効果の高い
ゼロトラスト アーキテクチャーの 7 つの要素

アーキテクト向けの Zscaler Zero Trust Exchange のガイド

攻撃への脆弱性が残る 従来のセキュリティ アーキテクチャー

ファイアウォールと VPN を用いたこれまでのセキュリティ アプローチでは、ユーザーがネットワークに接続されます。そのため、攻撃者がユーザーやデバイス、ワークロードを侵害し、水平移動で価値の高い資産に到達し、機密データを抽出することが可能となっています。

現在のハイブリッドな働き方に求められる ゼロトラストのセキュリティ アプローチ

組織の保護に向けて、最小特権アクセスに基づく包括的なセキュリティ アプローチ、ゼロトラストに注目が集まっています。このアプローチは、ユーザーやアプリケーションは本質的に信頼すべきではないという原則を活用したものです。

ゼロトラスト アーキテクチャーの実装

真のゼロトラストは、クラウドネイティブな統合プラットフォーム、**Zscaler Zero Trust Exchange** を通じて提供されます。本プラットフォームは、ネットワークに接続せずに、ユーザーやデバイス (IoT/OT)、ワークロードをアプリケーションに安全に接続します。

真のゼロトラスト アーキテクチャーの 基盤を形成する7つの要素

このユニークなアプローチにより、Zscaler は攻撃対象領域を排除して脅威の水平移動を防ぎ、ビジネスを侵害や情報漏洩から保護します。

1. 接続元の確認

リクエストされている接続を終了し、ユーザーや IoT/OT デバイス、ワークロードのアイデンティティーを検証します。

2. アクセス コンテキストの検証

接続のリクエスト元の役職や職責、リクエストの時間、状況などの属性を調べ、コンテキストを検証します。

3. 接続先の確認

接続先が既知のもので、詳細が把握されており、コンテキストに基づいた分類によってアクセスが許可されているかを確認します。接続先が未知のものの場合、フラグを立ててさらなる分析を行います。

4. リスクの評価

AI を活用して、デバイス ポスチャー、脅威、接続先、動作、ポリシーなどの要因に基づいて、接続についてのリスク スコアを動的に算出します。

5. 侵害の防止

トラフィックとコンテンツをインラインで検査し、悪意のあるコンテンツを識別、ブロックします。

6. 情報漏洩の阻止

アウトバウンドのトラフィックを検査して機密データを識別し、流出を防止します。

7. ポリシーの施行

セッションごとにポリシーを施行し、リクエストされた接続に関して実行する条件付きアクションを決定します。「許可」の決定が下されたら、インターネットや SaaS アプリ、または内部アプリケーションへの安全な接続が確立されます。

ゼロトラストにおけるこれらの 7 つの基本要素をビジネスに適用することで、**攻撃対象領域を排除し、脅威の水平移動を防ぎ、組織を侵害や情報漏洩から保護する方法をご覧ください。**

eBookを読む

Experience your world, secured.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.jp