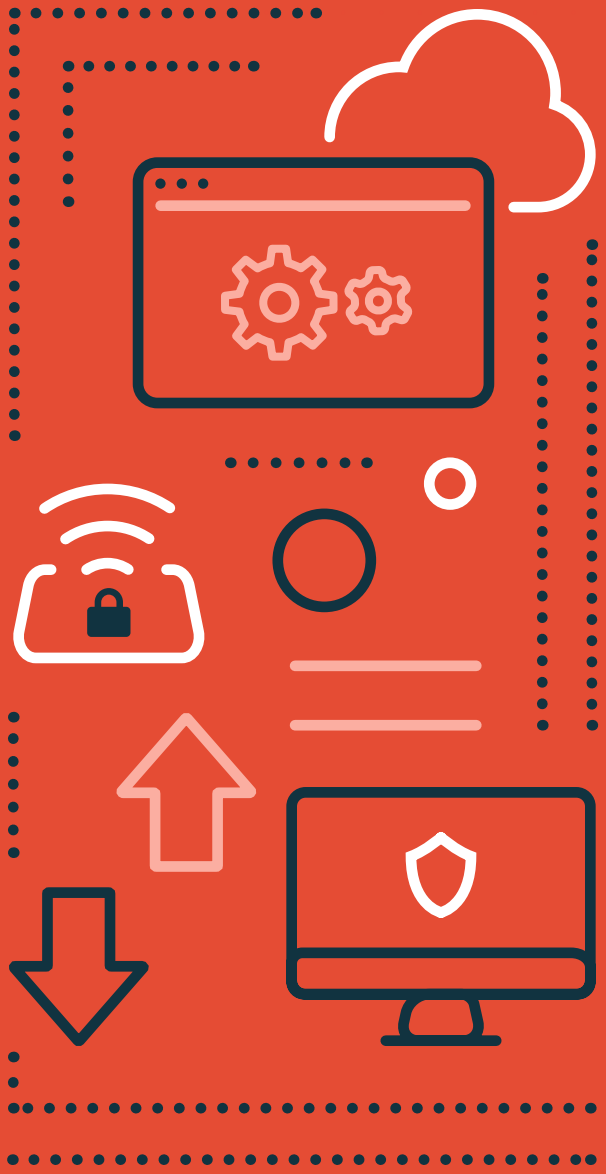


ゼロトラスト ネットワーク アクセス

初心者ガイド

jamf

「ゼロトラストネットワークアクセスという言葉さえ聞いたことがない」そんな方のためにご説明します。

Gartner社によると、ゼロトラストネットワークアクセス（ZTNA）とは、**単数または複数のアプリケーションの周りにアイデンティティとコンテキストベースの論理的な壁（境界）を構築する製品またはサービス**のことを指します。

簡単に言えば、ZTNAはVPN（仮想プライベートネットワーク）の後任のようなものです。しかし、1996年にPPTPをベースにして作られたVPNとは違い、**Jamf ConnectのZTNAソリューションは最新のコンピューティング技術を念頭に置いて作られて**おり、リスクを意識したポリシー管理とアプリケーション特定のマイクロトンネルを備えたアイデンティティベースのセキュリティモデルを取り入れています。ユーザのアクセスは使用を許可されたリソースのみに制限され、すべてはたったの数クリックで管理や機能の拡張が可能なクラウドベースのインフラに組み込まれています。メンテナンスが必要となるハードウェアは必要ありません。

このEBOOKで手に入る基礎知識

- Jamfソリューションの仕組み
- Jamfソリューションに含まれるセキュリティ機能
- ネットワーク認証とセキュリティへの取り組みを見直すことの重要性

セキュリティのスタート地点としてぜひご活用ください。

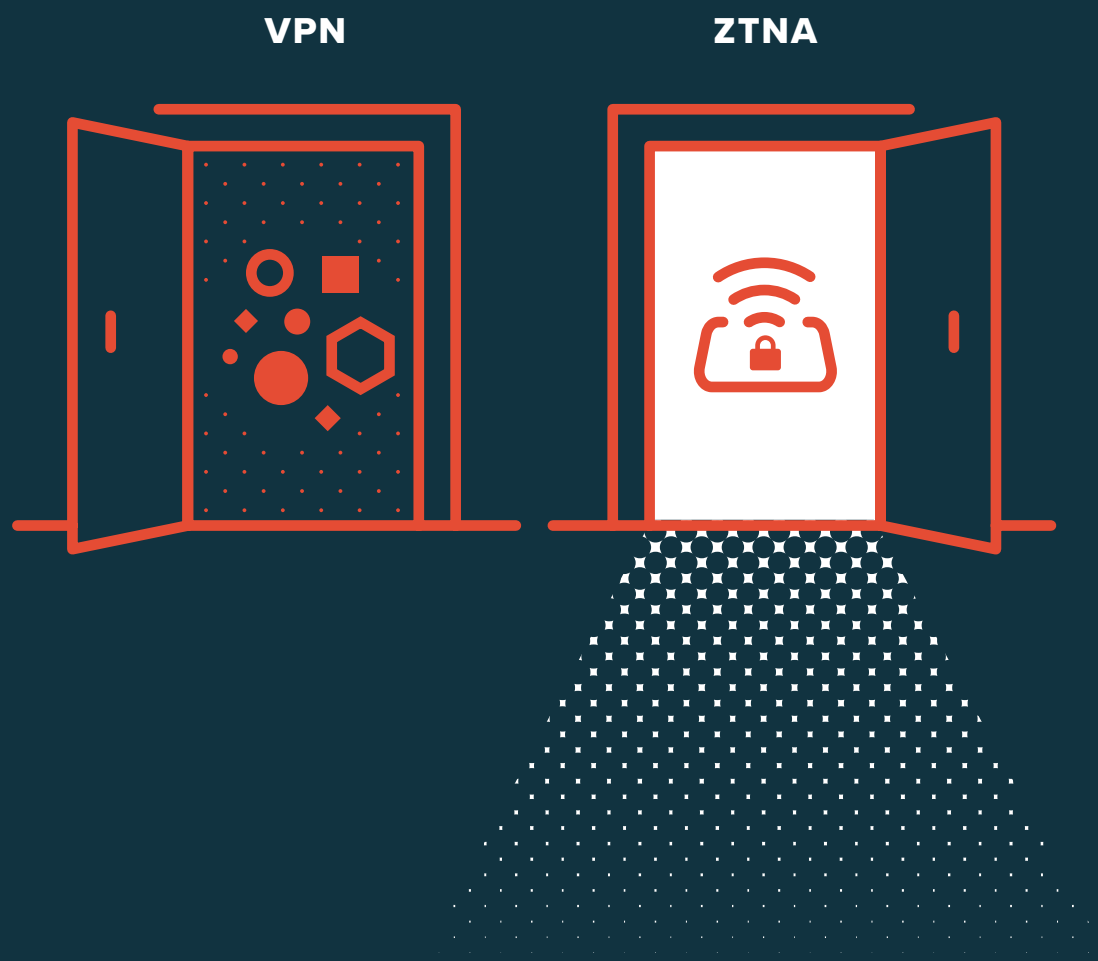
「もはや誰も信用できない」

『遊星からの物体X』でカート・ラッセルが演じたR・J・マクレディは、ストーリーが進み問題が山積みになる中で仲間に不信感を抱くようになります。最小特権の原則や「決して信頼せず必ず確認せよ」のモットーに基づくセキュリティ構成を採用した技術であるZTNAは、マクレディのこの心理と多くの共通点を持ちます。

ZTNAでは、最小特権をリアルタイムのデバイスポスチャチェックと組み合わせて適用することで、**個人の認証情報を使ってアクセスをリクエストする特定の認証されたユーザのみに、各アプリケーションに対するクラウドベースのアクセスを許可します。**

つまり、ユーザがクラウドIDの認証情報でデバイスにアクセスすると、業務用の接続を維持しながら、スプリットトンネリングと呼ばれるプロセスで非ビジネスアプリケーションをインターネットに直接つなぎ、エンドユーザのプライバシーを保護しながらネットワークインフラストラクチャを最適化します。これにより、接続やマイクロトンネルの確立に効率性を持たせ、基盤となるネットワークをさらに最適化することができます。マイクロトンネルを活用することで、許可されたユーザ、デバイス、アプリをエンドツーエンドで保護することが可能になるのです。例えば個人所有のデバイスで、アクセスを許可する基準が構成されていない場合、適切な認証情報を入力しても、企業リソースへのアクセスは許可されません。

アクセス権が全体的に付与され、ネットワーク全体のリソースへのアクセスがユーザに提供されるVPNとは異なり、ZTNAの粒度の細かいアプローチはセキュリティをさらに強化します。ユーザが必要なタイミングで必要なものだけにアクセスを許されるからです。コンプライアンス要件に合わせてカスタマイズされたポリシーによって組織のセキュリティを強化すると、エンドユーザや組織のデバイス、データの安全がより包括的にサポートされるようになります。



「お前たちのルールにはいい加減ウンザリしてきたぜ」

映画『ニューヨーク1997』で、悪名高いスネーク・プリスキンが、市民に与えられた自由と、平和と秩序を維持するための法律の狭間でこの言葉を呟いたように、IT管理者もしばしば同様の悩みに直面することがあります。

エンドユーザが必要とするリソースやデータへのアクセスの提供とセキュリティのバランスを保つために、組織ができることは？

この問いに答えてくれるのが、Jamfのソリューションです。

ユーザがアクセスすべきでないデータやアプリの見つけやすさを排除しながら、アイデンティティとアプリを軸にしたポリシーで生産性の向上を実現するJamfのソリューションは、データセンターや複数のクラウドインフラストラクチャ、SaaSアプリケーションだけにとどまらず、あらゆる最新のオペレーティングシステムや管理パラダイムにおいて、一貫したアクセスポリシーが適用されるようにします。

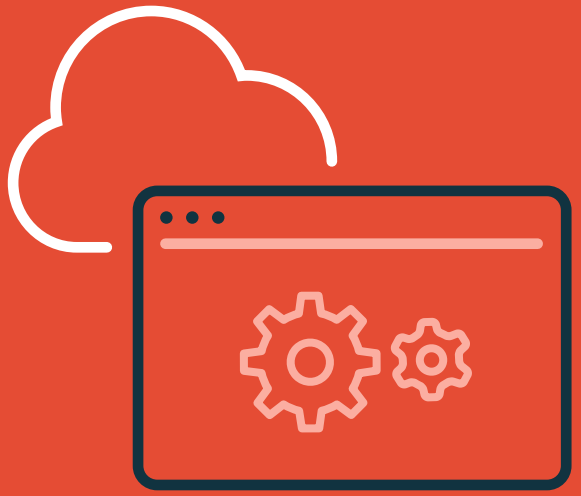
セキュリティを強化するポリシーの中でも特に、リスクを意識したアクセスポリシーは、リソースへのアクセスを阻止し、デバイスの定期的なチェックによる健全性評価やネットワーク全体のセキュリティポスチャはもちろんのこと、安全性が損なわれたデバイスや、リソースへの安全なアクセスに深刻なリスクをもたらすデバイスの特定を積極的に行います。

「もう心配はいらない、ヒーローの登場だ」

強固なクラウドベースの基盤に構築されたJamfソリューションのインフラストラクチャは、ハードウェアの管理やサポート契約を必要とせず、複雑なソフトウェアのインストールや構成も必要ありません。

忘れてはならないのが、すべてが一元化され拡張性にも優れたクラウドなら、フリートの規模やデバイスの物理的なロケーションに関わらず、すべてのデバイスがサービスに登録された瞬間からデータが保護されるということです。必要なのはネットワーク接続だけです。

『ゴーストハンターズ』のクールな主人公ジャック・バートンのように、Jamfソリューションもユーザやデータを守るために常に忙しく働いています。クラウドベースという特性と機能拡張を叶える統合によって強化され、接続の暗号化やデバイスの健全性モニタリング、検出された問題を自動的に修復するワークフローにより、エンドポイントを保護し、デバイスのパフォーマンスを最適に保ってくれます。



JAMFソリューションの仕組み

一言で言えば、“頑張らずにスマートに働く”ツールです。

ZTNAアーキテクチャにとって不可欠な統合のひとつが、任意の**クラウドID プロバイダ（IdP）**を介したシングルサインオン（SSO）によるユーザ認証を可能にしてくれる機能です。これにより、ユーザやデバイスの証明書を管理する手間が省けるため、専用の認証局（CA）を維持する必要がなくなり、リモートまたはハイブリッドの環境でこの種のインフラのセキュリティを構成する際に必要なあらゆるネットワーク上の手続きもなくなります。

これにより、各デバイスのネットワーク接続を効果的に活用し、「頑張らずにスマートにクラウドに接続」することが可能になります。オーバーヘッドが少ないということは、効率が良いということであり、それは決して悪いことではありません。また、オーバーヘッドの点で言えば、Jamf Connectのエージェントはデバイスやユーザ、データに最高レベルの保護を提供することだけでなく、それを最小限のリソースで実現することを念頭に置いて作られています。

JamfはOktaとAzureのネイティブサポートを提供していますが、Azureフェデレーション経由でGoogleやPingなどの主要なIdPもすべてサポートしています。

JAMFソリューションの
セキュリティ機能

アイデンティティ中心のセキュリティモデル

認証されたユーザのみにビジネスアプリケーションへのアクセスを許可し、データセンター、クラウド、SaaSアプリケーション間で一貫したポリシーが適用されるようにします。

アプリケーションベースのマイクロトンネル

アクセスが許可されているアプリにのみユーザを接続します。マイクロトンネルは、最小権限のアクセスを適用し、ネットワークの横方向移動（セキュリティ侵害の一般的なベクトル）を防ぎます。

最新のクラウドインフラストラクチャ

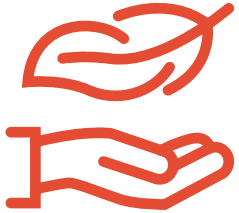
ハードウェアの管理やサポート契約の更新、複雑なソフトウェアの構成は必要ありません。セキュアなアクセスを可能にするためのデバイス管理さえ必要なくなります。

IDサービスとの統合

シングルサインオン(SSO)によるユーザ認証を可能にし、証明書を管理する必要性をなくします。

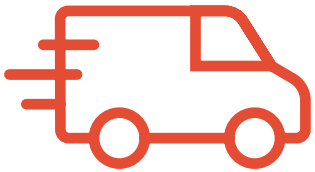
リスクを意識したアクセスポリシー

侵害された可能性のあるデバイスやユーザからのアクセスを阻止し、セキュリティを強化します。



軽量なアプリケーション

アプリケーションの接続時にトンネルを自動的に確立し、中断した場合はシームレスに再接続します。



高速で効率的な接続

バッテリー駆動時間に影響を与えることなく、ビジネスアプリへの妥協のないアクセスを実現し、ユーザエクスペリエンスを妨げることなくバックグラウンドで静かに稼働します。

インテリジェントなスプリットトンネリング

業務外のアプリケーションをインターネットに直接ルーティングさせ、エンドユーザのプライバシーを守り、ネットワークインフラストラクチャを最適化しながら、業務上の接続を確実に保護します。

統合アクセスポリシー

すべてのホスティングロケーション（オンプレミス、プライベートクラウド、パブリッククラウド、SaaSアプリケーション）、すべての最新OS、およびすべての管理パラダイムに対応します。

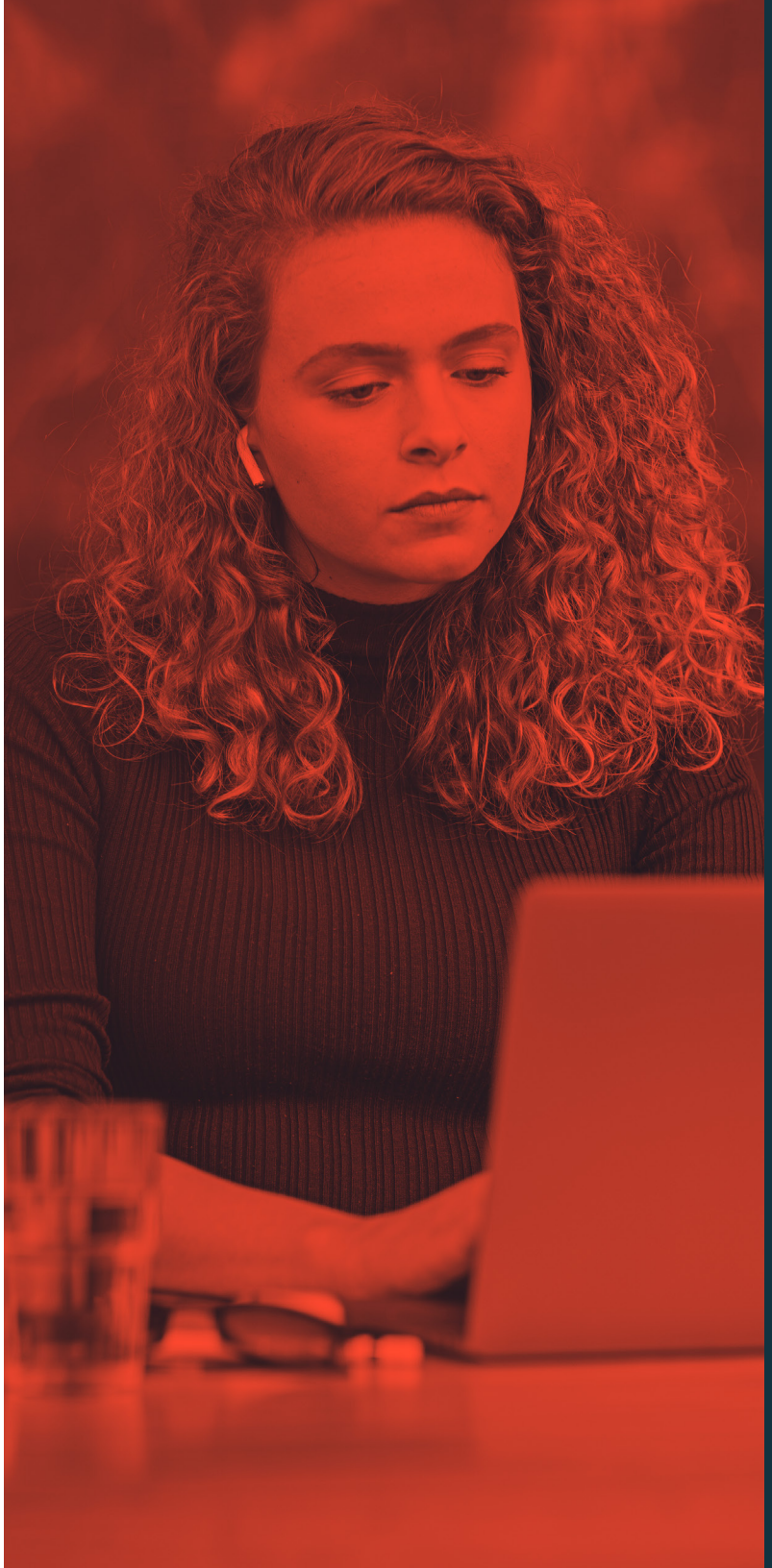
VPNの代わりに ZTNAを採用すべき理由

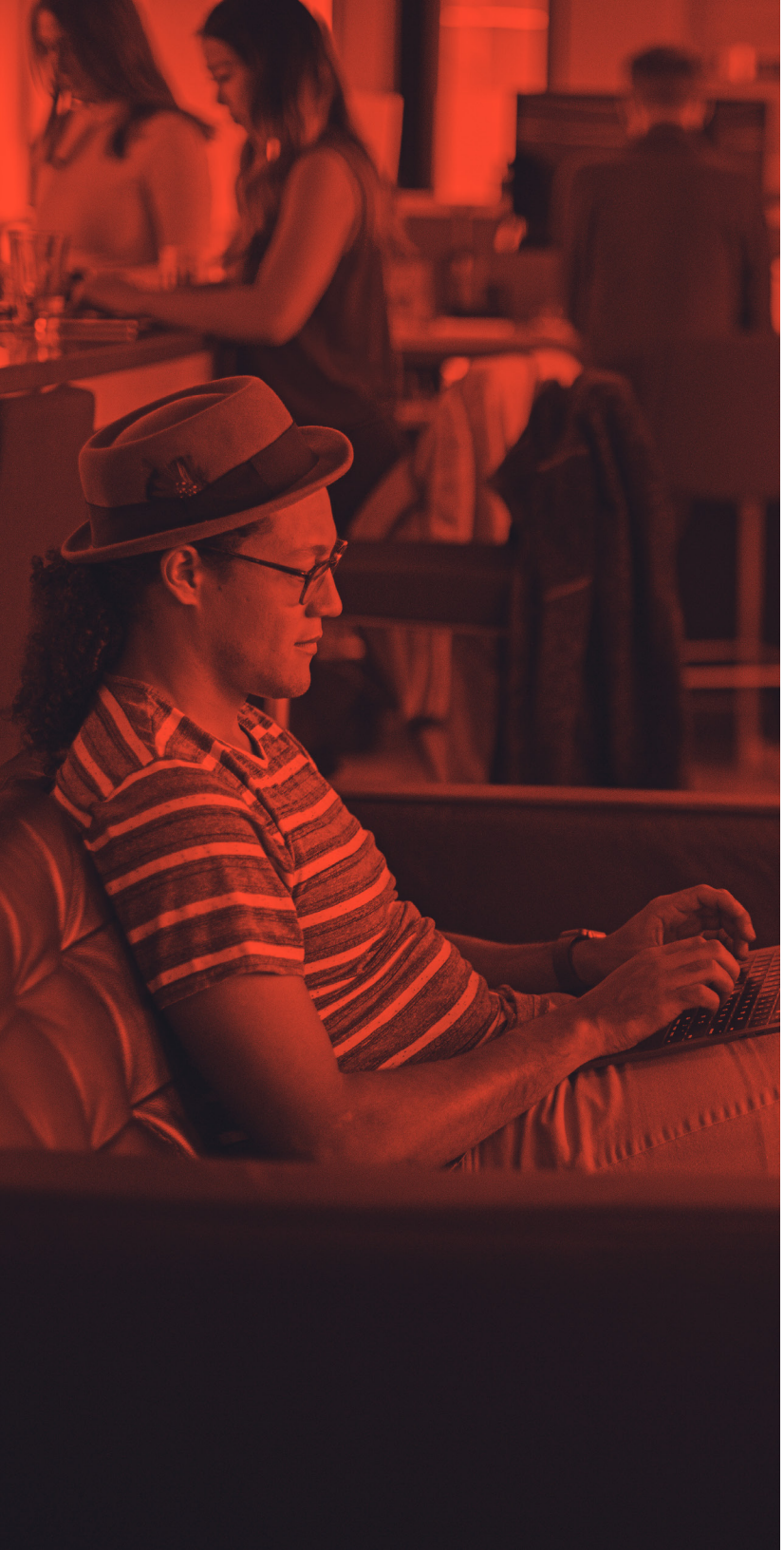
VPNでセキュリティリスクがすべて解消しても、残る問題がひとつあります。ユーザが実際にVPNに接続しなければならないという点です。組織がVPN接続に消極的であったり、単に知識が不足しているために、ネットワーク上の安全な場所にデータを置くことを怠り、セキュリティリスクを引き起こしてしまうことがよくあります。

ZTNAを使えば、ユーザは保護されたサイトへのアクセス方法やそのタイミングについて考える必要がなくなります。デバイスにログインさえすれば、いつでも必要な時に保護されたデータにアクセスすることができるのです。ZTNAが裏側でユーザの認証と承認を行い、データにアクセスしようとしているのが信頼できるデバイスであることを確認してくれています。つまり、エンドユーザにデータへの簡単なアクセスを許すと同時に、組織がデータを正しく保護できるよう働きかけてくれるのです。

VPNへの接続の仕方を忘れてばかりいるユーザのためにデータを危険にさらす必要はもうありません。

ZTNAでは、ユーザが使用しているデバイスの種類やOSに関係なく、アプリケーションが接続しようとするタイミングで自動的にマイクロトンネルが確立されるため、セッションの終了やサービスの中断の際にも同じように簡単に再接続することができます。また、Jamfのソリューションは貴重なハードウェアリソースを占有したり、使用していないときにバッテリーを消耗させることがありません。





その代わりに、保護されたデータへのアクセスを必要とするアプリケーションやユーザーリクエスト、またはサービスが動き出すのを待ち、ユーザがアクセスできないはずのデータやアプリを発見するのを防ぎながら、リソースの保護とシームレスなユーザエクスペリエンスの維持を並行して行います。また、各アプリケーションの分離した接続を介して移動するデータを保護するクラウドベースのSDP（Software-defined Perimeter）を提供します。

さらに、JamfのソリューションをAppleのプライベートリレー（訪問したウェブサイトからユーザのIPアドレスや位置情報を隠して個人のプライバシーを保護する新しいiCloudサービス）と併用することで、従来の企業向けVPNのパフォーマンス、プライバシー、セキュリティ上の課題を伴わないビジネスアプリケーションへの安全なアクセスが可能になります。

このコンビネーションにより、ユーザのインターネット閲覧におけるプライバシーは仕事とプライベートの両方で守られます。個人所有のデバイスであっても、Jamfを導入することで、業務関連のトラフィックの保護・ルーティングを行いながら、プライベートでのインターネット閲覧に関してはiCloudプライベートリレー経由でプライバシーの保護を行うことができます。JamfのソリューションとiCloudプライベートリレーを併用することは、パフォーマンスやエンドユーザーエクスペリエンスを犠牲にせず、プライバシーとセキュリティの両方を確保するもっとも最適な方法と言えます。

次のステップ

リモートワークやハイブリッドワークの環境においては、最新のセキュリティアプローチでデバイスやユーザ、データを保護することが非常に重要です。Jamf のソリューションを使って、アイデンティティベースのセキュリティに基づいた最小権限アクセスを適用することから始めましょう。

- デバイスの健全性チェック
- リスクを考慮したポリシーに基づく修復ワークフローの自動化
- 直感的なユーザエクスペリエンスを損なうことなく、クラウドベースのコンソールからこれらを一元的に実行

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製品取扱店までお問い合わせください。

トライアルに申し込む