ホワイトペーパー

ゼロトラストの歴史：エンタープライズセキュリティの再考における主なマイルストーン

なぜゼロトラストなのか

ITセキュリティ関係者の多くは、ゼロトラストが革命的な効果をもたらし、エンタープライズセキュリティとネットワーク保護を根本から再考させるものであり、最も優れたアイディアと優秀な人材を結びつけ、革命的な生産性を実現するツールへのアクセスを可能にするものだと考えています。

しかしながら、ゼロトラストモデルがサイバーセキュリティにおいてどれほど革命的なものであるかを理解するには、従来のネットワークセキュリティアプローチの弱点と、ゼロトラストアーキテクチャのアイデアがどのように進化を遂げることで数十年前の考え方を根本的に変えるものになったのかを理解する必要があります。

2Dネットワークと「城を堀で囲む」方式のセキュリティ

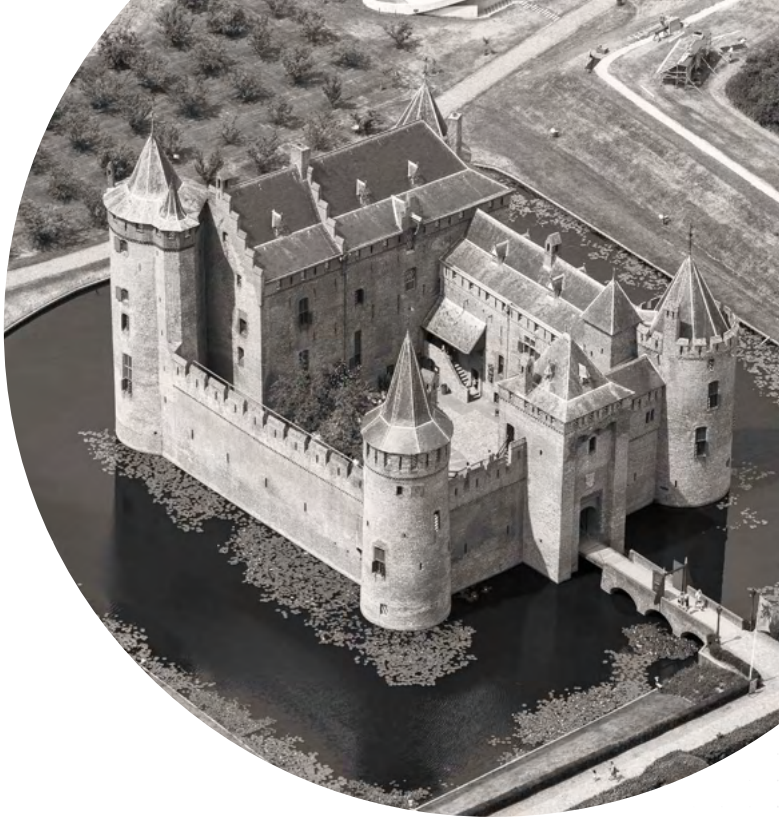
ハブ&スポークや城を堀で囲む方式は、従来型のネットワークアーキテクチャとネットワークセキュリティの説明で使用されることが最も多い2つの喩えです。どちらもかなり前から使われています。

ハブ&スポーク方式のネットワークアーキテクチャとは、中央のハブを取り巻く形で存在する衛星ネットワークのことで、このモデルでは、内部や外部のトラフィックがプライマリデータセンタのセキュリティスタックを経由した後に、送信先にルーティングされます。このアプローチが有効な方式として利用されてきましたが、クラウドが採用され、従業員が分散して働くようになり、ビジネスにおけるモビリティの重要度が高くなったことで、複雑化し、多くのコストが必要とされるようになりました。

これに対し、城を堀で囲む方式のセキュリティは、敵を壁の外側に止め、味方のトラフィックを許可するように設計された自己完結型ネットワークです。内部のセキュリティアプライアンスが入口に立つ門番としての役割を果たし、略奪者の侵入を阻止して、味方の入場を許可します。アプリケーションのクラウドへの移行が大きく前進し、さらには、企業の境界の外で働く従業員が増加したことで、このアプローチは、城を攻撃する砲弾より早く、時代遅れのものになりました。

VPNとWi-Fiで問題がさらに複雑化しました。城を堀で囲む古いアーキテクチャでは、ゲストをネットワークに接続しつつ、アクセスを一定の範囲に制限する手段がありません。何らかの形のセグメンテーションで保護することなくエンドポイントをネットワークに接続する良い方法がなく、

優れた方法が必要だったのです。



802.1XとNACの問題

IEEE Standards Associationが2001年に、NAC(ネットワークアクセスコントロール)向けの802.1Xプロトコル標準を発表しました。

「ポイントツーポイント接続の特性のLANポートに接続されたデバイスを認証して許可し、 認証プロセスが失敗した場合にそのポートへのアクセスを防止する手段」

IEEE 802.1X →

発表後すぐに、接続を許可する前にネットワークによるエンドポイントの認証を可能にする無線デバイスに802.1Xサプリカント（クライアント）が組み込まれるようになりました。この進歩により、有線や無線のネットワークをロックダウンする機能が提供され、管理対象デバイスと承認されたユーザのみに接続を許可できるようになりました。サプリカントは、ネットワークの入口で入場を許可するか否かを判断する番人にアイデンティティを提示します。

ところが残念なことに、NACモデルは万能ではなく、暗黙の信頼を前提に設計された内部ネットワークに認証/承認を後付けしようとするのは極めて面倒なことでした。NACを完全に有効にするには、すべてのアクセス可能なポートをロックダウンする必要がありますが、すべてのデバイスが802.1X対応であるとは限らず、インターネット接続されたプリンタ、バッジリーダ、およびその他のネットワーク対応デバイスの採用の増加は、明らかなセキュリティホールでした。複数の（場合によっては数十の）出入口があるのに、ネットワークの正面玄関にしか門番がいないようなものです。

ジェリコの壁を倒してセキュリティにおける境界の役割を再考する

パーソナルデバイスの使用が増加し続けるのは明白であったことから、2003年までの段階で、城壁の背後にある保護されていないマシンを保護する方法の検討を始める必要がありました。さらには、暗号化の使用の増加に伴い、境界ファイアウォールの有効性が低下し、復号化とインスペクションによって生じる処理能力の課題を解決するために、スケールアップか暗号化されたトラフィックを無条件に通過させるかのいずれかの選択を強いられることになりました。

2003年にヨーロッパの複数の国のテクノロジリーダーが参加するグループが、ユーザ認証、暗号化、アイデンティティ管理、ポリシー適用などの問題の解決に向けて議論し、2004年にジェリコフォーラムが正式に設立された後に、「脱境界」の概念が世界に向けて発表されました。

聖書に登場する、古代都市のジェリコの壁を倒したイスラエル人の話を彷彿とさせる名前のこのフォーラムは、「企業間の安全で境界のない情報のフローを可能にする」方法の問題の解決に取り掛かりました。

このグループは、名称が的確であっただけでなく、ジェリコフォーラムの戒めとして、境界のないネットワークの管理に関するこれまでで最も真実に近い定義を残しましたが、残念ながら、当時のほとんどの企業は、そこで規定された一連のコントロールと軽減の方法を展開または管理する能力を持ち合わせていませんでした。

「ゼロトラスト」という言葉がIT辞書に登場

ForresterのアナリストであるJohn Kindervag氏が2010年に、「No More Chewy Centres: Introducing The Zero Trust Model of Information Security」と題する論文を発表すると、このゼロトラストというフレーズはた

ちまち、ネットワークセキュリティの新しい考え方を表す言葉として注目されるようになりました。この論文の重要な主張は、ネットワークに存在するというだけでは信頼（トラスト）を与える十分な条件ではないということです。

ゼットスケーラーのフィールド担当CTOであるLisa Lorenzinは、次のように述べています。「この頃から、アイデンティティが新しい境界だというようなフレーズを聞くようになりました。つまり、ユーザを認証し、そのアイデンティティを使用してユーザに何を許可するか判断するのです。場合によっては、管理対象デバイスか否かといったコンテキストも収集し、そのような情報に基づいてアクセスについて判断するということも可能になるでしょう。」

このような進展がありましたが、企業のセキュリティがネットワークそのものの保護から脱却することはなく、完全に放棄ができる段階に至っていませんでした。この大胆な変革を可能にするアプローチが欠如していたため、このような原則の採用が再び失敗することになったのです。一例を挙げると、レイヤ2の802.1XやRADIUS、レイヤ3のアイデンティティ対応ファイアウォールなどの、ネットワーク中心の同じツールセットが引き続き利用されていました。

新しいのは、NACという目新しい名前だけだったのです。

Beyond Corp

これと同時期に、中国人民解放軍（PLA）と関連性のあるハッカーによって、テクノロジ業界の最も優秀な人たちが信頼の問題に対する考えを再考することになりました。Googleによる2010年の発表で、Akamai、Adobe、Juniper Networksを含む複数の有名ハイテク企業を標的にした攻撃が2009年に発生していたことがわかりました。McAfeeのセキュリティ研究者がこの大規模攻撃を「オーロラ作戦」と命名しました。

ITエンジニアリングのエリートが集まる蜂の巣を蹴飛ばすという中国のハッカーによる行為が、国内を代表するテクノロジ研究機関におけるゼロトラストアーキテクチャに対する取り組みを図らずも加速させることになりました。Googleがオーロラ作戦をきっかけに開発したBeyondCorpは、**「アクセスコントロールをネットワーク境界から個々のユーザに移し、従来のVPNを必要とすることなく、事実上あらゆる場所から安全に作業を進められるようにする」ことに重点を置くものでした。**

しかしながら、Lorenzinは次のように説明します。「Googleはエンジニアが経営するエンジニアのための企業であり、その予算は事実上無制限であり、多くの企業と比べると古いインフラストラクチャが少ない会社です。そのような会社でも7年を要し、6件のホワイトペーパーに相当する設計と実装が必要だったのです。」

Googleから明確に文書化された例が提示されたにもかかわらず、真のゼロトラストアーキテクチャは、ほとんどの企業にとって現実的なものではありませんでした。「他の組織がゼロトラストネットワークを実装するための道を切り開く」ことが期待されたにもかかわらず、Googleが想像していた未来までの道のりは遠いものだったのです。

その一方で、ユーザにとっては、クラウドが人気を博し、モビリティ重視が継続したことで、より多くのデータを利用できるようになり、ネットワーク境界の内側より外側からデータにアクセスする必要がありました。信頼への広範なアプローチのニーズが、かつてないほど高まりました。

ガートナーとゼロトラストネットワークアクセスの最終的な登場

テクノロジ調査会社のガートナーは、ゼロトラストが広く適応可能なフレームワークとして次の段階へと大きく進歩する重要な役割を果たしました。ガートナーがCARTA（Continuous Adaptive Risk and Trust Assessment）を発表した2010年には、「ゼロトラスト」というフレーズが話題に上ることはありましたが、今ほど声高に叫ばれることはありませんでした。

このホワイトペーパーで説明されているのは、誰がアクセスを要求しているかを理解し、環境、利用可能なコンテキスト、ユーザの責任などに基づいてアクセスを許可する必要があるということです。

LorenzinはCARTAを「十分に評価されることのなかった優れたモデル」と表現しています。

当初のフレームワークがテクノロジ担当者の支持を得られなかった後に、ガートナーは最終的に、CARTAを「ゼロトラストネットワークアクセス」(ZTNA)いう名称に変えました(アクセスの対象としてネットワークが中心であり続けている点に注目してください)。しかしながら、ゼロトラストの歴史におけるCARTAの重要性は今も変わらず、それは、CARTAで提案された原則がZTNAという形で今も存続しているためです。

ガートナーがこの議論に次いで、ネットワーキングとセキュリティの領域のコンバージェンスが進むという認識においても大きく貢献することになりました。ガートナーは2019年に、このコンバージェンスの名称として、セキュアアクセスサービスエッジ(SASE)を発表しました。しかしながら、このコンバージェンスは短命に終わり、2021年までに、SASEとSD-WANというセキュアサービスエッジ(SSE)市場カテゴリの発表によって、再びカテゴリが分割されることになりました。

名称に変遷はあったものの、ガートナーはこの段階までに、ゼロトラストで成し得ることと成し得ないことを明確にする調停役としての地位を確立しました。ベンダは、その新しい市場カテゴリの1つに自らを当てはめようと一斉に行動を開始しました。

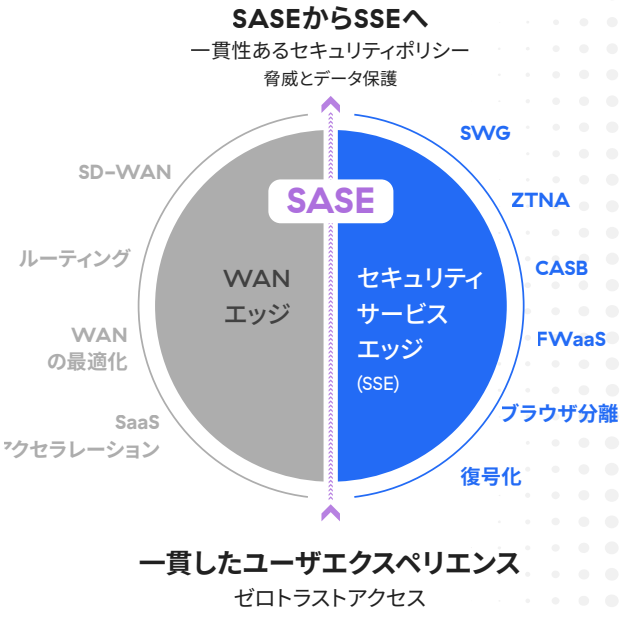
NISTやOMBなどの政府機関が議論に参加し、ZTAを支持

米国国立標準技術研究所(NIST)が2020年に、ゼロトラストアーキテクチャのNIST 800-207標準により、この議論が新たな方向へと向かうことになりました。このサイバーセキュリティの新しいパラダイムは、リソース保護に重点を置き、信頼を暗黙的に付与することなく継続的に評価する必要があるという前提に立つものでした。

この標準により、境界とVPNという足枷からついに解放され、ネットワークの保護から、ネットワーク経由でやり取りするユーザ、データ、アプリケーションの保護へと重点が移行することになりました。ゼロトラストは、単にコンテキストベースの最小特権アクセスを意味するものであり、はるかに広範なユースケースとトラフィックフローに適用できるものです。

800-207スタンダードは、ゼロトラストのための重要な原則と前提を規定しています。(長いリストの中で)最も重要なのは以下3つのポイントです:

1. どのリソースも本質的に信頼されるべきではない。
2. ネットワークの場所に関係なく、すべての通信を保護する。要求のターミネーションとインスペクション。ユーザと要求に関連付けられているすべての利用可能なコンテキストに注目する。
3. すべてのリソース認証と承認は動的であり、アクセスを許可する前に厳格に適用する必要がある。



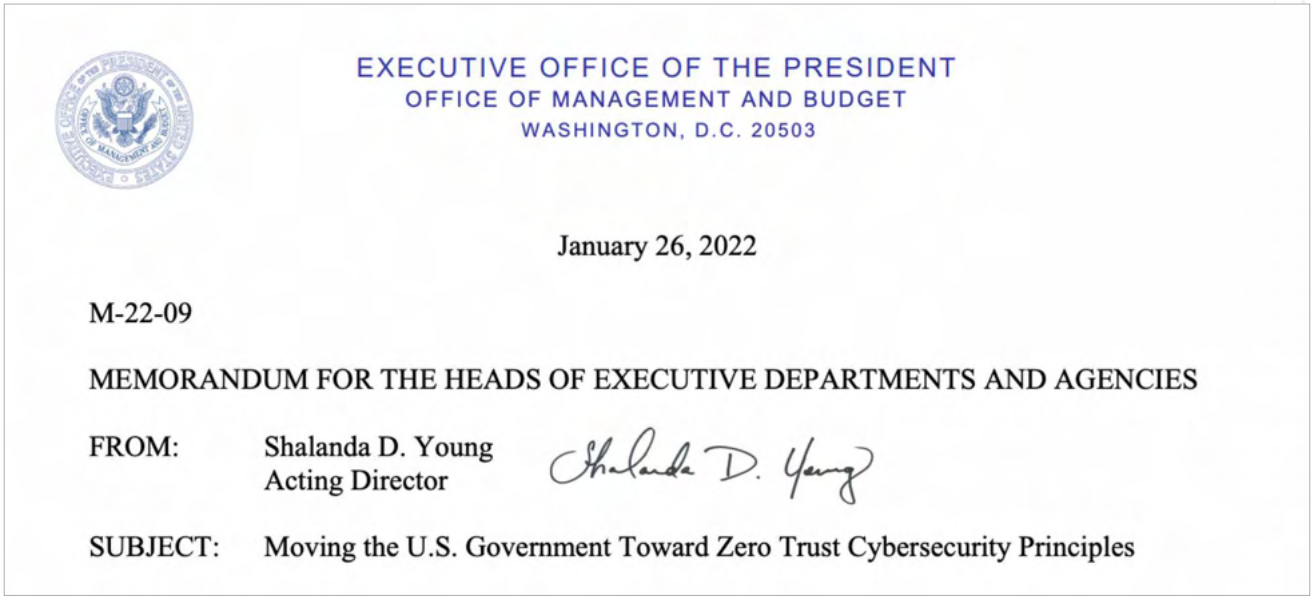
しかしながら、少なくとも米国において最も重要だったのは、ゼロトラストの原則の推進は後戻りができないものだということです。大統領の政策の実施を担当する米国管理予算局が2022年にM-22-09指令を発行し、連邦政府のすべての部局に2024年までのゼロトラストアーキテクチャの採用を義務付けるとし、採用までの明確なマイルストーンと期日の概要を示しました。

「これで、ガイダンスとなる文書、管理者モデルが出揃いましたが、あくまでもこれは、連邦政府のゼロトラスト戦略の出発点に過ぎません」と、Lorenzinは説明します。

IT管理プラットフォームのSolarWindsに対するサプライチェーン攻撃が2021年に明らかになり、州、財務、国土安全保障、商業、エネルギーを含む少なくとも9つ連邦機関が侵害されたことは、おそらくはオーロラ作戦以降で最も大胆で被害の大きい、国家が支援する攻撃でした。この攻撃をきっかけに、連邦政府はゼロトラストの採用に本格的に取り組み、以降の数年間のサイバーセキュリティの指針としてゼロトラストのアプローチを採用することになりました。

ゼロトラストの実装

ゼロトラストアーキテクチャに対するゼットスケーラーのアプローチは、NISTのZTAフレームワークやガートナーのSSEの定義と密接に一致していますが、そのようないかなる標準も上回るものであり、ゼロトラストの思え方を根本的に前進させる3つの要素にコミットしています。これらの高度な原則を組み合わせることで、ゼロトラストの適用を一定の論理的な結論へと引き上げることができます。



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

すべてのトラフィックはゼロトラストトラフィックである

ゼロトラストは、ネットワーク保護の新しい方法として始まり、最終的には、オンプレミスネットワークにとどまらない範囲にまで広がりましたが、その主な重点がプライベートアプリケーショントラフィックであることに変わりありま

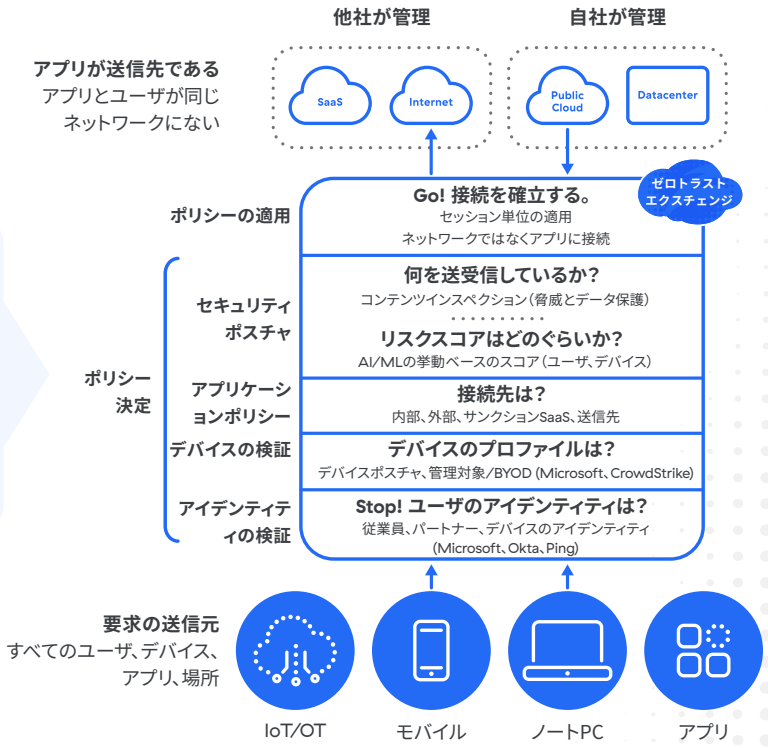
せん。あまりにも長きにわたり、ネットワークから完全に脱却するのではなく、ネットワークとの関係を前提に考慮されてきました。

ところが今、SaaSアプリケーション、パブリッククラウドとの間のトラフィック、さらにはパブリックインターネットにアクセスするユーザの保護にゼロトラストの原則を適用できることが知られるようになりました。そのトラフィックの送信元は、ユーザだけでなく、ワークロードである場合もあります。転送手段に依存しないアクセスを可能にし、ルータ、有線または無線、4Gまたは5Gなどの任意のネットワーク経由でトラフィックが送受信されます。

送信元や送信先に関係なく、すべてのトラフィックにゼロトラストの原則を適用するべき時を迎えています。信頼できるものか否か、オンネットワークかオフネットワークか区別はすでになくなりました。次に取り組むべきは、どのエンティティがどのネットワークに接続するかという考えから脱却し、ゼロトラストを採用して、すべてのエンティティをビジネスポリシーを使用してダイレクト接続することです。インターネットを新しい企業ネットワークと考え、すべてのトラフィックが公正に処理されるようにします。

Zscaler Zero Trust Exchange アーキテクチャ

世界中の150のDCでのセッション単位のポリシーの判断と適用



1 アイデンティティとコンテキストは常に接続の前に置かれる

アイデンティティの検証がゼロトラストの中心に存在するものではあるものの、過去には、アイデンティティと接続が混同され、そのことで、誤ったモデルへと進んでしまったことがありますが、IPアドレス、MACアドレス、ポートとプロトコルはアイデンティティではありません。

OTデバイスで工場からネットワークに接続でき、ユーザはコーヒーショップからログオンできます。ただし、そのことは、デバイスやユーザについて知っていることを意味するわけではありません。だからこそ、アイデンティティとコンテキストから始める必要があり、接続の承認は必ずそこから始めるべきなのです。

ユーザがリソースへのアクセスを要求する場合、ユーザが誰で、役割や部門が何か、さらには、使用デバイスなどの情報やリソースに関するその他の情報を最初に判断した後に、セキュリティポリシーを考慮する必要があります。ユーザが何をしようとしていて、どこに接続しようとしているのか、そして、環境において何を基準に、その行動を許可するか拒否するかを判断するのでしょうか?

アイデンティティだけにとどまらないコンテキストが継続的に評価され、位置情報、IPアドレス、デバイスポスチャ、時刻などの要素もクロスチェックされます。ゼロトラストソリューションはさらに、トラフィックを復号化し、脅威とデータの持ち出しのリスクをインラインかつスケーラブルにインスペクションできるものでなければなりません。

Zero Trust Exchangeでは、ゼットスケーラーのグローバルクラウドからの脅威インテリジェンスに加えて、セキュリティやアイデンティティ検証のベンダなどのサードパーティテクノロジパートナーからの脅威インテリジェンスも関連付けることで、リスクを判断し、ポリシーやアクセスが判断されます。

2 アプリケーション、さらにはアプリケーション環境さえも認証されていないユーザに見えないようにする必要がある

ユーザが誰かをアクセスを付与する前に知るという問題が解決したら、次の課題、すなわち、リスクを軽減し、侵害の可能性を最小限にしつつ、ユーザを承認されたリソースにどのように接続するかという問題を解決します。ユーザ、デバイス、ポリシー、環境を取り巻くコンテキストが収集され、解決に向けて次の段階に進むことができます。

ゼットスケーラーは、リモート接続のインバウンドリスナを排除することで、外部の攻撃対象領域を排除します。攻撃対象領域を排除しないと、攻撃者がいとも簡単に脆弱なVPNゲートウェイや外部に公開されているアプリケーションを特定し、攻撃の標的にすることができます。インバウンド接続を待機するVPNは、攻撃者にとって格好の標的です。これはベンダに関係なく存在する、アーキテクチャモデルを変更することによってのみ解決できる問題です。

Zscaler Zero Trust Exchangeは、暗号化されたマイクロトンネルを使用して、ユーザとアプリケーション環境の両方からセキュリティクラウドへのアウトバウンドのみの接続を形成し、要求とその送信先の間の接続を仲介することで、これを実現します。

このオンラインの「第3の場所」は、検証済みユーザと、アクセスが許可されているリソースとの間のバッファの役割を果たします。ユーザが要求した資産に接続されると、きめ細かなポリシーによって、それを上回る選択肢がないことが保証され、水平移動は不可能になります。

3 結論

前述の原則により、ファイアウォールで保護されるネットワーク境界とVPN経由で接続されるリモートエンドポイントについての理解を根本的に変え、従来の考え方から永遠に脱却することができます。既存のセキュリティコントロールをクラウドでホスティングされる仮想インスタンスにそのまま複製するものではなく、オンネットワークとオフネットワークについての人為的な理解に依存するものでもありません。

ゼロトラストセキュリティをユーザ、ワークロード、アプリケーション、OT、IoTデバイスなどに提供するように設計された包括的アーキテクチャが、リスクを軽減し、保護を強化し、ユーザエクスペリエンスを簡素化し、エンタープライズセキュリティに関する考え方を根本的に変革させます。

zscaler™ | Experience your world, secured.™

Zscalerについて

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタルトランスフォーメーションを加速しています。Zscaler Zero Trust Exchangeは、ユーザ、デバイス、アプリケーションをどこからでも安全に接続させることで、何千人ものお客様をサイバー攻撃や情報漏洩から保護しています。世界150拠点以上のデータセンタに分散されたSASEベースのZero Trust Exchangeは、世界最大のインライン型クラウドセキュリティプラットフォームです。詳細は、**zscaler.jp**をご覧いただくか、Twitterで**@zscaler**をフォローしてください。

03-4243-6320 Zscaler, Inc.(本社) – 120 Holger Way – San Jose, CA 95134 zscaler.jp