへの保護的なアプローチを行います。

Active DirectoryへのAppleデバイスをバインドするべきでない理由
デプロイに関しては、Macは従来のワンツーワンデプロイとは異なります。Enterprise ConnectとNoMADのようなツールがあれば、バインディングは過去のものとなります。外部に公開したDomain Controllerを組織が持っていない場合、コンプライアンスDEPワークフローをバインディングするだけでなく、組織の活用するバインディングは遠隔ユーザに新しいデバイスを直送する能力を逃してしまいます。バインディングは選択肢ですが、Jamf Proのようなソリューションを使っている組織は、接続について心配したり、ADとの同期を逃すことを考えたりせずに、同じパスワードの複雑性と満期要項を適用しローカルアカウントを管理できます。エンドユーザは少ないパスワードですみ、ITヘルプデスクも少ない電話ですみます。

クラウドサービスがAppleデバイスと機能する方法
クラウドへの移行は成長しています。クラウドホスティングで、ネットワークのサーバに待機しているよりも、サーバデータベースへのアクセスは制限されます。数十年間、組織は会社の周りに「壁」を築いて、最初のディフェンスラインとしてネットワーク境界を活用しました。職場環境がより可動的になり、データはもはやファイヤーウォールの裏側に存在するわけではないので、組織はより現代的で、アイデンティティベースモデルのセキュリティーに移行する必要があります。

Microsoftは、Azure Active Directoryで企業データをクラウドに移動させています。信頼できるアプリを使った、信頼できるデバイス上の、信頼できるユーザだけが、クラウド内の企業データにアクセスしていることを確認し、MicrosoftとJamfは、プロキシフリーの機密アクセスを実現するため専用的な統合を提供します 。

詳細は以下をご覧下さい: https://www.jamf.com/resources/white-papers/conditional-access-going-beyond-perimeter-based-security/.

モバイル職場形態への移行とクラウドへの依存の増加は一時的な流行ではありません。

85%
85パーセントの組織は、重要な情報をクラウドに保管しています。

80%
80パーセントの従業員は、仕事に承認されていないSaaSアプリを使っています。

41%
41パーセントの従業員はモバイルビジネスアプリが作業形態を変化させたと答えています。

業界のセキュリティー規準を強化する方法
強化はセキュリティー基準がどんなものかに依存しており、コンプライアンス基準を満たす必要があります。SOC 2はHIPAAとは異なり、PCIはCISと異なります。何に固く付き従うかを知るのは重要な最初のステップです。

Jamf Proは、多くの共通する規制規準を順守するようサポートする柔軟なフレームワークを提供します。ITは適用可能な規準を簡単に定義し、対応するプロファイルとポリシーを構築して、適用します。これらのクラウドには、iCloud Driveのような、消費者を規制する特徴を含んでおり、安全なアプリだけがダウンロードされることを確認してGatekeeperを強化し、Macを暗号化するのにFileVaultを強化し、または、全ての管理Appleデバイス全体から規制されたアプリ(またはmacOS)を探して規制し、見つけ出したら削除します。ITは単に設定が何かを定義し、その情報を使って設定プロファイル、ポリシーを構築しデバイスに適用する必要があります。

この白書を確認して、Center for Internet Security (CIS)ガイドラインに付き従う方法を学習できます: https://www.jamf.com/resources/white-papers/macos-security-checklist/.

Apple発展プログラムを使うべき理由

企業用のApple展開プログラム、DEPとVPPは無料でApple専用です。これらのプログラムは、より高いレベルのデバイスセキュリティーだけでなく、スケールでITにデバイスセットアップを自動化、または、個人化する能力を与えます。

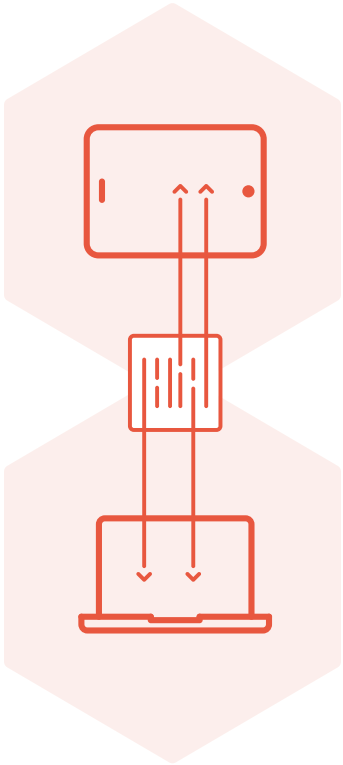
- DEPは、直観的に所有するAppleデバイスを安全で管理された状態に持っていくためにAppleが好む方法です。DEPはゼロタッチデプロイを可能にします。これは従来のイメージングプロセス、または、マニュアルIT構成の必要性とセットアップが取り除かれるという意味です。ユーザは自分を素早くシームレスに環境に登録でき、オンボード時間を最小限に抑えつつ、数回のクリックでエンドポイントの安全性を守ります。Appleから直接オーダーされたデバイス、または、Apple Authorized Resellerは、DEPを扱う資格があり、最初のセットアップ時に管理に自動で登録されます。
- macOS、iOS、tvOSデバイス用に、DEPは追加管理制御が利用可能で、より深いレベルでの管理を行う権限を与えます。
- モバイルデバイス管理、またはMDM(Appleのビルトイン管理フレームワーク)と合わせると、最終状態はダイナミックな方法を通して、ワンサイズフィットオールイメージを焼くのとは対照的にユーザのニーズに基づいて提供されます。
- VPPはITにApp Storeからアプリを許可して、個人かデバイスにソフトウェアを配信できるようにします。デバイスに直接的に配信された場合、Apple IDは必要ありません。Apple IDはユーザーを判別し、iCloud、iTunes、App Storeなど、Appleサービスへのアクセスを許可します。
- ITは、従業員が会社を去ったり、特定のアプリを必要としなくなった場合に、購入済みVPPアプリを管理し、再配信のために再度要求することができます。

Appleデバイスマネジメントソリューションがすべてプログラムとサービスをサポートするわけではありません。斬新な変更と同様に、こうしたプログラムをベンダーがサポートしているか確認してください。」

すでに持っているものを活用するために利用可能なApple統合とは何か

存在しているITテクノロジー記憶装置を使ってどのようにApple（とJamf）を統合するか

組織、IT、従業員は狭い世界で生きているわけではありません。Appleは、モダンで安全なビジネスサービスを提供するため、Ciscoのようなテクノロジー企業とパートナーシップを組むことで企業へのコミットメントを証明していました。



多くの企業は、Appleエコシステムの外側でサービスを必要としています。安全で互換性のある統合で、組織は持っている環境の全ての面を活用し、ビジネスを前に進めるためのサービスの配列を受け入れることができます。

例には以下が含まれます：

- 存在するITツールとの統合を構築して、柔軟性をもたらす、Jamfのアプリケーションプログラミングインターフェース（API）。
- JamfとのMicrosoft EMS統合は、Mac上で条件アクセス用の専用プロキシフリー統合を提供します。
- Cisco ISEは、会社のネットワークに接続されたデバイス用のセキュリティーとポリシーへのアクセスを作成し強化します。
- Cisco Fast Laneは、アプリの優先順位を定め、自動でサービスのクオリティーを設定して、ネットワークバンド幅上で保存します。
- ServiceNowは、オペレーション管理用にITとビジネスプロセスを自動化します。

現代の組織はCiscoのような企業ツールに移行しており、Mac管理にJamfを加えることは、どんなサポートプラットフォームを怠ることなく、完全に統合されたソリューションを提供します。

加えて、識別管理会社Okta Inc.は、最近発表されたSecurity Data Reportの名中で、企業内でのサイバーセキュリティーアプリケーションの急増に焦点を当てた幾つかの調査結果を発表しました。今年初めて、Jamfのようなセキュリティツールは全て、最も成長しているアプリのトップ１５にランクインしました。

釣り合わないデバイス管理とセキュリティーへのApple + Jamf
最も安全なプラットフォームは、全ての可能性のあるセキュリティー特徴が強化されインストールされているかを確かめるため最も堅固な管理ソリューションを必要としています。Appleとそのサービスとより良く統合した他のモバイルデバイス管理会社は、Jamf以外になく、Appleアクセスを確実に行うのにこれ以上適したプロバイダはありません。

そのため、Jamfは、米国銀行のトップ１０のうちの10行、トップ10テクノロジー企業のうちの９社など、セキュリティー意識の高い組織から、Apple環境の管理のための信用を得ています。

Appleのオペレーティングシステムとフィーチャ用のゼロデイサポートで、Jamfは、Appleを取り入れて従業員を強化しようとしているビジネスから、製品への信用を得ています。

Jamfは、組織が時間を節約し、ユーザエクスペリエンスを向上して、ビジエスを成功に導くことを可能にする戦略的タスクに集中するための自由を持てるようにする一方、100台であれ、100000台であれ、Appleデバイスを守るため必要なツールを提供します。

Jamfの顧客の96パーセントは来る年も来る年も、契約を更新しています。Jamf ProがAppleデバイス管理に与える影響の詳細については以下をご覧ください jamf.com/ja/products/Jamf-Pro.

jamf

www.jamf.com

Jamf ProがMacとiOSの管理に与える影響の詳細については以下をご覧ください。jamf.com/ja/products/jamf-pro