ゼロ信頼セキュリティの検証に関するホワイトペーパー

内容

概要

このドキュメントでは、ゼロトラストに関連する情報と、ゼロトラストを使用して企業を保護する方法について説明します。

要旨

ゼロの信頼とは、ネットワークの内外を問わず、ユーザ、デバイス、またはアプリケーションが安全と見なされず、それぞれがネットワーク資産へのアクセスを許可される前に検証される必要があることを前提としたモデルを表します。

この概念は、仮想化、およびオンプレミスのリソースのパブリック、プライベート、ハイブリッドクラウドへの迅速な移行においてより重要になっています。

Zero Trustという用語は、Forresterが2010年にZero Trustネットワークアーキテクチャレポートをリリースしたときに作成されました。

ゼロトラストは、重要なビジネス上の利益とイニシアチブを保護するためのビジネスレベルの戦略として開始する必要があることを理解することが重要です。

ゼロトラストの柱

ゼロ信頼とは

ゼロトラストは、今日のインフラストラクチャに対してより実用的なセキュリティを実現するために、さまざまなテクノロジーを含む戦略的アプローチです。これは、今日のテクノロジー、プラクティス、ポリシーの組み合わせを効果的に調整するために設計されたセキュリティアーキテクチャとエンタープライズ手法です。

セキュリティに対するシスコのアプローチの進化を表し、複数のベンダーの製品とサービスを組み込んだ、包括的で相互運用可能な包括的なソリューションアプローチを提供します。

ゼロトラストは、ネットワークセグメンテーション、多要素認証、ネットワークアクセスコントロールなど、確立された多くのテクノロジーに基づいています。

ゼロ信頼が重要な理由

ゼロトラストは、不正なユーザ、侵害、およびサイバー攻撃から企業を保護するのに役立ちます。セキュリティイベントのリスクを最小限に抑えるために、ユーザとデバイスのIDを継続的に確認し、作業に必要な権限のみをユーザに許可することができます。

市場調査によると、世界のゼロトラストセキュリティ市場の規模は、2022年の270億ドルから2027/2028年には600億ドルに拡大し、その時点で年平均成長率が17%程度になると予測されています。

動機：

- 標的型サイバー攻撃の頻度が高まる
- データ保護および情報セキュリティに関する規制の増加
- ビジネスおよび組織のリスクを軽減する必要性の高まり
- より多くのサービスがクラウドに移行されると、一元化されたデータ導入はデータの境界を超え、セキュリティリスクを増大させます。
- 最初だけでなく、アクセスプロセス全体を通じてユーザの身元を確認する必要がある

1回のランサムウェア攻撃で500万ドルの損失が発生します。サイバー犯罪者は、ビジネスをターゲットにするときに差別を行いません。

最近のCIOおよびCISOの調査によると、Zero Trustは上位5つの優先事項の1つです。CISOによると、リモートワークへの移行、人手不足、サイバーセキュリティ攻撃の急増により、企業の既存システムのセキュリティを確保する必要があります。

従来のモデルとゼロ信頼モデル

従来の環境では、環境の構築後にセキュリティが追加されています。通常、これらはフラットなネットワークであり、インターネットからの攻撃を防ぐためにネットワークのエッジを中心に防御が構築されます。

Zero Trustは一般に、暗号化、安全なコンピュータプロトコル、動的なワークロード、およびデータレベルの認証と許可を組み合わせて、複数のレベルで組織のシステムとデータを保護する必要性に焦点を当てることで認識されており、外部ネットワークの境界だけに依存しているわけではありません。

従来の境界中心のセキュリティアーキテクチャでは、クラウドからのワークロードの配信が増加し、モバイルエンドポイントがアプリケーションとデータアクセスの標準となっているため、効果が低くなっています。

ゼロトラストアーキテクチャフレームワーク

ゼロトラストアーキテクチャフレームワークは、特にアクセスが必要で検証済みのユーザとデバイスに対するシステム、アプリケーション、およびデータリソースへのアクセスの制限を扱います。アクセスを提供する各リソースに対して適切な許可を確保するには、IDおよびセキュリティポスチャに対して継続的に認証される必要があります。

このフレームワークは、ゼロトラストセキュリティの概念を企業環境に移行して導入するためのロードマップを提供するもので、NIST特別公開文書800-207に基づいています。

効果的なゼロトラストアーキテクチャフレームワークは、これら7つの主要なコアコンポーネントを調整および統合します。

- ゼロトラストネットワークは、ネットワークをセグメント化したり、ネットワーク資産を分離したり、ネットワーク間の通信の制御を維持したりする機能を指す、ゼロトラスト戦略の重要な特徴です。また、信頼性の高い接続を保護し、リモートで使用できるように職場環境を拡張します。
- Zero Trust Workforceには、ユーザアクセスを制限および適用する方法が含まれます。これには、ユーザの認証、アクセス権限の継続的な監視および制御を行うテクノロジーが含まれます。このアクセスは、DNS、多要素認証、ネットワーク暗号化などのテクノロジーによって保護されます。
- Zero Trust Devicesは、モビリティとInternet of Thingsの追加によって拡大したネットワーク接続デバイスをすべて隔離、保護、管理し、攻撃者が悪用する大きな脆弱性を作り出す必要性に対処します。
- Zero Trust Workloadsは、重要なビジネスプロセスを実行する前面から背面へのアプリケーションスタックを保護します。データセンター内のアプリケーション、データ、およびサービス間の水平方向のトラフィックを保護し、重要なアプリケーションの保護を強化します。
- ゼロトラストデータとは、データを分類および分類する手法を指し、データの暗号化を含むデータを保護および管理するためのテクノロジーソリューションと組み合わされます。
- 可視性と分析とは、自動化とオーケストレーションを認識するテクノロジーを指します。管

理者は、リアルタイムの脅威の存在など、環境内のアクティビティを確認するだけでなく理解することができます。
- 自動化とオーケストレーションには、機械学習アルゴリズムや人工知能などのツールやテクノロジーが含まれ、ネットワークやデータセンターの資産を自動的に分類し、セグメンテーションやセキュリティ対策、ポリシー、ルールを提案して適用し、自動的に適用します。そのため、セキュリティチームの負担を軽減し、攻撃の軽減を促進します。

ゼロトラストとセグメンテーション

すべてのネットワークベースのリソースは、最小権限の原則に従って保護およびセグメント化する必要があります。これは、クレデンシャルとアクセスをあらゆる目的で制御する資産管理システムを通じて実現するのが最適です。

ゼロトラストのセグメンテーションの必要性には、ブランド保護、攻撃対象領域の制限、ネットワークの安定性の向上、迅速なサービス展開の実現が含まれます。

個々のリソースの保護をさらに実現するために、マイクロセグメンテーションを使用できます。Scalable Group Tag（SGT；スケーラブルグループタグ）は、イーサネットフレームにタグ値を挿入してリソースを一意に識別する場合に使用できます。さらに、インフラストラクチャデバイスには、各リソースを保護するゲートウェイデバイスとして使用できるインテリジェントスイッチ、ルータ、または次世代ファイアウォールが含まれます。

可視性、分析、自動化

組織のすべての資産と、それらの資産に関連する活動を完全に把握しておくことが重要です。これがゼロトラストの基盤です。

動的なポリシーと信頼に関する意思決定を行うには、分析を継続的に収集する必要があります。デルのゼロトラストアーキテクチャのアプローチでは、ポリシーエンジンとポリシー管理者を使用してSDN戦略のコア論理コンポーネントに焦点を当て、コントロールプレーンを形成し、データプレーン内のポリシー適用ポイントを介したリソースへのアクセスを制限します。

Zero Trust Architectureに必要な機能は、ネットワークコンテキスト、学習、および保証を強化し、その使命を安全に達成するために必要です。

- ユーザ、デバイス、アプリケーション、ワークロード、およびデータへのアクセスの詳細なマイクロセグメンテーション
- LAN、WAN、データセンター、クラウド、エッジなど、動作する場所にセキュリティポリシーを適用します。
- 包括的なID管理：IDとアクセス管理を拡張して、ユーザー、デバイス、アプリケーション、ワークロード、データのIDを含めます。これらのIDは、ソフトウェア定義のアクセスを介して新しい微小な境界となります。
- グローバルな脅威インテリジェンスとフィードを活用した統合型脅威防御
- 組織のネットワークを完全に自動化し、俊敏性に優れた方法で制御することで、目的の達成に必要な規模、パフォーマンス、信頼性を確保して安全に機能させることができます。

信頼をゼロにするステップ

包括的なゼロトラストセキュリティの鍵は、LAN、データセンター、クラウドエッジ、クラウドなど、ネットワーク環境全体にセキュリティを拡張することです。コンプライアンスはもちろん必須です。

このセキュリティには、組織のネットワーク環境の総合的な可視性が含まれている必要があります。包括的なゼロトラストセンターの主なステップ：

- デバイスと機密データを特定します。デバイス、機密データ、ワークロードの特定と分類を実行します。
- 機密データのフローを把握します。
- ゼロトラストのセグメンテーションポリシーを設計します。各ネットワークベースの資産は、最小限の特権と厳密に適用された細かい制御の原則に従って適切に保護およびセグメント化する必要があります。これにより、ユーザは業務の実行に必要なリソースにのみアクセスできます。
- ポリシーとポスチャを実装します。これは、Cisco DNACやISEなどのプラットフォームで実行できます。
- ゼロトラスト環境を継続的に監視します。セキュリティ分析を実装して、セキュリティインシデントをリアルタイムで監視および分析し、悪意のあるアクティビティを迅速に特定します。内部および外部の両方ですべてのトラフィックを継続的に検査し、ログに記録します。

信頼できるアクセスの実現

包括的なゼロトラストのセキュリティを実現するには、組織はゼロトラストのアプローチを従業員、職場、ワークロード全体に拡張する必要があります。

- Zero Trust Workforce：ユーザとデバイスは認証および承認を受ける必要があり、アクセスと権限は継続的に監視および管理されてリソースを保護します。
- Zero Trust Workplace：クラウドとエッジを含むワークプレイス全体でアクセスを制御する必要があります。
- ゼロトラストワークロード：アプリケーションスタック全体に対して、きめ細かなアクセス制御を適用する必要があります。これには、クラウド内のコンテナ、ハイパーバイザ、マイクロサービス間や、従来の機関のデータセンター間などが含まれます。

Forresterが認定したゼロトラストリーダーであるシスコは、オンプレミスとクラウドの両方で、ネットワーク全体でゼロトラストを実現することを強く提唱しています。ゼロトラストアーキテクチャの重要な基盤としてシスコのネットワークインフラストラクチャを活用できるだけでなく、ゼロトラストへの移行を支援するCisco Zero Trustの主要なセキュリティ機能についても学習できます。

Cisco Secureポートフォリオ

次のコマンドを使用して、正常なゼロ信頼フレームワークを構築できます。

- **Cisco** Duoによるユーザ、デバイス、およびアプリケーションへの円滑でセキュアなア**クセス**
- **Cisco** Umbrellaによる柔軟なクラウドセ**キュリティ**
- **Cisco Secure** Firewallを介したインテリジェント**パケットインスペクション**
- **Secure Endpoint**（旧称AMP）による高度なマルウェア防御
- **Cisco** AnyConnectによるセキュアなVPNとリモ**ートアクセス**
- **Cisco** Tetrationによる全体的なワークロ**ード保護**

- Cisco Identity Services Engine(ISE)による保護されたネットワークセグメンテーション
- Cisco Secure Workloadによるアプリケーションの可視性とマイクロセグメント化
- Cisco SecureXによる統合セキュリティプラットフォーム
- Cisco+ Secure Connectによるas-a-serviceサブスクリプションを備えたUnified SASEソリューション
- Cisco Zero Trust Strategy Serviceからのエキスパートガイダンス
- コンサルティング、アドバイザリ、およびソリューションサービスを通じたサポートおよびエンドツーエンドサービス

要約

ゼロトラストについて考える最も簡単な方法の1つは、「決して信頼せず、常に検証する」ことです。 これは、すべてのネットワーク接続、すべてのセッション、および重要なアプリケーション、ワークロード、およびデータへのアクセスのすべての要求に適用されます。

ゼロトラストのセキュリティフレームワークは、組織のネットワーク内の各リソースの周囲に局所的なミクロ境界の防御を作成します。正しく設計されていれば、フレームワークは資産の場所に関係なく資産を保護できます。

リスクを軽減する効率的な方法は、特権データと共有データへのアクセスを制御し、最小特権の原則を採用することです。このセキュリティモデルにより、APIを介したオーケストレーションが可能になるほか、ユーザとアプリケーションの可視性を提供するワークフロー自動化プラットフォームとの統合も可能になります。

ゼロトラストの実装が成功すれば、組織のIT環境全体にわたって安全でシームレスな運用を確保し、組織の重要なワークロード、アプリケーション、およびデータへの継続的で信頼できるアクセスを実現して、組織のミッションを強化できます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。