SOPHOS

ゼロトラストについて

企業ネットワークと単一のセキュリティ境界を構築する時代は終わりつつあります。ユーザーは、公共のインターネットを介してリモートで作業をすることが増えています。SaaS (Software-as-a-Service) アプリ、クラウドプラットフォーム、およびその他のクラウドベースのサービスの増加により、主な要素としてネットワークを使用してリソースを保護する効果が失われてきています。ネットワーク間の境界があいまいになっているため、単一で外部から隔離された企業ネットワークに依存することはもはやなくなり、ネットワーク内に存在するすべてのシステムを信頼する余裕がなくなりました。

ゼロトラストへの参入とは、セキュリティについて熟考し、どのように対応するかに関するサイバーセキュリティの理念です。 ゼロトラストは、「何も信頼せず、すべてを検証する」という前提に基づいており、物理的またはデジタル的な場所に関係なくリソースを保護し、初めから何も信頼しないことに重点を置いています。

ゼロトラストを実現させるベンダー、製品、テクノロジーは、ありません。むしろ、組織内の文化的な変革と、リソースを保護するパラダイムを変化させるさまざまなソリューションが必要です。

このホワイトペーパーでは、ゼロトラストの概念、ゼロトラストモデルを実装するメリット、および組織がゼロトラストモデルへ移行するために必要な手順について説明します。

時代は変わりました

特に信頼が暗黙的で無条件に当たり前であると思われる場合は、この信頼は、情報技術の分野では危険な言葉となります。

企業が外部から隔離された大規模なネットワークセキュリティの境界を造り上げ、内部のすべてを信頼することは、間違ったデザインであると証明されています。この防御の緩さはハッカーにとって夢のような場所です。一旦内部に侵入すると、多くの場合、見えなくなります。ネットワーク全体に分散して、重要なシステムへアクセスすることは、セキュリティ制御と最も強力なチェックが境界にあるだけなので簡単です。

好まずとも、境界線は失われてきています。

ユーザーは、カフェにある公共 Wi-Fi のような信頼されていないネットワークを使用してテレワークを望んでいます。そして、必要なときにいつでもデータにアクセスできるように、データをクラウドに保存したいと考えたり、企業のデータやリソースにアクセスするために、個人所有のデバイスを使用したいと考えています。ユーザーは、いつでも、どこでも、好きなときに作業できるように、スムーズなアクセスを求めています。

SaaS (Software-as-a-Service) アプリ、クラウドプラットフォーム、その他のクラウドベースのサービスの使用により、データが企業の境界外に残り、パブリッククラウドプラットフォームは、企業の境界内で実行されたデバイスやサービスを多くが境界外で実行されるようになります。ソフォスのワークロードは、所有、制御、信頼できるネットワークから離れた場所で、最もコスト効率の良い方法で処理できるようになります。

すべてがどこにでもあります。静的な防御機能を備えた旧式の「企業ネットワーク」モデルでは、データ、ユーザー、顧客を同時に保護しながら、企業がクラウドなどを併用することはできませんでした。そこで、パラダイムシフトが必要となります。

ゼロトラストの参入

ゼロトラストとは、こうした脅威に対するセキュリティへの総合的なアプローチで、組織の取り組み方における変化を示します。これは、セキュリティについて熟考し、どのように対応するかを考えるモデルと理念であります。

企業ネットワークの内部であれ外部、またはネットワーク自体であっても、疑うことなく誰かや何かを信じたりするべきではありません。従来のファイアウォールのような静的防御を使用して、暗黙的な信頼をネットワークの場所に基づいて制限する必要があります。

最終的には何かを信頼する必要がありますが、ゼロトラストでは、この信頼は一時的なものであり、これまでに使用した以上に複数のデータソースから動的に確立され、常に再評価されます。データソースに含まれるものは、アクセス要求、ユーザー情報、システム情報、アクセス要件情報、脅威インテリジェンスに関する情報です。さらに、データやリソースへのアクセスは、必要に応じて、接続ごとにのみ許可されます。

信頼されていないネットワークに関しては、インターネットを日常的に使用することで何度も経験しています。公共のインターネットを使用するコンピュータは、従来の境界内のコンピュータとはまったく異なる方法でセキュリティが保護されます。外部の脅威からコンピュータを保護するには、特別な監視と多層防御が必要となります。

ゼロトラストモデルでは、すべてのデバイスをインターネットに接続しているかのように使用できます。

単一の境界を設定するのではなく、すべてのデバイス間にチェックとコントロールを適用して、多数のマイクロ境界 (マイクロセグメント) を作成する必要があります。

ゼロトラストを採用する主なメリット

ゼロトラストモデルを採用することで、数多くのメリットが生じます。お客様の生活をよりスムーズにするためにコアモデルのいくつかをご紹介します。

IT 資産全体の管理

オフィス内から、ユーザーが使用するクラウドプラットフォームまでを制御企業の境界外での制御が不足したり、リモートユーザーとの連携に苦労することはもうありません。

すべてのユーザーを同じ方法で管理、保護

企業の境界の内側や外側がなくなったため、すべてのユーザーを同じように扱うことができます。これにより、IT セキュリティが簡素化されるだけでなく、すべてのデバイスとユーザーが等しく扱われるようになります。

使用中のインフラストラクチャを完全に制御していない場合でさえも、セキュリティを保持

アイデンティティ、場所、デバイスのセキュリティ状態、MFA、オーバーレイの監視と分析を使用することで、あらゆる種類の環境、プラットフォーム、サービスにわたって強力なセキュリティを維持できます。

マルウェアや攻撃者の動きが大幅に減少

攻撃者は一旦内部に侵入したら、ネットワーク全体をすべて思い通りにするというよりも、侵害されたユーザーがアクセスした最小限のシステムにしかアクセスしません。認証されたユーザーを信頼し続けないことで、システム間でチェックが実施され、分散する機能がさらに制限されます。

ゼロトラストの概要

ゼロトラストとは大きな発想であるため、それに関して多くの議論が展開されています。基本的に、経験に沿って心に留めておくべきいくつかのゼロトラストに対する主な概念を要約しておきます。

ネットワークに「内部」は存在しない

例えば、カフェの公共 Wi-Fi など、信頼できない場所から仕事をしているとします。そこで、すべてのデバイスが公共のインターネットなど、すべてのネットワークの中で最も危険な場所に直接接続されていると想定しましょう。これが実際に起こっていると想像することで、従来の企業の境界を盾にする方法でないやり方で、セキュリティを適用しなければいけません。

管理システムや社内システムには常に企業の「信頼できる」ネットワークが存在していますが、アプリケーションプロキシやそのほかのテクノロジーを使用して、通常のユーザーをネットワークから距離を置いた状態に保ち、攻撃対象領域を大幅に削減することが目標です。

何も信頼せず、すべてを検証

ネットワークの内部と外部の両方に攻撃者がどのような時も存在し、常に攻撃をしていると想定します。ユーザーやデバイスは自動的に信頼されないようにし、接続を考慮する前に認証する必要があります。あらゆる方向から常に攻撃を受けていることを想像することで、強固な認証とリソースへの承認を構築し、防御を強化し、常にユーザーの領域で発生するすべてを管理、分析します。

セキュリティはリアルタイムな適用が必要

ゼロトラストを実現するために導入するセキュリティポリシーは、できるだけ多くのデータソースとできるだけ多くの異なる技術からの洞察に基づき、動的で自動的に変更される必要があります。「このデバイス」上の「このユーザー」のような静的ポリシーは、もしそのユーザーがデバイスを使用している時にデバイスが侵害された場合は、そのデバイスは保護されません。悪意のある動作の識別のように、ユーザーのポリシーがデバイスのセキュリティ状態も考慮している場合、ポリシーは、この考慮を適用して、管理者の作業をまったく行わずに状況に動的に適応できます。

これは、サイバーセキュリティにおけるソフォスの戦略および理念の一環であり、長年にわたり続けてきたことです。Synchronized Security とは、ソフォスの製品がお互いに独自のインサイトを共有できるものだということをご存じかもしれませんが、これにより、適応性の高い動的なポリシーが作成され、すべてのインサイトを活用することで、ポリシーが静的で簡単に回避されるようなことがなくなります。

その多くは、ユーザーがすでに行っている可能性のある優れたセキュリティポリシーとベストプラクティスです。もし GDPR に備えていたら、もうすでに多くの作業を行っています。

ゼロトラストの原則

絶対に何も信頼しない。.何も信頼しない場合は、リスクがある場所に関連するセキュリティ対策を講じる必要があります。

すべてを検証する。小切手を渡せば自然と信頼をもたらすと思い込んではいけません。認証情報を持っているということは、本当の意味での信頼ではありません。それは、ただ単に認証情報があるというだけです。認証情報は盗まれる可能性があります。

このことを 4つのシンプルな原則に分類するので、ご留意ください。

常に識別

単一の信頼できる ID が必要となり、SSO (シングルサインオン) 使用してあらゆる場所で使用できます。すべては、多要素認証 (MFA) を使用して認証される必要があります。ユーザーがどこにいても、アクセスしようしているものが何であれ、認証情報を検証し、二要素 (多要素) 認証があることを検証し、定期的に再認証をしてください。

認証情報が盗まれたり、システムが乗っ取られた場合、MFA と通常の再認証により即座に攻撃者を阻止します。

常に制御

必要な個所に制御とチェックを適用し、最小権限の原則を採用して実行します。ユーザーは、ジョブを実行するために必要な最小限の権限のみにアクセスできるようにする必要があります。例えば、ドイツ人のスタッフのみが使用する人事システムがある場合は、ドイツ人のスタッフのみがアクセスできるようにします。たとえアクセスのリスクが低いと思われていても、誰にでもアクセス権を与えるべきではありません。

常に分析

認証が上手くいったり、そのユーザーまたはデバイスにアクセスが許可されたからといって、信頼できるという意味ではありません。インサイダーの脅威や悪意のある攻撃者が、有効な認証で情報にアクセスする可能性もあります。すべてのネットワークおよびシステムアクティビティを記録し、定期的にアクセスを分析、検証して、認証後に発生することを確認します。SIEM (セキュリティ情報およびイベント管理)、EDR (Endpoint Detection and Response)、MDR (Managed Detection and Response) は、まさにこのニーズに対応するために登場しました。

常に保護

サイバーセキュリティに対して「インサイドアウト」のアプローチを使用します。重要なデータに焦点を当て、データが作成された瞬間から削除される瞬間までのネットワーク内のデータの流れに従って、脆弱性のポイントを特定する必要があります。

コンプライアンスや規制ではなく、その他のすべてのリスクを常に考慮してください。コンプライアンスチェックや規制要件をただ満たすためだけにセキュリティを適用することは危険です。コンプライアンス要件は、ネットワーク、フロー、ワークロード、システム、テクノロジーの内容を把握していません。ネットワークのすべての要素に関連するリスクを把握しているわけではありません。リスクを考慮し、組織が直面する脅威がモデル化することで、セキュリティを強化する個所、緩和する個所、マイクロセグメントを作成する個所が確実に把握できます。

ゼロトラストへの移行

ゼロトラストに移行して、そのメリットのすべて活用するにはどうすればよいでしょうか？

サーフェスを定義し、リソースを識別 | 標準パスと特権パスのマッピング | ゼロトラストネットワークの構築 | ゼロトラストポリシーの作成 | 境界の監視と保守

サーフェースを定義し、リソースを識別

まず、保護、制御、監視するサーフェスを定義する必要があります。業務で使用しているすべてのリソース、サービス、アプリ、デバイスは何ですか。ネットワーク全体で使用されているすべての範囲を明確に把握することで、新しいゼロトラスト考え方を適用することができます。

標準パスと特権パスのマッピング

すべての範囲を設定したら、標準パスをマッピングする必要があります。標準パスと想定されるすべての間にあるフロー、動作、関係は何ですか。ユーザーグループは、アプリケーションにアクセスして、デバイスはネットワークに接続します。サービスは、データストアなどを使用しますが、特権パスは何でしょうか。管理者は、管理コンソールに接続し、RDP (リモートデスクトッププロトコル) を使用して機密データなどをホストしているサーバーにアクセスします。特権パスでは、通常、追加のセキュリティや制御を適用する必要があります。

ゼロトラストネットワークの構築

範囲内のものと、すべての間にある関係がどのようなものであるかが分かったので、ゼロトラストの理念を適用し始めることができます。適用するセキュリティ対策とアクセス制御を特定し、どこで、どの技術がどのリスクを最も軽減するかを特定します。

ゼロトラスト ポリシーの作成

次に、ゼロトラストポリシーを実装して、できるだけ多くの異なるデータソースを使用して、任意の接続または要求にコンテキストを追加する必要があります。

境界の監視と保守

最後に、最も重要なのは、新たに作成された境界を維持できるように、すべてを詳細な監視でオーバーレイする必要があることです。

これは、管理者が直面する最大の変更点の 1つです。一旦ウイルス対策をインストールして設定して、ゼロトラストで信頼性のないコンソールを見る必要がない場合は、習慣を変える必要があります。

EDR などのツールを利用して、発生したイベントを監視し、脅威が環境に侵入した原因と、検出前または潜在的な侵害後に発生したイベントを把握する必要があります。

MDR のようなサービスは、この分野で非常に役立ちます。サイバーセキュリティの専門家は、ユーザーに代わって、ネットワークの監視や脅威の破壊を支援します。

ゼロトラストのテクノロジースタック

ネットワーク上のすべてのリソースとアセットを保護するには、多くの技術を必要とします。すべての問題を解決する単一のベンダー、製品、またはテクノロジーは存在しません。

ゼロトラストのテクノロジースタックは、ゼロトラストの管理と、さまざまなリソースとアセットにおけるセキュリティと制御という 2つの主要な領域に対応する必要があります。

管理は、次の 3つのサブ領域に分類されます。

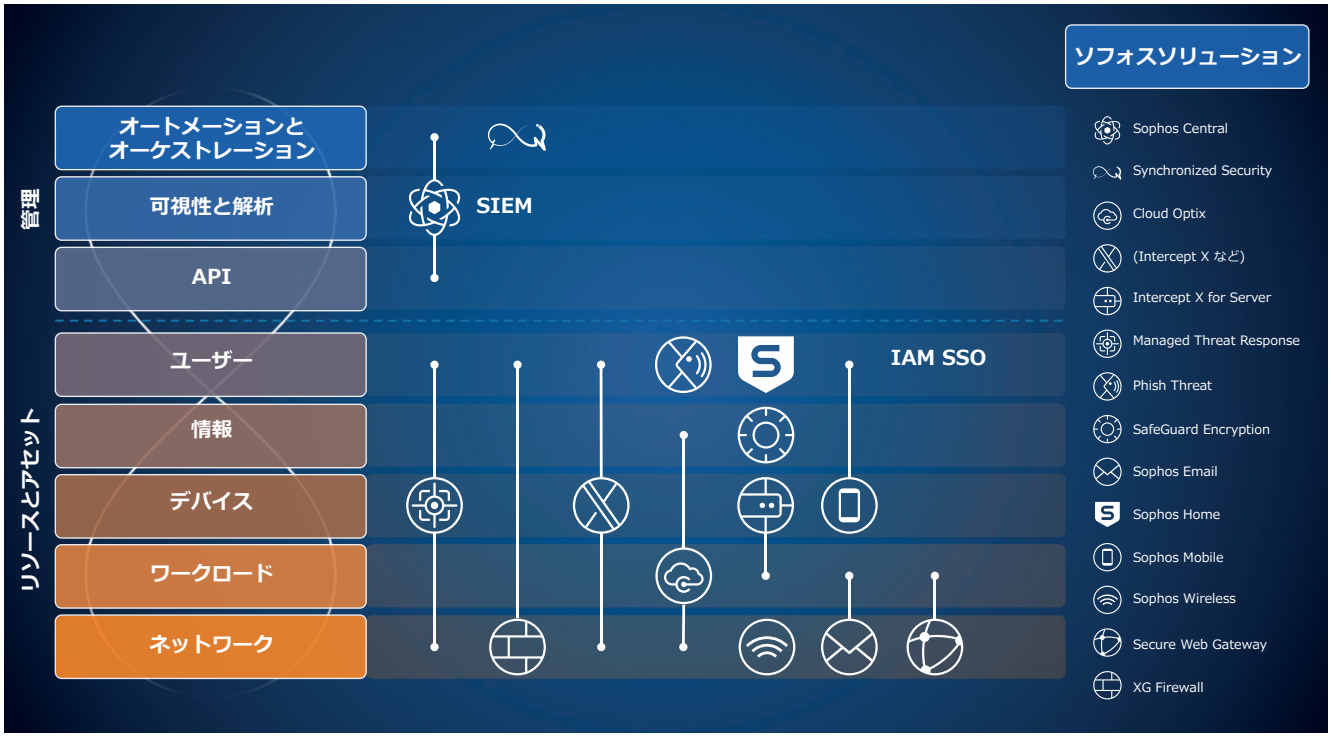
1. オートメーションとオーケストレーション – 動的なポリシーの定義、さまざまな技術の調整、すべての実装を行う
2. 可視性と解析 – ネットワークを常に監視し、すべてが正常に機能していることを確認するだけでなく、脅威や侵害が発生した場合はそれらを特定
3. API – さまざまなテクノロジーを統合して、1つのシステムから別のシステムにデータを取り込むことが可能

リソースとアセットは、次の 5つのサブ領域に分類されます。

1. 従業員 – 業務をする上で連携するユーザー、管理者など
2. データ – すべての組織にとって必要不可欠であり、最も大切な資産
3. デバイス – 業務の遂行に使用するサーバー、ノート PC、仮想マシンなど
4. ワークロード – データ処理、計算処理、レポート生成などに使用するサービスとアプリ
5. ネットワーク – データフロー、Web、メール、Wi-Fi、インターネットなどの通信チャネル

ソフォスが提供するサポート

シングルベンダーが組織をゼロトラストモデルに移行することはできませんが、ソフォスにお問合せ頂ければ移行に役立つさまざまなテクノロジーをご紹介させていただきます。



ゼロトラストの管理

Sophos Central クラウドネイティブのサイバーセキュリティプラットフォームにより、ゼロトラスト環境を管理すべてのテクノロジーをシングルコンソールでオーケストレーションして、1か所で監視し、API を使用してお客様が現在お使いの他のサードパーティ技術と連携させます。

また、SIEM を使用して、ソフォス以外の製品やソフォス製品からログを集約し、現在の状況を完全に監視することが容易になります。ソフォスの API を使用すると、Sophos Central プラットフォームから情報を簡単に入手し、使用しているどんな SIEM にもアクセスできます。

Sophos Synchronized Security (Sophos Central で制御) もここで大きな役割を果たします。Synchronized Security を有効にすると、ソフォスソリューションは情報を相互に共有し、インシデントに自動的に対応します。ゼロトラストのコンテキストでは、ソリューションは動的なポリシーを通じて状況に適応し、マシンの隔離などのような複雑なタスクを自動化できます。

リソースとアセットのセキュリティと制御

ソフォスの製品の多くは、複数のリソースとアセットを同時に保護するのに役立ちますが、決して 1つの技術を採用して移行するという意味ではありません。たとえば、ユーザーを保護するには、強靭なゼロトラストのアーキテクチャネットワークの一部として、多数の異なるテクノロジーが必要となります。

Cloud Optix は、無防備な状態のクラウドセキュリティのギャップやコンプライアンスのギャップを検出、対応、防止する際に必要な継続的な分析と可視化を組織に提供します。ゼロトラスト環境では、Cloud Optix はパブリッククラウド、データ、デバイス、ワークロード、ネットワーク内のセキュリティを確保するのに役立ちます。

Intercept X は、比類のないエンドポイント保護を提供し、ディープラーニングによるマルウェアの検出、エクスプロイト対策、動作検出、ランサムウェア対策など独自の組み合わせにより、多種多様な攻撃を阻止します。ゼロトラスト環境では、Intercept X を使用してすべてのリソースとアセットを保護できます。

Intercept X for Server は、クラウド、オンプレミス、ハイブリッド環境のサーバーを保護するように設計されています。ゼロトラスト環境では、Intercept X for Server を使用してユーザーのデバイスとワークロードの両方を保護できます。

Managed Threat Response (MTR) とは、専門家のリードによる脅威対応ソリューションです。機械学習と専門家の知識を融合し、脅威ハンティング、検出、対応機能を年中無休で提供します。ゼロトラスト環境では、MTR を使用してすべてのリソースとアセットを保護できます。

Phish Threat とは、専用のフィッシング対策です。従業員にセキュリティ意識向上トレーニングだけでなく、フィッシング脅威の準備状況を評価できるように設計されたレポートを組織へ提供します。Phish Threat は、ゼロトラスト環境内で、従業員の安全を確保するのに役立ちます。

SafeGuard Encryption は、コンテンツの作成と同時に暗号化を実施します。暗号化されたデータにアクセスを許可する前に、デバイスのユーザー、アプリケーション、セキュリティの統合性を継続的に検証することで、データをプロアクティブに保護します。これにより、ゼロトラスト環境内でデータを保護できます。

Secure Web Gateway は、高度な Web 保護を容易にし、Web セキュリティ、制御、インサイトをかつてないレベルで提供します。ゼロトラスト環境では、Secure Web Gateway を使用してネットワークとワークロードの両方を保護できます。

Sophos Email は、人工知能を活用して、よりスマートな予測型のメールセキュリティ対策を提供します。ゼロトラスト環境では、Sophos Email を使用してユーザーのネットワークとワークロードの両方を保護できます。

Sophos Home は、ご自宅にあるコンピュータを保護するように設計されており、ソフォスの多くのビジネス製品に搭載されているのと同じ技術をベースにしています。Sophos Home は、ゼロトラスト環境内で、従業員の安全を確保するのに役立ちます。

Sophos Mobile は、デスクトップやモバイルデバイスなど、エンドポイントのセキュリティ管理に割ける時間や労力が限られている企業に最適な UEM (Unified Endpoint Management) ソリューションです。Sophos Mobile は、ゼロトラスト環境内で、デバイス、データ、従業員の安全を確保するのに役立ちます。

Sophos Wireless は、簡単かつ効果的なワイヤレスネットワークのセキュリティ管理を実現します。Sophos Wireless は、ゼロトラスト環境内で、ネットワークの安全を確保するのに役立ちます。

XG Firewall は、包括的な次世代型ファイアウォール機能を提供。ネットワークに潜むリスクも可視化したり、未知の脅威をブロックしたりするだけでなく、インシデントにも自動対処します。ゼロトラスト環境では、XG Firewall を使用してすべてのリソースとアセットを保護できます。

これらの技術を採用することで、ゼロトラストモデルに移行する時も安心です。ただし、前述したように、ソフォスを含むベンダーやテクノロジーが、ゼロトラスト環境に移行することはできません。ユーザーがどこにいてもクラウドサービスを利用できるようにするには、すべてのシステムとサービスで単一の信頼できるアイデンティティソースを使用するために、SSO (シングルサインオン) を備えた強力な IAM (アイデンティティとアクセス管理) が必要になります。これは、ゼロトラストの重要な部分です。

製品やサービスの詳細、インスタントデモの開始については、www.sophos.com をご覧ください。

サイバーセキュリティにおけるソフォスのビジョン

ゼロトラストとサイバーセキュリティにおける当社のビジョンである Synchronized Security は、多くの同じ目標を共有し、相互に補完します。

Synchronized Security はシステムとしてのサイバーセキュリティ (Cybersecurity as a System) 対策です。 IT 部門における最も複雑なタスクを継続的に分析、適応、自動化しながら、すべてのシステムアクティビティ、ユーザーの行動、ネットワークトラフィック、コンプライアンス状態をリアルタイムで動的に監視します。すべてのテクノロジーは相互に情報を共有し、状況が見えない相互に対して洞察や可視性を提供します。

テクノロジーは情報を共有する必要があります。この情報共有を通じてのみ、複数のデータソースに基づいて、必要な適応型ポリシーや動的なポリシーを実現し、ゼロトラストネットワークを実現できます。

結論

現状では、ゼロトラストはサイバーセキュリティに対する基本的理念にすぎず、すぐに受け入れられることはほとんどありません。しかし、セキュリティの境界が頻繁に失われてくるにつれ、導入の必要性がますます高まっています。サイバー犯罪者は革新的になってきているので、防御策として対応するのに苦労しています。ゼロトラストモデルとは、サイバーセキュリティプロトコルの新しい基準を設定しながら、脅威を最小化する方法です。

今までの考え方を変えていきましょう。今こそサイバーセキュリティを進化させるときです。

ソフォス株式会社営業部
Email: sales@sophos.com

20-03-10 WP-JP （ DD ）