AWSとZscalerの統合ソリューション: 強力かつ拡張可能なクラウドセキュリティを実現

目次

クラウドの課題: 迅速かつ安全な拡張

*VPN*などの境界ベースのセキュリティ対策では、クラウド時代の最新の課題に対応できません。それでは、どのような選択肢があるのでしょうか。

2020年には、半数以上の企業がワークロードをクラウドに移行し、そのうち76%がAmazon Web Services (AWS) を選択しています。クラウドを導入するメリットは、コスト削減から迅速な拡張までと幅広く、その効果に疑いの余地はありません。しかし、クラウドで事業を展開する企業は2つの新しい課題に直面しています。1つは、リモートおよびハイブリッドワークが急速に進む中でのアクセスと運用の管理、もう1つはマルウェアやランサムウェアによる脅威の巧妙化です。

従来、安全な環境を実装するにはネットワーク中心のVPNが必要でしたが、その結果、スピードや使いやすさ、制御面の柔軟性などが問題となっていました。企業のクラウドへの移行やIT運用の規模の拡大が進められている今、VPNのメリットよりもデメリットの方が大きくなっています。

VPNは、本質的に安全なインターネットアクセスを提供するようには設計されていません。強力なインターネット接続や最新のセキュリティ対策を講じようとすれば、そのしわ寄せは従業員に及んでしまいます。また、クラウドへの移行を進める企業が場所を問わず働くユーザを採用するにつれて、インバウンド接続が拡大して、DDoS攻撃の機会が増加します。これにより、ネットワーク上で誰が何をしているかを把握するための可視性が低下し、アクセスセグメンテーションの複雑化をもたらします。これらのハードルは拡張性を結果的に制限し、コストの増加だけでなく生産性やユーザエクスペリエンスの低下を招きます。場合によっては、最終的なエンドユーザである顧客にも影響が及ぶことがあります。

これらの弊害を、ネットワークとセキュリティ業界に変革をもたらすZscalerのZero Trust ExchangeとAWSが解決します。AWSのアドバンストテクノロジパートナーとして、Zscalerはゼロトラストモデルに基づくサービスとしてのセキュリティを提供し、企業が現在と将来にわたって真のクラウドトランスフォーメーションを安全かつシンプルに達成できるようサポートします。

Zscalerの近代的かつ総合的なクラウドファーストソリューション

マルチクラウドの複雑性に対応した構成可能な製品スイートでアクセスの簡素化とセキュリティの強化を実現

企業がワークロードをクラウドに移行しようとしている場合でも、あるいは単にVPNから移行しようとしている場合でも、ZscalerとAWSを組み合わせることで、最先端のテクノロジとゼロトラストモデルを通じて、トップレベルのセキュリティと優れたユーザエクスペリエンスが提供されます。

Zscalerが提供するアプリケーションを中心としたセキュリティサービスは、最初からクラウド上に構築されており、従来のインバウンドとアウトバウンドゲートウェイを置き換える形で、より現代的なアプローチを実現します。これは、AWSを利用する企業に最適です。以下の3つの主要なサービスにより、AWSのお客様はクラウドオペレー ションを最大限に活用できます。

Zscaler Private Access (ZPA) は、ユーザをネットワークではなくアプリケーションに接続し、インターネットからアプリケーションを削除して、より安全な環境を実現しながらバックエンドの複雑性を軽減することができるため、時代遅れのVPNが不要になります (ユーザが関与しないバックエンドのツールや操作をよりスムーズに管理) 。

Zscaler Internet Access (ZIA) は、従来のSecure Web Gatewayアプローチのコストや複雑性を軽減するクラウド提供型の完全なセキュリティスタックです。

Zscaler Digital Experience Monitoring (ZDX) は、組織内のすべてのユーザのデジタルエクスペリエンスを調査、評価、測定するマルチテナント監視プラットフォームです。

組織が次のことを実現できるように、ZscalerとAWSは共同でサポートします。

- エンドユーザエクスペリエンスを向上させる常時アクセス
- レイテンシの削減とリリースまでの時間の短縮を可能にするより効率的なルーティング
- 脅威を排除するより強力で総合的なセキュリティ体制
- ダウンタイムを最小限に抑える迅速なアプリの移行
- 競争力につながるビジネスのアジャイル化の強化
- 他の業務に活用できる資金を捻出するためのコスト削減

これらのツールは、すべてのビジネスに将来性を考慮した効果を発揮しますが、特にリスクの高いユースケースではその価値が顕著に現れます。たとえば、ZscalerはITチームが合併や買収時に直面する技術的な問題点の大半を解消します。セキュリティのベストプラクティスを実践しながら、シンプルな統合プロセスを提供するZscalerは、技術的なセットアップにかける時間を数か月から数週間に短縮させてきました。合併後の企業は、ネットワークの構築や移動に伴う手間や遅延を発生させることなく、従業員をアプリケーションに直接接続させることができます。

数字で見るZscaler

1日当たり

70億
件の脅威をブロック

2,000億
件以上のリクエストを処理

20万
件以上の独自のセキュリティアップデートを提供

ZPA: プライベートアプリ向けのシームレスでクラウドファーストのゼロトラストアクセスソリューション

時代遅れの*VPN*からストレスのないアクセスへ - プライベートアプリをインターネットに公開せず、外部の脅威アクターから不可視化 -

VPNはかつてプライベートアクセスに最適なオプションでしたが、クラウドベースの世界では基本的にユーザをネットワークにルーティングして送り返すだけの煩雑かつ脆弱なシステムになっています。リモートワーカー向けのアプリ接続が世界中を横断する際にファイアウォールからロードバランサーまでのさまざまなタッチポイントを通過するため、今まで以上に多くのステップをもたらします。さらに、VPNを使用するユーザは、どのプロファイルを使用するべきなのか、どのリソースがネットワークに接続させてくれるのかを理解する必要がありますが、これは技術力が高くない従業員にとっては快適なユーザエクスペリエンスとは言えません。

サテライトオフィスが軌道から外れないために

ZPAは、VPNを使わずにアプリへの安全なリモートアクセスを提供します。ネットワークから完全に独立しているため、IP中心の物理アプライアンスや仮想アプライアンスに依存することはありません。ZscalerのグローバルセキュリティクラウドでAWS App Connectorを通じて確立するインサイドアウト接続を活用するゼロトラストは、ソフトウェア定義の境界 (SDP) ソリューションを使用して、AWSへのアプリ移行前、移行中、移行後の承認済みユーザアクセスを管理します (AWS Native Security GroupsとAWS Direct Connectも無料)。ユーザが内部アプリケーションに接続しようとしている場所に関係なく、ZPAはアプリの迅速な移行、コスト削減、脅威ターゲットの減少 (プライベートデータセンタに依存している企業の場合でも) を実現するため、スケーラビリティと敏捷性の両立に最適です。

ZPAの導入事例: GROWMARK

作物の成長を維持するさまざまな原料とサービスを提供する北米の農業会社であるGROWMARKは、500以上の農村地帯に従業員を抱えていたこともあり、不安定なインターネット環境という課題に直面していました。コロナ禍でサプライチェーンが打撃を受けて以来、業務を円滑に進めることがこれまで以上に重要になりました。GROWMARKは、近代化へ向けた取り組みの一環として何百ものアプリをAWSに移行しましたが、一部のアプリを引き続きオンプレミスでホストしているため、ハイブリッド構造で機能するソリューションを必要としていました。ZPAを選択したGROWMARKは、従業員に安定した接続を提供すると同時に、プライベート環境からパブリックインターフェイスを削除し、最終的に攻撃対象領域を削減することができました。コロナ禍のピーク時においても、98%の従業員を問題なくZPAに接続することができました。

ZIA: 信頼性の高いサービスとしてのクラウドセキュリティスタック

従来の境界型セキュリティからゼロトラストのクラウド保護へ - リスクとネットワークコストを削減 -

データセンタと境界ベースのセキュリティモデルで運用されている企業は、クラウド移行はより安全なWebゲートウェイアプローチを意味すると実感しています。

データセンタからクラウドに移行すると、アプリケーションは新しい環境に置かれます。これまでアクセスを簡素化し、コストを削減してきた一元化されたゲートウェイは、ユーザのトラフィックが直接クラウドに向かうことで生じる新しい脆弱性にもはや対処できません。これにより、従来のセキュリティ境界に基づくフレームワークが足かせとなります。さらに、新しいセキュリティアプライアンスが次々と登場し、すでに過負荷状態となっているゲートウェイに追い打ちをかけ、IT部門が対応することが困難な状況となっています。

エラーの余地を完全に排除

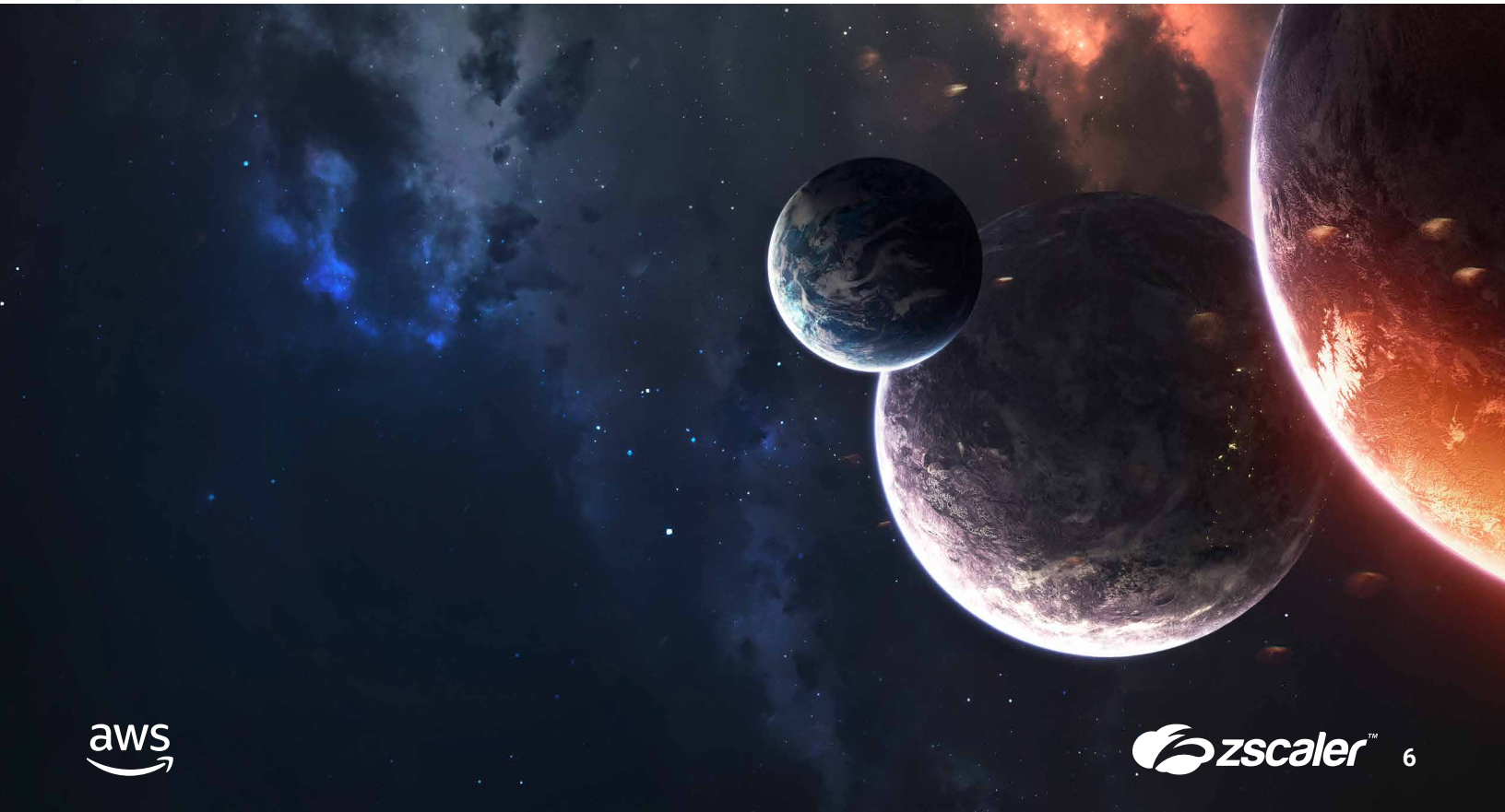
ZscalerとAWSはゼロトラストで動作するため、未知の領域に直面した場合でも確実に保護します。Forresterの見解では、ゼロトラストはビジネスの一歩前進につながり、セキュリティアーキテクチャの最適な選択肢とみなされています。

ZIAを使用すると、企業はサービスとしてのソフトウェア (SaaS) ソリューションへのより安全な接続を浸透させ、AWS上の内部アプリケーションへのリモートアクセスをシンプルかつ安全に保ちながら、企業のユーザ全体のすべてのインターネットアクティビティを可視化できます。

Zscalerの構造とサービスを通じて、攻撃対象領域の削減、アクセス制御の向上、データ保護の強化を実現し、きめ細かなポリシーを大規模に適用できます。

ZIAの導入事例: MAN Energy Systems

ドイツの製造輸送サービス会社であるMAN Energy Systemsは、ディーゼルエンジンやターボ機械など、世界の運輸業界において重要な役割を担う製品やサービスを提供しています。同社は市場競争力を維持するためにワークロードをAWSに移行しましたが、事業成長に伴い世界中に分散したチームは、アプリやカスタムビジネスツールへのモバイルアクセスをこれまで以上に必要としていました。個人レベルで膨大な数のアプリにアクセスするため、認証やアクセスに時間がかかり、セキュリティリスクが高まるだけでなく、従業員の不満が募る状態を招くことになりました。同社の管理層は、VPNからの移行と同時に、信頼できるアプリケーションへのアクセスは信頼できるユーザだけ許可するZIAを採用し、モバイルワーカーが常にどこからでも安全にMANのSaaSアプリケーションに接続できるようにしました。



ZDX: エンドユーザのための高速でシームレスなエクスペリエンス

アプリ、エンドポイント、*CloudPath*のパフォーマンスメトリクスの統合ビューを通じて、ユーザエクスペリエンスに関する実用的な深いインサイトを獲得

私たち消費者は、高いレベルのユーザエクスペリエンスに慣れすぎており、ソーシャルメディアが一時的に停止するだけでニュースになってしまうほどです。企業がオフィス内テクノロジでユーザエクスペリエンス向上に努める一方で、リモートやハイブリッドチームはインターネット接続性の問題やさまざまな (時には時代遅れの) パーソナルモバイルデバイスがもたらすハードルの格闘を余儀なくされており、こうしたボトルネックはより一般的に見られるようになりました。これがタイムアウトと絶え間ない再接続という形で顕在化すると、ヘルプチケットが積み重なり仕事が完遂できず、それぞれの問題の原因 (および解決策) を割り出すプレッシャーがIT部門に集中します。

すべてのエンドユーザにストレスゼロのエクスペリエンスを提供

ZDXは、組織内のすべてのユーザのデジタルエクスペリエンスを調査、評価、測定するクラウドベースのマルチテナント監視プラットフォームです。リアルタイムで問題の原因 (インターネット接続とISPプロバイダなど) をトリアージし、リモートトラブルシューティングを展開します。この分析機能は、場所、ユーザ、部門ごとに時系列でパフォーマンスを測定し、傾向を把握して改善につなげることができます。その結果、真のセキュアアクセスサーバーエッジ (SASE) アーキテクチャが、優れたユーザエクスペリエンスとIT部門へのヘルプチケットの削減を実現します。

ZDXの導入事例: Liberty Mutual

Liberty Mutual Insuranceは、データセンタとISPの帯域幅に関しては万全の体制を確保していましたが、在宅勤務の従業員には、同じ水準のインターネット接続を保証できずにいました。 2020年当時は、どの企業もこうした状況に直面していました。 同社のセキュリティチームは、コンセプトの実証を行うために100ユーザからスタートし、最初のユースケースとして長期的な問題を抱えるユーザにZDXを展開しました。その結果、ホームネットワークに関するユーザの問題を簡単に解決できるレベル2ヘルプデスクチームに問題を引き渡せるようになりました。 現在は、組織全体でZDXを統合し、サービスプロバイダの遅延の問題、ワイヤレスルータの問題、デスクトップコンピュータのメモリリーク、ページフェッチ時間に関するISPの問題などを特定して排除しています。

簡単導入、素早い運用を可能にした共同ソリューション

スピードアップを念頭に設計された導入プロセスとアクセスを管理するZscaler Client Connectorにより、わずか数分で稼働を開始

新しいプラットフォームとITインフラストラクチャへの移行は複雑で長期化する傾向にあるため、Zscalerはスピードとシンプルさを重視した導入プロセスを構築し、ZscalerとAWSを使用することで安全なクラウドベースの運用と適切な対象者のためのスムーズな移行がいつでも容易に行えます。

ZPA、ZIA、ZDXはそれぞれ単独でも使用できますが、これらを組み合わせることでより優れたフレームワークとして機能します。その際、プロセスの中心にあるのはZscaler Client Connector (ZCC) です。

ZPAはClient Connectorを使用して、ゼロトラストアプローチを通してユーザをプライベートアプリケーションに接続しますが、Webのみのプライベートアプリケーション用にBrowser Accessも利用できます。

ZIAはClient Connectorを使用して、企業ネットワーク外のユーザを保護し、Zscalerのサービスを介してインターネットトラフィックを転送し、きめ細かいセキュリティポリシーの確実な適用を保証します。

ZDXはClient Connectorを使用して、目的のSaaS (サービスとしてのソフトウェア) アプリケーションまたはインターネットベースのサービス (Salesforce、Zoomなど) に対して総合的なプロービングを実行します。

VPNからの脱却

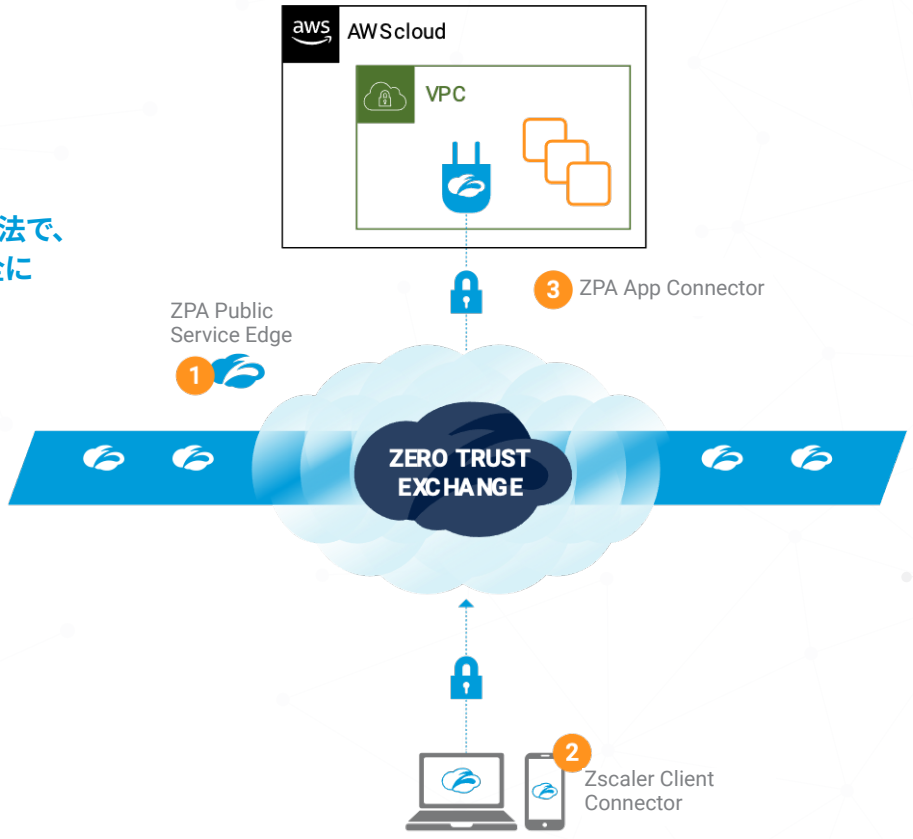
Zscalerをご利用のお客様は、VPNから当社の迅速で簡単なインストールに切り替えています。

1. IT部門は、ユーザがアクセスしたいアプリにZscalerが到達できるように、アプリケーションが存在するAWSにアプリコネクタをインストールします。
2. ZPAのポータル内で、アプリケーションとコネクタを定義し、サーバーグループに割り当てます。
3. インストールが完了すると、Client Connectorはリクエストのバインド先、送信先、ユーザの接続先を決定できるようになります。

Client Connectorの構成の設定に関する詳細はこちら

Zscalerをご利用のお客様は以下の方法で、VPNからの完全移行を素早くかつ安全に実現しています。

1. **ZPA Public Service Edge**
   ポリシーエンジンをホストし、接続を仲介
2. **Zscaler Client Connector**
   エンドポイントエージェントがZscalerのクラウドにトラフィックを転送
3. **.ZPA App Connector**
   プライベートアプリに接続し、新しいアプリを検出



今こそ、クラウドセキュリティの変革を始めるときです

ユーザアクセスの新しい道を切り開いたZscalerとAWSは、無限の可能性を秘めています。AWS Marketplaceで、Zscalerのソリューションをご確認ください。

7日間の無料ホスト型ZPAデモはこちら

数回クリックするだけで、インターネット上のどこに脆弱性があるかを示すクラウドセキュリティの詳細なポスチャ評価レポートを作成します。インターネット脅威分析をお試しください。