ZscalerとAWS

すべてのユーザー、データ、ワークロードを保護するゼロトラストセキュリティ

Available in AWS Marketplace

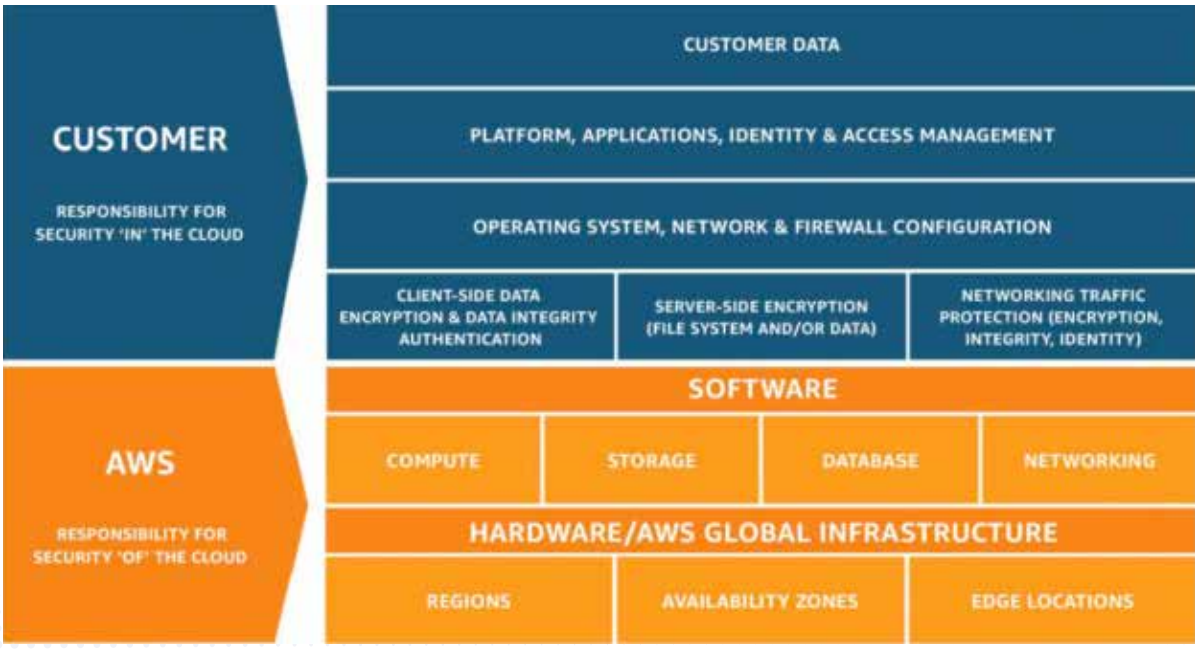
はじめに

多くの組織や公共機関が Amazon Web Services (AWS) にワークロードを移行し始めていますが、その大きなきっかけとなったのが世界的なパンデミックです。ビジネスの継続性と回復力の確保、コストの削減、新たな効率性の獲得などを実現するうえで、デジタル化の加速と重要なアプリを AWS に移行するための明確な戦略がいかに重要かを示したのが、この未曽有の事態でした。現在の IT 環境は、オンプレミスの物理サーバーから複数の AWS リージョンでアプリケーションやワークロードをサポートする仮想化インフラへと進化しており、ユーザーは時間や場所に左右されることなく、これらのアプリケーションにアクセスできるようになっています。

現代のビジネス ニーズに対応できない境界ベースのセキュリティ

一般的なクラウド セキュリティは、責任共有モデルに基づいています。このモデルは、AWS が基盤となるクラウド インフラストラクチャーのセキュリティを請け負い、企業がクラウド内のワークロードとアプリケーションを保護する責任を負うというものです。

AWS責任共有モデル



出典：https://aws.amazon.com/compliance/shared-responsibility-model/

過去 30 年にわたり、企業は広範囲におよぶ複雑なハブ&スポーク型ネットワークを構築、最適化することで、プライベート ネットワークを介してユーザーや拠点をデータ センターに接続してきました。こういったハブ & スポーク型ネットワークは、城と堀のセキュリティと呼ばれるアーキテクチャーを使用して、VPN やファイアウォールなどのセキュリティ アプライアンスで保護されていました。このアプローチは、従業員の大多数がオフィスで作業し、データとアプリケーションがデータ センターで管理されている場合は十分に効果を発揮していました。

ところが現在、ユーザーはさまざまな場所で作業し、クラウドに存在するアプリケーションやデータに頻繁にアクセスしています。スピーディーかつ生産的なコラボレーションには、時間や場所に左右されないアプリへの直接アクセスが不可欠です。AWS でホストされているアプリケーションにアクセスするために、アクセスやセキュリティの目的で、ユーザーのトラフィックをデータ センターに戻すことにもはや意味はないのです。

サイバー攻撃はより巧妙化し、ユーザーの働く場所も多様化しつつある今、VPN やファイアウォールを使用した境界セキュリティは、不完全で一貫性のないセキュリティや貧弱なユーザー エクスペリエンスなどといった課題を生み出しています。この背景として、次のような理由が考えられます。

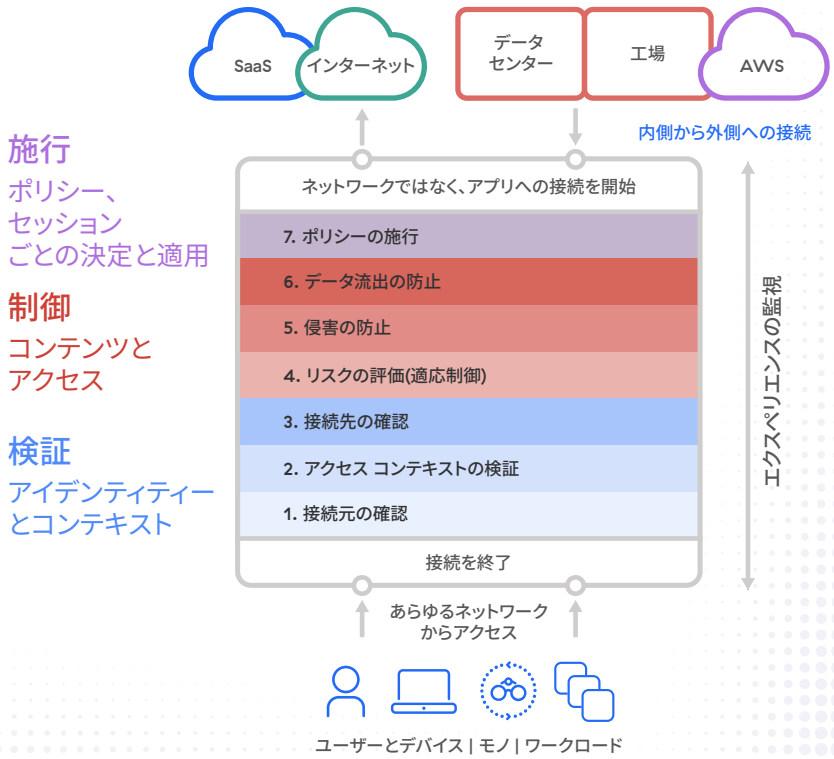
- VPN やファイアウォールは、企業ネットワークを拡張して攻撃対象領域を拡大させるため、脅威が速やかに水平移動できるようになり、セキュリティ侵害が発生する
- 旧式のセキュリティ ポイント製品の寄せ集めは、コストや複雑性の課題を生み出し、結果的に攻撃に対処できない
- アクセスとセキュリティの目的でリモート ユーザーのトラフィックをデータセンターにバックホールすると (ヘアピン処理)、レイテンシーが発生したり、パフォーマンスやユーザー エクスペリエンスが低下したりする
- 複数のベンダーの製品を使用している場合、ユーザー、デバイス、場所で一貫性のないセキュリティが生まれ、脅威の優先順位付けが困難になる (複数のダッシュボード)
- 攻撃者は従来の防御を回避して、レベルの高い脅威を大規模に展開する
- 多くの組織がアプリを AWS に移行したり、SaaS アプリを採用したりすることでアプリの変革を進めている。ファイアウォールや VPN に基づく城と堀のセキュリティから、時間や場所に左右されないアプリへの高速な直接アクセスを保護する最新のアーキテクチャーに移行する必要があります。

組織は今こそ、ゼロトラスト アーキテクチャーを採用する必要があります。

Zscaler Zero Trust Exchange

AWS アドバンスト ティア ソフトウェア パートナーである Zscaler は、10 年にわたるゼロトラスト セキュリティのリーダーとして、Zscaler Zero Trust Exchange を活用しながら安全なデジタル化を実現できるように多くの企業を支援してきました。

Zscaler のゼロトラスト アーキテクチャーは、AWS のユーザー、デバイス、アプリケーション間の接続を仲介する効率的なスイッチボードとして機能する統合プラットフォームです。すべてのリクエストは、デバイスの種類、場所、アプリケーション、コンテンツなどのアイデンティティーとコンテキストを基に検証されます。アイデンティティーとコンテキストが検証されると、ゼロトラスト アーキテクチャーは接続リクエストに関連するリスクを評価し、サイバー脅威や機密データの有無を確認する目的でト



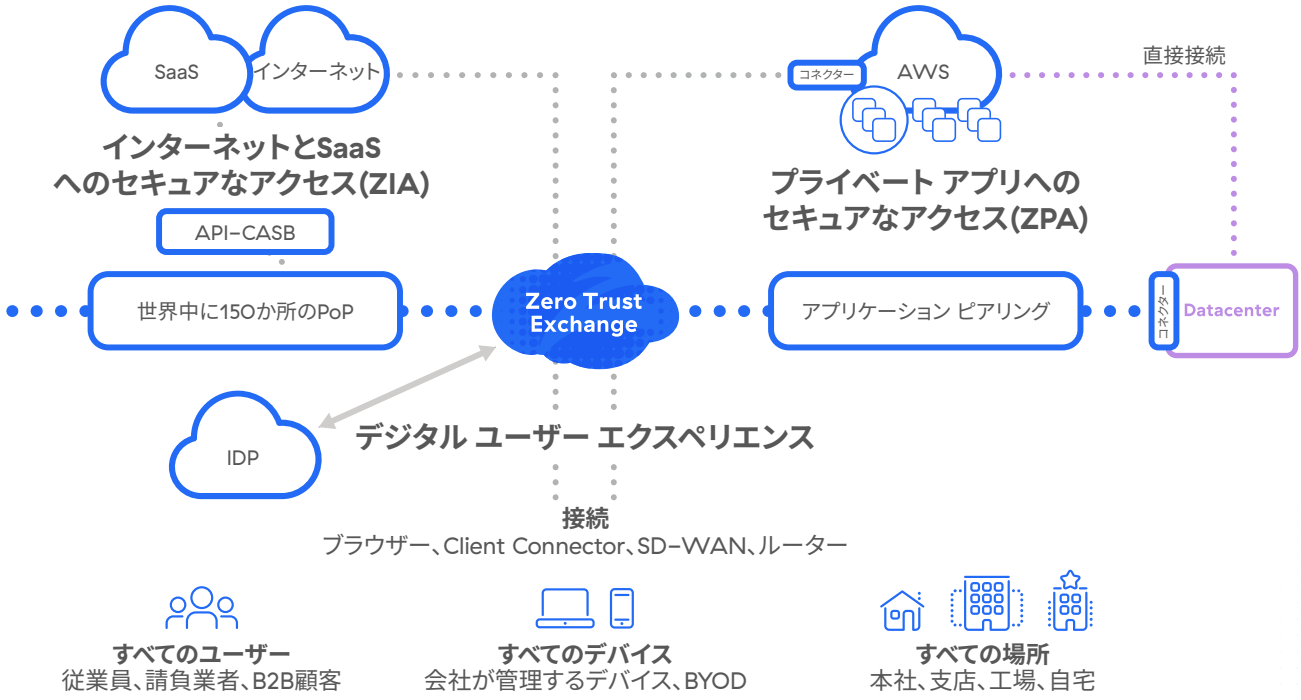
ラフィックを検査します。そして AWS アプリケーションへの接続を確立する前に、ポリシーを施行します。この最新のアプローチにより、セキュリティ、ネットワーク、バックホール / パフォーマンスの課題が解消され、組織は優れたセキュリティと快適なユーザー エクスペリエンスを提供しながら、AWS へのアプリとワークロードの移行を加速できます。

世界最大のセキュリティ クラウドである Zero Trust Exchange は、世界中に 150 か所を超えるポイント オブ プレゼンス (PoP) を構え、GovCloud East および West を含む、世界中のほとんどの AWS リージョンに存在します。パフォーマンス ハブを備えた分散アーキテクチャーにより、あらゆる通信を効率的かつ安全に AWS に直接送信できるようになります。

Zscaler と AWS が実現するセキュア デジタル トランスフォーメーション

1. ユーザーの保護

ユーザー重視のセキュアなハイブリッド ワークを強化するには、あらゆる場所やデバイスで従業員とサード パーティーをサポートできる柔軟性が不可欠です。また、AWS 内のデータやアプリ、ワークロードへの高速でセキュアな信頼性の高いアクセスを提供するユーザー エクスペリエンスのほか、ビジネスに合わせて拡張し、既知および未知の脅威から保護するソリューションも求められます。



Zscaler は、以下の方法で AWS ユーザーを保護します。

- ユーザーを AWS の特定のワークロードに直接接続し、ネットワークには接続しない。これにより、脅威が水平方向に伝播して他のユーザー、デバイス、アプリケーションに感染するリスクを排除できます。
- ユーザーとアプリケーションを Zero Trust Exchange の背後に配置して、インターネットから見えないようにする。悪意のあるアクターは見えないものを攻撃できないため、ユーザーがマルウェアやランサムウェア、フィッシングなどのサイバー脅威の影響を受けることはありません。

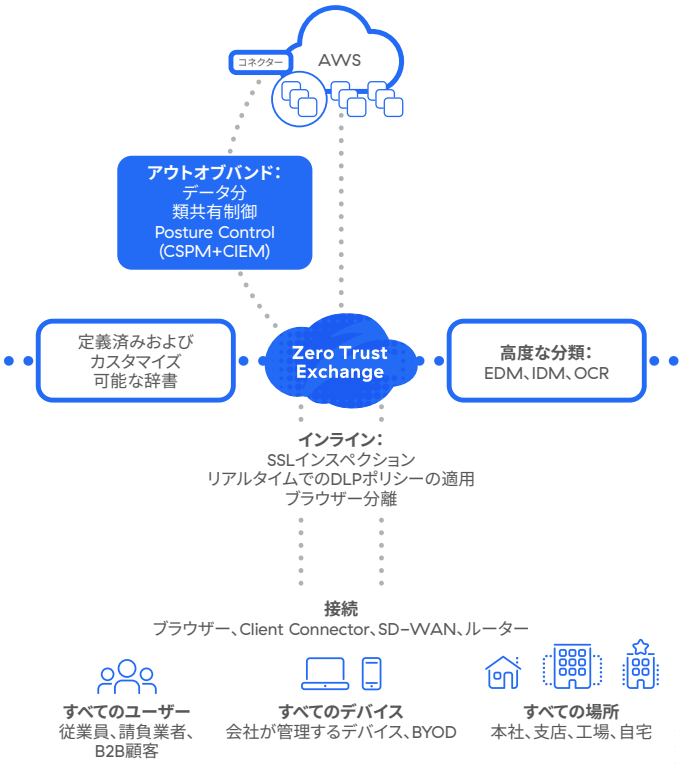
このようにして、組織はリスクを大幅に軽減し、生産性を向上させると同時に、優れたユーザー エクスペリエンスを提供できるようになります。

Zscaler は、統一性のない旧式のポイント製品をリプレースする統合クラウドネイティブ ソリューションを提供し、AWS のワークロードをサポートするために主要なテクノロジーを 1 つにまとめることで、セキュリティ サービス エッジ (SSE) のビジョンを実現します。これには以下が含まれます。

- Zscaler Internet Access (ZIA): クラウド セキュア Web ゲートウェイ (SWG)、クラウド アクセス セキュリティ ブローカー (CASB)、クラウド情報漏洩防止 (DLP) に対応
- Zscaler Private Access (ZPA): 次世代ゼロトラスト ネットワーク アクセス (ZTNA) に対応
- Zscaler Digital Experience (ZDX): デジタル エクスペリエンス モニタリング (DEM) に対応

2. データの保護

ユーザーはさまざまなデバイスからリモートで作業し、S3 などの AWS 製品のデータにアクセスしてアップロードします。境界型のセキュリティ アプライアンスではこういったデータを保護できず、新しいユース ケースごとに異なるポイント製品で対応する必要が出てくるため、余分なコストや複雑性が発生します。



Zscaler Data Protection は、データがどこに移動しても追跡し、ゼロトラストの原則を施行します。データはインラインでスキャンされ、リアルタイムの分類とポリシーが施行されます。ブラウザー分離は、データを管理対象外のデバイスにピクセル データとしてストリーミングすることで流出を阻止します。AWS に保存されているデータは、機密情報を確認し、リスクの高い共有を自動的に取り消す目的でスキャンされます。Posture Control は、例えば意図しないパブリック S3 バケットなど、機密データを公開する恐れがある設定ミスと権限を修正します。

Zscaler Data Protection には、次のような特徴があります。

- 一般的な SSE 以上のメリットを実現する最も包括的なセキュリティ プラットフォームの一部
- データがどこに移動しても一貫して保護する統合ポリシー・エンジン
- 世界最大かつ最も高性能なセキュリティ クラウドによるフル SSL インスペクション
- 世界中の大手企業によって大規模に展開された実績を持つプラットフォーム

3. ワークロードの保護

さまざまなワークロードがクラウドに移行するにつれ、ビジネスの競争力を確保するために、ネットワークとセキュリティの近代化が多くの組織の急務となっています。静的な環境向けに設計された境界ベースのネットワークでは、クラウド接続のニーズに対応することはできません。このため、攻撃対象領域の拡大、脅威の水平移動のリスク、生産性とコラボレーションの低下、そしてハイブリッド ワーカーとクラウドベースのアプリケーションを保護するためのネットワーク セキュリティ アーキテクチャーの管理が生み出すコストや複雑性など、組織にとって重大な課題が生じます。

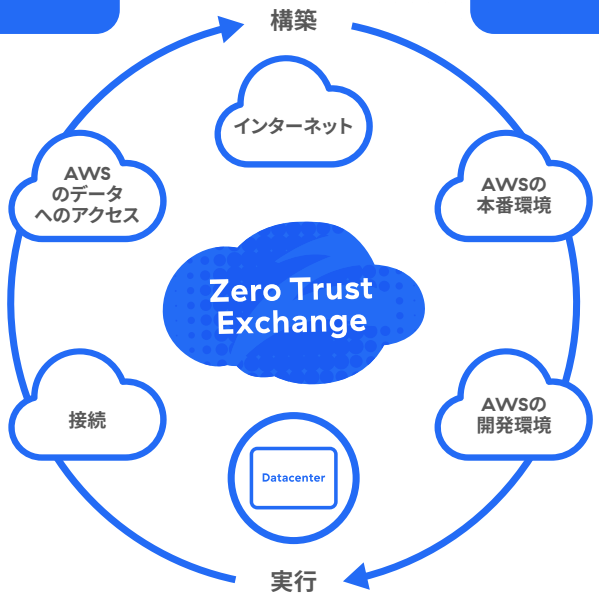
Zscaler は、構築から実行までアプリケーションを保護する包括的な Zscaler for Workloads ソリューションを提供することで、AWS を使用する組織のこうした課題に対処します。革新的なゼロトラスト アーキテクチャー上に構築された Zscaler for Workloads は、Posture Control (CNAPP) と Zscaler Workload Communications を強力に組み合わせたものです。従来のセキュリティ ポイント製品からゼロトラスト用に設計された完全なソリューションに移行することで、AWS で動作するクラウドネイティブなアプリと VM ベースのアプリの両方のセキュリティを統合します。この統合されたアプローチにより、コストと管理オーバーヘッドを増加させるポイント製品ソリューションが不要になるだけでなく、部門間のコラボレーションが強化され、デジタル トランスフォーメーションが加速します。

AWS向けクラウド セキュリティ ソリューション

Posture Control (CNAPP)

公開状況の検証 (エージェントレス)
- 公開されたアセットや脆弱性 (攻撃対象領域) の特定
- 機密データの検出

構成の検証
- 設定ミスの特定と優先順位付け
- ユーザーやワークロードに付与された過剰な権限の特定



Workload Communications

ワークロードからインターネット
- 攻撃対象領域の削減
- 仮想ファイアウォール / プロキシーを使用しないランタイムの侵害と情報漏洩の防止

ワークロードからワークロード
- AWS アカウント
- AWS からデータ センター

セグメンテーション
- ネットワーク セグメンテーションを使用しないユーザーとアプリ間、アプリ間のセグメンテーション
- AWS のワークロードのアイデンティティーを基にしたマイクロセグメンテーション

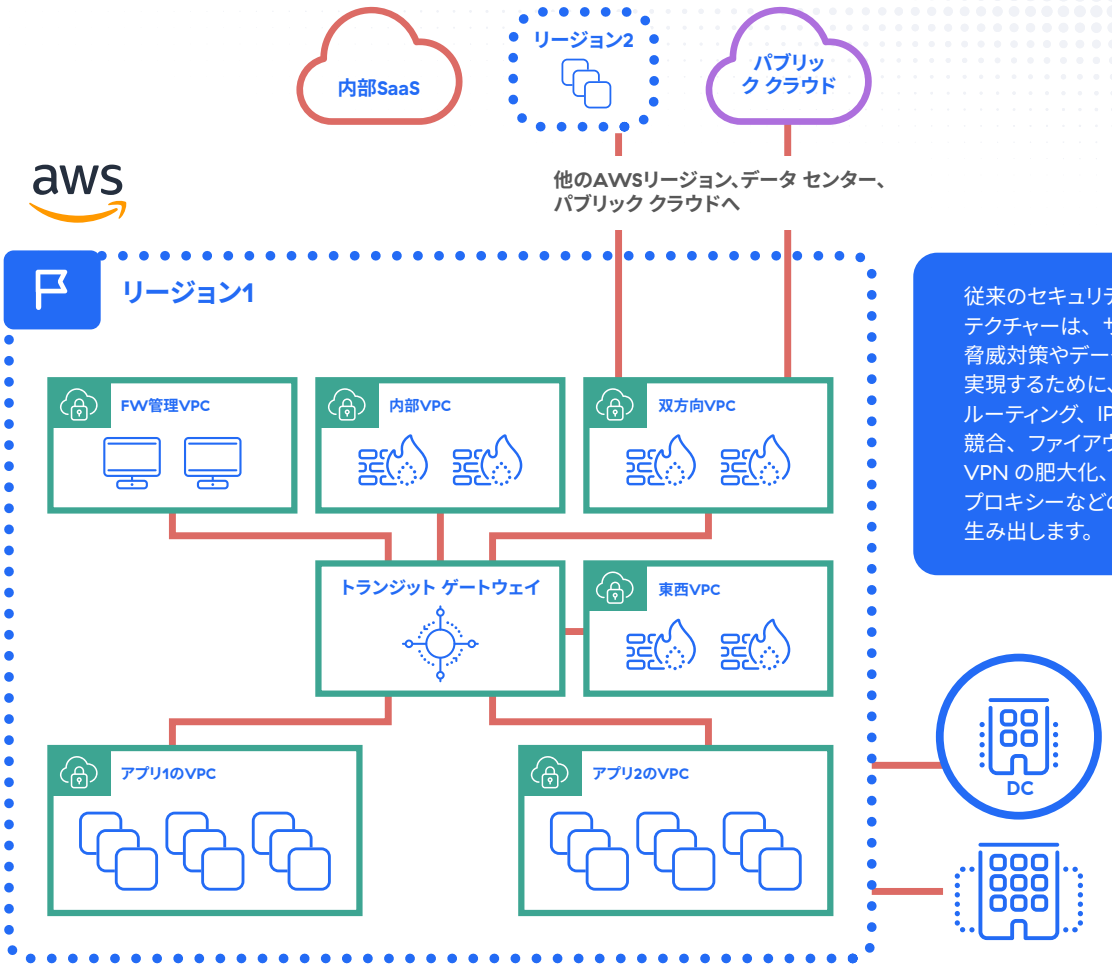
1. Posture Control (CNAPP)

クラウドネイティブ アプリケーション保護プラットフォーム (CNAPP) である Posture Control は、機械学習を使用して、AWS デプロイメントの設定ミス、脅威、脆弱性に起因する隠れたリスクを相関させる 100% エージェントレス ソリューションとして、クラウドネイティブ アプリケーション セキュリティを再構築します。これにより、セキュリティ、開発、DevOps などの各部門は、開発サイクルのできるだけ早い段階で、クラウドネイティブ アプリや VM ベースのアプリのリスクを効率的に優先順位付けし、修正できるようになります。

主なメリット
- 複数のポイント ソリューションの管理に伴う複雑性やコストを削減して、クラウド環境を保護し、コンプライアンスを維持
- 統一されたポリシー エンジンを使用して、すべてのクラウド サービスに一貫したセキュリティ ポリシーを施行
- リソースや技術的スキルの不足から生じる設定ミスやセキュリティの問題を防止
- 開発者のワークフローにセキュリティを組み込み、アラート疲れを軽減しながら重大なリスクに優先順位を付けて修正
- 強力な視覚化とレポートで、セキュリティの脆弱性、設定ミス、権限、公開データなどを明確に表示

2. Workload Communications

Zscaler Workload Communications は、インターネットやプライベート アプリケーションへのワークロードのシンプルでセキュアなアクセスを提供するクラウド ワークロードのゼロトラストを実現することで、クラウド接続を完全に再構築しています。従来のネットワーク ソリューションとは異なり、Workload Communications は、アイデンティティーとコンテキストに基づいて信頼を検証する、実績ある Zscaler Zero Trust Exchange プラットフォームを使用して AWS への直接接続アーキテクチャーを提供します。これにより、ワークロードとインターネット間の通信、複数のリージョンと AWS アベイラビリティー ゾーンにわたるワークロード間の通信、AWS 環境内のワークロード間の通信が保護されます。

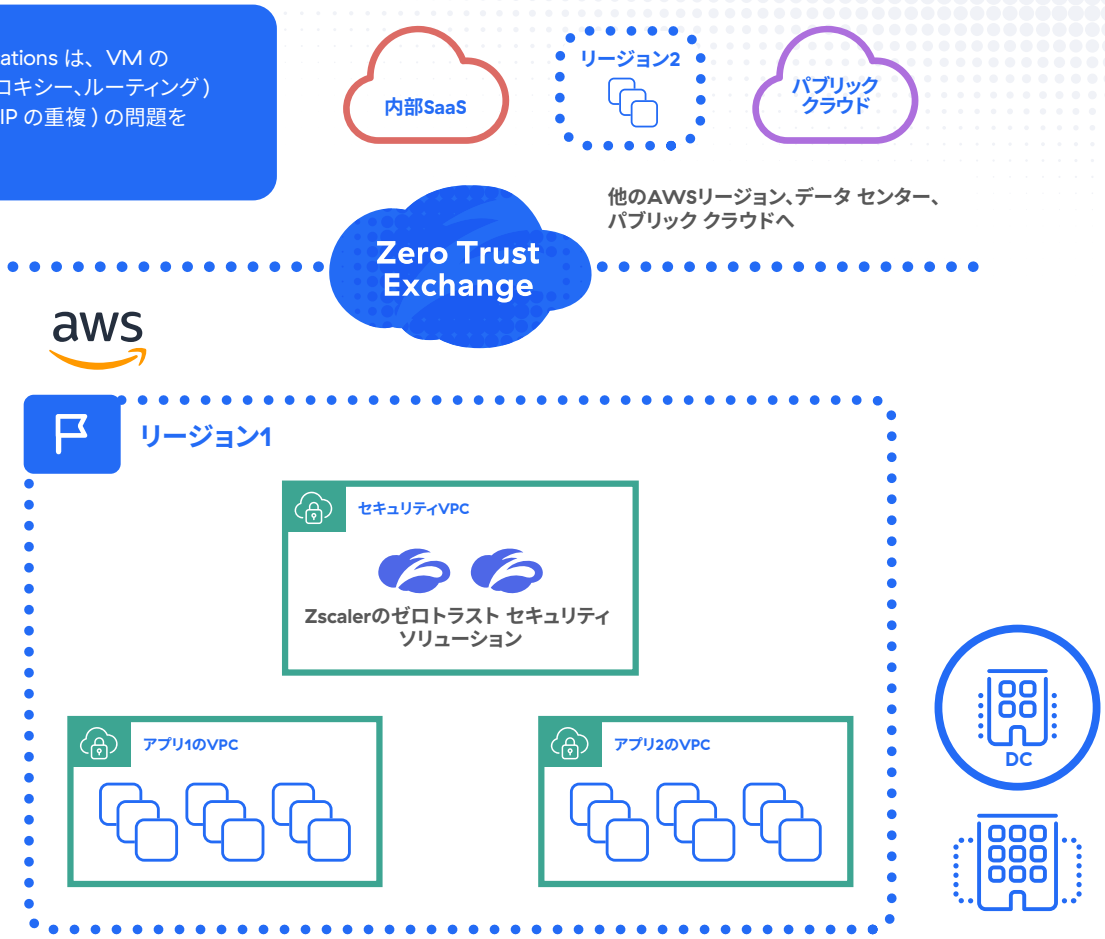


主なメリット

Workload Communications は、完全なプロキシー アーキテクチャーを使用してワークロードをインターネットやプライベート アプリケーションに直接接続することで、ネットワークの攻撃対象領域を排除します。このアーキテクチャーでは、ルーティング、VPN、トランジット ゲートウェイ、トランジット ハブ、ファイアウォールが廃止されるため、接続が劇的に簡素化されると同時に、実績ある ZIA と ZPA のポリシー フレームワークを使用することで、柔軟な転送と容易なポリシー管理が可能になります。この独自のアプローチにより、主に次のようなメリットが AWS ユーザーに提供されます。

- 攻撃対象領域を排除して情報漏洩を防止：クラウドへの直接接続アーキテクチャーを使用してトラフィックを企業ネットワークから切り離すことで、AWS 環境のアプリケーションはサイバー脅威から見えなくなり、情報漏洩のリスクを低減します。
- シンプルなクラウド接続：ゼロトラスト アーキテクチャーでは、IP 重複の問題が解消され、ルートの分散が不要になり、ワークロードが他のアプリケーションに直接接続されるため、パフォーマンスのボトルネックも回避できます。
- 優れたアプリケーション パフォーマンスを大規模に実現：Zscaler は真の分散アーキテクチャー上に構築されており、サービス エッジに到達するすべての通信がアイデンティティーとコンテキストに基づいて即座に処理されます。GovCloud East および West を含む、世界中のほとんどのリージョンにおける AWS とのピアリング関係により、アプリケーションがホストされている場所に左右されることなく、アプリケーション間の最短パスが確保され、レイテンシーの削減とアプリケーション パフォーマンスの向上を実現します。

Workload Communications は、VM の肥大化 (FW、squid プロキシー、ルーティング) や複雑なルーティング (IP の重複) の問題を解消します。



概要

Zscaler と AWS は連携して、組織がセキュア デジタル トランスフォーメーションの取り組みを推進できるようサポートし、以下を実現します。

- レイテンシーを削減し、AWS へのワークロードの移行を加速する効率的なルーティング
- ファイアウォールや VPN を排除して、ネットワークとセキュリティのアーキテクチャーを簡素化
- エンド ユーザー エクスペリエンスを向上させる常時アクセス
- クラウド ネイティブ アプリケーションへの脅威を排除する、より強力で包括的なセキュリティ態勢
- 競争力につながる強化されたビジネス アジリティー
- コストを削減して、事業の他の部分に費やすべき資金を確保

ユーザー、データ、ワークロードの保護に必要な機能をすべて網羅する Zscaler のゼロトラスト セキュリティ ソリューションは、AWS Marketplace で購入できます。

Zscaler for AWS の詳細はこちら

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、ユーザー、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、数多く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 センターに分散された 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。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp