ホワイトペーパー

ゼロトラスト・アーキテクチャ構築に向けた詳細な計画

目次

はじめに

ゼロトラストの概念は 2009 年から存在します。この年、Forrester Research が初めてゼロトラストの概念を掲げ、ネットワーク境界を通過したユーザーやアプリケーションに自由なアクセス権を付与する従来の方法を見直して、フルアクセスを許可する前に、すべてのデバイス、ユーザー、ネットワークフローを検証する必要があると組織に警告しました。その後の数年間は、多くの要因が寄与し、ゼロトラストの概念を採用する緊急性が高まる一方でした。

今日のハイブリッドワークフォースはさまざまな場所から業務を行っており、BYOD プログラムによって従業員は管理対象デバイスと管理対象外デバイスの両方を使用して会社のアプリケーションやリソースにアクセスできるようになっています。アプリケーションは、クラウド、オンプレミス、ハイブリッドなど、あらゆる場所でホストされています。これらの変化の最終的な結果として、かつてのような形のネットワーク境界は存在しなくなりました。ランサムウェア攻撃の頻度と巧妙さが高まったため、攻撃者が防御を侵害するチャンスが増え、攻撃が行われた場合に発生するコストが増加しました。「IBM Cost of a Data Breach 2024 Report」によると、米国ではデータ漏えいによって生じる平均コストが世界で最も高く、936 万ドルに達しています。さらに、モノのインターネット（IoT）デバイスなどのネットワークに接続されたデバイスが増加すると同時に、パートナーや顧客によるネットワークアクセスがますます求められるようになったため、企業のアタックサーフェスが大幅に拡大しました。

このように進化し続けるサイバーセキュリティ情勢の中で、ネットワークおよびセキュリティソフトウェアのベンダーは既存の製品をゼロトラストとしてブランディングしたり、新製品を導入したりすることに急いで取りかかりました。それと同時に、コンサルタントやアナリストは新しい略語や専門用語を使用するようになりました。しかし、セキュリティチームはこの動きに取り残され、時として複雑であるそのような概念を説明したり、ゼロトラスト戦略に移行するための土台となる購買意思決定を行ったりすることに苦労しています。

このホワイトペーパーは、何から始めるべきかを明らかにし、重要な差別化要因の概要を説明することにより、セキュリティチームがゼロトラスト・テクノロジーへの投資の詳細な計画を策定できるようにすることを目的としています。

ハイブリッドワークとクラウドアプリによりネットワークセキュリティのパラダイムが崩壊

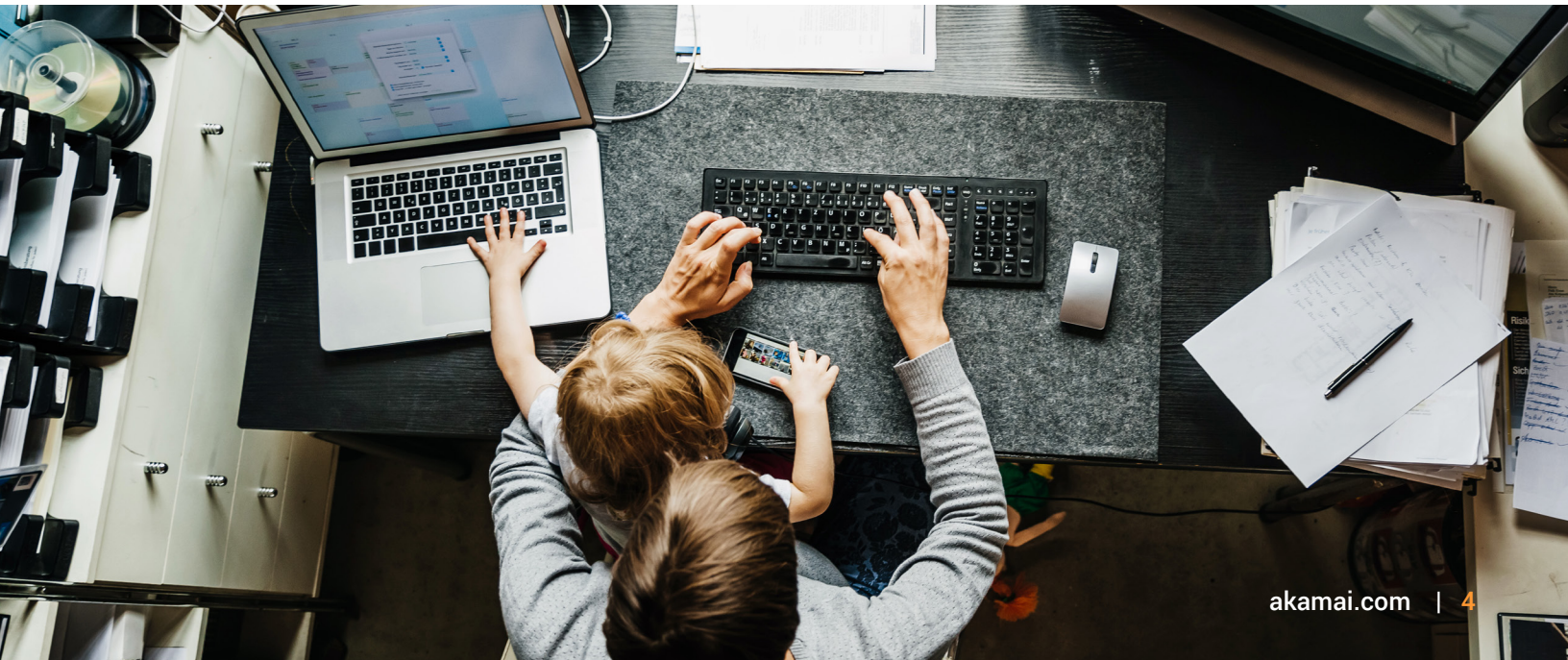
人々が仕事をするタイミング、方法、場所が、いずれもオフィスの四方の壁の外へと広がりました。

その結果、ネットワーク境界は、少なくとも認識できる形では、もはや存在しなくなりました。ユーザーは、堀の内側と同じように堀の外側にも存在しているはずです。また、SaaS（Software as a Service）やマルチクラウド実装として使用するアプリケーションが急増しています。高度かつ持続的な脅威が存在するため、攻撃者にネットワークへ侵入されると、最も価値のある資産へのアクセスをうかつにも許してしまう可能性があります。包括的なゼロトラスト・プログラムを導入していなければ、一度侵入した攻撃者は思いのままに行動できます。

これは単なる理論上の話ではありません。近年は多額のコストを生じさせるデータ漏えいが広く発生しており、その大部分がネットワーク境界内に対する信頼が悪用されたことで発生しました。

ネットワーク境界内で使用するように設計されたアプリケーションは多くの場合、セキュリティプロファイルが一番低く設定されています。とはいえ、もしもあなたが開発者で、システムにアクセスできるのは許可された正当な従業員だけであると想定していたなら、どうしたでしょうか。膨大な数のハッカーが自分のインターネットベースアプリケーションを攻撃すると知っている現在の開発者と同等の防御策を講じたでしょうか。

市場を見渡すと、このような課題に対するソリューションとして、ゼロトラストがあります。



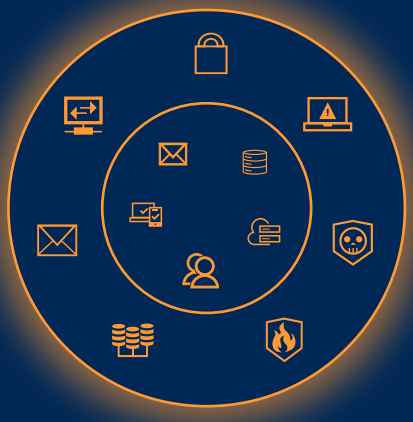
ゼロトラスト・セキュリティ・アーキテクチャ

ゼロトラストの背後にある本質は非常にシンプルですが、非常に強力です。それは、信頼とは場所に帰属するものではないということです。ファイアウォールの内側にあるというだけで、そこにあるものを信用すべきではありません。そうではなく、どんなアクションも、発生する場所を問わず、明示的に許可されている場合のみ信用しなければなりません。究極的には、発生すべきアクションのみが発生してよいということです。組織は不要なアクションに対する暗黙的な信頼をすべて排除する必要があります。たとえば、財務システムへのアクセス権を必要とする経理グループのユーザーは一握りだけであるにもかかわらず、経理グループのすべてのユーザーにアクセス権を付与するのは、リスクを生むだけで、価値は生みません。

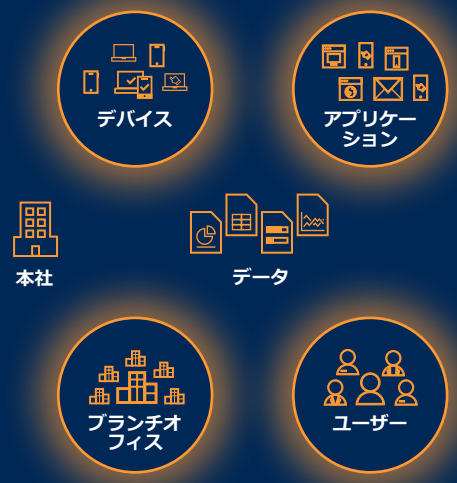
証明には強力な認証と認可を使用し、信頼が確立されるまでシステム間でのデータ転送はいっさい行うべきではありません。さらに、分析とロギングを使用して、ふるまいを検証し、侵害の兆候を継続的に監視しなければなりません。

このように考え方を根本的に変えれば、過去 10 年間に発生した膨大な数のセキュリティ侵害に打ち勝つことができます。攻撃者は時間をかけて境界の弱点を悪用することができず、堀の内側に侵入しても機微な情報やアプリケーションを悪用することができません。もう堀などないのです。あるのはアプリケーションとユーザーのみであり、アクセスするためには、それぞれが事前に相互認証し、認可を確認する必要があります。

従来のセキュリティアーキテクチャ



今日の現実



ゼロトラスト・アーキテクチャの構築方法

まず、すべての企業が既存の環境に対する戦略を策定し、新しい人材を雇用する必要があるかどうか、そしていつ雇用する必要があるかを判断する必要があります。プロセス全体の中でもこのステップはそれだけで論文を書けてしまうほど重要ですが、ゼロトラスト戦略の実行を支援する実際の製品は次の 3 つの目標を達成するように作られていなければなりません。

1

いかなるエンティティも信頼せず、常に検証する。

理論上は、「信頼せず、常に検証する」というのは非常に簡単なことように思えます。単にすべてのシステムとすべてのデータへのすべてのアクセスを切断すれば、ネットワークを封鎖できます。真の課題は、ほとんどのシステムが暗黙的な信頼を念頭に置いて設計されている中、ビジネスの大規模な中断を引き起こすことなく常に検証を行うことです。あらゆる種類のアクセスに対する幅広い可視性と制御、そしてポリシーを適用して維持するためのシンプルで実用的な手段が必要です。

2

検証後、最小限のアクセス権を付与する。

ゼロトラスト環境では、ユーザーを検証したら、当該ユーザーの役割に必要なアクセスのみを付与しなければなりません。

3

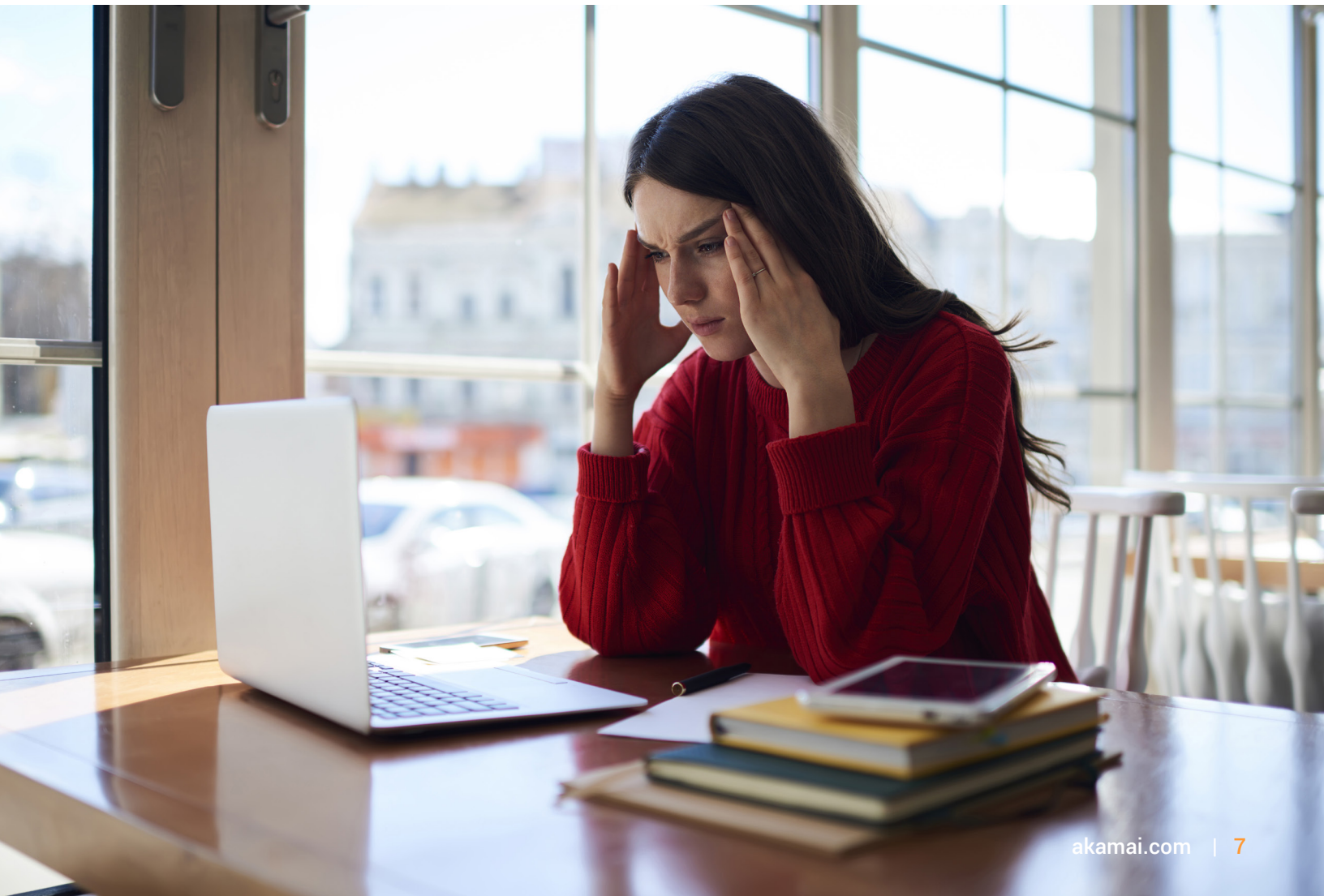
脅威を継続的に監視する。

ほとんどの業界の専門家が言うとおり、ゼロトラストは継続的な活動です。攻撃者は企業の防御を侵害するため、ますます高度化しており、組織は継続的にアクセスを監視、検証、制限する必要があります。ゼロトラスト・モデルの利点の 1 つは、攻撃者が行っていることではなく、企業自体が行っていることに重点を置いているということです。真のゼロトラスト・ポリシーを導入していれば、攻撃者は企業が導入しているすべての対策を即座に打ち破る必要があるため非常に困難となります。理想的には、企業はすべての攻撃をチェーンのどこかで阻止できます。まだ考え出されてもいない攻撃さえも阻止することができます。ゼロデイ攻撃であってもそうでなくても、ゼロトラストはそれを緩和できます。

ゼロトラストのダークサイド

しかし、ゼロトラストの導入に着手する際、組織はこのような信頼の欠如とアクセス制限の裏の側面も考慮する必要があります。ゼロトラストでは基本的に、主に許可リストを使用してアクセスを制限します。つまり、何を許可するのかを判断するということです。他のすべてはデフォルトで拒否されます。しかし、悪性キャンペーンを実行する攻撃者の能力を低下させた結果、意図せずして、従業員の業務遂行を妨げてしまう場合があります。また、ワークロードやデバイスを繰り返しチェックするのは、遅延やフラストレーションの原因になる可能性もあります。従業員が効率的に仕事をすることを妨げるゼロトラスト戦略は、戦略とは言えません。

有効なゼロトラスト戦略とは、セキュリティとアクセスのバランスが取れたものです。また、効果的な業務遂行とセキュリティチームのリソース（予算と人員の両方）のバランスを取る必要があります。

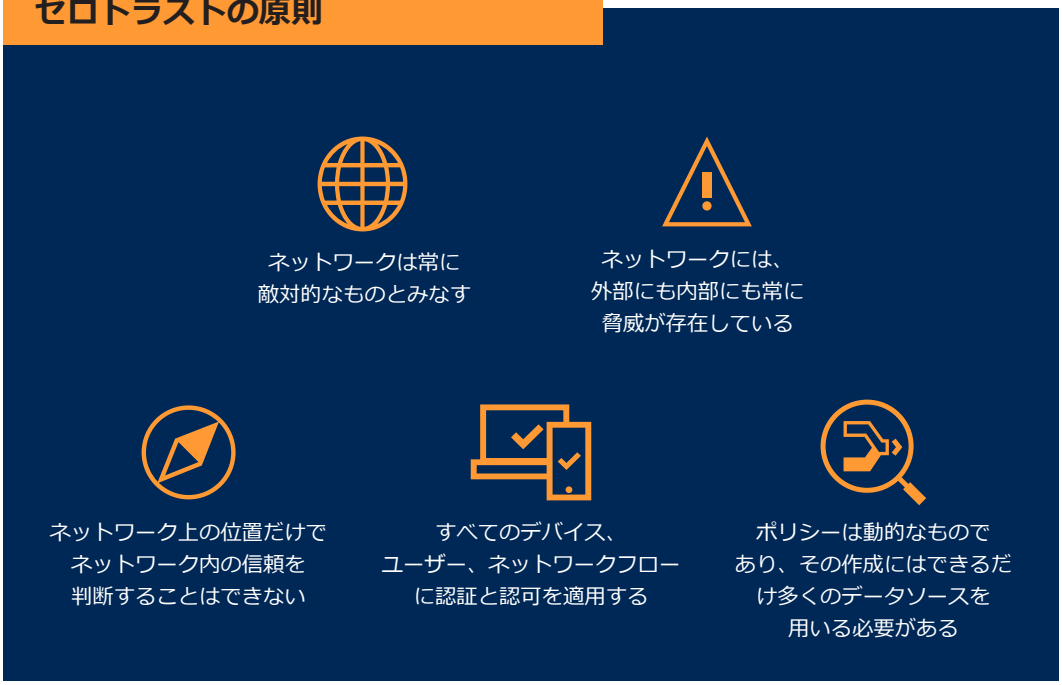


ゼロトラストの要素

Forrester が最初にゼロトラストの概念の概要を示してから 15 年が経過しました。現在、多くの組織はゼロトラストへの移行を開始したばかりであり、ソフトウェア製品の複雑な市場に直面しています。長年にわたってゼロトラスト・アーキテクチャの一部に対応してきた製品がありますが、他にも新製品が登場しており、多くのソフトウェアプロバイダーがゼロトラストという名称を使用して、既存の製品をリブランディングしています。さらに、多くのアナリストや業界オブザーバーが、「ゼロトラストは製品ではなく、包括的な戦略である」や「ゼロトラストはゴールではなく、継続的な取り組みである」と言います。しかし、このようなよくある主張は、ゼロトラスト・テクノロジー・ソリューションの購買決定に直面している人にとってあまり役に立たず、実際にはより混乱を招く可能性があります。

企業にゼロトラストをもたらす単一の製品はありません。各組織には異なる優先事項と脆弱性があるため、企業によってスタート地点は異なります。しかし、テクノロジーの進歩と業界の統合により、現在ではゼロトラスト・ポリシーを導入するために必要なツールを単一のソースから入手できます。アナリスト企業もこの事実を認識し始めています。

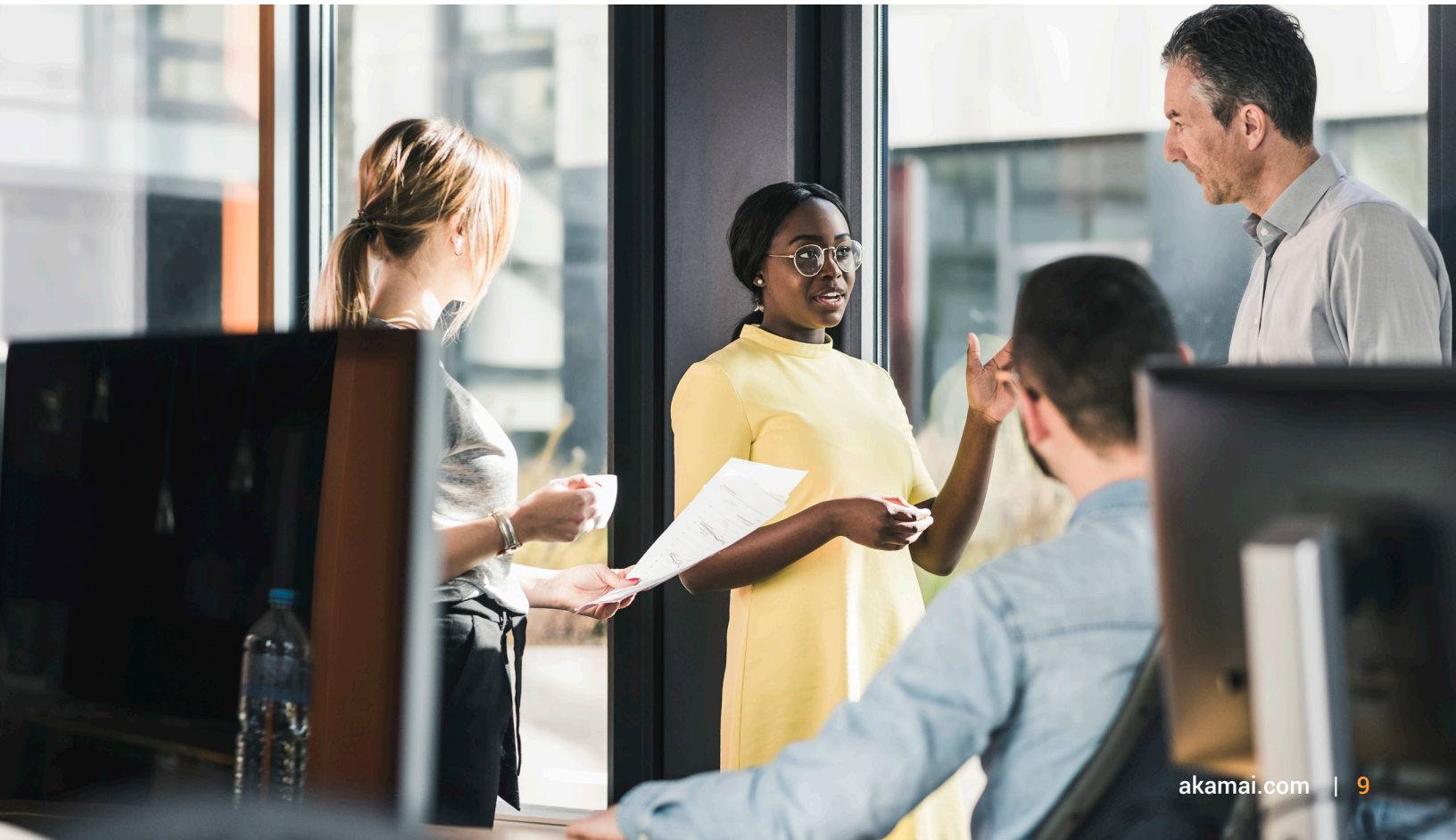
ゼロトラストの原則



Gartner はセキュア・サービス・エッジ（SSE）というものを追跡しています。これは、セキュア Web ゲートウェイ、クラウド・アクセス・セキュリティ・ブローカー、ゼロトラスト・ネットワーク・アクセス（ZTNA）を組み合わせたものです。レポート「What Are Practical Projects for Implementing Zero Trust?」（ゼロトラストを実装するための実践的なプロジェクトとはどのようなものか）において、Gartner はマイクロセグメンテーション（同社はワークロード間セグメンテーションと呼んでいる）も取り上げており、「実践的な実装に移行することを目指している組織は、ユーザー・アプリケーション間セグメンテーション（ZTNA）とワークロード間セグメンテーション（アイデンティティベースのセグメンテーション）という 2 つの主要なプロジェクトに重点を置く必要がある」と推奨しています。

同様に、IDC はゼロトラストを安全なアクセスとセグメンテーションに分けています。同社はこれを、論理的なセグメンテーション、アクセス制御、脅威検知によってコンピューティングシステム、リソース、データを保護するために使用される新しいテクノロジーと古いテクノロジーを総合的に捉えたものであると考えています。

しかし、これらの個別のシステムを 1 つの統合戦略にまとめることが中核的な課題となります。CIO、CISO、その他のセキュリティ専門家が自社に適したゼロトラスト・アーキテクチャを構築する際に追求すべき重要な要素は何なのでしょうか。



ゼロトラスト・ネットワーク・アクセス

ZTNA はゼロトラストに対するアプローチ全体を指すものと誤解されることがありますが、テクノロジースタックの基本的な要素です。安全なアクセスは、ゼロトラスト・フレームワークの重要な最初のステップです。残念ながら、プロセスの多くの要素と同様に、ZTNA は思ったよりもすぐに複雑化してしまいます。安全なアクセスは、二者択一の判断ではありません。ユーザーやアプリケーションがより広く分散されるようになったため、適切なユーザーに適切なアプリケーションへの適切なレベルのアクセス権を適切なタイミングで提供することは、はるかに困難になっています。実際、現在ではユーザーの定義に、顧客、サプライヤー、パートナー、そして従業員が含まれます。一方、アプリケーションにはレガシーアプリ、SaaS、モバイルアプリが含まれ、データセンター、インターネット、クラウド環境との間のアクセスが必要です。

効果的な ZTNA ソリューションは、ユーザーのアイデンティティとデバイスの健全性を確認し、ユーザーやデバイスの場所を問わず、必要なアプリケーションにアクセスできることを検証します。これにより、攻撃可能な領域が減少し、柔軟性と監視が強化されます。数十年にわたり、組織はアイデンティティプロバイダーがサポートする仮想プライベートネットワーク（VPN）を利用してアクセスを提供してきました。現在とは異なる時代向けに設計されたそのような VPN は、現在の分散した従業員の規模と範囲に対応するためには不十分です。ZTNA は進化を遂げ、単なる VPN の代わり以上のものになりました。現在ではユーザーとそのデバイスのアイデンティティの検証だけでなく、日時、ジオロケーション、デバイスポスチャーなどの属性に基づいてアクセスを許可し、適切な信頼レベルを付与します。

ゼロトラスト・ネットワーク・アクセス・ソリューションを購入する際の重要な考慮事項

企業が古い VPN からより高度なアイデンティティ管理ソリューションへの置き換えに着手する際、検討すべき領域がいくつかあります。今日では、アイデンティティおよびアクセス管理、アプリケーションセキュリティ、多要素認証（MFA）、シングルサインオンをすべて組み合わせて、1 つのインターフェースで管理の可視化と制御を行えなければ、高度なソリューションとは言えません。ゼロトラストの実現を目指す組織は、自社の現在のニーズに対応できるだけでなく、事業に合わせてスケーリングできるソリューションを探す必要があります。そのようなソリューションを利用すれば、合併した企業や買収した企業の従業員を迅速にオンボーディングしたり、さまざまな市場や地域での製造や生産を可能にしたり、業務委託先を簡単に追加および削除して変化するビジネスニーズに対応したり、セキュリティを犠牲にすることなくクラウドにアプリケーションをコスト効率よく移行したりすることができます。

組織は、既存のアイデンティティインフラに複数のディレクトリやアイデンティティ・サービス・プロバイダーが含まれている場合でも、そのインフラと直接統合できるソリューションを模索する必要があります。これにより、既存のアイデンティティインフラやアーキテクチャを変更する必要なく、ZTNA サービスを迅速に展開できます。

エッジに着目

また、市場の製品を選択する際には、ゼロトラスト購買チームが見落としがちな重要な差別化要因があります。エッジ・クラウド・プラットフォームと組み合わさったソリューションは、エッジプラットフォームへの接続を抽象化するアイデンティティ認識型プロキシとして機能し、すべての認証がエッジや、データセンターから離れた場所で行われるため、さらなるメリットをもたらします。一部の企業は DMZ 内で実行されるプロキシアーキテクチャへのアクセスを求めていますが、それではクラウドの機能を活用して攻撃をより効果的に吸収したり、キャッシング用の帯域幅を提供したり、必要に応じて自動スケーリングしたりすることはできません。

クラウドに組み込まれたアイデンティティ認識型プロキシは、オンデマンドでのスケーリング、CPU 負荷の大きいリソースの実行、攻撃の吸収を行うことができます。また、これはインターネットから直接アクセスできないプライベート IP アドレス上に配備されます。パフォーマンスとセキュリティが最も重視されるアクティビティが、エンドユーザーに最も近いエッジで実行されます。さらに、アプリケーションへの機微なイングレス（入方向の通信）経路はアプリケーションのリバーストンネルを介するため、境界の IP は見えなくなり、ボリューム型攻撃のリスクが軽減されます。

> **エッジ・クラウド・プラットフォームと組み合わさったソリューションは、アイデンティティ認識型プロキシとして機能し、さらなるメリットをもたらします。**

ゼロトラストの実現に向けた詳細な計画を策定する上での多要素認証に関する考慮事項

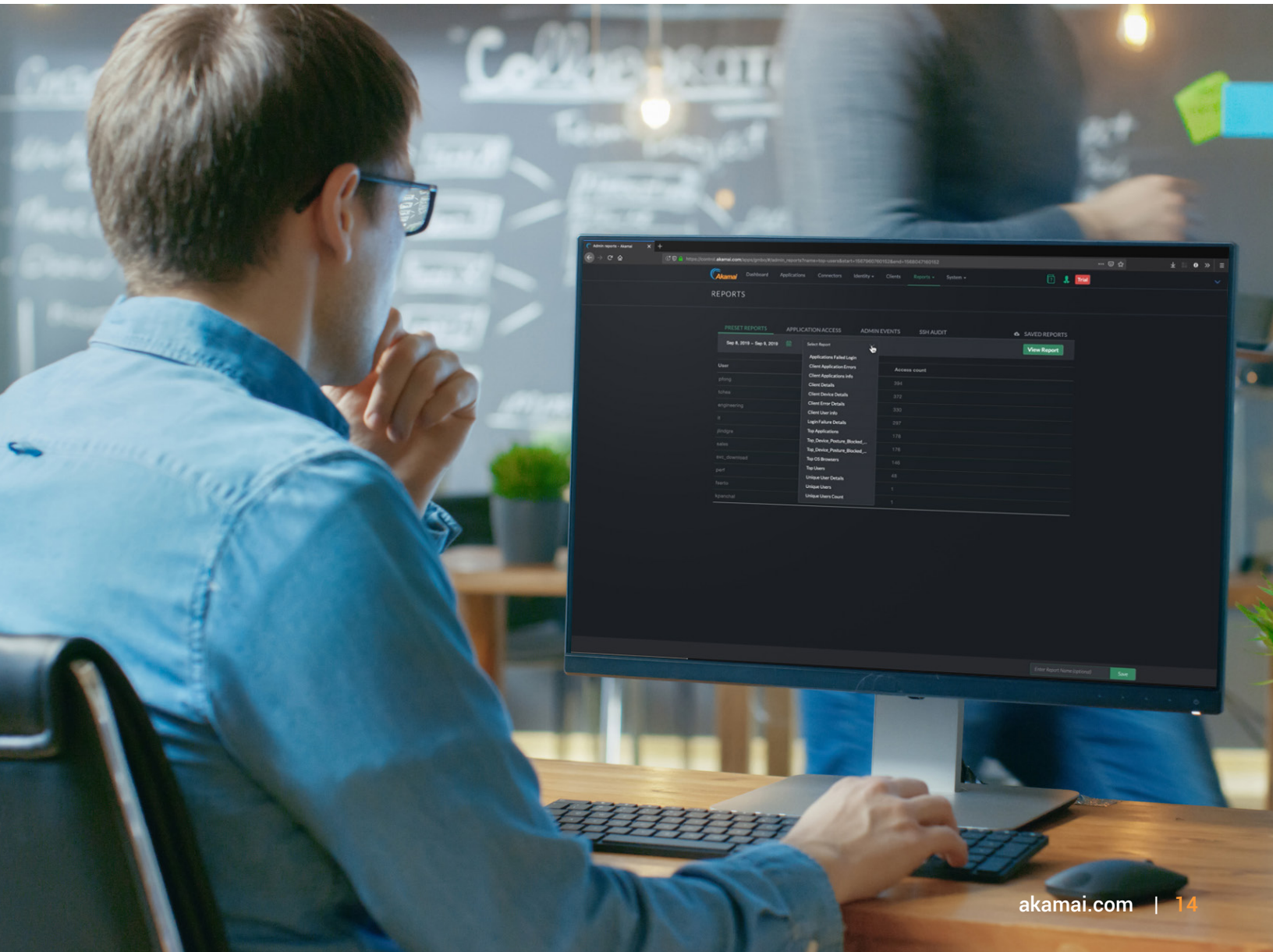
ハイブリッドワークが広まり、アクセスの強化が必要になったため、ほとんどの組織はすでに MFA を採用し、何らかのソリューションを導入しています。しかし、エンタープライズ全体でのアクセスと MFA の組み合わせは、それぞれの単なる寄せ集めではなく、それ以上の効果を発揮するということを認識しておくことが重要です。MFA は単なるパスワード以上のものを求めるため、信頼の概念の中核となります。よくある信頼の悪用の被害を回避するためには、2 つ目の検証が必要です。また、すべての MFA ソリューションが同じというわけではないことを覚えておくことも重要です。

ゼロトラスト戦略の一環として MFA ソリューションを評価する際、組織は次のようなソリューションを探す必要があります。

- アイデンティティ管理やエンタープライズアクセスと統合されている
- FIDO2 準拠により、ユーザー認証情報を分散、分離し、ユーザーの個人デバイスで暗号化することが可能。これは、フィッシング攻撃を回避するうえで特に重要な役割を果たしている
- 物理的なキーを使用せずに、スマートフォンを介してユーザーを確認できる

マイクロセグメンテーション

完璧なゼロトラストは存在しません。極めてしつこい攻撃者が発見して悪用する可能性のあるギャップが必ずあります。したがって、ゼロトラストに対する包括的なアプローチには、マイクロセグメンテーションが必要です。現在、ほとんどのネットワークにはセグメントがまったくないか、ほとんどありません。実際に組織はこれまでファイアウォールで重要なアプリケーションを保護してきましたが、これは多くの理由で困難であることがわかります。ファイアウォールでは基本的に、ネットワークポリシーを適用する必要があるため、渋滞ポイントが発生します。ファイアウォールを通過するためにはネットワーク接続が必要ですが、ファイアウォールはすぐにコストが増大し、現代のネットワークトラフィックに存在する多くのリスクを認識しておらず、変更が極めて困難です。そのため、多くの組織はファイアウォールではなくソフトウェアベースのマイクロセグメンテーションを選択し、そのような手間のかかるプロセスの多くをシンプル化しています。



マイクロセグメンテーションの差別化要因

マイクロセグメンテーションはゼロトラスト戦略の主要な要件ですが、多くの場合、中核的な ZTNA ソリューションとは分けて考えられてきました。また、マイクロセグメンテーションは、セキュリティ・プラットフォーム・プロバイダーによって販売されることも、スタンドアロンソリューションとして販売されることもありますが、バイヤーが理解する必要のある主な違いがいくつかあります。

どこに展開できるか。購買を検討しているバイヤーは、セキュリティ第一のアプローチではなくネットワークツールとして構築されたマイクロセグメンテーションソリューションや、オンプレミスシステム用に構築されたマイクロセグメンテーションソリューションに注意する必要があります。現代のツールは、クラウド、オンプレミス環境、デバイス上（エージェントをインストールできないデバイスを含む）、ハイブリッド環境のコンテナの中で展開できなければなりません。そのためには通常、クラウドベースのソフトウェアが必要です。自社の環境の 80% しかカバーできないマイクロセグメンテーションソリューションでは不十分です。

どの程度の可視性をもたらすか。マイクロセグメンテーションソリューションはアクセスを制限しますが、過剰な制限はビジネスプロセスを中断させ、COO からの苦情につながる可能性があります。マイクロセグメンテーションを実行するためには、自社の環境を深く理解する必要があります。どのサーバーがどのサーバーにアクセスできるでしょうか。Kubernetes クラスターと Windows 2008 サーバーの間でポリシーを定義できるでしょうか。多くのツールは、2008 年まで遡れるエージェントがないか、Kubernetes にポリシーを適用できるほど先見性を持って作られていません。ゼロトラストを効果的に展開するためには、マイクロセグメンテーションソフトウェアがこのような複雑な課題に対処できなければなりません。

さらに、マイクロセグメンテーションソフトウェアのバイヤーは、製品がサポートするポリシーのきめ細かさを考慮する必要があります。ほとんどのシステムは、ポートやプロセスのアプリケーション層でポリシーを適用します。より高度な製品は、マイクロサービス層でポリシーを適用できます。たとえば、攻撃者は一部の svchost のサービス（Task Scheduler など）を使用して、ネットワーク全体でラテラルムーブメント（横方向への移動）を実行できます。しかし、svchost はあまりにも多くの重要なことを実行するため、企業は svchost を完全にブロックすることはできません。マイクロサービス層でポリシーを適用するマイクロセグメンテーションソリューションは、そこで違いをもたらします。

実装はどの程度困難か。現在必要なポリシーをどれくらい簡単に表現できるかは、マイクロセグメンテーションソリューションを評価する際の重要な考慮事項です。また、今後何が必要になるかを考慮することも同じく重要です。計画段階である場合でも、封じ込めなければならない脅威が自社の環境に存在している場合でも、投資するエンジンがその両方を簡単にサポートできるものであることを確認しなければなりません。

マイクロセグメンテーションプロジェクトにおいて初めに許可リストを作成する際には、必要なアプリケーションやサービスを誤って拒否してしまうリスクがあるため、セキュリティチームが怖気づく可能性があります。洗練されたマイクロセグメンテーションソリューションには、すばやく簡単に展開できるテンプレートが含まれているため、プロジェクトの短期的な成果を挙げられます。短期的な成果を挙げたら、引き続き、正確な依存関係マッピング機能や状況の沿ったインベントリマッピング機能を含む、許可リストによる包括的な保護へと進むことができます。

> **購買を検討しているバイヤーは、セキュリティ第一のアプローチではなくネットワークツールとして構築されたマイクロセグメンテーションソリューションや、オンプレミスシステム用に構築されたマイクロセグメンテーションソリューションに注意する必要があります。**

DNS ファイアウォール

ゼロトラスト環境では、人だけでなく、インターネット自体も信頼できません。従業員はインターネットにアクセスする必要があります。SaaS やモバイルアプリケーション、クラウドサービス、ハイブリッドワーク、IoT デバイスなどが広まることにより、組織のアタックサーフェスも拡大します。マルウェア、ランサムウェア、フィッシング、データ窃取などの脅威から組織とユーザーを守ることが、これまでとは比べものにならないほど難しくなっています。組織には、セキュリティ制御ポイントの複雑さや、古いオンプレミスソリューションのセキュリティギャップを管理するためのリソースが限られています。

人とインターネットの間にゼロトラストを適用するためには DNS ファイアウォールが必要です。これがゼロトラスト戦略の中心的な機能になります。

DNS ファイアウォールに投資する際の主要なゼロトラスト要件

一見すると簡単ですが、DNS ファイアウォールに投資する際にテクノロジーバイヤーが考慮しなければならない要件があります。多くの組織はオンプレミスの DNS ファイアウォールを展開していますが、現在では場所に関係なく、その保護をユーザーに拡張する必要があります。アイデンティティ管理と同様に、堅牢なエッジプラットフォームを備えたプロバイダーは通常、その拡張プラットフォームから得られる脅威インテリジェンスのおかげで強固な DNS セキュリティを備えています。意思決定者は次の主要な要件を慎重に検討する必要があります。

DNS 検査。プロバイダーは高度な脅威インテリジェンスを使用してすべてのドメインをリアルタイムで検査し、悪性ドメインを自動的にブロックできなければなりません。また、ソリューションはあらゆるポートおよびプロトコルにおいて有効であるよう設計されていて、標準の Web ポートやプロトコルを使用しないマルウェアから保護する必要があります。DNS 検査の品質はプロバイダーによって大きく異なる可能性があり、バイヤーは市場での経験と顧客を成功に導いた実績のあるプロバイダーを探す必要があります。

すべてのデバイスの保護。プロバイダーには、ラップトップ、スマートフォン、タブレットなど、ネットワーク上やネットワーク外で使用されるデバイス向けのエージェントがなければなりません。

柔軟な DNS オンボーディング。プロバイダーは、DNS 要求を DNS ファイアウォールに転送して、最大限の柔軟性を実現し、すべてのユースケースをカバーするための複数の方法を備えていなければなりません。

DNS 窃取の特定とブロック。DNS 窃取、特に低スループットの DNS 窃取により、攻撃者は DNS チャネルを介してデータを窃取できるようになる可能性があります。独自の検知アルゴリズムに基づいてインラインとオフラインの両方の DNS 窃取検知を行うプロバイダーを探すことが重要です。

脅威の監視

ゼロトラスト・テクノロジーの最後の要素は、脅威の監視です。ゼロトラストの前提は、いかなるものも暗黙的に信頼しないということですが、組織は発生中の攻撃や新たな攻撃、潜在的なリスク（誤設定や過度に許可されたアクセス権など）を発見するために警戒を維持しなければなりません。セキュリティチームは、市場のソフトウェアを評価する際に、脅威の効果的な監視に関する次の 3 つの考慮事項を確認する必要があります。

主要な考慮事項

効果的なアルゴリズム
脅威監視サービスには、ユーザーやネットワークのアクティビティの異常、実行可能な分析、ログ分析などに基づいた成功実績のある高度なアルゴリズムが組み込まれている必要があります。

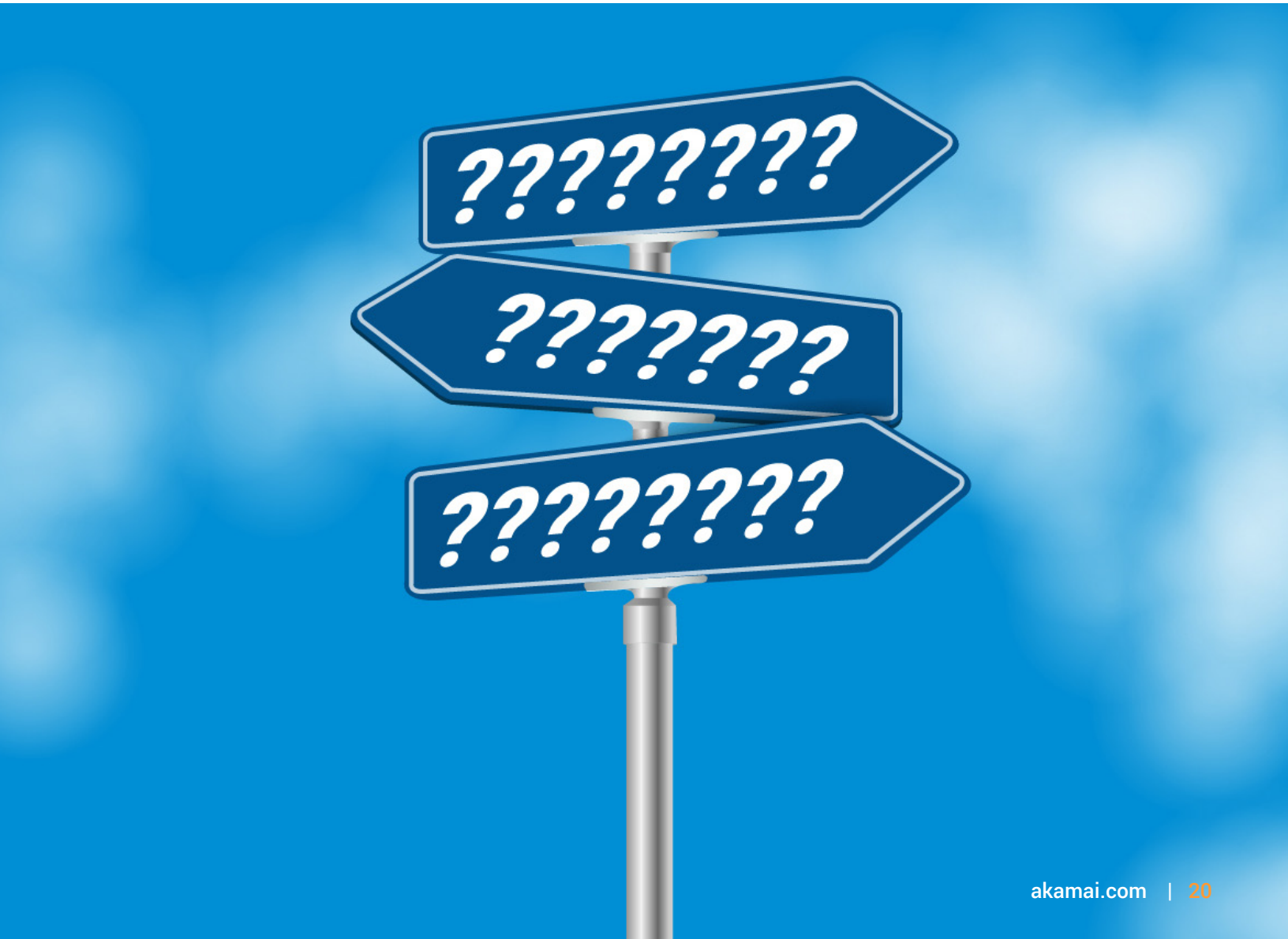
強力な信号検知
ソフトウェアと人工知能は脅威の監視に不可欠なツールですが、ゼロトラストの意思決定者は、自社が提携しているベンダーの社内専門知識を評価する必要があります。脅威監視サービスは、アラート疲れを回避するために適切な信号と悪い信号を区別し、即座にインシデントを通知できなければなりません。また、注目度の高いキャンペーンの分析など、定期的なレポートを提供しているプロバイダーを選択することが重要です。

経験豊富なスタッフ
チームは、攻撃対応、インシデント対応、データサイエンスなど、幅広い背景を持つ人員で構成されており、年中無休の 24 時間体制で対応できなければなりません。この点において大きなメリットをもたらすのが、コンテンツ・デリバリー・プロバイダーです。コンテンツ・デリバリー・プロバイダーは、数百テラバイト／秒の監視を通じて、さまざまな知見を得ており、あらゆる信号検知に対して独自の視点を持っています。

どこから始めればよいのか

ゼロトラスト戦略が完了することはありません。ソフトウェア、ハードウェア、採用の要件を検討している企業にとって最大の疑問となるのは、「どのテクノロジーから始めればよいのか」です。

多くの物事と同様に、その答えは各企業のニーズ、リスク評価、相対的な強みと弱みによって異なります。多くの業界オブザーバーにとって、答えは ZTNA の導入から始めることです。実際、垂直方向（North／South）の悪性トラフィックから組織を保護することは、賢明な出発点となり得ます。しかし、マイクロセグメンテーションを使用した水平方向（East／West）のアプローチ、特にソフトウェア定義のマイクロセグメンテーションから始めた方が良いと考える人もいます。



マイクロセグメンテーションから始めるケース

ほとんどの専門家と同様に、完璧な防御など存在せず、最終的には攻撃が防御を突破すると考える人は、最も価値のある資産を保護したいと考えます。それを可能にするのがマイクロセグメンテーションです。組織がマイクロセグメンテーションに消極的になる理由の 1 つが、マイクロセグメンテーションは複雑だとの印象を持っていることです。

まず、マイクロセグメンテーションはオール・オア・ナッシングのアプローチではありません。ゼロトラスト自体と同様に、段階的に実行できます。最も価値のある資産を特定することから始めることができます。極めて重要なものに重点を置き、何者かがシステムに侵入しても、ビジネスが停止しないようにします。資産の重要性は、その資産内のデータや既存の保護レベルに基づきます。

多くの場合、レガシーシステムをカバーするマイクロセグメンテーションソリューションが必要です。なぜなら、そのようなシステムはビジネスクリティカルなアプリケーションを実行していることが多く、とりわけ脆弱だからです。そのようなレガシーシステムのセキュリティ確保をサポートしていないマイクロセグメンテーションソリューションもあります。

次に、ソフトウェア定義のマイクロセグメンテーションにより、マイクロセグメンテーションは複雑であるという印象の多くは解消されます。ハードウェアに対処したり、ネットワークアーキテクトやセキュリティアーキテクトを何度も訪ねたりする必要はありません。ソフトウェアを展開するだけであるため、マイクロセグメンテーションを開始することに対する抵抗が大幅に軽減されます。

マイクロセグメンテーションを開始したら、早々に効果が表れ、プロジェクトの残りの部分を推進するための後押しとなります。たとえば、環境内で何が起こっているのかを把握するための信頼できる情報源が確立されます。ポリシーを適用しなくてもすぐに状況を把握し、フローがどのように発生しているかを十分に理解できるようになります。さらに、アプリケーションのリングフェンシングを開始したら、重要なアプリケーションを迅速かつ簡単にロックダウンし、特定のポートやプロセスを介してのみ通信を行うようにすることができます。

また、すぐに成果を挙げる方法は、脅威固有のポリシーをターゲットにすることです。高度なマイクロセグメンテーションプラットフォームには、拒否リストが組み込まれています。つまり、リモート・デスクトップ・サービスとインターネット間の不要な接続を停止するポリシーをすばやく作成できます。たとえば、Colonial Pipeline への攻撃につながった脆弱性を迅速に封じ込めることができます。

出発点がどこであっても、継続的なゼロトラストの鍵はバランスです。アイデンティティ管理が世界トップクラスでも、セグメンテーションや Web アクセスの保護が不十分であれば、優れたセキュリティは生まれません。

プラットフォームと専用ツールの比較

多くのテクノロジーに関する意思決定と同様に、ゼロトラスト・ソフトウェアを購入する際には多くの場合、個別の専門ツールを選ぶか、複数のコンポーネントを組み合わせたプラットフォームを選ぶかの二者択一になります。ゼロトラストの影響はセキュリティチーム、インテグレーター、アーキテクト、アナリストに及び、複数のコンソール、異なるエージェント、複数の統合でポリシーを維持する必要があるため、プラットフォームの方が説得力のある選択肢となります。これは、熟練したサイバーセキュリティ専門家が不足している厳しい労働市場において特に当てはまります。複数のベンダーのソリューションを管理する場合、人件費が大幅に増加します。なぜなら、効果的に相互通信できないソリューションがフォールス・ポジティブ（誤検知）を引き起こし、それがエンドユーザーの負担となり、追加のサポートやトレーニングが必要になる可能性があるからです。

さらに、サポートおよび契約交渉に関しては、「ワン・ハンド・トゥ・シェイク」（手を結ぶべきは 1 社だけ）という有名な言葉があり、これはプラットフォームプロバイダーと協力してゼロトラストを導入すべきであることを訴えています。

理想的には、柔軟なアプローチを備えた単一のプロバイダー、すなわち包括的なゼロトラスト・プラットフォームと個々のポイント製品を提供するプロバイダーを探すべきでしょう。この柔軟性により、単一のプロバイダーの利点を享受しながら、より簡単にゼロトラストを実現できるようになります。

> **組織がマイクロセグメンテーションに消極的になる理由の 1 つが、マイクロセグメンテーションは複雑だとの印象を持っていることです。**

ゼロトラストの要素の再確認

ユーザーを知る。
確実にユーザーを検証する。

資産を保護する。
すべてのトランザクションに認証／認可を適用する

ユーザーを保護する。
ユーザーのマルウェア感染を防ぐ

結論

結局のところ、サイバー攻撃からの保護に関心のあるほとんどの組織は、ゼロトラスト・アーキテクチャへの移行を早く開始する必要があることを認識しています。多くの組織はすでに、テレワークの増加への対応として、徐々にまたは急速に取り組みを開始しています。しかし、攻撃者の巧妙化に伴い、アタックサーフェスが拡大しています。また、より多くのユーザーがリモートアクセスを求めるようになっており、連携性に優れた総合的なソリューションポートフォリオの必要性は高まる一方です。

ゼロトラストに対する Akamai のアプローチについて、詳しくは akamai.com/zerotrust をご覧いただくか、Akamai のエキスパートへお問い合わせください。

Akamai のセキュリティについて

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。公開日：2024 年 10 月。