Duo Security はシスコの一員となりました。

エッセンシャルガイド

企業におけるデバイスの信頼

エンタープライズ IT ネットワークは、ここ数年で大きく変化しています。

企業は、クラウドとモバイルテクノロジーを活用して、デジタル トランスフォーメーションのスピードを早めています。それに伴い IT チームは、コストと生産性を最適化する必要に迫られています。エンタープライズ ネットワークのパラダイムが、従来のオンプレミス環境からハイブリッド IT 環境やマルチクラウド環境にシフトしたことで、組織は、**新しい境界**の保護についての考え方を改めなければなりません。すなわち、ネットワーク中心のセキュリティアーキテクチャから、ユーザ、デバイス、アプリケーション中心のアーキテクチャに移行する必要があるということです。

組織は、通常であれば企業の EMM（エンタープライズモビリティ管理）や MDM（モバイルデバイス管理）ソリューションの管理対象外であるさまざまなユーザ（リモートワーカー、ベンダー、請負業者）とそのデバイスが、ビジネスアプリケーションに安全に直接アクセスできるようにする必要があります。そのため、管理対象デバイス、個人所有デバイス（BYOD）、サードパーティ（請負業者またはパートナー）持ち込みデバイス全体に一貫したセキュリティポリシーを適用することが、セキュリティチームにとって大きな課題となります。IT セキュリティチームには、エンドポイント、特に管理対象外のデバイスに対するアクセス権を決める際に必要な、インサイトと適用メカニズムが欠けています。

デバイスが信頼できるかどうかを判断するために、組織は、アクセスを許可する前に、以下のような重要なポスチャチェックを実施する必要があります。

- デバイスは管理されているか。
- オペレーティングシステム(OS)のバージョンとパッチレベルは最新か。
- エンタープライズウイルス対策（AV）エージェントがインストールされ、実行されているか。
- デバイスがマルウェアに感染していないか。
- ディスク暗号化は有効になっているか。
- デバイスにパスワードは設定されているか。
- モバイルデバイスはルート化またはジェイルブレイクされていないか。

デバイスの信頼を確立する上での課題

あらゆる規模の組織が、企業データにアクセスするエンドポイントの管理に苦労しています。企業の EMM および MDM ソリューションの管理対象外である多数のデバイスによって、セキュリティリスクが増大しています。

Verizon 社の ***2019 年モバイル セキュリティ インデックス*** で調査対象となった企業の 33% が、デバイスベースの侵害を経験し、その大多数が大きな影響を受けたと回答しています。ユーザエクスペリエンスとプライバシーに大きな影響が及ぶ可能性があるため、ユーザは EMM と MDM に登録することに消極的です。IT 部門は、ユーザに登録を強制することはできないものの、アプリケーションへのアクセスを制限することはできます。ただし、それによって生産性が低下する可能性があります。そこで IT 部門は、ユーザエクスペリエンスと生産性に影響を与えないように、デバイスのセキュリティ態勢に基づいてアクセス権を判断するポリシーを設定する必要があります。

デバイスの信頼を確立する上での現在の課題を見てみましょう。

可視性が限られている

組織は、デバイスの管理と保護のためにさまざまなソリューションを導入できますが、オンプレミスおよびクラウドのアプリケーションにアクセスするデバイスをすべて可視化することはまだ困難です。これは、個人、請負業者、パートナーが所有するデバイスなど、IT 部門の管理外のデバイスに特に言えることです。これらのデバイスは、デバイス管理ソリューションに登録されていませんが、Office 365 や Dropbox などのクラウドアプリケーションにはアクセスする必要があります。IT チームには、これらのデバイスを可視化して、データへのアクセスを許可する前に正常性ステータスを確認する方法がありません。そのため、IT 規制に違反し、データ漏えいのリスクが高まる可能性があります。

ポリシーの適用が複雑

管理対象デバイスの場合、ポリシーに準拠させる方法の 1 つは、アクセス権を得るためには更新プログラムを適用しなければならないようにすることです。そうすることでユーザは、更新プログラムをインストールせざるを得なくなります。ただし、ユーザがプロジェクトで作業しているときや、顧客との会議中 / プレゼンテーション中に更新プログラムが強制的に適用されると、ビジネスの生産性とユーザエクスペリエンスの両方が低下します。

管理対象外デバイスの場合、すべてのユーザデバイスにパッチを適用するプロセスは、手動でのフォローアップが必要な場合があるなど、管理者にとって手間のかかる作業です。数ヵ月とは言わなくても、数週間かかることがあります。また、この期間は重大なリスクにさらされます。

アプリケーションにアクセスする重要なタイミングでセキュリティを適用するポイントがないと、管理者は、デバイスのセキュリティ態勢を評価できず、組織のネットワークに脆弱なデバイスがアクセスしてしまう可能性があります。

規制への準拠が困難

規制対象の業種に属している組織は、最新の IT 環境が、HIPAA、PCI-DSS、NIST などの規制要件に準拠していることを確認する必要があります。さらに世界中の政府が、GDPR や CCPA などのデータプライバシー法を導入しているため、組織は、顧客の個人情報 (PII) を保護する責任を負っています。これらのデータセキュリティ規制とデータプライバシー法では、リスクのあるデバイスをブロックし、安全なデバイスのみがデータにアクセスできるように、適切にセキュリティを制御することを求めています。また、要件に準拠していることを証明するために、管理者は、詳細なログ情報にアクセスして、監査証跡やコンプライアンスレポートを作成できる必要があります。

Duo の Device Trust ソリューション

Duo は、デバイスの信頼を確立するための新たな方法をいくつか開発しました。**Duo Device Trust** は、組織がリスクを最小限に抑えるための 3 つの重要な機能を提供しています。企業アプリケーションにアクセスするすべてのデバイスで信頼ステータスを検証し、セキュリティポリシーへの準拠を徹底することで、リスクを抑えられます。

ユーザがアクセスするデバイス

デバイスポスチャのアセスメント

デバイスヘルスチェック

- OS のバージョンとパッチレベル
- ブラウザのバージョン
- ディスクの暗号化
- パスワードおよび生体情報
- ホストファイアウォール (ワークステーション)
- ルート化 / ジェイルブレイク化 (モバイル)

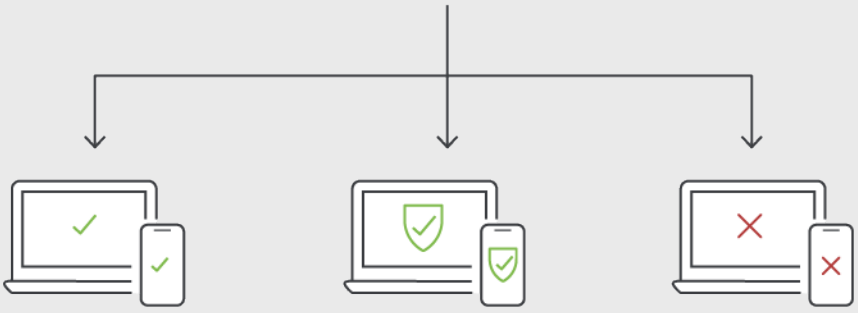
サードパーティのポスチャシグナル

- 管理ステータス
- エンドポイントエージェントの導入状況
- マルウェア感染状況

セキュリティポリシーの適用

ユーザ、デバイス、ロケーションなどのコンテキストに基づいて、アプリケーション固有のアクセスポリシーを設定

デバイスの信頼ステータスに基づいたアクセス制御



管理対象外のデバイスは、コンプライアンスに準拠して安全な場合にアクセスを許可

管理対象デバイスのみが秘密データにアクセスできるように制御

アクセスをブロックし、非準拠デバイスの自己修復を実現

1 デバイスの可視性の向上

デバイスの信頼ステータスを検証してポリシーを適用するには、可視化する必要があります。組織が **Duo** を導入すると、認証ワークフローの一貫として、保護されたアプリケーションのユーザログインプロセス中に、デバイスが信頼できるかどうかが検証されます。これにより Duo は、ユーザがアプリケーションに接続する方法や場所に関係なく、あらゆるデバイスを**詳細に可視化**できます。また、管理者は、デバイス管理システムへの登録ステータスに基づいて、企業が管理するデバイスと BYOD を区別できるようになります。

Duo の**ロギング機能とレポート作成機能**により、組織は、企業リソースにアクセスするすべてのデバイスのインベントリを管理できます。ダッシュボードを利用することで、管理者は、組織全体のセキュリティ態勢を把握できます。数回クリックするだけで簡単にドリルダウンできるため、リスクのあるデバイス(古いバージョンのオペレーティングシステム(OS)、ブラウザ、Flash、Java が実行されている)を使用しているユーザを特定できます。

このデータはすべて、任意のログ管理ツールおよび分析ツールに簡単にエクスポートできます。また、管理者は、レポート作成のスケジュールを設定することで、コンプライアンスを簡単に証明できます。

2 デバイスのセキュリティ態勢の評価

Duo は、エンドポイントの可視化機能を基盤としているため、組織は、企業アプリケーションへのアクセスを許可する前に、デバイスの信頼を簡単に確立できます。管理者は、企業のセキュリティポリシーを適用してコンプライアンスを確保し、準拠していないデバイスは認証時にブロックできます。

たとえば Duo は、アプリケーションへのアクセスを許可する前に、OS のパッチレベルや、パスワード、ファイアウォール、AV エージェント、ディスク暗号化、デバイス管理の各ステータスを確認できます。

デバイスの正常性を評価する Duo のアプローチは、エンタープライズ アプリケーションにアクセスするさまざまなデバイス（管理対象と管理対象外含む）に対応しています。Duo を利用することで、管理者は、さまざまなエンドポイントが企業のセキュリティポリシーに準拠していることを確認でき、エンドユーザは、**自分で修復**できるようになります。これにより、IT チケットの発行数やサポートヘルプデスクへの問い合わせ数が減少します。

vmware

Symantec.

Active Directory

AMP for Endpoints

jamf

Windows Defender

Microsoft Intune

CROWDSTRIKE

mobileiron

3 継続的なリスク評価

ゼロトラストセキュリティの基本理念は、「決して信頼せず、常に検証する (Never Trust, Always Verify)」ことです。Duo ソリューションの基本原則も同じです。Duo を利用すれば、アプリケーションに対する認証要求があるたびにデバイスのセキュリティチェックが実施されるため、組織は、非準拠デバイスがアクセスすることによるリスクを継続的に評価できます。Duo は、アプリケーション アクセス データを分析し、ユーザがアプリケーションにアクセスするために通常使用するデバイスを把握することで、不審なデバイスや通常とは異なるデバイスからのアクセスにフラグを設定します。いつもは既知の個人用デバイスからアプリケーションにアクセスするユーザのクレデンシャルが侵害され、そのアカウントが別のデバイスで使用されて、初めてアプリケーションにアクセスされる状況を考えてみましょう。Duo では、アクセスに最近使用されたデバイスとその相対的なアクセス頻度が表示されるため、このようなセキュリティイベントで該当のデバイスがめったに使用されない、または初めて使用されることがはっきりとわかります。

さらに、Duo を使用することで、IT セキュリティチームは、エンドポイントのセキュリティイベントを効果的にモニタして対応できます。特に、該当のデバイスが企業ネットワーク外にあり、インターネット経由でクラウドアプリケーションに直接アクセスできる場合に有効です。Cisco AMP for Endpoints と Duo を統合することで、組織はポリシーを設定し、マルウェアに感染したデバイスがアプリケーションにアクセスできないように自動的にブロックできます。Duo がブロックするのは感染しているデバイスのみのため、ユーザは、ポリシーに準拠した他のデバイスからログインして生産性を維持できます。

ユーザが自分のデバイスを利用してアプリケーションにアクセス

デバイスで動作する Cisco AMP がマルウェアを検出

感染したデバイスを AMP から Duo に通知

Duo が該当のデバイスによるアプリケーションへのアクセスをブロック

Device Trust の 5 つの主要なユースケース

1

課題

セキュアリモートアクセス機能を統合し、BYOD を可視化して管理する

ソリューション

ネットワーク上のすべてのデバイスを可視化

「KAYAK では BYOD 管理製品に満足していませんでした。また、当社が所有するデバイスと従業員が所有するデバイスでアクセス権を区別できるセキュリティ製品も導入されていませんでした。Duo を使用することで、何百台もの KAYAK 管理ラップトップを明確に識別し、従業員が社内環境に持ち込んだ他の個人所有ラップトップと区別できるようになりました。これらのデバイスの状態をトラッキングして、オペレーティングシステムとブラウザが最新であることも確認できます。1 つの製品だけでこれほどきめ細かいアクセス制御を実現できるのは、素晴らしいことです」

Steve Myers 氏
KAYAK 社 セキュリティ主任

2

課題

ユーザの情報と知的財産を保護する：Lyft 社は、承認された信頼できる個人が、企業が提供したデバイスを使用する場合にのみ秘密データにアクセスできるように、アプリケーションに対するアクセス制御を強化したいと考えていました。

ソリューション

管理されているデバイスだけが秘密性の高いアプリケーションにアクセスできるように制限する

「Duo Beyond は、強力なセキュリティと従業員の利便性を両立できる、数少ないソリューションだと実感しています。Duo Beyond を利用することで、ゼロトラスト戦略をより迅速に進めることができるようになりました。そのため、サポートが困難でコストのかかるクライアントシステム（具体的には ChromeOS）を利用することが可能になり、非常に少ない労力で新しいオンラインサービスを利用できるようにしながら、きめ細かくアクセスを制御できています」

Mike Johnson 氏
Lyft 社 最高情報セキュリティ責任者（CISO）

3

課題

アクセスを許可する前に、サードパーティデバイスのセキュリティ態勢を評価する

ソリューション

管理対象外デバイスによるセキュアアクセスを実現

「シスコには、世界中で 3,000 を超えるアプリケーション、4,000 人のエクストラネットユーザ (パートナー)、15,000 人の請負業者がいます。解決する必要があるセキュリティ上の大きな課題は、アクセスを許可する前に、すべてのデバイスの状態を評価して検証することです。Duo の Device Trust は、未知の世界を可視化することでこの課題を解決します。シスコのセキュリティ基準を満たしていないデバイスにはフラグを付け、ブロックします」

Rich West

シスコ 情報セキュリティ担当プリンシパルエンジニア

4

課題

貴重な知的財産を含む秘密性の高いアプリケーションを保護する: Inductive Automation 社は、すべてのデバイスにセキュリティエージェントをインストールし、ディスクを暗号化する必要がありました。

ソリューション

企業のセキュリティポリシーを適用

「Duo Device Health アプリケーションを利用することで、最も重要な時点、つまり、ユーザが秘密性の高いアプリケーションに接続したときに、企業のポリシーをシームレスに適用できます。社内のアプリケーションに接続するデバイスは、自社所有、最新、暗号化済み、パスワード保護、ファイアウォール適用、自社の AV/EDR を実行済み、という条件を満たしたものに限られています。Device Health アプリケーションを適用ポイントとして利用することで、コンプライアンスに反している可能性のあるアセットを絶えずトラッキングする必要がなくなり、IT チームの負担が軽減されます」

Jason Waits 氏

Inductive Automation 社 サイバーセキュリティリスク責任者

5

課題

医療情報（PHI）を保護し、HIPAA および EPCS のコンプライアンス要件を満たしながら、医師が安全に BYOD を利用できるようにする

ソリューション

コンプライアンス要件への対応

「モバイルデバイスに関するインサイトを得る方法として当社が唯一知っていたのは、モバイルデバイス管理（MDM）ツールをユーザのデバイスに導入することでした。しかしコストと複雑さから、このアイデアは実行したくありませんでした。一方 Duo は、簡単に導入してセキュリティを強化できるツールでした。すべての組織は今すぐ検討すべきです」

Chad Spiers 氏
Sentara 社 情報セキュリティ担当ディレクタ

Duo のメリット

Duo は、強力なセキュリティを提供する低コストのオールインワン ソリューションです。スケーラブルでエンドユーザや管理者が使いやすく、プラットフォームに依存しません。お客様に Duo を推奨する 3 つの主な理由を以下に示します。

非常に広範なカバレッジ

Duo は、現在の市場で最も包括的なユーザ信頼チェック機能とデバイス信頼チェック機能を備えています。これらの機能は、さまざまなユースケースと多様なワークフォースデバイス（管理対象および管理対象外）に対応しています。

使いやすい

Duo を利用すれば、ユーザエクスペリエンスを損なわず、生産性を維持しながらセキュリティを強化できます。ユーザがデバイスを自分で登録したり、修復したりできるため、IT 部門の負担が軽減されます。

総所有コストを削減可能

Duo は、スタンドアロンのセキュリティソリューションとしても利用できますし、**Cisco Secure ポートフォリオ**全体にも統合できるため、お客様は（規模の大小を問わず）、セキュリティベンダーを統合し、自動化してセキュリティ運用を効率化することで、総所有コスト（TCO）を削減できます。

多様なワークフォースがシームレスにデータにアクセスできるようにしながら保護するためには、管理対象デバイスと管理対象外デバイスに一貫してポリシーを適用し、デバイスの信頼性を検証できる機能が不可欠です。組織は、この機能を備えることで、生産性の向上、リスクの軽減、脅威の防止、セキュリティの強化を実現できます。

Duo を無料でお試しください

30 日間の無料トライアルをご利用いただくと、Duo がいかに簡単に導入でき、場所やデバイスに関係なくワークフォースを保護できるかをご自身で確認いただけます。