CISCO
SECURE

ホワイトペーパー
Cisco Public

MFA からゼロトラストへ：

ワークフォースを保護するための 5 段階のプロセス

目次

概要

ゼロトラストは、モビリティ、IT のコンシューマ化、クラウドアプリケーションによってもたらされる変化に対応するための主要なセキュリティモデルとなっています。John Kindervag 氏は、「ゼロトラスト」の原則を「決して信頼せず、常に検証する」と定義しています。1 つの検証ポイント（ファイアウォールやユーザログインなど）を通過した攻撃者は、本質的な信頼を悪用し、ネットワーク、アプリケーション、または環境内を水平移動して機密データを狙い撃つことができます。一旦信頼ゾーン内への侵入を許すと、権限昇格攻撃を実行されてしまいます。そこで、検証を常時行うことで、こうした頻度の高い攻撃を特定して阻止します。

しかし、ゼロトラストという考え方の導入により、新たな課題も生まれました。

本書では、「ワークフォース（あらゆるユーザとデバイス）を対象としたゼロトラスト」を実装するための 5 段階の実践的なアプローチをご紹介します。組織のユーザとそのデバイス、またユーザによるアプリケーションへのアクセス方法について説明します。このアプローチは反復的です。特定のユーザから始め、アプリケーションの対象範囲を拡大し、デバイスの対象範囲を拡大します。この明確に定義された範囲内で常に信頼を検証する体制を整えたら、一連の合理的なポリシーを適用して信頼を確立し、組織を保護します。最後に、この範囲を組織のより広範囲な IT およびセキュリティ業務と統合し、継続的な改善へと移行します。

これらの手順に従うことで、ゼロトラストの変革を段階的に達成できます。

本書では、「*ワークフォース（あらゆるユーザとデバイス）を対象としたゼロトラスト*」を実装するための 5 段階の実践的なアプローチをご紹介します。組織のユーザとそのデバイス、およびユーザによるアプリケーションへのアクセス方法について説明します。

ゼロトラストアプローチ

ゼロトラストの原則は、セキュリティの基本と多くの共通点があります。デフォルトでの拒否と同様に、信頼が実証され確立されるまで、ゼロトラストはアクセス権ゼロで始まります。最小権限の原則と同様に、ゼロトラストは最低限の信頼に依存し、過剰な信頼を極力減らします。ゼロトラストは、次のような概念に基づいて構築されています。

可視性がポリシーに情報を与えます。情報に基づいたポリシーを作成するために、テクノロジーを管理する人々に可能な限り多くのインテリジェンスと洞察を提供します。

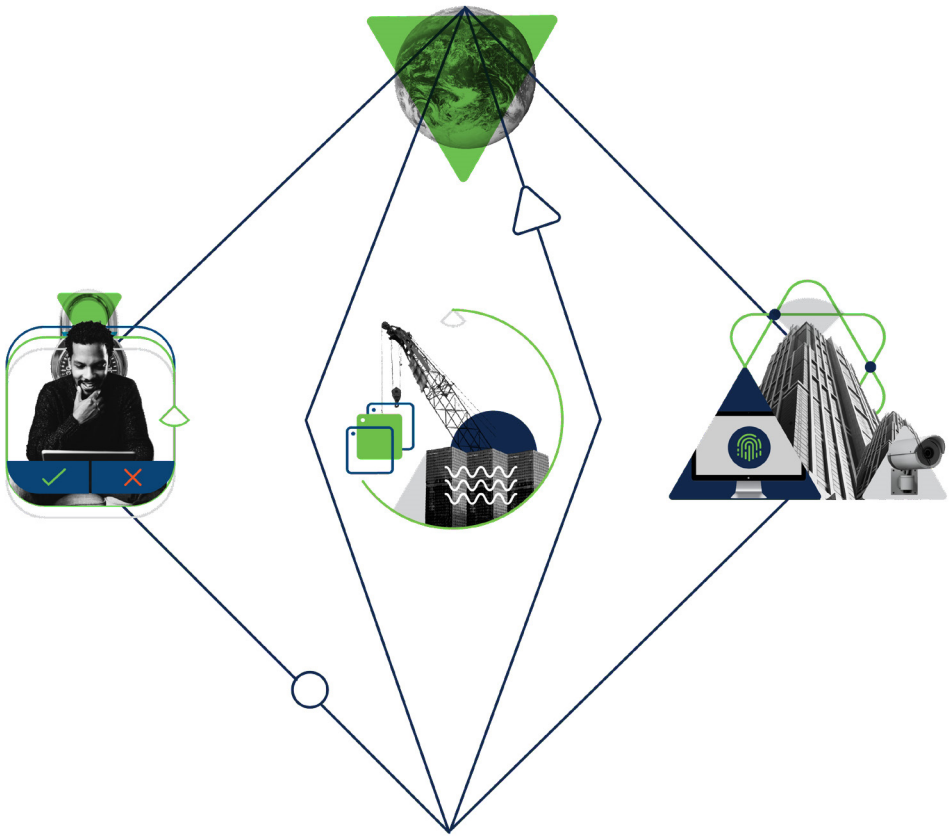
信頼はバイナリでも永続的でもありません。ユーザ、デバイス、アプリケーションのポスチャを継続的に再評価し、それに応じて信頼を調整します。新たに発見された脅威や脆弱性を封じ込めることで、リスクレベルを高めるイベントに対応できるよう準備します。

これは、所有者に基づいた制御ではありません。BYOD（個人所有デバイス持ち込み）や IoT（Internet of Things）デバイスから、SaaS やパブリッククラウドまで、自分が所有または管理していないデバイス、アプリケーション、ネットワークの信頼を検証し、拡大します。

境界とは、アクセス制御の判断を行う任意の場所です。ネットワーク層、アプリケーション層、ID の検証時点、またはトランザクション ワークフローのいずれの段階であっても、環境に適した層と処理ポイントを選択します。

アクセスの判断は、毎回の信頼の再確立に基づきます。あるグループ内のメンバーシップ、ある階層内のアプリケーションサービス、あるネットワークロケーションに接続されたデバイスというだけでは、アクティビティを承認するのに不十分です。

封じ込め。最小権限とセグメンテーションを対応機能と組み合わせて、脅威アクティビティを監視し、デフォルトで脅威の拡散を制限します。



ゼロトラストの 3 つの柱

ワークフォース（あらゆるユーザとデバイス）を対象としたゼロトラスト：従業員、請負業者、パートナー、ベンダーなど、個人所有デバイスまたは企業が管理するデバイスを使用して業務アプリケーションにアクセスするユーザ。この柱は、適切なユーザと安全なデバイスだけがアプリケーションにアクセスできるようにします。

ワークロード（あらゆるアプリケーション）を対象としたゼロトラスト：クラウド、データセンター、および相互にやり取りするその他の仮想化環境で実行されるアプリケーション。この柱は、API、マイクロサービス、またはコンテナがアプリケーション内のデータベースにアクセスする際の、セキュアなアクセスを重視します。

ワークプレイス（あらゆる場所）を対象としたゼロトラスト：この柱は、企業ネットワークに接続するあらゆる機器へのセキュアなアクセスを重視します（ユーザエンドポイント、物理サーバおよび仮想サーバ、プリンタ、カメラ、HVAC システム、キオスク、輸液ポンプ、産業用制御システムなど）。

ワークフォース
（あらゆるユーザとデバイス）

ワークロード
（あらゆるアプリケーション）

ワークプレイス
（あらゆる場所）

このガイドを使用して、ワークフォースを対象としたゼロトラストを実現

本書では、ワークフォースを対象としたゼロトラストを実現するための反復的なアプローチを推奨します。組織の 1 つの側面の範囲を厳密に定め、その範囲に 5 つのフェーズを適用したら、その範囲を組織のゼロトラストアーキテクチャに統合します。このアプローチは、各イニシアチブがより大きな変革の中の自己完結型のプロジェクトであることを意味します。本書を各イニシアチブの範囲内で使用するには、プロセスの各フェーズで次のセクションを活用してください。

説明と目標ゼロトラストへの移行における 5 つのフェーズの概要を、各フェーズを完了するために達成する必要がある目標とともに示します。これらの目標は、組織全体ではなく、ゼロトラストのイニシアチブを対象としています。たとえば、ユーザの信頼とデバイスの信頼を確立することは、ゼロトラストアーキテクチャに移行しようとしている組織内のユーザとデバイスに固有の目標です。

トランスフォーメーション各フェーズを開始する際は、ワークショップを開催し、合意やサポートを得て、次のステップを理解してもらう必要があります。推奨される参加者は、セキュリティ業務、IT 運用およびサポート業務、およびこのイニシアチブの範囲内の事業部門の関係者です。戦略、管理、運用の各分野に即した質問が出されます。1 ～ 5 段階評価でこれらを採点することで、特定のフェーズにおける組織の成熟度を判断できます。

コンポーネントと課題変革を成功させるには、弱点を回避しながらテクノロジーを統合する必要があります。コンポーネントセクションには、ワークフォースを対象としたゼロトラストイニシアチブの、特定のフェーズで推奨されるテクノロジーが記載されています。課題では、よくある懸念事項と考えられる解決策を説明します。

メトリック変革に沿ってアクションを導き、成果を追跡するため、メトリックを実装する必要があります。このセクションでは、リスク管理、セキュリティ、IT サポート、および IT 運用に関するメトリックを示します。特定の範囲の各イニシアチブで、これらのメトリックを活用してフェーズを進めます。範囲を指定したイニシアチブが完了した後も、メトリックを収集し続けることで、ゼロトラストアーキテクチャ全体の有効性を測定できます。

フェーズ 1：ユーザの信頼性を確立

承認されたユーザのみがリソースへのアクセスを試行できるように、適切なメカニズムとプロセスが設けられていることを確認します。これはさまざまな方法で実現できます。多要素認証（MFA）は一般的に使用されるテクノロジーです。新たなオプションとして、パスワードを使用しない、単一の強力な認証要素があります。

説明

境界とは、アクセス制御の判断を行う任意の場所です。ワークフォース（あらゆるユーザとデバイス）を対象としたゼロトラストでは、ユーザがアプリケーションにアクセスすると境界が確立されます。この瞬間は一見シンプルです。クリックしてしばらくすると、アプリケーションが開きます。しかしその間、多くのタスクと検証が実行されています。さらに多くのことが可能です。認証ワークフロー内にあるため、コントロールポイントで信頼を評価して適用できます。ゼロトラストアーキテクチャを確立する最初のステップは、この ID 検証を制御可能にすることです。

権限とは、シスコが？保護する IT を使用してユーザが何をできるかを示します。信頼とは、それらの権限をユーザが適切に使用する、と確信できるかどうかです。最小権限の原則は、必要な権限のみを割り当てることが主眼ですが、ゼロトラストの原則も同様に、必要なユーザのみを信頼することに重点を置きます。

ユーザを信頼する領域と、ユーザが信頼を確立または喪失する可能性のある手段を把握する必要があります。これはユーザのタイプごとにアプローチできます。たとえば、特権アクセスを持つユーザやリモートアクセスを持つユーザなどです。あるいは、アクティビティごとにアプローチすることもできます。たとえば、重要なプロセスや、頻繁に攻撃の対象となるプロセスなどです。ゼロトラストの適用対象を 1 つの領域に絞り込み、関係者とテクノロジーを評価します。

ユーザ信頼の適用範囲を絞り込んだら、3 つのワークストリームが必要になります。1 つ目はセキュリティの強化です。2 つ目はユーザビリティの管理、3 つ目はユーザが順応できるよう、今後の変化を伝えることです。ユーザビリティに関しては、ほとんどの状況で ID 検証を迅速かつ便利に、ほぼ不可視の状態で行う必要があります。ただし、セキュリティ上、疑わしい場合は、ID 検証がアクセスを防止するコントロールポイントを提供します。この 2 つのバランスを取ることが、ユーザの信頼を確立するための成功要因となります。

ゼロトラストアーキテクチャを確立するための最初のステップは、セキュリティシステムがユーザを信頼できるようにすることです。これにはユーザ認証が基礎となります。ユーザ名とパスワードに加えて、二要素認証(2FA)または多要素認証（MFA）により、ユーザが本人であることをより確実に確認できます。ユーザの行動などが原因で信頼が疑われる場合、もしくはある操作により組織がリスクにさらされ、追加の信頼が必要な場合、セキュリティシステムは、ユーザに再認証を要求したり、追加の認証フォームを生成したりできる必要があります。これにより、ゼロトラストアーキテクチャのさまざまな状況で、強力なアイデンティティが確立され、維持されます。

ゼロトラストアーキテクチャを確立するための最初のステップは、セキュリティシステムが**ユーザを信頼できるようにすること**です。

目標

- 役割と情報へのアクセス権ごとにユーザのリスクをランク付けする
- 従業員にとどまらず、請負業者、派遣社員、その他の安全性の低いグループも対象とする
- MFA の使用を拡大する
- 強力な認証用のパスワードレスの使用について評価する
- ゼロトラストアーキテクチャを使用する人数を拡大する
- すべてのユーザが継続的に検証されるようにする

トランスフォーメーション

戦略面

ここでの目標は、組織の方向性が確立されているか、広範な議論ができる可能性があるかどうかを判断することです。

組織に明確なアイデンティティ戦略はあるか。

- 明確なビジョンと方向性があるかどうか、この戦略の責任者は誰か、組織内でどのように管理されているかを判断する
- 組織にとって明確になるように、または容易に理解できるように戦略を公開する
- 戦略の範囲と、サードパーティ、パートナー、クラウドプロバイダーなどの外部リソースの使用を対象とするかどうかを決定する
- 戦略は効果的で、明確な測定値が提供されているか
- 変更と改善をどのような方法で測定し、特定して実装しているか

管理

組織の ID 管理とアクセス管理（IAM）要件がどの程度理解され、日常的に管理されているかを明らかにすることが目標です。

明確に定義された IAM 業務はあるか。

- 組織の IAM 要件を管理する正式なグループはあるか
- 使用している IAM システムのセキュリティレベルはどの程度か
- 社員のユーザ、移動を伴うユーザ、退職するユーザの完全な一貫性を確保するために、ビジネスの他の側面とどのように整合させているか
- IAM 業務から提出されるレポートはどの程度明確か
- 実装された変更の速度と一貫性を確認し、ビジネスの変更に見合っているかどうかを判断する

MFA プログラムの実装の進捗状況を特定することが目標です。これにより、IAM 業務から切り離された ID が保証されます。

MFA ソリューションは実装されているか。

- ソリューションが特定され、実装されているか
- そのソリューションは IAM 戦略にどの程度統合されているか
- MFA ソリューションはどの程度 IAM に統合されているか
- 実装に関して明確なフィードバックとレポートが提供されているか

運用

ユーザベース全体でソリューションが実装されている範囲を特定することが目標です。

何割程度のユーザが MFA を使用しているか。

- ソリューションは実装されているか
- 登録ユーザ数を示す明確なメトリックはあるか
- ユーザベースに関して信頼できるメトリックはあるか
- ユーザ、グループ、またはビジネス領域ごとに実装を細分化するメトリックはあるか
- 完全な導入が実施され、測定され、監視されるように計画する

MFA は他の業務に統合されているか。

- ソリューションは実装されているか
- 特にセキュリティと IT について、MFA 機能の恩恵を受ける可能性がある領域を特定する
- MFA ソリューションからどのような成果が得られているか
- どのような方法で成果を他の業務と共有したり、自動化したりしているか
- MFA ソリューションが他の業務をどのように改善するかを示すメリットステートメントを作成する

コンポーネント

ID データベース。ユーザに関する情報と属性を保持し、組織、地理、またはその他の側面に従って、必要に応じてそれらをグループ化します。これは通常、**アイデンティティ プロバイダー (IdP)** サービスによって提供されます。

強力な認証。2FA または MFA は、アカウント侵害を困難にする戦略にとって不可欠です。さらに、MFA チャレンジを完了するよう要求することは、信頼を再確認する手段となります。

課題

エンドユーザは変更を非常にためらう傾向があります。エンドユーザは、過去のセキュリティ変更により作業が困難になったため、将来の変更に抵抗を感じているのです。ゼロトラストへの道のりでは、変化の必要性を伝え、浸透させると同時に、人々への影響を最小限に抑える必要があります。

シスコはリモートアクセスの保護に重点を置いています。リモートアクセスは、ゼロトラストイニシアチブの論理的な出発点です。クラウドに移行するアプリケーションが増加するにつれ、リモートの定義が拡大し、境界が曖昧になります。リモートアクセスで勢いをつけ、進化したワークフローに進みましょう。

組織全体でワークフローを中断することはできません。組織の業務を停止することは、セキュリティイニシアチブの歩みを止めること以外の何物でもありません。慎重に計画し、テストし、使いやすさを重視しながら、一度に 1 つのワークフローでゼロトラストを実現していきましょう。

メトリクス

リスク

- 全体的なリスクレベル
- リスク登録 : 問題の軽減
- コンプライアンスの監査 : 問題の軽減

セキュリティ

- インシデントの削減率
- アカウント乗っ取り (ATO)
- ビジネスメールの侵害 (BEC)

サポート

- FTE の使用
- ユーザ MFA サポートチケット
- ユーザ MFA サポート満足度 (NPS)

運用

- MFA で設定されたアプリケーション
- MFA に登録されているユーザ数

フェーズ 2：デバイスとアクティビティの可視性

それぞれのアクセス要求で使用されているエンドポイント / デバイスはどれか。現在のセキュリティ状態はどうか、また、要求の送信元はどこか。これは、アカウント乗っ取りの試みなどのリスクを検出するための重要な段階です。

説明

ワークフォース（あらゆるユーザとデバイス）を対象としたゼロトラストの実装は、検証済みユーザと、使用する検証済みエンドポイントデバイスの組み合わせが基礎になります。最初のフェーズでは、ゼロトラストアーキテクチャの範囲内にいるユーザを拡大し、それらのユーザの信頼性を検証する手段を深めることに重点が置かれます。第 2 フェーズでは、対象範囲内のデバイスとアプリケーションの拡大に重点が移ります。これにより、アプリケーションにアクセスするデバイスにおけるユーザのワークフローを可視化できます。このワークフローは、今後の基盤となります。

アクセスの決定は、ユーザがアクティビティを実行するたびに信頼を再確立することに基づいています。アクティビティとは、組織の業務をサポートするために行われる、特定のユーザグループによる一連のアプリケーションの使用です。ここでは、以前に定義した範囲に焦点を当てます。まず、ターゲットユーザが使用するアプリケーションのインベントリ作成、リスクランク付け、優先順位付けを行います。アプリケーションをゼロトラストアーキテクチャに移行するには、次の 3 つの条件を満たす必要があります。強力な認証を統合すること（通常は Radius、SAML または AD FS を使用）、アプリケーションにどこからでもアクセスできるようにすること（通常はネットワークゲートウェイまたは VPN を使用）、アプリケーションの起動方法を統一すること(通常はシングルサインオンポータルを使用）です。多くの場合、組織には数百または数千のアプリケーションが存在し、アクティビティは時間の経過とともに変化するため、アプリケーションを特定してゼロトラストアーキテクチャと統合するプロセスは継続的なものになります。

アクティビティは、デバイス上で検証されたユーザによって実行されます。ゼロトラストでは、デバイスは認証デバイスとアクセスデバイスの 2 つのカテゴリに分類されます。認証デバイスとは、信頼を確立して維持するために、エンドユーザが強力な認証を実行するために使用するデバイスです。アクセスデバイスとは、エンドユーザがアプリケーションを起動して操作するデバイスです。ユーザは多くの場合、組織所有のデバイスや個人所有のデバイスなど、多数のデバイスを使用して作業を実行します。犯罪者は、デバイスのセキュリティの脆弱性を悪用して、デバイスを盾に取り見返りを要求したり、機密データにアクセスしたり、組織を混乱させたりする可能性があります。ゼロトラスト セキュリティ システムでは、次のようないくつかの指標によりデバイスの信頼性を評価できます。

- **このデバイスは以前からあったか**
- **デバイスのオペレーティングシステムとソフトウェアは最新か**
- **改ざんの兆候はあるか**

このフェーズの目標は、これらのデバイスと、デバイスに関連付けられたこれらの信頼要因を可視化することです。

ゼロトラストアーキテクチャを確立する第 2 のステップは、アプリケーションを認証してアクセスするデバイスを、セキュリティシステムが信頼することです。まず、アプリケーションとデバイスのインベントリ作成と優先順位付けを行います。セキュリティの目標は境界を確立することであり、境界とは、セキュリティシステムが特定のアプリケーションのユーザに関するアクセス制御を決定する場所を指します。つまり、継続的なワークストリームの 1 つは、アプリケーションをゼロトラスト認証およびアクセス制御と統合することです。境界が上手く機能するかどうかは、それが実行されているハードウェアによって決まります。また、アクセスデバイスと認証デバイス、およびそれに伴うセキュリティポスチャの可視性を向上させることも、継続的なワークストリームです。これによりデバイスとアクティビティのポートフォリオが構築され、これらを後でゼロトラストアーキテクチャで使用して、ポリシーと適用の判断を行うことができます。

目標

- アプリケーションのリスクランク付けと優先順位付け
- 使用中のデバイスとアプリケーションを可視化
- オンプレミスのアプリケーションを超えて、クラウドアプリケーションの保護を実現
- ゼロトラストアーキテクチャのアプリケーションを拡張
- すべてのアプリケーションへのアクセスを継続的に検証

トランスフォーメーション

戦略面

管理対象と対象外のデバイスにおいて、デバイスの可視性をもたらす明確な戦略があるかどうかを確認することが目標です。

管理対象と対象外のデバイスの間に明確な区別はあるか。

- 非企業デバイスを使用したリソースへのアクセスに関するポリシーや指針があるかどうかを確認する
- リソースと資産に異なるリスクレベルが割り当てられていて、個別のアクセスポリシーを作成できるかどうかを確認する

管理

デバイスインベントリとデバイスステータスが運用上どの程度理解され、管理されているかを明らかにすることが目標です。

ユーザがアプリケーションへのアクセスを完全に制御できるか。

- アプリケーションの明確なインベントリがあるかどうかを確認する
- アプリケーションは侵害のリスクレベルについて評価されているか
- 内部ユーザと外部ユーザの範囲について明確な区別があるか
- アプリケーションへの外部アクセスを制御し、他の資産の使用を明確に制限するポリシーが設定されているか
- ポリシー更新プロセスを管理するガバナンスプロセスはあるか

デバイスインベントリは最新で、定期的にレビューされているか。

- 資産インベントリの所有者とそのメンテナンスの責任者を特定する
- インベントリはどのような方法で更新しているか
- アクセスポイントでのデバイス ID の使用が実装されているかどうかを確認する
- アクセスポイントでのデバイス ID は資産インベントリにリンクされているか
- インベントリステータスとアクセス制御の間で、継続的なフィードバックとレビューが行われているか

デバイスの健全性チェックは実施されているか。

- デバイスの健全性状態を確認するソリューションが実施されているかどうかを判断する
- ソリューションは組織内でどの程度まで実装されているか
- ソリューションは他のセキュリティおよび IT 業務と統合されているか
- 進捗状況が明確に測定され、報告されているか
- ソリューションを管理するガバナンスプロセスはあるか

運用

ソリューションがユーザベース全体でどの程度実装されているか、およびそれが他のセキュリティ業務にどの程度効果的に貢献しているかを確認することが目標です。

管理対象と対象外のアプリケーションの割合はどのくらいか。

- クラウドベースおよびネットワークベースのアプリケーションの明確なインベントリがあるかどうかを判断する
- セキュリティソリューションやアプリケーションとの統合があるかどうかを判断する
- すべてのアプリケーションがエンドユーザに同様の方法で表示されるかどうかを確認する
- ユーザの期待と承認評価の測定値があるかどうかを確認する
- 改善点と例外が明確な所有者に報告されているかどうかを確認する

管理対象と対象外のデバイスの割合はどのくらいか。

- 管理対象と対象外のデバイスを特定するプロセスが明確に定義されているかどうかを判断する
- デバイスのインベントリが一元化されているかどうかを判断する
- インベントリを定期的にメンテナンスするプロセスはあるか
- デバイスのレポートを確認する
- レポートは監査、もしくは検証されているか

デバイスの可視性は他の業務に統合されているか。

- デバイスを可視化するソリューションが実装されているかどうかを判断する
- デバイスの可視性を活用できる、特にセキュリティと IT の領域を特定する
- そのようなソリューションからどのような成果が得られているか
- どのような方法で成果を他の業務と共有したり自動化したりしているか
- デバイスの可視性強化により他の業務がどのように改善するかを示す、メリットステートメントを作成する

コンポーネント

アプリケーション インベントリ データベースタイプ、目的、リスクランク、アプリケーション所有者など、最新のリポジトリに保持されているアプリケーションとアクティビティのリスト。

アクセスプロキシこのサービスは、接続とポリシー適用を実行します。より複雑なアクセスプロキシでは、トラフィック ロード バランシング、Transport Layer Security (TLS)、認証、アクセスコントロールリスト (ACL) の評価、認可およびユーザ向けセルフサービスを提供できます。

シングルサインオン (SSO) すべてのアプリケーションとシステムにアクセスできる 1 つのポータルを提供することで、操作が大幅に容易になります。

課題

すべてのアプリケーションとデバイスをカバーするにはリソースが足りません。多くのチームは余力がなく、アプリケーションやデバイスが増えることで管理の負担も増大する可能性があります。幸いなことに、これはすべてか無かという問題ではありません。拡張性があり、運用が容易なゼロトラストアプローチを選択しましょう。優先順位を付けた体系的な方法で、対象範囲を着実に拡張します。

コンプライアンスのためにアプリケーションで必要なのは 2FA のみです。ミッション完了です。ゼロトラストの最初のビジネスケースにコンプライアンスが含まれる場合、これらの要件が満たされると、イニシアチブが停滞する可能性があります。新しい各アプリケーションワークフローを使用して、ゼロトラストに対する組織のコミットメントを再確立します。

メトリック

リスク :

アプリケーションリスクの軽減 : コアアプリケーション

セキュリティ :

管理対象外アプリ

管理対象外のデバイス

サポート :

アプリケーション統合 MFA サポートチケット

アプリケーション統合 MFA サポート満足度 (NPS)

運用 :

MFA で設定されたコアアプリケーション

SSO で設定されたコアアプリケーション

認証デバイス : 既知のデバイス

フェーズ 3：デバイスの信頼

企業所有のデバイスかどうか、管理対象のデバイスかどうかを問わず、組織は、登録済みのデバイスを信頼できるデバイスとしてマークし、特定のユーザと関連付けられていると想定します。

説明

ゼロトラスト以前の従来の環境では、デバイスの信頼は場所に基づく傾向がありました。デバイスが企業ネットワーク上にあれば、そこにあるべきデバイスだと考え、すべての要求に対してアクセス権が与えられました。これらの「テスト」はいずれも、パスワードの盗難からネットワークアドレスの偽装、エンドポイントの侵害まで、さまざまな理由で失敗しました。ゼロトラストアーキテクチャでは、デバイスへの認証要素や条件など、信頼を得るまでにより多くのチェックポイントが必要になります。これらの条件の 1 つは、管理対象の企業所有のエンドポイントであるかどうかです。

管理対象エンドポイントは、組織が所有しているか、少なくとも組織が把握しているものと推定されます。前のフェーズでのデバイスの可視性により、エンドポイントの数が明らかになります。管理対象デバイスは、インベントリの一部として追跡され、設定およびパッチ管理プログラムに登録され、セキュリティイベントが監視されます。そのため、管理されていない個人のデバイス以上に、信頼できるデバイスとして選択されるようになります。多くの組織では、ビジネスデータにアクセスできるのは、自社が所有し、スタッフに割り当てたエンドポイントに限定するというポリシーを定めています。しかしながら、チェック手段がない場合は特に、このポリシーを適用することが難しいことがあります。

デバイスを管理する方法はいくつかあります。エンドポイントに VPN クライアントがインストールされている場合、そのエンドポイントは承認および管理対象の資産であると見なされます。そのため、そのエンドポイントを使用しているユーザは誰でも、外部（自宅、ホテル、コーヒーショップなど）から内部ネットワークにアクセスできます。共通のポートベースのネットワーク アクセス コントロール（NAC）では、エンドポイントに 802.1x 証明書がインストールされている場合、そのエンドポイントは承認および管理対象の資産であると見なされます。そのため、そのエンドポイントを使用するユーザは誰でも、建物内から内部ネットワークに接続できます。最後に、モバイルデバイス管理(MDM) システムにデバイスを登録すると、エージェントをインストールすることで設定ポリシーを適用できます。

上記のいずれの場合も、エンドポイントに何かをインストールする（または 2 番目の要素を考慮すれば、「何かを持たせる」）ことで、エンドポイントを信頼できるものとしてマークしました。エンドポイントを管理できない場合、そのエンドポイントの所有者に何かをインストールするように説得するのは一般的に困難です。証明書またはその他のフィンガープリント手法は軽量であり、実行するソフトウェアをインストールするよりも受け入れられやすくなります。ただし、重要な要件は、そのマーキングを偽造できないようにすることと、別のデバイスにコピーされないようにすることです。重要な点は、以前に確認済みのデバイスにアクセス権を付与することです。未確認の、攻撃者によって使用されている可能性のあるアプリケーションにエンドポイントがアクセスしようとしているのとは異なります。

マーキングの有無に基づいて信頼を判断することから、これはもう 1 つの認証要素として機能します。ユーザのプライマリクレデンシャル（ユーザ名とパスワード）と 2 番目の要素（ワンタイムパスワード、U2F デバイス、プッシュベース認証など）を保護する必要があるのと同様に、これらも保護しなければなりません。証明書は、デバイスを管理対象として識別する手段になります。さらなる対策として、証明書にデバイスとユーザのデータを含め、それらを結び付けることで、どのクレデンシャルも単独で利用できないようにすることも可能です。

その結果、信頼を確立するためのテレメトリを提供する、さまざまなデバイス管理オプションが得られます。組織が提供する完全に管理されたデバイスを使用でき、あらゆるエージェントを活用してすべてのアプリケーションや操作を可視化できます。従来の BYOD モデルでも、個人所有デバイスで MDM などの単一のエージェントを実行し、明確に定義された領域を可視化して制御できます。また、Cookie や証明書などの軽量のコントロールを使用して、Web ブラウザのユーザエージェントや認証時のユーザのヒントから利用できる情報を、可視化できます。デバイスをポートフォリオとして管理し、特定のアクティビティを実行するための特定のレベルで信頼を持たせることで、管理およびサポートコストを簡素化できます。

このフェーズの目標は、デバイスの制御と、デバイス管理テレメトリに基づいて利用可能な信頼要素を確立することです。

防御の観点から、ユーザが攻撃者にクレデンシャルを奪われた場合を考えてみましょう。デバイスの信頼を設定している場合、攻撃者がアプリケーションにアクセスするには、そのユーザに属する有効なエンドポイントを使用する必要があります。別の社内デバイスでユーザ名とパスワードを取得するだけでは不十分です。適切なユーザがいる場合にのみデバイスを信頼することは、ゼロトラストアーキテクチャによって可能になる、より強固なセキュリティを実現するための次のステップです。

目標

- デバイスのリスクランク付けと優先順位付け
- 組織所有のデバイスだけでなく BYOD も含める
- MDM や VPN など、デバイスを信頼するためのテクノロジーのポートフォリオを確立する
- ゼロトラストアーキテクチャにおける信頼できるエンドユーザデバイスを拡張する
- すべてのアクセスおよび認証デバイスが継続的に検証されるようにする

トランスフォーメーション

戦略面

アクセスポイントにおけるデバイスのポリシー主導の評価に関して、明確な戦略があるかどうかを確認することが目標です。

信頼できるデバイスに関する既存の戦略はあるか。

- 信頼できるデバイスの評価と制御に関する戦略またはプログラムがあるかどうかを確認する
- 企業所有デバイスと個人所有デバイスを管理するためのアプローチを確立する
- エンドポイントデバイスに付与する信頼レベルを特定するために、リスクベースのポリシーが適用されているかどうかを確認する

管理

ユーザデバイスのポリシー主導の評価が、どの程度適切に更新、レビュー、適用されているかを明らかにすることが目標です。

ポリシーは既知の脆弱性に対して常にレビューされているか。

- ポリシーが設定されている場合、それらのポリシーの責任者は明確に任命されているか
- ポリシーの作成と脆弱性の識別の間に関連性があるかどうかを確認する
- ポリシーの修正が脆弱性の識別に基づいていることを確認する
- ポリシーの修正がどこで追跡および記録されているかを特定する
- ポリシーの更新によって資産インベントリがどのように修正されるかを特定する

ログイン段階でデバイスは常にチェックされているか。

- ログイン段階でポリシーステータスをチェックするソリューションがあるかどうかを判断する
- 組織内でどの程度までソリューションが実装されているか
- ソリューションが他のセキュリティおよび IT 業務と統合されているかどうかを判断する
- 進捗状況が明確に測定され、報告されているかどうかを判断する
- ソリューションを管理するガバナンスプロセスがあるかどうかを判断する

運用

エンドユーザがデバイスの更新に関与できるようなソリューションがどの程度実装されているか、およびそれが他のセキュリティ業務にどの程度効果的に貢献しているかを特定することが目標です。

アクセス権を維持するため、ユーザにデバイスの更新を求めているか。

- ポリシーの非準拠を特定するプロセスが明確に定義されているかどうかを判断する
- ポリシーの非準拠がエンドユーザに通知されているかどうかを判断する
- ポリシーに準拠させるためにユーザにデバイスの更新を案内しているかどうかを確認する
- ポリシーの非準拠がユーザから報告されているかどうかを判断する

デバイスの信頼性は他の業務に統合されているか。

- デバイスに対するポリシー制御を提供するソリューションが実装されているかどうかを判断する
- デバイスの信頼性から利益を得ることができる、特にセキュリティと IT の領域を特定する
- そのようなソリューションからどのような成果が得られているか
- どのような方法で成果を他の業務と共有したり自動化したりしているか
- デバイスの信頼性強化により他の業務がどのように改善するかを示す、メリットステートメントを作成する

コンポーネント

デバイス インベントリ データベースタイプ、目的、ネットワークアドレス、資産タグ、コンポーネント、設定、責任者または保守担当者を含む、ネットワークへのアクセスを許可するすべてのデバイスに関する情報の最新リポジトリ。

管理デバイスさまざまなツールセットとアプローチを実装します。企業所有デバイスには、Endpoint Detection and Response（EDR）を含む多数のエージェントを搭載できます。BYOD にはモバイルデバイス管理（MDM）を搭載できます。信頼できるが完全に管理されていないその他のデバイスについては、デバイスの信頼性と健全性を評価します。

証明書発行者管理対象デバイスまたは承認済みデバイスに、クライアント側の証明書を使用してマークを付けるために使用されます。使用する証明書のタイプによっては、この証明書の公開キーインフラストラクチャ（PKI）がすでに別のセキュリティ製品に含まれている場合があります。

課題

エンドユーザは、デバイスにソフトウェアをインストールすることに抵抗を感じます。プライバシーに関する懸念から地域の規制まで、さまざまな理由により、ユーザはスマートフォンやデバイスにエージェントをインストールしたくないと考えます。プライバシーの問題を発生させることなく、認証時にセキュリティの健全性と有効なセキュリティ機能を検証するテクノロジーを選択しましょう。

すべてのデバイスを管理するにはリソースが足りません。多くの場合、デバイス管理には時間がかかります。ゼロトラストアーキテクチャでは、アクセスデバイスと認証デバイスの信頼評価が優先されます。拡張性に優れた簡単な方法で、対象範囲を着実に拡大できます。

すでにモバイルデバイス管理（MDM）プラットフォームがあります。デバイス管理用のフル機能のプラットフォームがすでに導入されている場合もあります。MDM や VPN など、デバイスを信頼するためのテクノロジーのポートフォリオを、ゼロトラストアーキテクチャの確立に使用できる可能性があります。すでに行っている投資を活用するところから始めましょう。

メトリクス

リスク：

- アプリケーションリスクの軽減:重要なアプリケーション

セキュリティ：

- インシデントの削減率
  - デバイスに対するセキュリティ侵害
- 認証デバイス：脆弱なデバイス
- アクセスデバイス：脆弱なデバイス

サポート：

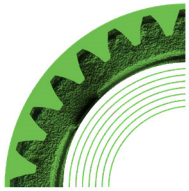
- デバイス MFA サポートチケット
- デバイス MFA サポート満足度（NPS）

運用：

- MFA で設定された重要なアプリケーション
- SSO で設定された重要なアプリケーション
- アクセスデバイス：信頼できるデバイス

フェーズ 4：適応型ポリシー

リソースの機密性と既知のセキュリティ状態に基づいてアクセス要件を実装し、リスクレベルを適切に管理します。これらのポリシーには、企業が管理するデバイスのみを許可するものから、パッチを適用した特定バージョンのソフトウェアを要求するもの、暗号化、またはユーザの動作に基づくステップアップ認証まで、さまざまなものがあります。



説明

最も重要なデータやアプリケーションにアクセスするために、既知の承認済みエンドポイントを使用することを要求するポリシーを設定できます（たとえば、特権ユーザは企業所有デバイスを使用しなければならないなど）。アクセスプロキシは、従来の境界の外部にあるか内部にあるかに関係なく、企業リソースへのアクセスを適用する役割を果たします。適用戦略は、リスク許容度を表す 1 つの方法です。これらのポリシーの適切な規模は、機密性、脅威、ユーザコミュニティ、規制要件、およびその他の考慮事項などの要因によって変わります。

従来のネットワーク境界セキュリティモデルの主な欠点は、組織内のすべての場所で信頼レベルを 1 つしか設定しない傾向があることでした。異なる階層で構築するにはネットワークのセグメンテーションが必要ですが、それは多くの場合実装するには複雑すぎました。ゼロトラストアプローチは、アプリケーションレイヤで信頼レベルを区別します。そのため、この段階的アプローチでは、重要かつ機密性の高いデータやアプリケーションがどこにあるかを早期に判断することが重要になります。これらにアクセスするには、ユーザとデバイスにより高いレベルの信頼が必要になります。つまり、より多くのテストに合格し、より厳しい要件に準拠する必要があります。

まず、アクセス対象に関係なく、すべてのユーザとすべてのデバイスの基本となる信頼レベルを設定し、さらに信頼レベルを追加していくことで、重要度の高い階層へのアクセスに必要なリスク管理レベルを実現します。ユーザの信頼レベルは、そのユーザを初めて確認したかどうか、ユーザ認証にどのような要素を使用したか、偽装または悪意のあるアクティビティの兆候があるかどうかによって判断できます。デバイスの信頼レベルは、そのデバイスを初めて確認したかどうか、管理されているかどうか、最新のオペレーティングシステムと Web ブラウザを実行しているか、画面ロックや暗号化などのセキュリティ機能が有効になっているか、感染や改ざんの兆候があるかどうかによって判断できます。ゼロ トラスト アクセス ポリシーは、この情報を使用して、アクセスを許可する、アクセスを許可するが修復を促す、信頼を改善するために修復を要求する、もしくは信頼できないものとしてアクセスを完全にブロックするように、柔軟に対処できなければなりません。

最も重要なことは、許可したくないデバイス、ソフトウェア、ソース、動作を区別し、それにより攻撃の危険性を減らすことです。組織のセキュリティ体制を変えるには献身的な作業が必要ですが、ユーザ、デバイス、アプリケーションなど、それぞれにふさわしい制御を適用することで、現在の伝統的なセキュリティの枠組みにおけるギャップに対処し、さらにその先へと進むことができます。

目標

- リスク許容度を表す適用戦略を確立する
- 信頼指標に基づいて認証ワークフローにポリシーを適用する
- 継続的に検証されているユーザとデバイスに対応する

トランスフォーメーション

戦略面

資産と、組織内の資産へのアクセスを制御するユーザに基づいて、ポリシーに関する明確な戦略を特定し、確立することが目標です。

デバイスとユーザの信頼に基づいてユーザのアクセスを制御するポリシーが実装されているか。

- 資産へのアクセスを、ユーザとデバイスの文脈から導き出されたリスクベースの判断に基づくポリシーによって制御するための明確な戦略があるか
- そのような戦略の所有者と責任者を特定する
- これらのポリシーが組織で適用されているかどうかを確認する

管理

適応型のポリシー主導型アプローチがどの程度管理され、更新されているか明らかにすることが目標です。

ユーザはポリシーに従って一貫して管理されているか。

- ポリシーが設定されている場合、それらのポリシーの責任者は明確に任命されているか
- ポリシー制御が明確に定義されていることを確認する
- ポリシーが実装されているプロセスを特定する
- ポリシーの実装に関する測定値を特定する

ユーザ権限を更新するプロセスはあるか。

- ポリシーの作成と、デバイスおよびユーザを管理するポリシーの間に関連性があるかどうかを確認する
- デバイスおよびユーザポリシーの変更が、資産へのアクセス制御に反映されるようにするための明確なポリシーセットがあるか
- 資産、特にアプリケーションに関するリスク評価の結果が、ポリシー更新プロセスに関連しているかどうかを判断する
- ポリシーの更新は明確に測定され、報告されているか
- ポリシー更新プロセスを管理するガバナンスプロセスはあるか

運用

デバイスとユーザに対する可視性、および例外を管理するプロセスがあるかどうかを確認することが目標です。

ポリシーに違反するユーザとデバイスが特定され、報告されているか。

- ユーザとデバイスの両方のポリシー非準拠を特定するプロセスが明確に定義されているかどうかを判断する
- 非準拠に関して明確な報告が行われているかどうかを判断する
- ポリシー更新プロセスで例外レポートを考慮しているかどうかを確認する
- 例外レポートと必要なアクションの明確な所有者が設定されているかどうかを確認する
- 例外が他の IT およびセキュリティ業務に報告されているかどうかを特定する

ポリシーに違反するユーザを管理するための例外ワークフローはあるか。

- 例外が認識され、対処されているかどうかを判断する
- 結果が運用上のアクションにどのように統合されているかを特定する
- その統合は自動化されているか、手動で行われているか
- プロセスは測定され、報告されているか
- プロセスとその継続的な開発の明確な所有者が設定されているか

コンポーネント

アクセス制御エンジン「このユーザグループのみが、最新の割り当て済みの管理対象デバイスとともに、この機密アプリケーションを使用できる」など、すべてのアクセスポリシーのリポジトリ。

信頼の推論特定のデバイスに信頼を置く条件、または信頼を失う条件（ハードウェアの変更など）を決定します。信頼の推論は、選択したソースからのデータの安定した入力に依存します。たとえば、デバイスが暗号化されているか、すべての管理エージェントが動作しているか、ソフトウェアが最新か、デバイスに関するすべての情報が最新かを確認することなどが含まれます。

課題

組織全体でユーザをブロックすることはできません。組織の業務を停止することは、セキュリティイニシアチブの歩みを止めること以外の何物でもありません。ポリシーはまず小さな規模から始め、適切な結果を得るためにポリシーのモデリングとテストを行います。

リスク管理は明確に定義されておらず、リスク許容度についても合意していません。リスク軽減について広範囲に議論するのではなく、ポリシーで対処する特定のリスクに的を絞りましょう。たとえば、医師はジェイルブレイクされたデバイスから電子カルテにアクセスすることはできません。ポリシーの効果は、それが防止する脅威シナリオにおいて明白に示されます。

IT 部門、セキュリティ部門、事業部門は、ポリシーをめぐって対立します。関係者によって、理解や優先順位が異なることが多いためです。ポリシーの決定の重要性を踏まえて、ゼロトラストイニシアチブのこのフェーズの早い段階で、これらの関係者を関与させるようにしてください。

ポリシーを適用すると、ヘルプデスクへの問い合わせ件数が増加します。追跡すべき重要なサポートメトリックは、ゼロトラストプロジェクトに関連するサポートチケットの数です。このメトリックをフィードバックとして使用し、ゼロトラストを実現するための今後のプロジェクトで、ヘルプデスクへの影響を軽減します。

メトリック

リスク：

- アプリケーションのポリシー対象範囲
- デバイスのポリシー対象範囲

セキュリティ：

- インシデントの削減率

サポート：

- ポリシーの例外（ワークフロー）
- ポリシーのサポートチケット
- ポリシーのサポート満足度（NPS）

運用：

- ポリシーの適用
- ポリシー準拠
- アカウント：非アクティブ
- アクセスデバイス：非アクティブ
- 認証デバイス：非アクティブ
- 認証デバイス：共有

フェーズ 5：ワークフォース（あらゆるユーザとデバイス）を対象としたゼロトラスト

この時点で、前述の段階で範囲内のすべてのアプリケーションとシステムについて説明しました。脅威シナリオに対する監視と対応が継続的に行われています。さまざまなデバイスやアクティビティで一貫したエクスペリエンスが実現しています。今こそ管理を最適化するタイミングです。

説明

本書で詳しく説明した反復的なアプローチにより、組織の IT における 1 つの側面がゼロトラストモデルに変わりました。最後のフェーズでは、この側面を組織全体の広範なゼロトラストアーキテクチャに統合します。統合と継続的な改善への移行は、エンドユーザ、IT 管理、およびセキュリティ運用に一貫したエクスペリエンスをもたらします。

この最後のステップは、振り返りから始まります。次のことを確認します。

- **成功基準に達したか**
- **ゼロトラストイニシアチブは期待どおりの結果をもたらしたか**
- **このイニシアチブは、組織の戦略と設計の原則に沿っていたか**

期待と結果の差（プラスとマイナスの両方）は、得られた教訓を活かす領域を示しています。メリットと結果を一貫した方法で測定して報告することで、個々のイニシアチブをトランスフォーメーションにおけるさまざまなイニシアチブと比較でき、得られた教訓を活かすべき別の領域がわかります。過去を振り返ることで、将来のイニシアチブに備えることができ、トランスフォーメーションのプロセス全体が加速します。

次に、イニシアチブをアーキテクチャ全体に統合します。段階的アプローチにより、トランスフォーメーションの管理と拡張が容易になります。ただしこれは、ある時点では一部の環境がゼロトラストではなく、一部がゼロトラストであり、一部が移行中であることも意味します。明確な統合戦略と計画がなければ、最終的に複数のサイロ化された環境が生まれることになりかねません。その結果、コスト、オーバーヘッド、複雑さが増大する可能性があります。そのため、テクノロジー、IT プロセス、セキュリティプロセスを統合することが重要です。アーキテクチャ全体で、共通の機能セットに沿って一貫したエクスペリエンスを提供する必要があります。これらの機能は、個々のゼロトラストイニシアチブに組み込まれています。

最終的に、継続的な運用と将来の反復が待っています。ゼロトラストアーキテクチャ全体でメトリックを追跡することで、機能している点や改善が必要な点を可視化できます。5 つのフェーズで追跡した個々のイニシアチブは終了し、運用に引き継がれて、継続的なサポートと改善が図られます。その後のイニシアチブでは、この勢いを維持し、ゼロトラストアーキテクチャに移行させる組織のユーザ、デバイス、アプリケーションを増やしていきます。

目標

- ゼロトラストイニシアチブを組織全体のゼロトラストアーキテクチャに統合する
- 継続的改善にシフトする
- 得られた教訓と勢いを活かし、その後のゼロトラストイニシアチブを推進する

トランスフォーメーション

戦略面

実装されているゼロトラスト戦略が利益を達成しているかどうかを確認し、ゼロトラスト戦略と IT 部門および事業部門の整合性が明確に取れているかどうかを確認することが目標です。

ゼロトラストが IT およびビジネス戦略全体にもたらすメリットについて、明確な説明があるか。

- 一連の原則に従った明確なゼロトラスト戦略があるかどうかを特定する
- その戦略の結果期待されるメリットについて、明確な説明があるか
- 戦略と組織の IT およびビジネス戦略との間に明確な関連性があるか

- そのような戦略の継続的な開発に対する所有者と責任者を特定する
- 利益は体系的に測定され、報告されているか

管理

ゼロトラスト戦略がどの程度適切に実装されているかを明らかにすることが目標です。

明確なゼロトラストアーキテクチャが確定され、実装されているか。

- 戦略的アーキテクチャは、組織の IT 環境全体をカバーしているか
- アーキテクチャが実装されている範囲を明らかにする
- アーキテクチャを見直し、改善または適応を確認するプロセスを特定する
- アーキテクチャのメリットは体系的に測定され、報告されているか

運用

ゼロトラスト戦略が、セキュリティリスクを軽減しながら、エンドユーザのエクスペリエンスを向上させるために実装されているかどうかを確認することが目標です。

セキュリティ機能に統合されているか。

- セキュリティ業務内のすべての要素、またはセキュリティ業務の影響を受けるすべての要素が明確に特定されていることを確認する
- 責任者とプロセスの変更が文書化されているか
- 統合が測定され、例外が特定されているか
- 継続的改善のための明確なプログラムがあるか
- セキュリティ業務のメリットと改善点が特定されているか

課題

レガシーテクノロジーは今もあります。多くの組織は、数年または数十年前のテクノロジーをサポートする必要があります。すべてをゼロトラストアーキテクチャに接続する必要はありません。リスクを軽減し、最も理にかなったセキュリティの改善を実現するために、ワークフローをセキュリティモデルに慎重に移行することが目標です。

ゼロトラストモデルの準備には 3 ～ 5 年はかかります。新しいパターンややり方を導入するには、かなりの時間と計画が必要です。本書で説明したゼロトラストへの取り組みでは、一連のプロジェクトを使用してワークフローを保護するため、必要に応じて迅速に、または時間をかけて移行できます。

メトリクス

- ゼロトラストアーキテクチャにアップグレードされたワークフローの数

概要

本書では、ゼロトラストへの変革の道のりを示しました。成功の鍵の 1 つは、具体性です。イニシアチブの範囲を特定のアクティビティに絞り込みます。つまり、組織の業務をサポートするために行われる、特定のユーザグループによる一連のアプリケーションの使用です。ユーザとデバイスに信頼を確立するように要求するのは、どのような脅威シナリオを回避するためなのかを具体的に示します。成功へのもう 1 つの鍵は反復です。1 つのアクティビティをゼロトラストアーキテクチャに変換するイニシアチブを開始します。その過程で学習したことを活かしながら、プロセスを繰り返します。

シスコでは、20 年にわたり、過剰な信頼を排除することについて議論してきました。信頼を継続的に評価するためのテレメトリとモニタリング技術について議論してきました。近年になり、ようやくテクノロジーがこの哲学に追いついてきました。本書の手順に従うことで、市販のソフトウェアにより、持続可能なペースでこれらのアイデアを実装できます。ゼロトラスト革命は現在進行中です。一緒に取り組みましょう。

Cisco Secure Access by Duo について

シスコグループの一員となった Cisco Secure Access by Duo は、業界をリードする多要素認証（MFA）およびセキュア アクセス プロバイダーです。Cisco Secure Access by Duo は、Cisco Secure のゼロトラスト製品の重要な柱の 1 つであり、さまざまな IT アプリケーションと環境において、あらゆるユーザ、デバイス、場所からのアクセスを保護する最も包括的なアプローチです。Cisco Secure Access by Duo は、Bird、Facebook、Lyft、ミシガン大学、Yelp、Zillow など、世界 25,000 社以上のお客様に信頼されているパートナーです。Duo はミシガン州アナーバーで設立され、テキサス州オースチン、カリフォルニア州サンフランシスコ、ロンドンにもオフィスを構えています。https://www.cisco.com/jp/go/tryduo で無料でお試しいただけます。

導入事例：cisco.com/c/ja_jp/about/case-studies-customer-success-stories/duo.html