jamf

ホワイトペーパーパー

Conditional Access: 境界ベースのセキュリティを超える

モダン ワークプレイスと次世代のセキュリティ

組織は、防御の最前線として、何十年にもわたって自身の会社や利用しているネットワーク境界の周囲に「壁」を構築しました。しかし、ワークスペースの流動性がより高くなってきたことに伴い、セキュリティ境界が変化しました。ネットワークを構築し、ファイアウォールで守るというコンセプトは不十分かもしれません。従来の境界ベースのセキュリティ モデルを見直す時期です。

オフィス ワーカーが全員朝 9 時から夕方 5 時まで働く時代は過去のことです。人々は、月曜日から金曜日まで働くだけにとどまりません。

自宅、コーヒー ショップ、ホテルのロビー、仕事の現場で、それぞれの都合に合わせた勤務時間で働いています。そしてこの場合、会社のリソースへのアクセスが必要なだけではなく、「従来の」勤務時間外でのアクセスが必要となります。

新しい「ワークスペース」は流動的なものであり、人々は今やツールを使ってデバイス、アプリ、自分たちのいる場所間でデータを取得する必要があります。.

ここでクラウドの出番です。

ファイアウォールを超えたクラウド サービスは、この新しい仕事を中心とする柔軟な環境の構成要素です。また、これらのサービスでは、ユーザーがあらゆるマシンから Web ページやアプリにログインして

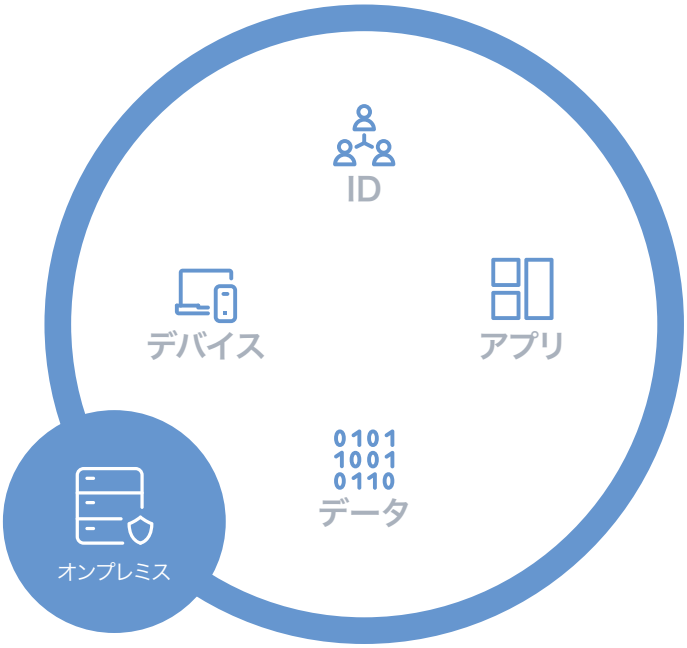
情報にアクセスできるため、情報にアクセスしやすくなっています。さらに最新のクラウド サービスは、組織がこれらのサービスの多くにかかっていた費用の何分の 1 かの費用で運用を自動化することを可能にします。

このワークプレイスの変移と、クラウドへの依存の高まりは、Apple デバイスの管理制品を開発する Jamf Software の年次ユーザー カンファレンス「Jamf Nation User Conference 2017 」で Microsoft シニア プロダクト マネージャーのヴラディーミル・ペトロシアン氏 (Vladimir Petrosyan) がプレゼンテーションの中で用いた言葉を借りると、単なる一時的な傾向以上のものです。

- 組織の 85 % が機密情報をクラウドで維持管理している
- 従業員の 80 % が承認されていない SaaS アプリを仕事に利用している
- 従業員の 41 % がモバイル ビジネス アプリが働き方を変えていると話している

かつてシャドー IT (個人所有パソコン、スマートホン、タブレット型端末などを会社の許可を得ずに業務に利用すること) に端を発した変わりゆく状況とともに進化しようとする企業が増えていくにつれて、セキュリティ パラメーターや、セキュリティ パラメーターを使用してユーザー、デバイス、アプリを保護する方法も進化する必要があります。オンプレミス インフラストラクチャとサーバーは、今なお多くの重要なアプリやサービスに使用されていますが、コンテンツ プラットフォーム、コラボレーション プラットフォーム、オフィス向けクラウド パッケージ、デバイス以外のデータを保存するモバイル デバイスの使用に端を発するクラウドベースのツールの利用が、組織の間で増えつつあります。従業員はファイアウォール外で働いているだけでなく、従業員がアクセスするアプリケーションやデータのほとんどがクラウド内にあるのが現実です。言うまでもないことですが、多くの人々が個人所有デバイスから組織のリソースにアクセスを試みています。インフラストラクチャのクラウドへの移行に着手し始めた企業が増えてきましたが、企業のサービスにアクセスするためのセキュリティの強化が求められています。そのため、企業は準拠とセキュリティを維持する新しいより良い方法を模索しています。

肝心なのは、ユーザーが生産性を最大限に維持するとともに、会社の重要なデータを継続的に保護できるよう適切なバランスをとることです。



従来のセキュリティ モデル

今日の企業におけるセキュリティ転換

セキュリティ境界は変化しました。デバイスやデータがもはやオンプレミスでホストされていないため、ネットワークを構築し、ファイアウォールで守るというコンセプトはもう完全に通用しなくなっています。デバイスは世界中で利用されており、いつでもどこからでもクラウド サービス、電子メール アプリケーションやその他の機密である可能性のある企業のリソースに直接アクセスできます。

上記は、ファイアウォールの内側に保護のための境界を設けた従来のセキュリティ モデルの例です。

ですが、これは、私たちの同僚や彼らのデバイスが現在アク

最新のセキュリティ モデル

セスしているもののごく一部を表しているにすぎません。ファイアウォール外の複数のデバイス間でのクラウド ストレージや業務効率化アプリが新たな常識です。私たちが現在頼りにしているものの普及度合いを考えれば、組織が境界ベースのセキュリティ モデルを引き続き活用する場合、いかに攻撃を受けやすいかが簡単にわかります。

ユーザーが必要とするデバイスとリソースの大半がクラウドに移行しつつあるため、組織は従来のオンプレミスの ID 管理を使ってサービスへのアクセスを提供することはもうできなくなっています。ユーザーがどこにいようと、潜在的なセキュリティの脆弱性を軽減し、ユーザーの生産性を維持するには、ID が、私たちがアクセスしているクラウドと同様にどこからでもアクセスできて柔軟な従来の境界ベースのセキュリティ モデルを見直す時期です。

デバイスとアクセス:セキュリティ レイヤー

セキュリティと認証には 3 つの共通の要素がありますが、どれ 1 つとして欠かせません。

- デバイスベースのセキュリティ
- ユーザーベースのセキュリティ
- 多要素認証

デバイスベースのセキュリティ

このセキュリティ手法は、対象管理の企業デバイスや、組織のセキュリティ ポリシーに準拠していない管理対象のデバイスに適用できます。このセキュリティ モデルは、フィッシング (詐欺) 行為や「当てずっぽう」で資格情報が取得されてしまうとデイバスを保護できません。また、これは多くの場合に当てはまることですが、デバイスが管理対象ではない場合、デバイスは安全ではなく、組織の基準に準拠していないことになります。

ユーザーベースのセキュリティ

このセキュリティ レイヤーは、ユーザーのユーザー名とパスコードをアクセスに使用するデバイスに適用できます。しかし、企業のサービスやリソースにアクセスする管理対象外のデバイスまたはコンピューターが紛失または盗難に遭った場合や、ユーザーの資格情報が悪意の目的で取得された場合は、ネットワーク全体が危険にさらされます。

多要素認証

多要素認証は、ユーザーが複数の検証要素の提示に成功した後に自分のデバイスと企業のリソースにアクセスを認められるセキュリティ レイヤーです。個人を特定できる資格情報の例には次のようなものがあります。

- 知っている情報 (パスワード)
- 所有しているもの (セキュリティ トークン)
- 自己を証明するもの (指紋)

ユーザー名、パスコード、セカンダリ物理認証 (RSA トークンなど) を必須にすることがユーザーを検証する確実な方法のように思われるかもしれませんが、それでもなお、デバイスが提供可能な豊かで複雑なコンテキストを活用できるツールや、一連の広範な使用事例、ユーザー、ユーザーのいる場所を保護する方法が組織には欠落しています。

Tこの物語の教訓は、安全なユーザー認証や物理認証では不十分かもしれないということです。組織にはこれら両方が必須ですが、それ以上に、エンド ユーザー エクスペリエンスを損ねないようにする必要があります。

ID は新たな境界です

Centrify、Duo Security、Microsoft、Ping Identity、Okta、Sailpoint、Salesforce など、ID の管理とサービスへのアクセスをサポートするベンダーが数多く台頭してきています。これらのツールの多くは、Active Directory などの既存の認証インフラストラクチャと連携可能であり、Oauth、SAML、OpenID などのプロトコルでクラウド サービスに ID を拡張できます。

ID はユーザーのすべてのデバイスに共通して使えるものであり、単純なユーザー、デバイスまたはトークンベースのセキュリティに勝るものです。セキュリティ管理プロセスに ID 管理を要素として組み込むことが、モバイルのクラウドコンピュー

ティング世界で安全な環境を構築する鍵となります。

Microsoft コーポレート バイス プレジデントのブラッド・アンダーソン氏 (Brad Anderson) 曰く、「セキュリティ侵害と攻撃は、人知や人の手だけではもはや手に負えない高度な次元と拡散率に達しています」。

> Microsoft Enterprise Mobility + Security: https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security

組織には、ID のリスク、デバイス リスク、アプリケーション リスクの把握を助ける一連の能力が必要であり、最終的には信頼されたユーザーだけが、信頼されたアプリケーションを使って信頼されたデバイス上でデータにアクセスできることを保証することが必要です。

ユーザーが Microsoft Office 365 にアクセスする際、Microsoft は ID を駆使したセキュリティを介して、Azure Active Directory (AD) に対してユーザー資格情報の認証を行います。アンダーソン氏によると、この ID 認証は1 日あたり 150 億回行われています。

世界の 90 % 以上が、企業 ID の信頼されたソースとして Active Directory をオンプレミスで使用しています。クラウドでは、企業 ID の信頼されたソースとして

Azure AD が広く採用されています。Microsoft で構築されているすべてが、Microsoft のクラウドの Azure AD 上に構築されています。

セキュリティ ギャップのソリューション

「Jamf Nation User Conference 2017」にて、アンダーソン氏は先進的なセキュリティのギャップに対応するソリューションについて説明しました。

「Jamf Pro は Azure Active Directory 内で “Microsoft Workplace Join” 機能を使って、企業の会社所有デバイスまたは個人所有デバイスの残りのすべてと一緒に、Jamf に登録された Mac を Azure Active Directory に参加させます。Workplace Join (社内参加) が完了すると、Intune は、Intune に登録されたデバイス上で報告するのと同じ方法で、Workplace Join 上で報告できるようになります」アンダーソン氏は、「つまり、企業が、ユーザーの資格情報だけでなく、Mac の準拠にも基づいて、自社の企業リソースにアクセスを提供できるということです。これは、私たちが条件付きアクセスと称しているものです」、と説明を続けまし。

Apple デバイス管理の標準である Jamf Pro は、EMS 条件付きアクセスを活用してデバイスに対してポリシーを施行し、デバイスが Office 365 にアクセスできるようにします。Jamf で管理された Mac コンピューターは、Microsoft のクラウド内で Workplace Join (社内参加) するために必要な、各組織のニーズに合わせてカスタマイズできる Intune デバイス準拠ポリシーを満たすことを条件に、Microsoft のクラウド内に Workplace を参加させることができるようになります。コンピューターのデータがクラウド内に存在するようになると、Microsoft Intune および Enterprise Mobility + Security (EMS) が Jamf と完全統合してそうしたデバイスを管理できるようになります。

管理対象外の Mac が電子メールまたはその他のクラウドサービスにアクセスを要求する場合、IT 部門は Jamf Pro からユーザーが開始した登録処理を有効にし、アクセス権を付与するまえに安全ではないデバイスや管理対象外のデバイスを管理下に置くことを確実にすることができます。

Intune でパスワード要件などの Mac のポリシーを定義し、IT 部門がそのポリシーをシステム全体に適用することもできます。Jamf と Microsoft の連携は、ローカル ツールへのアクセスに関して、Apple のモバイル デバイス管理 (MDM) フレームワークが許可する範囲を超える働きができるという点において、ユニークです。たとえば、管理者は、パスワードの強度を高めたり検証したりする構成プロファイルを作成できます。これは、組織のポリシーと、Mac の従来の MDM オプションを介してすぐに利用できることとのギャップを埋めます。

Microsoft がユーザーの資格情報を検証し、Jamf がデバイスの資格認証を検証すると、リアルタイムで、ユーザー リスク、デバイス リスク (組織のポリシーに準拠しているか否か) およびアプリケーション リスク (どのアプリが使用されているか) の分析を実行し、クラウド リソースへのアクセスを許可またはブロックするかどうかを判断します。

ユーザーに重点を置くにあたり、多要素認証では不十分な場合、この新しい手法を使って、信頼された ID が準拠デバイス上の認証済みユーザーと一致するよう、ユーザーが情報をやり取りする方法にまで信頼を広げます。

組織は、次の検証済み準拠を介して、多要素認証の拡張機能を取得できるようになりました。1) ユーザー名とパスワード、2) コードとトークン、および 3) デバイス

準拠 — また、組織は、今日のマルチデバイス、マルチロケーション ワーカーが求める適応力のある柔軟な境界を効果的に実現するために、ユーザー、デバイス、使用事例のコンテキ

ストに基づいて、適切なアクセス権を状況に応じて動的に付与できるようになりました。

プロキシを使わない条件付きアクセス

EMS 条件付きアクセスは、この次元のセキュリティと、ID、デバイス、アプリケーションに伴うリスクを自動的に検証する能力を実現するものを現実のものにする鍵となります。

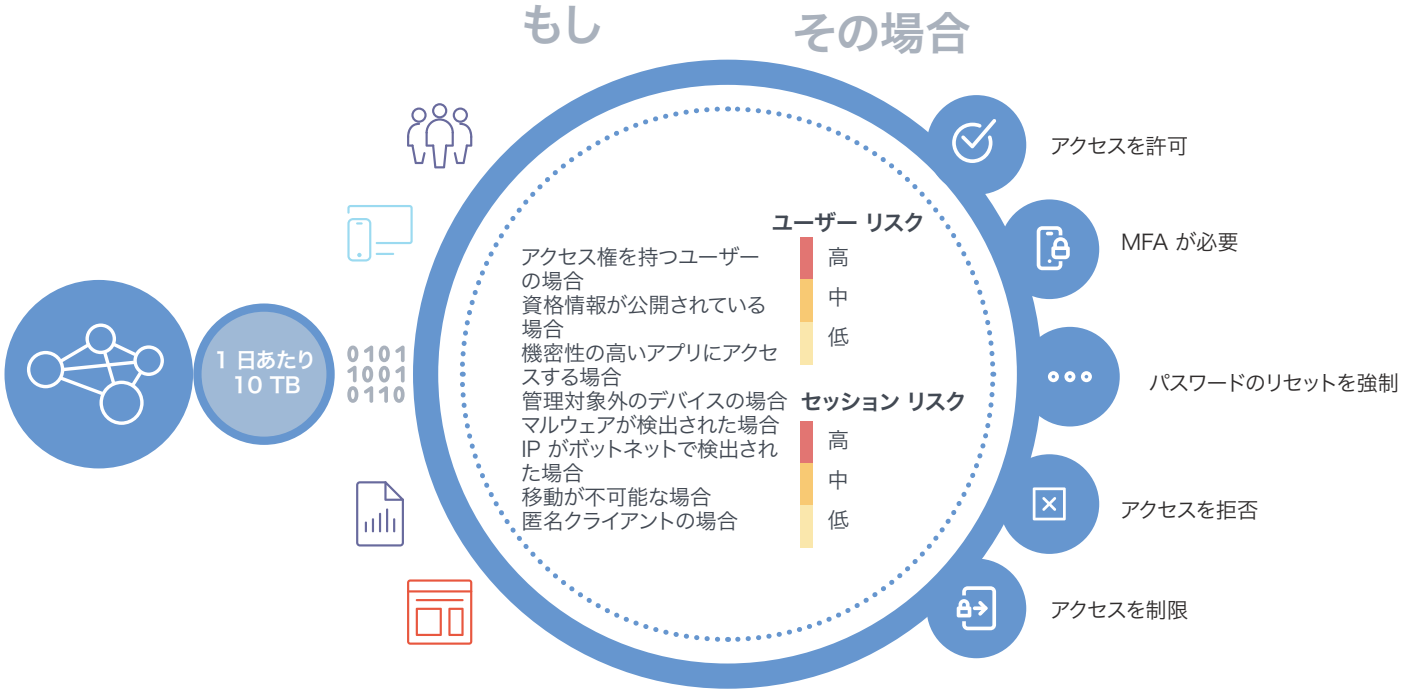
これにより、IT 部門は、ユーザーがリソースにアクセスできる条件を定義するコントロールを与えられます。

多くのエンタープライズ モビリティ管理 (EMM) プロバイダーは、リモート デバイスに資格情報を付与して組織のネットワーク境界内で稼働するリソースに対して認証を行うために、プロキシ サーバー経由で条件付きアクセスをサポートするソリューションを用意しています。プロキシ サーバーは、他のサーバーのリソースを探し求めるユーザーの要求の仲介役として機能するサーバーです。これは、トラフィックがネットワークに出入りできるようにするためです。Jamf と Microsoft の独自の連携の場合、プロキシは必要ありません。パートナーシップにより、すべては、信頼できる唯一の情報源である Azure Active Directory と直接やり取りします。この場合のデバイスの準拠は、各種サービスにアクセスするための前提条件として利用できるようになります。つまり、アクセスを判断、またはネットワーク インフラストラクチャの追加要素として機能するためのネットワーク構成の維持を必要とするプロキシ サーバーなどの仲介役が存在しません。これにより、障害点が 1 つ少なくなると同時に、認証機能を Azure Active Directory と Intune に直接組み込むことでより優れた操作性を実現します。

企業の組織は、Mac の迅速な導入を認めて受け入れてきました。そのため、その他のデバイスと同様に、境界ベースのセキュリティを越えるソリューションを必要としています。分かりやすく言うと、ユーザーを信頼するまえに、まず認証時にユーザーが使用しているデバイスを承認する必要があります。

元々のユーザー エクスペリエンスはそのままに、Jamf と Intune の両方の長所を活かして、それぞれの組織が単独で提供できるものをはるかに超えるソリューションを顧客のために構築するために、Microsoft と Jamf が協力し、認証基盤となる Azure Active Directory と Intune 技術スタックを完全統合する独自のソリューションを構築しました。

MICROSOFT と JAMF のパートナーシップ



EMS 条件付きアクセス

Jamf と Microsoft の EMS パートナーシップは、Azure AD 認証で設定されるアプリケーションにアクセスする Mac コンピューター向けに自動化された準拠管理ソリューションを提供します。この連携では条件付きアクセスを活用し、準拠デバイスの信頼されたユーザーのみが承認されたアプリケーションを使って会社のデータにアクセスできることを確実にします。

Jamf と Microsoft が共同で、不正ユーザーがデバイスを

使って組織が提供する特定のリソースにアクセスできないようにします。これらのデバイスは、個人所有デバイス、管理対象外のデバイス、またはセキュリティ ポリシーに準拠していないため、企業データにアクセスを試みるセキュリティ脅威をより受けやすい管理対象の会社所有デバイスである可能性があります。そのため、Microsoft Office 365 や Azure AD によって検証されたその他のアプリケーションへのアクセス時にユーザーが使用を希望するデバイスの登録を義務付けることでアクセスを制限します。

この処理が、条件付きアクセスを要求する他のベンダーの処理とは違う独自な点は、デバイスがプロキシを通過する必要がないことです。プロキシを回避することで、組織はデバイスを保護するアプローチをより合理化できます。

そしてエンド ユーザー エクスペリエンスはどうなるのでしょうか?有益で容易です。デバイスが準拠していない状態で、ユーザーが認証を行ってアクセス許可を得ようと試みる場合ユーザーは、特定の要件を満たしていない旨を示すメッセージをデバイスで受け取ります。ユーザーは、このメッセージをクリックし、準拠に関する問題を解決するための手順を一通り確認できます。

メッセージは、発生している内容とデバイスが準拠していない理由をユーザーに知らせます。パスワードに関する問題であれば、ユーザーは単に「問題を解決する」をクリックするだけで、パスワードを更新して準拠した状態にすることでアクセス許可を得られます。

Jamf が Microsoft に提供する情報によって、セキュリティがより堅固かつインテリジェントになるため、合理化されたエンド ユーザー エクスペリエンスを可能にするより優れた管理ソリューションを実現します。

アンダーソン氏曰く、「ユーザーに愛され、IT に信頼される」ソリューションです。

先進的で、質を高める安全なエクスペリエンスを実現するために、管理ワークフローは、人々の働き方や働く場所、人々が使用するツールとの整合性を図る必要があります。IT 部門は、保護プロトコルを自然な形で取り入れ、ガイドラインを設定することで、ユーザーが準拠していない状態の場合、会社のデータをリスクにさらさずにユーザーを準拠した状態に戻すシームレスな方法が存在するようにします。

Jamf と Microsoft が共同で、IT 部門が ID ベースのセキュリティを介してこれを実行する権限を付与します。これにより、ユーザーにアクセスを解放しますが、プロキシを通過する必要はありません。

組織は、防御の最前線として、何十年にもわたって自身の会社や利用しているネットワーク境界の周囲に「壁」を構築しましたが、内部セキュリティは後からのちょっとした思いつきにされています。データは進化し、世界は変わり、これらの先進的なソリューションはこうした変化に対処しています。

セキュリティ実践を進化させる方法を見い出し、IT 部門が必要なツールを持ち、ユーザーが選んだデバイスでユーザーの安全性と生産性が維持されるようにしましょう。

より優れたセキュリティはここから始まります

jamf

www.jamf.com

MacとiOS管理に対するJamf Proの作用の詳細については、-
jamf.com/jaをご覧ください。