セキュリティ アーキテクチャーの評価：ゼロトラスト モデルとネットワーク中心のモデル

セキュリティ製品を検討するなかで必ず遭遇する言葉の一つに「ゼロトラスト」があります。しかし、「ゼロトラスト」とゼロトラストで置き換えるべき従来のネットワーク中心のセキュリティについて十分な理解がなければ、組織のデジタル トランスフォーメーションをサポートできないセキュリティ アーキテクチャーを選んでしまうリスクがあります。

ゼロトラスト アーキテクチャー

ゼロトラストでは、ネットワークへのアクセスをユーザーやエンティティーに一切拡張することなく、Any-to-Anyの安全な接続を提供します。このアーキテクチャーは、ファイアウォールやVPNのようなネットワーク中心のツールでは構築できません。最小特権アクセスの原則に基づき、ユーザーは自分の仕事に必要なリソースのみに接続できます。真のゼロトラスト プラットフォームはクラウドネイティブです。グローバルに展開され、インテリジェントな交換機として機能する専用クラウドを通じてユーザー、拠点、アプリケーション間の直接接続を仲介し、ネットワーク中心のモデルの弱点に直接対処します。

ネットワーク中心のアーキテクチャー

ネットワーク中心のセキュリティは、主にファイアウォールやVPNなどのツールで構築されています。このアプローチでは、ユーザー、拠点、アプリを信頼されたネットワークで接続することでアクセスが確立されます。そして、ネットワークを守るための安全な境界を構築するため、「境界ベース」のアーキテクチャーとも呼ばれます。デジタル トランスフォーメーションを進める組織が引き続きこのモデルを使用するには、増え続けるリモート ワーカーやクラウド アプリなどにネットワーク境界を拡張する必要があります。ただし、この戦略は大きな複雑性やサイバー リスクを伴い、他にもさまざまな問題を引き起こします。

ゼロトラストやクラウド型をうたうセキュリティ製品の多くは、実際にはネットワーク中心のアーキテクチャーで構成されています。以降のページでは、真のゼロトラストを実現するプラットフォームを確実に選択するためのチェック項目を紹介していきます。セキュリティ アーキテクチャーの正確な評価にお役立てください。

© 2025 Zscaler, Inc. All rights reserved.

ゼロトラストを評価する際の重要ポイント

真のゼロトラスト アーキテクチャーを実現するには、以下の5つの領域のポイントを押さえることが重要です。



01

攻撃対象領域の削減

ネットワークの拡張が不要

ゼロトラスト アーキテクチャーは、アプリへの直接接続を提供します。つまり、ITリソースへのアクセスを可能にするためにネットワークを拡張する必要はありません。ネットワーク中心のアーキテクチャーでは、ネットワークをユーザー、拠点、デバイス、クラウドに拡張し、ユーザーがアプリにアクセスできるようにします。その結果、ネットワークが拡大し、攻撃者に悪用され得る侵入口が無数に生まれます。

パブリックIPの排除

ファイアウォールとは違い、ゼロトラストではWeb上で攻撃者に発見され得るパブリックIPアドレスを必要としません。ゼロトラストでは、攻撃対象領域を拡大するインバウンド接続ではなく、インサイドアウト接続を使用します。アプリの前面に配置されたコネクターによって、ゼロトラスト クラウドに接続し、これを介してユーザーとアプリ間で完全な接続を確立します。どのようなユーザー接続のシナリオ(エージェント、ブラウザー分離、拠点のトラフィックなど)においても、コネクターがインサイドアウト接続をサポートしていないプラットフォームは避ける必要があります。



02

不正侵入の防止

プロキシベースのアーキテクチャー

ゼロトラストは、プロキシベースのアーキテクチャーを通じて提供されます。これにより、完全なトラフィック検査を実行し、アクセスのコンテキストとリスクを判断しながら、リアルタイムのセキュリティ ポリシーを施行して不正侵入を防止できます。ネットワークを中心としたファイアウォールベースのアーキテクチャーで行われるトラフィック検査は完全ではなく簡易的なもののため、重要なコンテキスト要素を十分に可視化できず、多くのトラフィックはセキュリティが確保されていない状態で通過します。結果として、脅威の検知と対応は事後対応的なものになります。

暗号化トラフィックに潜む脅威の阻止を可能にするクラウドネイティブの拡張性

クラウドネイティブのゼロトラスト プラットフォームは、暗号化されたトラフィックを大規模に検査し、そこに潜む脅威を阻止するために必要な拡張性を提供します。現在のWebトラフィックの95%以上は暗号化されており、その検査には高いパフォーマンスが必要となるため、この特長は重要です。(物理アプライアンスか仮想アプライアンスかによらず)処理能力が固定されるアプライアンスに依存したネットワーク中心のモデルは、拡張性に欠け、暗号化されたトラフィックを大規模に検査できないため、不正侵入が検出されない可能性があります。

© 2025 Zscaler, Inc.All rights reserved.

03

ラテラル ムーブメントの防止

アプリケーションへの直接接続

ゼロトラスト アーキテクチャーは、組織のネットワークではなく、アプリへの直接接続を可能にします。脅威がネットワークに侵入した場合、接続されたリソース間でのラテラル ムーブメントを通じて侵害範囲が拡大する可能性があるため、これは最小特権アクセスを確保するには不可欠な機能です。ネットワーク中心のアーキテクチャーでは、その名のとおりネットワークへのアクセスを伴うため、ネットワーク全体にわたる脅威のラテラル ムーブメントが発生する可能性があります。

接続の完全な仲介

ゼロトラスト クラウドは、組織のすべてのトラフィックの中継地点となり、接続を完全に仲介します。インテリジェントな交換機として機能し、許可されたエンティティーがITリソースに1対1で安全にアクセスできるよう接続元と宛先を結びます。一方、ルートベースの接続やルーティング可能なIPを使用したアーキテクチャーでは、ユーザーをネットワークに接続するため、ラテラル ムーブメントのリスクが高まります。

04

包括的なデータ保護

暗号化トラフィック内のデータの保護を可能にするクラウドネイティブの拡張性

前述のように、クラウドネイティブのゼロトラスト プラットフォームは、暗号化されたWebトラフィックの大規模な検査に必要なパフォーマンスを提供します。これにより、暗号化トラフィックに含まれる機密データを発見して保護し、漏洩を未然に防ぐことが可能です。ネットワーク中心のアーキテクチャーとアプライアンスでは、(物理アプライアンスか仮想アプライアンスかを問わず)暗号化されたトラフィックを大規模に検査できず、そこに含まれるデータを保護できません。

データ漏洩のすべての経路に対応するセキュリティ

データの窃取や偶発的な漏洩は、暗号化されたWebトラフィック以外にも、メール、エンドポイント、BYOD、SaaS、IaaS、プライベート アプリケーションなど、数多くのチャネルで発生します。ゼロトラスト プラットフォームでは、あらゆるITリソースにアクセスするあらゆるエンティティーを保護するために、こうしたすべての経路で最小特権の原則に従ってデータを保護できる必要があります。

© 2025 Zscaler, Inc.All rights reserved.

05

クラウドネイティブのアーキテクチャー

クラウドネイティブのプラットフォーム

ゼロトラストは、専用のクラウドからサービスとして提供されます。変更の実装もこのクラウド上で処理し、レジリエンスを確保しながら、自動的かつスピーディーにサービスのアップグレードを行います。これは、パブリック クラウドに展開された次世代ファイアウォールのVM上に構築されたセキュリティ製品とは大きく異なります。こうした製品では、煩雑な変更の実装、レジリエンスを確保するための手作業、時間を要するサービス アップグレードが必要です。サービスがオンプレミスで管理されている場合は、管理者の介入も必要となります。さらに、ファイアウォールを基盤にプラットフォームを構築すれば、そのアーキテクチャーは必然的にネットワーク中心のものになり、ゼロトラストを実現することはできません。

包括的な統合プラットフォームとしての設計

包括的なゼロトラスト プラットフォームとして設計されたクラウド サービスでは、新しい統合機能をベンダーが簡単に構築し、顧客が簡単に展開できます。これによって、ポイント製品のアプライアンスが不要になり、その複雑さが解消されます。NGFWを基盤に構築された「ゼロトラスト」をうたう製品は、複雑さと管理負荷を増大させるボルトオンのポイント製品であり、実際にはゼロトラスト アーキテクチャーを実現できません。

マルチテナント

マルチテナントであれば、ゼロトラスト プラットフォームは必要に応じて動的に拡張できるため、トラフィック負荷の急増にも対処することが可能です。さらに、ポリシーの更新はミリ秒単位でクラウド全体に反映され、あらゆる場所のユーザーに適用されます。シングルテナント サービスでは、(自動スケーリングを使用しても)負荷の急増に対応できないほか、さまざまなサイトのテナント全体にポリシーの変更が反映されるまでに数分かかることもあり、リスクにさらされる時間が長くなります。

プライベート帯域幅の必要性の最小化

ネットワーク中心のアーキテクチャーとは異なり、ゼロトラストでは接続とセキュリティをネットワークから切り離します。トラフィックをバックホールするのではなく、最小特権の原則に基づいてアプリへの直接接続を提供することで、インターネットを組織のネットワークとして使用できるようになります。これにより、MPLS、Azure ExpressRoute、AWS Direct Connectのような高コストのプライベート接続の必要性を最小限に抑えることができます。

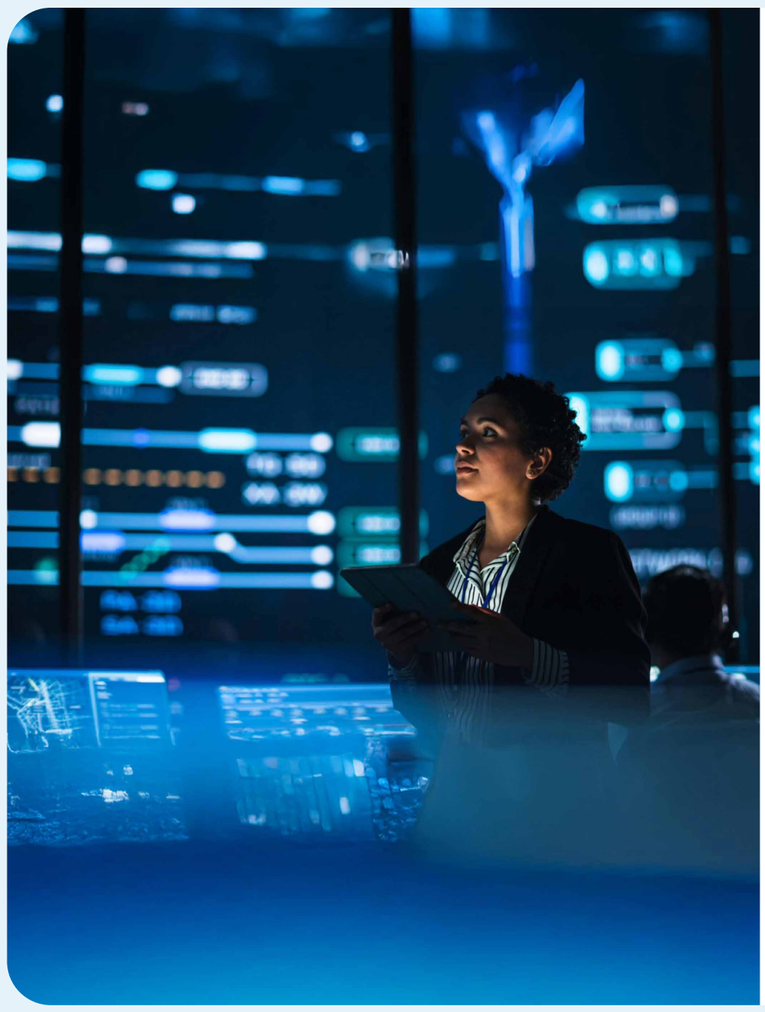
高度なコンピューティング能力を備えたエッジのポイント オブ プレゼンス(PoP)

ゼロトラストは、複数のPoPを介してサービスとしてエッジで提供されます。このPoPは高度なコンピューティング能力を備え、ここでトラフィックの処理やポリシーの施行が実行されます。一方、オンランプ型のサービス エッジしか持たないソリューションの場合、トラフィックはベンダーのネットワークに取り込まれ、離れた場所にあるコンピューティング拠点にバックホールされるため、こうしたベンダーは避ける必要があります(レイテンシーが増加します)。また、ユーザーの接続状況を完全に可視化し、デジタル エクスペリエンスをいっそう強化できるようなデジタル エクスペリエンス モニタリング(DEM)機能を提供しているベンダーを選択することも重要です。

© 2025 Zscaler, Inc.All rights reserved.

Zscaler Zero Trust Exchange™プラットフォーム

Zscalerは、ここで挙げたすべての条件を満たす真のゼロトラスト アーキテクチャーを提供しています。Zscalerは、ゼロトラストの草分けでありながら、現在も継続的なイノベーションでこの分野をリードし、ゼロトラスト アーキテクチャーの実現を目的にゼロから設計された拡張可能なクラウドネイティブ プラットフォームを提供しています。これは、競合プラットフォームとは根本的に異なります。こうしたプラットフォームの製品は、「ゼロトラスト」をうたいながらもファイアウォールやVPNを基盤に構築されており、ゼロトラストとは本質的に相反するネットワーク中心のアーキテクチャーが採用されています。



デジタル トランスフォーメーションを進める組織は、Zscalerを採用することで最新のアーキテクチャーを活用し、次のことを実現できます。

01 サイバー犯罪者が発見できる攻撃対象領域の最小化

02 不正侵入のリアルタイムでの阻止

03 ネットワーク上での脅威のラテラル ムーブメントの防止

04 転送先を問わないあらゆるデータの保護

05 クラウドネイティブ プラットフォームのメリットの活用

Zscaler Zero Trust Exchange™プラットフォームの詳細は、デモでご確認ください。

デモを依頼する

ゼロトラストについて詳しく学ぶには、ウェビナー シリーズ「Zero Trust, from Theory to Practice」をご活用ください。

詳細はこちら(英語)

© 2025 Zscaler, Inc.All rights reserved.