Whitepaper

ゼロトラストの解明

ゼロトラストへの道のりをシンプルに

Contents

はじめに

ゼロトラストは、リモートワークの普及に伴い、すべての中小企業で必要とされるようになったセキュリティモデルである。しかし、その新しさと市場への浸透により、バズワード的な地位を獲得し、ゼロトラストとは何か（そして同様に何がそうでないか）、企業はそれを必要とするか、そしてそれをどのように達成するかについて混乱を生じさせている。

ゼロトラストが生まれたのには理由があり、複雑であるという評判にもかかわらず、実際は次のようなものです。従業員は自分の仕事を遂行するために必要な量のアクセス権しか持ってはいけないということです。

しかし、ゼロトラストの導入には、その単純なコンセプトとは裏腹に、時間と計画が必要である。Forrester社の「Practical Guide to a Zero Trust Implementation」では、典型的なゼロトラストのロードマップは2〜3年かかると推定している。幸いなことに、企業が迅速かつコスト効率よく実施できるゼロトラストの勝因は数多くあり、また、ゼロトラストの目的で実施されなかったとしても、企業がすでに実施しているゼロトラスト要素（多要素認証（MFA）、モバイルデバイス管理（MDM）、ID管理プロジェクトなど）も数多くあります。これらの構造に少し手を加えたり、それらを基に構築したりすることで、計画やマッピングのプロセスとともに、ゼロトラスト全体の進捗を早めることができます。

このガイドは、ゼロトラストに関する複雑な問題を解明し、ゼロトラストへの長い道のりの一部として、組織内で迅速な成果を特定し、実施することを支援することを目的としています。本書は、ゼロトラストの定義や市場での位置づけの明確化から、ゼロトラストの進展を促進するための実行可能なステップの概要まで、ゼロトラストフレームワーク導入への行程に沿い、戦略的かつ長期的な計画とともに実践的なガイダンスを提供するために作成されています。

What Is Zero Trust?
What Isn't Zero Trust?

何も信用しない。全てを検証する。

What Is Zero Trust?

"ゼロトラスト"という言葉は、「最新かつ最高の」製品と過剰な売り込みによって、過度に複雑化されてきた。Forresterが言うように、「ゼロトラストは、セキュリティベンダーのコミュニティにおけるトレンドであり、バズワードの汚名を着せられている」このため、意味のある実践というよりも、混乱を招く専門用語のように感じられることもあります。

しかし、ゼロトラストは、市場で言われているよりもずっとシンプルなものであり、その背後にある感情も依然として強いままです。ゼロトラストは、「何も信用せず、すべてを検証する」というマントラを実践することであり、現代の脅威から組織を守るために不可欠なものです。

Recommended Reading

2021年8月にフォレスターが発表したこのガイドでは、ITプロフェッショナルがゼロトラストの成熟度を確認し、ゼロトラスト・セキュリティの目標を設定し、そこに到達するためのロードマップを作成するプロセスを案内しています。このホワイトペーパーと合わせて読むことで、ゼロトラストセキュリティの全体像を把握し、純粋なゼロトラスト・アーキテクチャへの長期的な旅を計画する方法を知ることができます。

What Isn't Zero Trust?

一部のベンダーや販売チームはそうではないと思わせたいようですが、ゼロトラストは製品やサービスではありません。ゼロトラストは今日の市場で製品化されていますが、ゼロトラストは購入したり、スタックに追加したりできるものではありません。ゼロトラストは、購入したり、スタックに追加したりできるものではなく、ITインフラストラクチャを保護するための最新のフレームワークです。製品やサービスはゼロトラスト・アーキテクチャの構築に役立ちますが、最新かつ最高のソリューションをすべて導入することは、長期的には有益であるどころか有害である可能性があります。その代わり、賢いゼロトラストへの道筋は、既存の環境の中で総合的に機能する戦略的なソリューションを探すことです。

ゼロトラストの原点

ゼロトラストは、オンプレミス環境を保護するために設計された、時代遅れの「城と堀」のセキュリティ手法の欠点に対応して開発されたものである。この方式では、企業はファイアウォール、侵入防御、VPNなどのツールを使って境界で強力なコントロールを構築し、ネットワークとリソースを保護し、境界の制御を通過して企業ネットワークに侵入したものは、本質的に信頼されます。

このようなセキュリティの境界アプローチは、ビジネスが実際の境界を持つ物理的なスペースに制約されていた時には理にかなっていました。サーバーはサーバールームに置かれ、デバイスはそこに配線され、オフィスは鍵と錠の下で保護されていました。しかし、現在では、仕事はリモートで、オフィスで、そして移動中に行われます。リソースは、それがどのような形態であっても、どこにあっても、どのようにアクセスされても、安全である必要があります。

この境界セキュリティの方法は、現代の環境では2つの点において欠点があります。まず、クラウドサービスやリモートワークによって、物理的な境界（かつてはレガシーな有線機器を備えたオフィスビル）という考え方が意味をなさなくなったことが挙げられます。境界のない環境では、主要な侵入口にセキュリティを配置することはもはや十分ではありません。実際、リソースがクラウドホスティングされ、どこからでもアクセスできるようになると、その侵入口がどこにあるのかを判断することさえ困難になります。むしろ、今日のセキュリティは、デバイス、アイデンティティ、およびアクセスの保護に焦点を当てる必要があります。

境界セキュリティの第2の欠点は、すべての安全対策を最初のアクセストランザクション（すなわち境界）に配置し、これらの安全対策を完全に信頼することで、境界の内側にいる誰もが信頼に足ると思い込んでいることです。サイバー犯罪者のスピードは非常に速く、巧妙であるため、セキュリティ専門家は、攻撃は避けられないと述べています。万が一に備えた対策を講じないセキュリティは、多くの境界線セキュリティと同様、セキュリティが全くないのと同じである。

ゼロトラストの実践

これらの欠点に対処するため、ゼロトラストは、外周部だけでなく、すべてのアクセストランザクションで安全な認証を行うことを規定しています。これは、仮想境界の複雑化に対応するものです。

ゼロトラストを完全に実装するには時間がかかるが、その中核となるフレームワークは非常に簡単である。実際には、以下の3つの要素が必要である。

- **最小権限の原則 (Principle of Least Privilege)**　PLPは、まさにゼロトラストの核心にあるものです。ゼロトラストの目標は、誰もアクセスできないはずのものにアクセスできないようにすることです。エンドユーザーはネットワークの設定を変更できないようにし、顧客は他の顧客のデータを見ることができないようにし、サイバー犯罪者は企業のリソースやデータにアクセスできないようにするのです。PLPは、すべての人が必要なものだけにアクセスできることを保証し、それ以上のことはさせません。
- **安全な認証**　パスワードは1960年代から存在しています。それから約60年後の今、サイバー犯罪者はパスワードを完全に浸透させる技術を習得しており、パスワードはもはや信頼できるセキュリティ手段ではなくなりました。実際、2021年の情報漏えいの61%はパスワードが原因であり、クラウドソースの計算能力により、パスワードクラッキングツールは8文字のNT-hashパスワードを約12分で解読することができます。このギャップを埋めるために、企業はMFAやパスワードレス認証など、より安全な認証方法を使用しています。
- **アクセス・トランザクションごとの認証**　ゼロトラストは、安全な認証を最初に使用したり、特定のリソースにゲートをかけるだけでは不十分で、あらゆる場所で、つまりあらゆるアクセス・トランザクションで安全な認証を行うことを規定しています。

ゼロトラスト:鍵と錠

ゼロトラストのコンセプトは、非常に身近な対人セキュリティである「鍵と錠」に由来しています。オフィスでは、従業員はしばしばバッジを所持し、本館への出入りを許可され、次に自分の担当するスイートや部屋への出入りを許可されます。他のオフィスやセキュリティの高い部屋への出入りを禁止している場合があります。バッジの中には、2つ目の身分証明書として写真入りのものもあります。ゼロトラストは、このセキュリティ・プロセスを仮想化します。ディレクトリ・プラットフォームを通じて、アイデンティティとその権限を作成・保存し、すべてのアクセス処理で信頼できるセキュリティを確保するために、二次的な検証方法を使用します。

この「どこでも」不測の事態は、境界線の消失に直接対応するものです。認証に成功すれば友好的であると考えるのではなく、ネットワーク内を移動するユーザーのアイデンティティに挑戦し続けるのです。アプリケーションからアプリケーションへ、さらにはシステム内でも。これにより、サイバー犯罪者があるリソースにアクセスできたとしても、ネットワークの他の部分へのアクセスは保証されないため、侵入された場合の横方向の動きを防ぐことができます。

中小企業におけるゼロトラストの導入メリット

セキュリティ

サイバー犯罪者は、大企業やフォーチュン500社だけをターゲットにしているわけではありません。サイバー犯罪のトレンドは、中小企業でも大企業でも同様のパターンを辿る傾向があり、しかも増加の一途をたどっています。リモートワークやハイブリッド型リモートワークへの移行は、セキュリティ上のギャップを生みました。多くの組織がリモートモデルを迅速かつ無計画に採用し、セキュリティはビジネスを維持するために後回しにされました。サイバー犯罪者は、企業の防御力が低下している間に素早く行動し、2020年にはサイバー犯罪が急増しました。今日も、悪質業者は企業のリモートおよびハイブリッドインフラのギャップを利用し続け、サイバー犯罪は増加し続けています。

リモート環境とハイブリッド環境には、最新のセキュリティが必要です。パンデミック以前は境界線方式で対応できたかもしれませんが、最新の環境と脅威を前にしては、もはや適切ではありません。実際、中小企業のIT担当者は、2021年と2022年の両方において、「レイヤー型セキュリティを追加して、どこからでも仕事ができるようにする」ことを最優先事項として挙げており、80%以上がリモートワークやハイブリッドリモートによってセキュリティへの関心が高まることに同意しています。

IT 業界の動向調査

JumpCloudは、2021年に2つの調査を実施し、急速に変化する職場における中小企業のIT担当者の技術に関する経験を評価しました。4月に実施された最初の調査では、リモートワークに直面して変化する組織の優先順位を反映しています。10月に実施した2回目の調査では、ITプロフェッショナルがセキュリティとどこからでも働けるモデルの採用に舵を切ったことが示されています。

ゼロトラストは最新のクラウド環境を保護するように設計されているため、サイバー犯罪に対する最善の防御策となり、中小企業が長期的にリモートワークやハイブリッドワークを行うための持続可能なセキュリティ基盤を提供することができます。

使いやすさ

ゼロトラストフレームワークは、レガシーリソースよりも使いやすく進化したクラウドリソースに対応するよう設計されています。クラウドリソースは、レガシーリソースに比べ、より使いやすく進化しています。そのため、ゼロトラストの実装は、同様にクラウドベースでユーザーフレンドリーなものになる傾向があります。パスワードの記憶と入力の必要性を減らし、オンボーディングとオフボーディングを自動化することで、ゼロトラストの実装は従業員の体験を向上させる傾向がある。純粋なゼロトラスト環境は、統合、自動化、および唯一の信頼できるソースデータを使用し、その結果、ユーザーに一貫した、直感的でシームレスなエクスペリエンスを提供します。

将来を見据えて

ゼロトラストは、クラウド環境で動作し、サポートするように設計されているため、旧来のセキュリティモデルよりもクラウドベースのリソースを保護するのに適している。レガシーからクラウドへの移行が加速する中、ゼロトラストは今後も普及し続け、境界型セキュリティ・モデルを置き換えていくと思われる。

さらに、ゼロトラストは物理的なインフラストラクチャから離れることで、従来の境界ベースのセキュリティよりも柔軟で適応性が高く、将来の変化への適応に適しています。ゼロトラストのツールや手法のほとんどはソフトウェア駆動型で、バーチャルに制御できるため、組織や技術の変化に合わせて適応・拡張することが可能です。これは、組織や市場が頻繁に変化する中で、機敏さと適応性を維持する必要がある中小企業にとって特に重要なことです。

管理者環境の向上

ゼロトラストはソフトウェア駆動型のアーキテクチャを採用しているため、IT部門による管理が容易です。その実装は大掛かりなものですが、その適応性、自動化、リモートアクセス性により、ハイブリッドリモート環境のIT管理者にとって使いやすいものとなっています。さらに、ゼロトラストアーキテクチャは、インフラストラクチャ全体とそのアクティビティに対する可視性を向上させることができます。これにより、セキュリティ管理が簡素化され、IT管理者は侵害に至る前に問題を発見し、対処することが容易になります。

IT管理者の作業を効率化することで、セキュリティを高めると同時に、スムーズな組織変更、拡張、ITメンテナンスを促進する環境を構築することができます。IT部門が疲弊している中小企業では、節約した時間を他のIT施策に振り向けることができ、セキュリティに妥協することなく、大きな効果を発揮することができます。

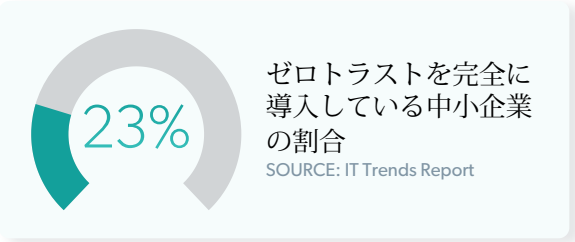
なぜゼロトラストを導入する中小企業が増えないのか？

2021年末に実施された調査によると、中小企業の半数強（58.6%）がゼロトラスト・セキュリティ・プログラムを追求または計画していると回答しています。同年実施された別の調査では、すでに完全に採用していると回答したのはわずか23%でした。ゼロトラストが中小企業にとって非常に有益であるとしたら、なぜまだ多くの中小企業が採用していないのでしょうか。

断片的な課題

"ゼロトラストの魔法の弾丸"と称するあまりにも一般的な製品は、ゼロトラストの導入に役立つというよりも、むしろ有害である。SaaS市場では、企業が最新かつ最高の技術を追い求める傾向があります。その結果、企業は、まとまりや戦略を欠いたセキュリティツールを自社のインフラに積み重ねることになるのです。このようなアドホックな購入アプローチと大量のツールは、企業をゼロトラストに近づけるどころか、さらに遠ざけてしまう傾向があります。

このような乱雑なインフラストラクチャでは、ツール同士を連携させるために多くの複雑な統合が必要になります。また、多くの依存関係 (すべて文書化されているわけではありません) が存在するため、ツールが約束する俊敏性が損なわれる可能性があります。ツールのアップデートからスタックへの新しい追加に至るまで、あらゆるものが1つの統合を壊し、インフラの残りの部分にドミノ効果をもたらす可能性があります。



そのため、このような環境下で働く企業は、ゼロトラストを採用するために抜本的な変更を行うことを躊躇してしまいます。ゼロトラストを達成するためにこのような断片的なルートを歩んできた企業は、セキュリティが向上しないまま複雑さが増すのを目の当たりにした後、その目的を断念しているかもしれません。

コストと労力

ゼロトラストへの断片的なアプローチは、ソリューションの購入だけでなく、その管理に必要な労力や専門知識という点でも、コストを膨れ上がらせる原因となる可能性があります。新しいソリューションを環境に導入するには、立ち上げにかかる時間とトレーニング、そして継続的な管理とメンテナンスが必要です。この継続的な労力は、社内で補うか、専門家を追加で雇うかのどちらかである。ポイント・ソリューションは蓄積される傾向にあるため、自社で管理する中小企業は、ITチームに負担をかけることになりがちです。新しい従業員や外部の人材を採用する場合、サイバーセキュリティの専門知識を得るのは難しく、費用もかかるため、この方法はすぐにコスト高になることが分かっています。

ゼロトラストの過度な複雑化

多くの人にとって、ゼロトラストは途方もない大仕事のように思われ、脅かされている。さらに多くの人にとって、ゼロトラストはどこか謎のままである。IT専門家は、最新で最高の「ゼロトラスト製品」について聞き飽き、ゼロトラストは単なる流行語の1つに過ぎないと感じている。さらに、「ゼロトラスト」のラベルが付いたさまざまなツールを目にすると、ゼロトラストのコンセプトがさらに混乱し、ゼロトラストの目標が広すぎて中小企業には達成不可能に感じられる。しかし、実際には、段階的に実施しても永続的な影響を与えることができる、分かりやすいコンセプトなのです。

ゼロトラスト導入への道のりをシンプルに

ゼロトラスト導入への道には、最終目標である純粋な ゼロトラストアーキテクチャに先立つ多くの段階があり、その達成には何年もかかります。計画する最善の方法は、境界とゼロトラストのハイブリッド状態を受け入れ、達成可能な小さなマイルストーンに目標を定めることである。Forrester 社は、「Practical Guide to Zero Trust Implementation」の中で、これらのマイルストーンを 3 つの主要なフェーズにマッピングすることを推奨している。

フェーズ毎で中間目標を設定

1. 現在のZero Trustの成熟度を評価する。
2. 既存のテクノロジーを活用できる場所を含め、現在のビジネスイニシアチブを理解する。
3. 将来の目標とそれを達成するためのタイムフレームを設定する。これがあなたのロードマップとなります。

ステップ3で作成した目標とロードマップは、5つのカテゴリーに分けることができ、Forresterは、ほぼ次の順序で取り組むことを推奨しています。

ロードマップステージ

1. Identity.
2. Workloads.
3. Devices.
4. Networks.
5. Data.

この順序により、セキュリティは既存の取り組みと複合的に構築され、ゼロトラスト・セキュリティの一貫したフレームワークを形成することができます。しかし、これらの段階は（意図的に）幅広いものです。インフラ全体を改革する必要がある場合、どこから手をつければよいのか分からないことがあります。

次のセクションでは、上記の5つのカテゴリーごとに、インパクトのあるゼロトラストの導入事例と、何から始めるべきかを判断するための方法を紹介します。

ゼロトラストの実践ステップ

フォレスターの「ゼロトラスト実装のための実践ガイド」は、ゼロトラスト導入のをAからZまで描くための全体的な方法を提供しています。しかし、開始を迫られている、賛同者を獲得しようとしている、ロードマップに圧倒されている、あるいは導入に行き詰まりを感じている場合は、どのステップを最初に踏むべきかで苦悩するよりも、少しでも前進する方が生産的だと思われます。

このセクションでは、IT担当者が方向性をすばやく見出せるように、ゼロトラストのロードマップの中核となる要素をいくつか紹介します。これらの実装は、ゼロトラストの3つの中核的要素、すなわち最小特権の原則（PLP）、安全な認証、およびすべてのアクセス・トランザクションでの認証に重要かつ直接的な影響を与えるものである。このリストは、すでに導入しているものや、自分の環境に簡単に導入できそうなものを確認するのに役立つはずです。

ゼロトラストの実現に向けた取り組み

Identity

- **どこでもMFA**　あらゆる場所にMFAを実装することは ゼロトラストへの大きな一歩となります。脆弱性の高いパスワードに依存していた組織を、ログイエ・セキュリティを大幅に向上させるだけでなく、侵入された場合の横方向の移動を防止する認証プロセスに移行させるのです。MFAツールは低コストで、アイデンティティ・アクセス管理（IAM）やディレクトリ・ソフトウェアに無料で付属しているものもあり、一般に簡単に実装できます。プッシュ通知や生体認証のような新しいMFAテクノロジーは、ユーザーにとって使いやすいものになるよう、操作性を向上させています。
- **IAM**　IAM の一貫したアプローチは、組織内のアイデンティティのための単一の真実のソースを作成します。これは、安全な認証方法を確立し、PLPを維持するために不可欠です。
- **オンボーディングとオフボーディングを合理化**　中小企業では、成長と解約が激しく、手動によるオンボーディングとオフボーディングは非効率的で安全ではありません。オンボーディングとオフボーディエグは、可能な限り自動化する必要があります。オンボーディングを自動化することで、従業員をリモートで雇用することができます。また、オフボーディングを自動化することで、ITチームが誤ってリソースのアクセス権を失効させるのを防ぐことができます。このステップは、一般的にIAMの導入後に行われます。ユーザーのアカウントを唯一の信頼できる情報源で追跡することで、アカウントのプロビジョニングとデプロビジョニングを自動化することができます。
- **シングルサインオン（SSO）**SSOは、ユーザーが1つの認証情報で必要なすべてのリソースにログインできるようにすることで、パスワードの使用量を減らすのに役立ちます。ゼロトラストの安全な認証の要件を満たすには、SSOをMFAで保護する必要があります。
- **条件付きアクセス。**条件付きアクセスは、コンテキスト情報を使用してログインの安全性を判断し、それに従って行動します。例えば、安全なログインの試行では MFA 要件を回避できますが、安全でないログインの試行（公衆無線 LAN を使用する未知のデバイスからの試行など）では、MFA を要求するか完全に拒否することができます。条件付きアクセスは、安全で予測可能な環境で摩擦が少ないユーザーに報酬を与え、疑わしい行動に対してセキュリティをロックダウンすることができます。

これらの実装は、ゼロトラストの3つの中核的要素に重要かつ直接的な影響を与る。PLP、セキュアな認証、そしてすべてのアクセス・トランザクションにおける認証です。

Workloads

- **リソースの可視化**　ネットワーク上のすべてのリソース(シ　ステム、ソフトウェア、ファイル、アプリケーショ(ス　、資産）を追跡および表示できる必要があります。これにより、すべてのリソースが適切に保護されていることを確認し、すべてのアクセス・トランザクションで安全な認証を実施することができます。
- **アクセス制御**　すべてのリソースに、PLPに基づくアクセス制御を割り当てる必要があります。ロールベースおよび属性ベースのアクセス制御方式は、安全かつ適切なアクセス許可を割り当てるのに理想的です。安全かつ適切なアクセス権を付与することができます。このステップでは、リソースの可視化とIAMプラットフォームが一般的に前提条件となります。さらに良いのは、会社のリソースにアクセス制御を実施できるIAMプラットフォームが、この2つを互いに連携して実装していることです。これにより、2つの重要な機能が統合され、直感的で文脈に応じたルールが、信頼できる情報源としてレポートされるようになります。

Devices

- **デバイスの可視性**　企業のリソースにアクセスするすべてのデバイスを確認し、管理することができるようにする必要があります。現在、環境の大部分がハイブリッドおよびリモートであるため、スマートフォンやその他のモバイルデバイス（会社支給と従業員所有の両方）が含まれる必要があります。
- **MDM**　MDMはデバイスの可視化から一歩進んで、企業が自社のリソースに接続するデバイスを管理する機能を提供します。MDMの必要性は、リモート企業やハイブリッド・リモート企業で高まっており、綿密な管理が行われないと、セキュリティがすぐに損なわれてしまいます。
- **パッチ管理**　最近の調査によると、侵入の60%は、侵入時に利用可能なパッチがあれば回避できた可能性があります。パッチ管理のプロセスとツールは、このギャップを埋めるために重要であり、デバイスがリモートで分散している現代の中小企業では特に重要です。パッチ管理は、企業のデータにアクセスするすべてのデバイスとソフトウェアが最新のパッチを適用していることを、いつでも自信を持って確認できるようにする必要があります。パッチマネジメントシステムは、次のような機能を備えている必要があります。
  - パッチの欠落を特定し、警告する。
  - パッチのスケジュール設定と適用。
  - パッチが適用されたデバイスと適用されていないデバイスの可視性を提供。

Networks

- **セグメンテーション** NIST は、マイクロセグメンテーションをゼロトラスト追求の重要な手法の 1 つと位置付けています。動的な VLAN 割り当てなどの戦略によるネットワークのセグメンテーションは、大規模なネットワーク構 造の中に小規模でソフトウェアベースの境界を構築するのに役立ちます。このような境界は、横方向の移動を防ぎ、コア資産を保護し、PLP を適用するのに役立ちます。
- **インフラの可視化**　セキュリティの維持には、可視性が重要です。イベントログ、SIEM ツール、脅威検出ツール、およびディレクトリテレメトリーはすべて、インフラの可視化に貢献します。

Data

- **データの暗号化**　データは、転送中と保存中の両方で暗号化する必要があります。クラウドプロバイダーは、クラウドベースのサービスについてこの点を管理する傾向があります。現在利用しているSaaSプロバイダーの慣行を監査することから始めましょう。暗号化を使用していないツールを修正するには、ツールの設定やライセンス（暗号化が提供されている場合）を変更するか、別の暗号化手段で補完するか、プロバイダーを変更する方法があります。デバイスに保存されたデータは、デバイス自体で保護する必要があります。フルディスク暗号化　JumpCloudのようなMDMおよびディレクトリソリューションの中には、フルディスク暗号化を自動的かつリモートで実施するものがあります。
- **セントラル・ディレクトリ**　セントラル・ディレクトリは、スタック内の事実上すべてのゼロトラスト・コンポーネントを唯一の信頼のできる情報源の下に統合することができます。最新のクラウドディレクトリは、ユーザー、デバイス、ネットワーク、アプリケーション、ファイル、機器など、さまざまな種類のリソースを接続するために安全なプロトコルを使用します。JumpCloudのように、MFA、MDM、パッチ管理、テレメトリーなど、ゼロトラスト主導の機能を搭載しているものもあります。セントラルクラウドディレクトリの導入は、ゼロトラストを実現するための1つのステップとなり得ます。

どこから始めるべきか？

何を優先させるかを決定する際、いくつかのアングルがあります。しかし、どの角度から見ても重要なのは、組織にとって最も意味のあるステップを優先させることです。以下に、どのステップが最も効果的かを判断する際の指針となる指標をいくつか示します。

スモールスタート

組織によっては，小さなステップが最善の方法である場合もあります。これは，IT チームが疲弊している場合や，小規模な組織，設立当初 の組織，指導者の賛同が得られない組織などに当てはまります。

小さな一歩が小さな影響をもたらすとは限りません。小規模で低コストの取り組みでも、セキュリティに大きな効果をもたらし、ゼロトラストの目標に大きく近づける可能性があります。

> どの角度から見ても、組織にとって最も意味のあるステップに優先順位をつけることが重要です。

スモールスタートでもインパクトのある取り組み例：

どこでもMFA。多くの組織では、すでに技術スタックの一部にMFAを導入しています。これをより多くの技術スタックに拡大し、最終的にはあらゆる場所に導入することで、大幅なセキュリティ向上が期待でき、費用対効果も高く、簡単に導入することができます。ほとんどのユーザーはMFAプロセスに慣れているため、通常、導入にかかる労力は最小限に抑えられます。MFAソリューションの中には、IAMやディレクトリ・ソフトウェアに無料で付属しているものもあり、ゼロトラストの進捗をさらに高めることができる。オフボーディングやパッチ管理の自動化など、他のゼロトラストの取り組みと同時に、この2つを実現できる1つのツールに投資することは、大きな前進を促す費用対効果の高い方法である。

トラフィック量の多いツールから始める

また、アクセス頻度の高い場所、つまり人々が最も頻繁に使用する場所から始めることもできます。たとえば、人事部のリーダーだけが使用する文書へのアクセ ス権を確保することは価値があるかもしれませんが、使用頻度 が低いため、コラボレーション・プラットフォームやプロジェクト 管理ツールなど、より頻繁に使用するタッチポイントに集中する間、そ れを待つことができるかもしれません。この方法は、特定のプラットフォームで多くのユーザーが作業している大規模な中小企業や、監視されていない環境での適切なツール使用を心配するリモートまたはハイブリッド中小企業にとって理想的な方法です。このようなトラフィックの多いツールの保護は、まず始めに行うべき、万全のセーフガードと言えます。

高いトラフィックツールから始めるの例：

シングルサインオン SSOは、全従業員、全リソースに適用できるため、セキュリティの歩留まりが高いツールです。SSOの導入は、低コストかつ低労力で、組織全体のセキュリティを即座に向上させることができる方法です。

最も重要な部分を優先する

この方法論は、まず最も重要なレベルのセキュリティにアプローチします。もちろん、理想的な世界では、インフラにあるすべての要素をすぐに保護することができます。しかし、あるものを優先すると、他のものの優先順位が下がるという性質があります。企業のインフラ、リソース、環境、脅威のベクトルを理解することは、こうした厳しい選択をする上で役立ちます。

したがって、このアプローチは、自社の環境、リソース、スタックをすでによく理解し、最も重要な資産を容易に特定できる組織でうまく機能します。インフラストラクチャのインベントリ作成が大きな作業となり、進捗が滞る可能性がある場合は、インフラストラクチャのインベントリと評価を行う際に、より消化しやすい別のステップから始めることを検討します。

最重要部分から取り組む際のステップ：

ネットワークのセグメンテーション 少なくともゲストレベル、企業レベルにネットワークをセグメント化することは、重要な資産を保護する上で非常に有効です。PLPに基づいて各セグメンテーションのリソースをセグメント化し、最重要部分は管理者/最高特権ネットワークでのみアクセスできるようにします。

操作性と賛同を軽視しない

どんなに優れたゼロトラスト計画も、ユーザー、IT部門、経営陣の賛同なしには定着しない。

ユーザーからの支持は、ユーザビリティに起因する。クラウドベースのツールがより使いやすくなり、人々がテクノロジーを私生活に深く取り入れるようになると、ユーザーは職場の中でも外でも、明確で直感的、かつシームレスなテクノロジー体験を期待するようになります。実際、従業員の体験は、従業員定着のための重要な差別化要因になりつつあります。したがって、ユーザーにとって摩擦を蓄積するようなセキュリティシステムを導入すると、回避、シャドーIT、ヒューマンエラー、さらには従業員の離職率の上昇を招くことになります。特にシャドーITとヒューマンエラーは、セキュリティ侵害の大きな要因となっています。

同様に、新しいセキュリティ対策を導入する際にも、ITチームは使い勝手を向上させる必要があります。最初の導入時には、作業や摩擦が生じることが予想されますが、長期的な計画では、ITチームにとってより良い管理体験が得られるはずです。そうでなければ、回避、回避策、メンテナンス不足、真実のソースの1つを維持できないといった同様の課題に直面することになります。これらの課題は、可視性が低く、一元管理ができない環境、つまりセキュリティ脅威の温床を生み出します。

最後に、リーダーシップと利害関係者からの支持を決して過小評価してはなりません。セキュリティ・プログラムを信頼するには、ユーザと管理者を信頼する必要があります。強力なセキュリティ文化を育成する必要がありますが、文化はトップから生まれます。リーダーシップは、セキュリティをどのように扱うかによって、セキュリティの取り組みを推進するかしないかを決定します。もしリーダーシップがセキュリティ・プログラムの重要性を信じていなければ、ユーザやITチームからの支持を得ることはできません。

一方、リーダーシップがセキュリティ対策を信じていれば、対策に投資するための資金やサポートが得られるだけでなく、組織全体でセキュリティのベストプラクティスを実施する際の援軍を得ることができます。全体として、どのゼロトラスト施策を行うかを選択する際には、ユーザー、ITチーム、リーダーシップの観点から賛同を得ることを考慮する必要があります。ポジティブなユーザー体験を提供し、既存の支持と一致する、または支持を容易に育成できる手順を選択することで、手順を確実に持続させることができます。

テクノロジーソリューションの選択

IT スタックに負荷をかけないことが重要であるが、ゼロトラストを実現するためには、どこかでテクノロジー・ソリューションに投資する必要があるでしょう。ソリューションを評価する際には、次の点に留意してください。

組織にとって意味のあるソリューションを選択する　自社で購入可能で、うまく管理できるツールを探す。フォーチュン500に選ばれているような堅牢で機能豊富なツールが、簡単な仕事をこなすだけの50人規模の組織にとって必ずしも適切であるとは限りません。同様に、人気のあるツールを複数購入しても、1つのツールでよりコスト効率の高い作業ができる場合は、組織にとって理想的とは言えないかもしれません。多くの場合、統合ツールは費用対効果と管理のしやすさの両方を提供し、中小企業にとって理想的な投資となります。

現在および将来の状態との互換性を検討する　ゼロトラスト導入への道が完了に近づいていない組織は、ツールが現在のアーキテクチャ（ゼロトラストと非ゼロトラストの要素を含む）と将来の状態の純粋なゼロトラスト環境の両方で動作することを確認する必要があります。ゼロトラストの旅路の最初または途中にある組織は、ツールの柔軟性と適応性を確認する必要があります。

先を見据える　今購入したツールは、あなたの環境に永続的な影響を与えるでしょう。たとえば、スタック内の他のツールとうまく統合できないツールは、今後数年間、あなたの環境を苦しめることになります。同様に、過度に複雑なツールは、多くの機能を提供するかもしれませんが、環境の変化に応じて維持管理が面倒になる可能性があります。多くの場合、維持管理は時間の経過とともに弱まり、新たなセキュリティ問題を引き起こす。例えば、ロールの権限を更新しないと、ユーザーが過剰な権限を持つことになり、ゼロトラストの対極にあるような状態になる可能性があります。管理者にとってのメンテナンスの効率化と、ユーザーにとっての使い勝手の良さを両立するツールを探してみてください。

Tool Tip

JumpCloudは、組織の規模や環境に応じて、さまざまなディレクトリやインフラストラクチャの実装コストを見積もる価格比較ツールを提供しています。

Try the Pricing Tool →

コストを総合的に考える　ソリューションの価格設定は、考慮すべき多くのコストのひとつに過ぎません。例えば、複雑な製品を維持するための運用コストは、価格が高くてもメンテナンスが簡単で諸経費が少ない製品よりも悪い投資となる可能性があります。また、複数の機能を兼ね備えたツールは、追加でツールを購入する必要がないため、TCOを抑えることができます。このような包括的なツールは、インフラストラクチャのより多くの要素がうまく機能するようにし、将来的に複合的なツールの依存関係を生み出す統合の必要性を最小限に抑えることで、維持管理も合理化します。

セキュリティから複雑さを取り除く

直感に反するように聞こえますが、複雑さはセキュリティにとって強みになるどころか、むしろ害になるのです。ゼロトラストの用語にまつわる複雑さは中小企業による採用を妨げ、ユーザー体験の複雑さはセキュリティの採用を妨げ、IT管理者の複雑さは長期にわたるインフラの劣化を招きます。また、IT管理者にとっての複雑さは、時間の経過とともにインフラの劣化を引き起こします。むしろ、わかりやすく、直感的で、まとまりのあるソリューションが、信頼できるセキュリティ・プログラムの最も強力な基盤を形成するのです。

JumpCloud®は、IT担当者がセキュリティ対策から不必要な複雑さを排除できるように、重要なセキュリティ概念を単純化し、IT担当者に実際の環境における実践的なセキュリティガイダンスを提供することを目的としたリソースライブラリーを作成しました。リソースライブラリ「Security Without the Complexity」をご覧いただき、セキュリティ戦略に磨きをかけてください。

1. https://jumpcloud.com/resources/forrester-research-practical-guide-to-zero-trust-implementation
2. Ibid.
3. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf
4. https://jumpcloud.com/blog/the-password-management-queens-gambit-how-to-manage-it-attack-it-and-counter-it
5. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf
6. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics
7. https://www.idtheftcenter.org/post/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/
8. https://jumpcloud.com/resources/creating-a-new-normal-for-sme-it-in-2022
9. https://jumpcloud.com/resources/it-trends-report-remote-work-security-cloud-services
10. https://jumpcloud.com/resources/creating-a-new-normal-for-sme-it-in-2022
11. https://jumpcloud.com/resources/it-trends-report-remote-work-security-cloud-services
12. https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf
13. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf