ホワイトペーパー

ハウツーガイド：ゼロトラスト・セキュリティへの変革

Akamai

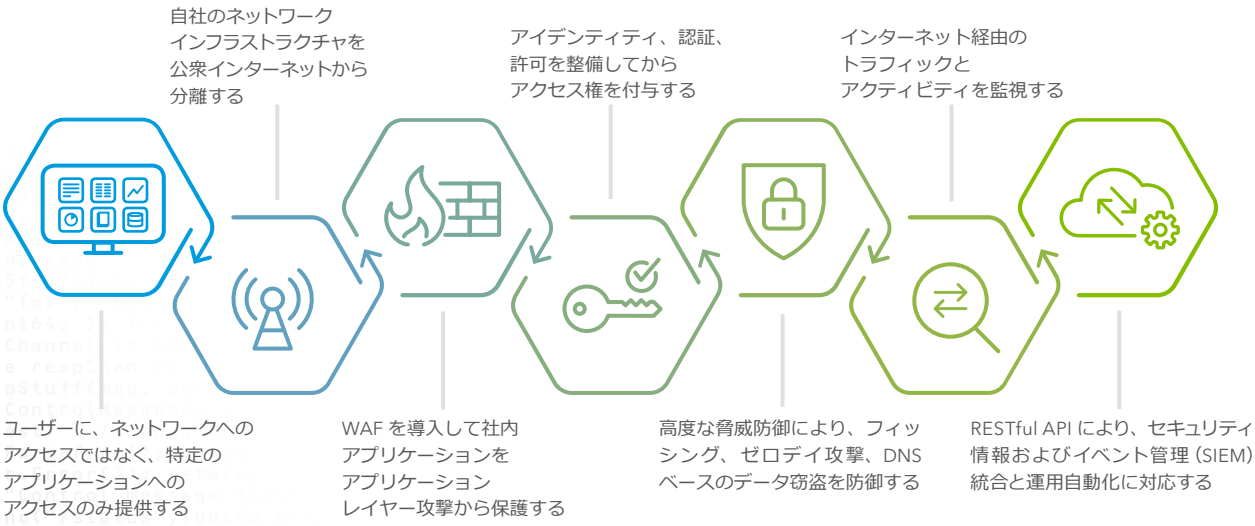
エグゼクティブサマリー

ネットワーク境界という考え方、つまり、エンタープライズ組織が制御する領域の外側にいるユーザーは悪意を持ち、内側にいるユーザーは誠実で善意を持つとする考え方は、今日のビジネス環境では当てはまりません。SaaS アプリケーションの普及、クラウドベースのアーキテクチャへの移行、リモートユーザーの増加、BYOD デバイスの出現により、境界ベースのセキュリティは通用しなくなりました。また、境界中心の防御には、機器やセキュリティポリシーの管理と頻繁なソフトウェアアップグレードが必要なため、運用が複雑化し、ただでさえ業務で手一杯の IT チームの負担が増します。アタックサーフェス（攻撃の対象となり得る領域）が拡大するなか、限られた IT リソースで、かつてないほど複雑化したネットワークアーキテクチャを管理するのは困難です。一方、サイバー犯罪者については、セキュリティ対策を迂回する技術がますます熟練・高度化しており、その動機も高まっています。必要なのは、このような固有の課題に対応するための戦略的なセキュリティフレームワークです。

ゼロトラスト・セキュリティとその重要性とは？

ゼロトラスト・モデルとは、境界中心のセキュリティに代わる新しいセキュリティアーキテクチャです。セキュリティとアクセスは、アイデンティティ、デバイス、ユーザーコンテキストに基づいて動的に判断されます。また、ゼロトラスト・セキュリティ・フレームワークでは、認証や許可を受けたユーザーおよびデバイスのみがアプリケーションやデータにアクセスできます。さらに、アプリケーションやユーザーをインターネット上の高度な脅威から保護します。

ゼロトラストへ移行し、ユーザーとアプリケーション、そして会社の未来を守るために、以下を実行することをお勧めします。



ユーザーに、ネットワークへのアクセスではなく、特定のアプリケーションへのアクセスのみ提供する

仮想プライベートネットワーク（VPN）などの従来のリモート・アクセス・テクノロジーでは、境界のない今日のデジタルビジネスにおいて高まるニーズには対応できません。従来の VPN ではファイアウォールに抜け穴ができ、ネットワークへの無制限のアクセスが可能になるため、エンタープライズのセキュリティが脅威にさらされます。侵入に成功した攻撃者は、横方向に自由に移動し、ネットワーク内のあらゆるシステムやアプリケーションにアクセスして悪用できます。従来の VPN は、企業にセキュリティリスクをもたらすだけではありません。ハードウェアとソフトウェアの管理に大量の IT リソースを必要とする複雑なソリューションでもあり、保守と拡張も高コストとなります。

無制限アクセスへの対抗策としてネットワークのセグメント化を採用する組織もありますが、コストが高く、実装が困難で、管理が煩雑です。しかも、結局はリスクの軽減にもつながりません。「すべてを許可」する方式のアクセス制御では、ネットワーク内でのラテラルムーブメント（横方向の移動）を許すことになるためです。ネットワークのセグメント化では、サブネット内の水平方向のトラフィックを区画化できるだけで、同一サブネット内でのラテラルムーブメントを阻止できません。

ゼロトラストを実現してビジネスを保護するためには、各自の役割に必要なアプリケーションへのアクセスのみを許可します。権限、ユーザーアイデンティティ、デバイスの状態、認証、許可に基づいてアクセス権を付与します。このベストプラクティスにより、ラテラル攻撃を抑制し、ネットワークへの露出を制限できます。従来の VPN から脱却することで、ユーザー体験の改善、従業員の生産性向上、ヘルプデスクチケットの低減が実現します。また、ファイアウォール、ハードウェア、ソフトウェアへの依存から抜け出すことで、IT 保守コストも削減できます。加えて、アプリケーションへのアクセスのみを許可することでガバナンスを強化でき、アプリケーションにアクセスしているユーザー、データの移動先、データへのアクセス方法などに関する可視性と知見も獲得できます。

各自の役割に必要なアプリケーションへのアクセスのみ許可します。権限、ユーザーアイデンティティ、デバイスの状態、認証、許可に基づいてアクセス権を付与します。

自社のネットワークインフラストラクチャを公衆インターネットから分離する

内部のアプリケーションやアクセスインフラストラクチャをインターネットにさらすと、DDoS や SQL インジェクションなどのアプリケーションレイヤー攻撃に対して脆弱になります。サイバー犯罪者の手口はますます巧妙化しています。かつてないほど進化した手法を用いて、エンタープライズのネットワーク設定をスキャンし、脆弱なアプリケーションや貴重なデータを見つけ出します。そのため、オープンなリスニングポートを使用する攻撃者の標的にならないよう、自社のアプリケーションとアクセスアーキテクチャを公衆インターネットから分離する必要があります。サイバー犯罪者がネットワークを見つけられず、標的デバイス上で実行されるアプリケーションやサービスを特定できなければ、攻撃することはできません。

WAF を導入して社内アプリケーションを保護する

現代のサイバー攻撃は高度標的型です。攻撃者はソーシャルエンジニアリング（メール、ソーシャルメディア、インスタントメッセージング、SMS など）を活用し、関連性の高い、パーソナル化された仕掛けを用いて標的を攻撃します。サイバー犯罪者は特定の役職やスキルセット、アクセスレベルなどを持つユーザーを見つけ出し、そのユーザーのアクセス権を標的にアプリケーション攻撃を開始します。

ユーザーのマシンに侵入したら、所有者に知られることなく、それをボット化した「ゾンビデバイス」として使用して、ファイアウォールの内側にある（安全だと思われている）社内アプリケーションを攻撃します。この種の攻撃から自社のインターネット接続アプリケーションを保護するために、ほとんどの組織が Web Application Firewall（WAF）を導入しています。しかし、多くの組織は WAF 保護をネットワーク内の社内アプリケーションには適用していません。WAF により、アプリケーションレイヤー攻撃やインジェクション攻撃（SQL インジェクション、悪意のあるファイルの実行、クロスサイト・リクエスト・フォージェリ―（CSRF）、クロスサイトスクリプティングなど）から社内アプリケーションとそのデータを保護できます。

サイバー犯罪者は特定のデバイスに狙いを定め、それをゾンビデバイスとして使用して、ファイアウォールの内側にある（安全だと思われている）アプリケーションを攻撃します。

アイデンティティ、認証、許可を整備してからアクセス権を付与する

デジタルシステムでは、各ユーザーのアイデンティティを検証することなく、正しいパスワードを入力したすべてのユーザーにアクセス権が付与されます。認証情報が脆弱だったり、パスワードの使い回しを行うと、エンタープライズ組織のアタックサーフェスとリスクが大幅に増大します。現在の脅威状況では、ユーザー名やパスワードなどの単要素認証では不十分です。多要素認証（MFA）は検証とセキュリティをさらに強化する認証方式です。検証済みのユーザーだけがビジネスクリティカルなアプリケーションにアクセスできます。

多要素認証は必要不可欠です。認証情報が脆弱だったり、ユーザー名やパスワードを複数のアプリケーションで再利用したりすると、エンタープライズ組織のアタックサーフェスが大幅に増大します。

MFA を通じて認証と許可を受けたユーザーは、シングルサインオン（SSO）により、1 組の認証情報ですべてのアプリケーションにログインできます。その結果、アプリケーションごとにアイデンティティを再確認したり、アプリケーション間で同期する必要がないため、生産性が向上します。多数の信号（IaaS、オンプレミス、SaaS の各アプリケーションにわたる MFA や SSO など）に基づいて、アクセスを継続的に制御することで、保護を強化し、エンドユーザーの利便性を改善できます。

高度な脅威防御により、フィッシング、ゼロデイ攻撃、DNS ベースのデータ窃盗を防御する

多くの企業が多層セキュリティを導入しているにもかかわらず、攻撃者はセキュリティの脆弱性を悪用してエンタープライズに侵入することに成功しています。ファイアウォール、セキュア・ウェブ・ゲートウェイ、サンドボックス、侵入防止システム、エンドポイントのウイルス対策を導入済みの企業であっても、フィッシング、ゼロデイ攻撃、DNS ベースのデータ窃盗の被害を受けています。このようなエンタープライズに不足しているものは何でしょうか？

DNS は見過ごされることが多い攻撃ベクトルです。サイバー犯罪者は、このセキュリティギャップを悪用するための専用マルウェアを開発することで、既存のセキュリティレイヤーを回避してネットワークに侵入し、データを盗み取ります。そのため、DNS プロトコルを活用したセキュリティレイヤーを追加することが重要です。DNS セキュリティソリューションは、最初のクエリー段階となる DNS プロトコルをセキュリティ・コントロール・ポイントとして使用することで、キルチェーンの初期段階においてサイバー攻撃を検知して阻止し、エンタープライズの事前対応型の保護を実現します。

DNS プロトコルをセキュリティ・コントロール・ポイントとして使用することで、キルチェーンの初期段階においてサイバー攻撃を検知して阻止することが重要です。

インターネット経由のトラフィックとアクティビティを監視する

企業は、環境が敵意に満ちていることを前提にすべきである。これがゼロトラストの基本的理念です。したがって、盲目的に許可するのではなく、すべてのアクティビティを監査し確認する必要があります。そのためには、豊富なトラフィックとインテリジェンスに基づいて、ネットワークの状態を可視化し、適切に比較しなければなりません。

企業ネットワーク内外のデバイス（ラップトップ、携帯電話、デスクトップ、タブレット、ゲスト Wi-Fi、IoT デバイスなど）から送信されたすべての DNS リクエストを監視および検証し、悪意のあるサイトや許容できないサイトにクエリーが向かわないように確認する必要があります。また、コマンド & コントロール（C & C）サーバーとの通信やデータ窃盗などの疑わしいアクティビティの兆候がないか、トラフィックのふるまいを調査し、問題があれば即座に IT チームに警告しなければなりません。グローバルでのトラフィック量や脅威傾向を把握することで、IT チームは異常なパターンや危険なパターンを特定しやすくなります。

RESTful API により、セキュリティ情報およびイベント管理（SIEM）統合と運用自動化に対応する

エンタープライズは数百または数千ものアプリケーションを使用します。これらのアプリケーションを迅速に一括展開するためには、API を介して設定する必要があります。また、アクセスに関するポリシー制御も設定しなければなりません。API は、大規模アプリケーション環境において従来の VPN アクセスからアプリケーション固有のアクセスに移行するために欠かせない機能です。API の導入はますます進んでいます。エンタープライズ組織が DevSecOps を採用し、監視と設定のための RESTful API を求めているためです。また、さらなる調査と相関分析を実行するために、脅威データとイベントデータを SIEM に組み込むためのプラグインも必要とされています。加えて、サードパーティーのエンドポイント検知および対応ソリューションに信号を送信し、ワークフロー自動化プラットフォームや脅威対処と統合できる、拡張性に優れたシステムも必要とされています。

結論

デジタル変革はすでに現実のものとなっています。エンタープライズ組織はゼロトラスト・セキュリティ・モデルを採用することで、セキュリティを損なうことなく、ビジネスを進化させ、イノベーションとアジリティを実現しなければなりません。ゼロトラスト環境を運用する主なメリットとして、すべてのアプリケーション（SaaS、オンプレミス、IaaS）にわたって高度な脅威防御、アプリケーション高速化、MFA、SSO を導入できる点が挙げられます。また、ゼロトラスト・セキュリティ・モデルにより、API を介した運用自動化や SIEM ／ワークフロー自動化プラットフォームとの統合が実現します。これにより、ユーザーやアプリケーションを可視化し、大規模展開に要する時間を数分の 1 にまで短縮できます。

Akamai は貴社のネットワークとセキュリティの進化を支援します。7 つの質問から成るゼロトラスト評価にご回答いただくと、自社のゼロトラスト・セキュリティ・フレームワークの準備レベルを把握できます。また、ご回答に応じた次のステップに関するアドバイスを受けて、ネットワーク変革を推進できます。ゼロトラスト環境への移行を開始するためのリソースについては、akamai.com/3waystozerotrust をご覧ください。