データ シート

Zscaler Private Access™

業界初の AI 活用型 ZTNA が実現する プライベート アプリへの高速かつ安全で 信頼性の高いアクセスで従業員を強力にサポート

Zscaler Private Access (ZPA) は、すべてのユーザーにゼロトラスト アクセスを提供し、プライベート アプリケーションへの直接接続を可能にするクラウドネイティブ ソリューションです。攻撃対象領域を最小化するとともに、ラテラル ムーブメントを排除し、高度な攻撃を阻止します。

ハイブリッド ワーカーとビジネスのニーズを満たせない従来のネットワーク セキュリティ アプローチ

従来のファイアウォールや VPN は、攻撃者に発見、悪用され得る膨大な攻撃対象領域を生み出しています。また、ユーザーをネットワークに直接接続するため、脅威のラテラル ムーブメントが発生します。ユーザーの資格情報が侵害された場合、攻撃者は組織の機密データに簡単にアクセスすることが可能です。ハイブリッド ワーカーやサードパーティーによるアクセスを可能にするために VPN を使用すると、サイバー リスクの増大、ユーザー エクスペリエンスの低下、管理オーバーヘッドの増加につながります。あらゆるデバイスや場所のユーザーに安全なアクセスを提供するには、より効果的なアプローチが必要です。

Gartner は 2025 年までに、新たに導入されるリモート アクセスの少なくとも 70% が、VPN サービスではなく主にゼロトラスト ネットワーク アクセス (ZTNA) で提供されるようになると予測しており、2021 年末の 10% 未満から大幅な増加が見込まれています。

主なメリット：

- **脆弱な VPN ソリューションのリプレース**
  ユーザーをネットワークではなくアプリケーションに直接接続することで、攻撃対象領域を削減するとともにラテラル ムーブメントを排除し、セキュリティ態勢を強化します。
- **サイバー攻撃の防止**
  Web やアイデンティティーの脅威に対するプライベート アプリの保護、完全なインライン検査による高度な脅威対策、情報漏洩防止により、侵害のリスクを最小化します。
- **ハイブリッド ワーカーの支援**
  プライベート アプリへの超高速アクセスを、ユーザー、本社、支店、サードパーティーにシームレスに拡張します。
- **運用の複雑さの軽減**
  ユーザー、ワークロード、OT/IT に対応するクラウドネイティブな統合 ZTNA プラットフォームを通じ、高額で複雑なポイント製品を使用することなく、安全かつ最適なアクセスを提供します。

過度に信頼し、必要以上のアクセス権を付与する城と堀のアーキテクチャーを悪用することで、攻撃者は従来のネットワーク セキュリティ アプローチを簡単に回避しています。他にも、次のような要素が悪用されています。

- **拡張性に欠け、高速でシームレスなユーザー エクスペリエンスを提供できないアーキテクチャー：**バックホールを必要とする VPN はコストと複雑さの問題だけでなく、現代のリモート ワーカーが許容できないほどの遅延を招きます。
- **大規模な攻撃対象領域を生み出す従来のファイアウォール、VPN、VDI、プライベート アプリ：**攻撃者は外部に公開された脆弱なリソースを見つけて攻撃します。
- **自由なラテラル ムーブメントを可能にする過剰なアクセス権：**VPN はユーザーを社内ネットワークに接続するため、攻撃者は機密情報に簡単にアクセスできます。
- **従来の制御を回避する侵害されたユーザーや内部脅威：**高度な攻撃者は認証情報を窃取してアイデンティティーを改ざんし、従来のリモート アクセス ツールを悪用してプライベート アプリにアクセスします。

今こそ、ユーザーを必要なアプリケーションに安全かつシームレスに接続する手段を再考するときです。同時に、ZTNA ソリューションでプライベート アプリのセキュリティも再定義する必要があります。

Zscaler Private Access™ (ZPA)

Zscaler Private Access (ZPA) は、業界初の AI 活用型 ZTNA であり、すべてのユーザーにゼロトラスト アクセスを提供してプライベート アプリケーションへの直接接続を可能にするクラウドネイティブなソリューションです。アプリを Zero Trust Exchange の背後に隠すことで攻撃対象領域を最小化し、AI を活用したユーザーとアプリ間のセグメンテーションによってラテラル ムーブメントを排除するとともに、統合されたトラフィック検査、アプリケーション保護、データ保護の機能で高度な攻撃を防ぎます。包括的なセキュリティ サービス エッジ (SSE) のフレームワーク上に構築されたレジリエントかつクラウドネイティブなサービスとして、短時間での導入を可能にし、従来の VPN やリモート アクセス ツールを置き換える形で以下を実現します。

- **攻撃対象領域の最小化：**アプリケーションはインターネット上で見えなくなり、権限のないユーザーやデバイスはこれらを検知できません。ユーザーとアプリ間にはインサイドアウト接続が使用されるため、アプリと IP が外部に公開されることはありません。
- **最小特権アクセスの適用：**アプリケーションへのアクセスは、IP アドレスではなくアイデンティティーとコンテキストに基づいて許可されます。アクセスのために、ユーザーがネットワークに接続されることはありません。
- **ラテラル ムーブメントの排除：**アプリケーションをセグメント化することでユーザーがアクセスできるアプリを制限し、ラテラル ムーブメントを抑制します。
- **フル インスペクションによるサイバー攻撃の阻止：**プライベート アプリのトラフィックはインラインで検査されるため、最も一般的な Web 攻撃から防御できます。
- **データ損失の防止：**プライベート アプリ向けの統合 DLP や高度なインシデント対応、データ分類で、重要なアプリを保護します。
- **優れたユーザー エクスペリエンスの提供：**ユーザーを直接プライベート アプリに接続することで、従来の VPN で発生していた低速でコストのかかるバックホールを排除します。同時にユーザー エクスペリエンスの問題を常に監視し、事前予防的に解決します。

2025年までに、新たに導入されるリモート アクセスの少なくとも70%がVPNサービスではなく主にZTNAで提供されるようになると予測されており、2021年末の10%未満から大幅な増加が見込まれています*

— Gartner

*Gartner、Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access、Nat Smith、Mark Wah、Christian Canales、2022年4月8日。

主なユース ケース

セキュア リモート アクセス (VPN のリプレース)
クラウド型かアプライアンスベースかを問わず、VPN ではサイバー攻撃のリスクが生じます。VPN は常に脆弱性の問題を抱えており、攻撃者によって頻繁に悪用されています。ネットワークを中心に設計されており、トラフィックのバックホールが発生するうえ、攻撃対象領域の拡大を招きます。また、ユーザーをネットワークに直接接続するため、ラテラル ムーブメントが可能になり、ランサムウェア攻撃につながります。VPN は安全性が低く、通信速度の低下を引き起こすほか、複雑な管理作業が必要です。

ZPA は、すべてのユーザーにゼロトラスト アクセスを提供し、プライベート アプリケーションへの直接接続を可能にすることで、こうした問題を解決します。アプリを Zero Trust Exchange の背後に隠すことで攻撃対象領域を最小化し、AI を活用したユーザーとアプリ間のセグメンテーションによってラテラル ムーブメントを排除するとともに、統合されたトラフィック検査、アプリケーション保護、データ保護の機能で高度な攻撃を防ぎます。
ZPA は、VPN 特有のセキュリティ リスクを生じさせることなく、160 以上のグローバルに分散したポイント オブ プレゼンス (PoP) を介してアプリケーションへの高速な直接アクセスを提供します。クラウドネイティブな性質を持つ ZPA により、IT 部門はロード バランサー、VPN コンセントレーター、その他のセキュリティ デバイスなどのインバウンド ゲートウェイ アプライアンスを排除し、コスト、複雑さ、管理オーバーヘッドを削減できます。ZPA は、すべてのアプリケーションへのゼロトラスト アクセスを提供し、Voice over IP (VoIP) アプリ、クライアント / サーバー型アプリ、さらにはビジネス パートナーがホストする (外部ネットワークの) アプリなど、コネクターを展開できない、ネットワークに接続されたアプリケーションにも対応します。

オフィス勤務およびハイブリッド ワークのユーザーによるアプリへのアクセスの保護
現在、ユーザーは自宅をはじめとするリモート環境、支店、本社など、さまざまな場所で勤務しており、従来のセキュリティの枠組みには疑問が生じています。組織では、災害時やインフラへのアクセスに問題が生じた際にも、ゼロトラスト セキュリティを損なうことなく、アプリケーションに中断なくアクセスできなくてはなりません。また、事業継続性を担保するには、コンプライアンス要件や規制基準を満たす必要があります。

ZPA Private Service Edge を使用すると、クラウドの機能をオンプレミスにも展開し、リモート ユーザーと同じセキュリティ制御を高いパフォーマンスで適用できます。Zscaler Private Service Edge と Private Cloud Controller をあわせて展開することで、ZPA は、障害検出時に完全に自動で事業継続性モードに切り替えられます。ポリシーと認証は、ZPA クラウドに到達できない場合でも適用されます。

BYOD とサードパーティー ユーザー アクセス
従来のサードパーティー アクセスは、VDI、RDP、SSH、VNC など、高額で複雑なリスクの高いソリューションを利用しており、ユーザーをネットワークに直接接続することで、組織内のシステムは信頼できないデバイスに公開されていました。

ZPA のクライアントレス アクセス機能を利用すると、サードパーティー アクセスを容易に行えるようになるとともに、コストの削減とリスクの最小化を図れます。
請負業者、ベンダー、パートナーなどのサードパーティーは、自分のデバイスから任意の Web ブラウザーを使用して、イントラネット Web サイト、内部システム、機器にクライアントなしで接続できます。サードパーティーのユーザーや管理対象外デバイスをネットワークやアプリケーションから分離し、機密データを不正なコピー / 貼り付け、印刷、アップロード / ダウンロードから保護します。ZPA と Google Chrome Enterprise Browser の統合によって、Chrome Enterprise Browser を検証し、追加のポスチャー情報を ZPA ポリシー チェックに組み込むことで、管理対象外デバイスや BYOD のセキュリティを強化します。クライアントレス アクセスにより、IT 部門は、従来の VDI の管理にコストをかけることなく、より快適かつ安全なユーザー エクスペリエンスを提供できます。M&A や事業分離にはネットワーク統合の問題が付きまといますが、ZPA はこのプロセスを数か月から数週間に短縮します。プライベート アプリへのシームレスなアクセスを提供することで、ネットワーク統合や新たな機器の導入は不要になります。

OT/IT のための特権リモート アクセス

従業員やサードパーティー ベンダーは、生産稼働時間を最大化し、機器やプロセスの障害による中断を回避するために、OT/IT の資産に定期的にアクセスする必要があります。ZPA は、現場や工場などのあらゆる場所から OT/IT 環境への安全で信頼性の高い高速アクセスを可能にします。ZPA for OT/IT では、ジャンプ ホストや従来型 VPN を使用してデバイスにクライアントをインストールすることなく、内部 RDP、SSH、VNC ターゲット システムへの完全に分離されたクライアントレス リモート デスクトップ アクセスが提供されます。

VDI のリプレース

IT 部門とセキュリティ部門は、管理対象外デバイスを制御できないため、ビジネス リスクが生じています。管理対象外デバイスでのアプリケーション アクセスをサポートするために、従来、組織は VDI を使用してきました。VDI によって、ユーザーはネットワークに直接接続され、内部アプリケーションは管理されていないエンドポイントに公開されます。さらに、VDI は高額であり、煩雑な管理を必要とするうえ、拡張性に欠けます。デジタル トランスフォーメーションが進む今、最新のアプリケーションは通常 Web ベースまたはブラウザーベースとなっており、VDI を介してデスクトップ全体をストリーミングしても、エンド ユーザーに優れたエクスペリエンスを提供することはできません。

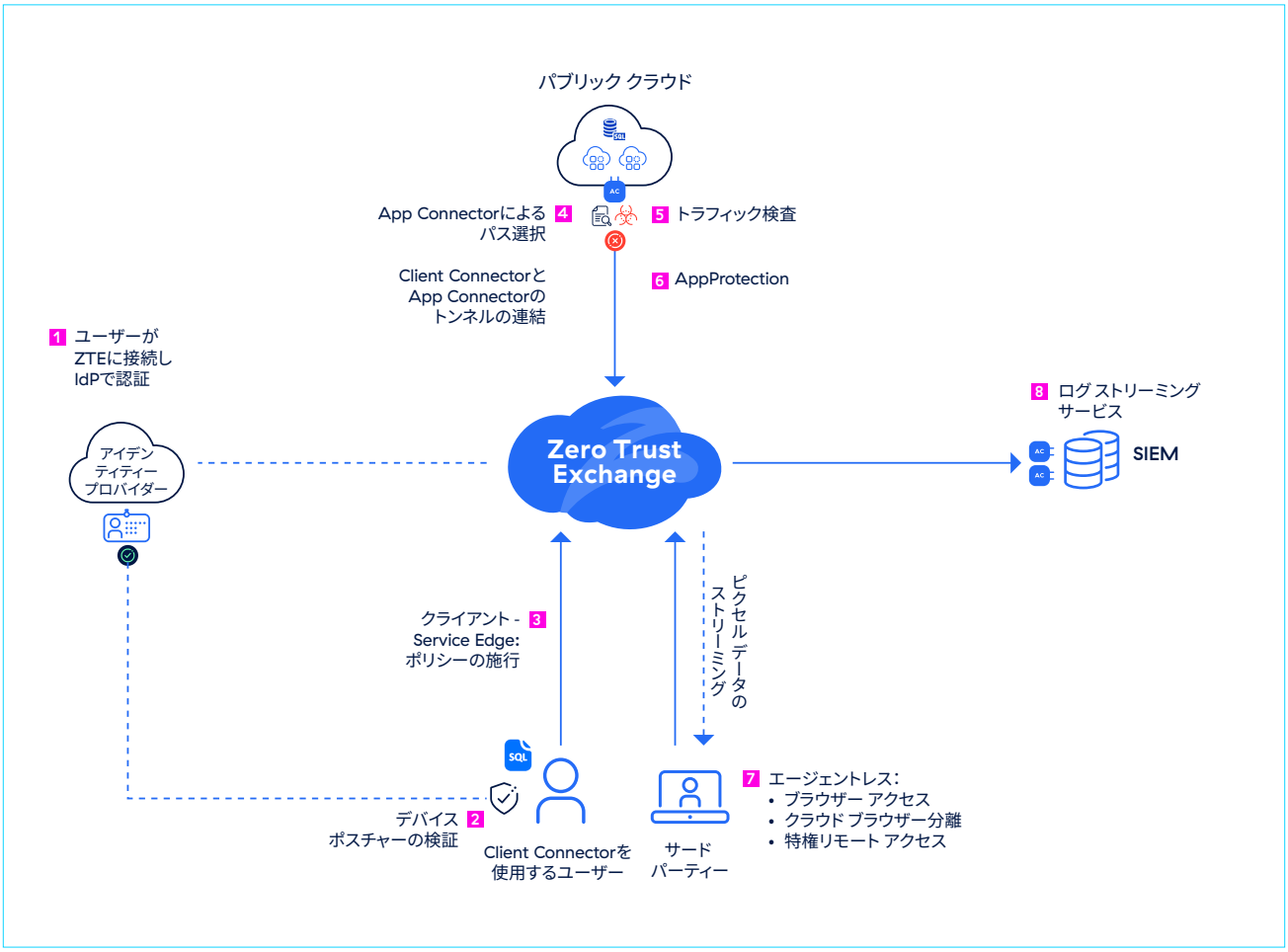
ZPA は VDI の効果的な代替ソリューションであり、エージェントレスのブラウザーベースの手法で、管理対象外デバイスからの安全なアクセスを可能にします。接続は最も近いサービス エッジによって仲介され、ユーザーはプライベート アプリに高速かつシームレスにアクセスできます。ZPA のアーキテクチャーによって、ユーザーはネットワークに接続されることなくアプリケーションに直接アクセスすることができ、プライベート アプリケーションへのアクセスが保護されます。ZPA のブラウザー アクセス機能を利用することで、ユーザーはデバイスに Zscaler Client Connector をインストールすることなく、Web ブラウザーを利用してユーザー認証やアプリケーションへのアクセスを行えます。ZPA には、ブラウザー分離機能が統合されており、実際のコンテンツではなく、ピクセル データのみをエンド ユーザー デバイスにストリーミングすることで、アプリ内のデータを安全に保ちます。管理者は分離ポリシーを作成して、分離環境内でユーザーに許可する操作を定義できます。

マイクロセグメンテーション

VPN などのリモート アクセス ソリューションは、ネットワークへのフル アクセスを許可し、IP とアプリケーションをインターネットに公開します。内部ネットワークはリモート デバイスに拡張され、設計上、インバウンド トラフィックが必要となるため、攻撃対象領域が外部に公開されます。適切なネットワーク セグメンテーションを行っていなければ、1 つのセグメントで発生した侵害によって、組織のネットワーク全体が危険にさらされる可能性があります。しかも、セグメンテーションの実装には、複雑なファイアウォール ルールが必要です。このルールは、管理が難しいうえ、しばしばアプリケーションの中断を引き起こし、VPN ユーザーによるアクセスを複雑化する可能性があります。大規模な組織では、多くの場合、高可用性、複雑なルーティング、高額なプライベート リンクが必要になります。

Zscaler の AI 活用型アプリ セグメンテーションは、ユーザーとアプリ間の詳細なセグメンテーションと、一貫性のあるポリシーを大規模に簡単に展開して脅威のラテラル ムーブメントを排除するための堅牢なソリューションを提供します。これにより、組織内のすべてのアプリケーションを検出するとともに、どのユーザーがどのアプリケーションにアクセスできるかについての視覚的なインサイトを得られます。機械学習モデルに基づいて App Segment とポリシーに関する推奨を自動的に生成し、実装を簡素化します。

ZPAの仕組み



仕組み

ユーザー (従業員、ベンダー、パートナー、請負業者) が内部アプリケーションにアクセスしようとすると、ZPA は以下の手順に従って安全な直接接続を提供します。

1 ユーザーは、Zero Trust Exchange を使用して Client Connector に接続し、アイデンティティー プロバイダー (IdP) で認証します。認証が成功すると、Public Service Edge に再接続し、このサービス エッジへの単一の永続的な TLS 接続を確立します。

2 ユーザー認証とサービス エッジへのトンネルの確立時に、Client Connector がデバイス ポスチャー チェックを含む設定をダウンロードします。

3 Zscaler のアプリが、ユーザーのトラフィックを最も近い ZPA Service Edge に転送します。ZPA Service Edge はブローカーとして機能し、ユーザーのセキュリティとアクセス ポリシーを確認します。

4 サービス エッジがデバイス上の Client Connector と App Connector からの 2 つの送信トンネルを連結します。

5 ユーザーのデバイスとアプリケーションの間に接続が確立されると、App Connector が自動的にトラフィックをインラインで検査し、侵害された可能性のあるユーザーまたはデバイスからの潜在的な脅威を検知して阻止します。

6 Zscaler の AppProtection が、包括的なレイヤー 7 の検査を通じて Web ベースおよびアイデンティティーベースの脅威からプライベート アプリケーションを保護し、全体的なセキュリティ態勢を強化します。

7 サードパーティー ユーザーの場合は、統合されたブラウザーベースのアクセスまたは管理対象外デバイスでのクライアントレス アクセス用の Zscaler Browser Isolation を使用してプライベート アプリに接続できます。

8 ログ ストリーミング サービス (LSS) によって、ユーザー アクティビティーなどのさまざまなログを SIEM にストリーミングします。

ZPA Service Edge には、Zscaler がクラウドでホストする ZPA Public Service Edge と、組織のインフラにてオンプレミスで実行する ZPA Private Service Edge があり、いずれもローカル アプリへの経路を短縮し、事業継続計画を支援します。

主要な機能

リスクベースのポリシー エンジン	強力なネイティブのポリシー エンジンを使用して、ユーザー、デバイス、コンテンツ、アプリケーションのリスク ポスチャーに基づいたアクセス ポリシーを継続的に検証し、認証されたユーザーのみがプライベート アプリにアクセスできるようにします。
統合されたクライアント アクセスとクライアントレス アクセス	組織のハイブリッド環境に応じて、最適な保護方法を選択します。クライアントベースのアクセスでは、管理対象ユーザーが企業ネットワークの外にいる場合でも、軽量の Zscaler Client Connector エージェントを通じて保護されます。クライアントレス アクセスは、管理対象外のユーザーが任意のデバイスや Web ブラウザーからスムーズにアプリにアクセスできるようにします。
ブラウザー アクセス	BYOD およびサードパーティーのユーザーが、自分のデバイスから任意の Web ブラウザーで内部アプリにシームレスかつ安全にアクセスできるようにします。クライアントは必要ありません。
オンキャンパス ZTNA	拠点内のユーザー向けに、ユーザーをオフィス内のアプリケーションに安全に接続する ZTNA を提供します。ユニバーサル ZTNA は、ユーザーやアプリケーションの場所を問わず、ユーザーに一貫したアクセスとポリシーを提供します。
事業継続性とディザスター リカバリー	お客様が管理するソリューションまたは完全なマネージド サービスとして、ZPA Private Service Edge を介して重要なプライベート アプリへのアクセス パスを作成し、ブラックスワン現象の発生時でも、ミッションクリティカルなアプリケーションにスムーズにアクセスできるようにします。
アプリの検出	特定のドメイン名と IP サブネットを使用してアプリケーションを自動的に検出してカタログ化し、プライベート アプリの資産と潜在的な攻撃対象領域に関する詳細なインサイトを取得します。
AI を活用したアプリのセグメンテーション	ZPA で自動的に配信される ML ベースのセグメンテーションの推奨事項を適用することで、合理的なアプリケーションのセグメントを迅速かつ容易に特定し、適切なアクセス ポリシーを構築します。ML ベースのセグメンテーションは、何百万もの Zscaler のお客様のシグナルと組織独自のアプリケーション アクセス パターンで継続的にトレーニングされる機械学習モデルによって強化されるため、効果的に内部の攻撃対象領域を最小化できます。
ユーザーとアプリ間のセグメンテーション	ユーザーとアプリ間のセグメンテーションを使用して、すべてのアプリケーション アクセスが最小特権ベースで許可されるようにし、ユーザーをネットワーク上に配置することなく、承認されたユーザーのみが特定のアプリケーションに安全にアクセスできるようにします。内部のファイアウォールを使用した複雑なネットワーク セグメンテーションは必要ありません。
AppProtection	脅威を明らかにするアプリケーション ペイロード全体の高性能なインラインのセキュリティ インスペクションにより、最も一般的な攻撃からプライベート アプリとインフラを保護します。OWASP Top 10 などの既知の Web セキュリティ リスクや、従来のネットワーク セキュリティ制御を回避する新たなゼロデイ脆弱性を特定してブロックします。

特権リモート アクセス	特権を持つ管理者やオペレーターが、VPN、VDI、または RDP、SSH、VNC などのリモート デスクトップ クライアントを使わずに、イントラネット Web サイト、内部システム、機器に安全に接続できるようにします。
脅威対策とデータ保護	コンテンツをすべて検査することで脅威のリスクを低減します。ユーザーとアプリ間の接続全体で、機密データを検出して管理します。
アイデンティティーとシングル サインオン (SSO)	既存のアイデンティティーおよび認証インフラと簡単に統合でき、SSO を活用して複雑さをさらに軽減します。
ネットワーク アプリへの 安全なアクセス	VoIP アプリケーションやクライアント / サーバー型アプリケーションなど、ネットワークに接続された従来型のアプリケーションへのアクセスを保護できます。
IPsec 接続	ビジネス パートナーやベンダーのネットワークでホストされている (外部ネットワーク上の) アプリケーションへのゼロトラスト アクセスを可能にします。

メリット

攻撃対象領域の最小化

脆弱な VPN を廃止してアプリをインターネットから不可視化することで、権限のないユーザーがアプリを見つけて攻撃できないようにします。ZPA は、許可されたユーザーと特定のプライベート アプリの間に 1 つのセグメントを作成し、すべてのインバウンド接続を排除し、暗号化されたマイクロトンネルを介したユーザーのデバイスへのインサイドアウト接続のみを許可します。また、管理者はアプリケーション検出機能を使用して不正なアプリケーション、サービス、ワークロードを自動的に検出してセグメント化できるため、攻撃対象領域がさらに減少します。

ラテラル ムーブメントの排除

最小特権アクセスに基づく接続により、権限のあるユーザーから指定されたアプリケーションへの 1 対 1 のアクセスが確立されます。ネットワークへのフル アクセスは付与されないため、アプリ間またはネットワーク上でのラテラル ムーブメントは不可能になります。IP アドレスをベースとしない ZPA では、複雑なネットワーク セグメンテーション、アクセス制御リスト (ACL)、ファイアウォール ポリシー、ネットワーク アドレス変換などの設定、管理が不要になります。

侵害されたユーザー、内部脅威、高度な攻撃者の阻止

統合されたインライン検査と DLP 機能によって、侵害されたユーザーやアクティブな攻撃者のリスクを最小限に抑えます。ZPA は OWASP Top 10 などの最も一般的な手法をすべてカバーし、ゼロデイ脆弱性に仮想パッチを即座に適用するカスタム シグネチャー サポートで Web 攻撃を自動的に阻止します。また、統合されたクラウド ブラウザー分離を使用して、アプリケーションへのアクセスを完全に分離し、管理対象外デバイスから機密データを保護することで、サードパーティーと BYOD のリスクを最小限に抑えます。

優れたユーザー エクスペリエンスの提供

VPN クライアントへのログインとログアウトを必要としない一貫した高速接続により、これまで以上に安全で効率的なアクセス エクスペリエンスがリモート ユーザーに提供されます。サードパーティーの請負業者、ベンダー、パートナーは、クライアントをインストールすることなく、あらゆるデバイスや Web ブラウザーからスムーズにアクセスできます。ユーザーは、既存の SSO 認証情報 (Azure AD、Okta、Ping など) を使用して登録します。さらに、管理者はプライベート アプリへのアクセスの問題、ネットワーク パスの停止、ネットワークの輻輳などによって生じるエンド ユーザーのパフォーマンスの問題をプロアクティブに検出して解決することで、ユーザーの生産性を維持できます。

アプリ、ワークロード、デバイス全体で安全なアクセスを可能にする統合プラットフォーム

プライベート アプリや OT/IT デバイスにゼロトラストを拡張し、個別のリモート アクセス ツールを簡素化して統合します。セキュリティとアクセス ポリシーを統合することで、侵害を阻止し、複雑な運用に伴う負荷を軽減します。

Zscaler Private Accessのパッケージ

	Zscaler Essentials Platform (ZS-ESS-PLATFORM)	Zscaler Private Access Platform (ZS-ZPA-PLATFORM)	Zscaler Platform (ZS-PLATFORM)
プライベート アクセス プラットフォーム サービス	✔ 登録ユーザー 20 人につき 1 人のユーザー（最小：500 人の登録ユーザー）	✔	✔
ユーザー、グループ、ポートごとのきめ細かいアクセス制御			
ログ ストリーミング サービス			
すべてのアプリの健全性の継続的な監視			
ソース IP アンカリング			
App Connector	$	システム上限まで必要に応じて	システム上限まで必要に応じて
ZPA Private Service Edge			
サードパーティアクセス	$	✔ PRA はユーザー数 500 超のお客様が対象	✔ PRA はユーザー数 500 超のお客様が対象
ブラウザーベースのアクセス			
ユーザー ポータル			
Privileged Remote Access (PRA) Standard			
デジタル エクスペリエンス モニタリング	$	✔	✔
ZDX Standard			
プライベート アプリのセキュリティ	$	$	✔ デセプションはユーザー数 500 超のお客様が対象
プライベート アプリのデータ保護			
リスク管理：デセプション			
セグメンテーション	20 のアプリ セグメント（推奨事項 10 件 /90 日、限定的な振り返り）	20 のアプリ セグメント（推奨事項 10 件 /90 日、限定的な振り返り）	20 のアプリ セグメント（推奨事項 10 件 /90 日、限定的な振り返り）
App Segments とセグメンテーションのプレビュー			
セグメンテーションのアドオン	✔ 推奨事項 100 件 /14 日 オンデマンド週次レポート、最大 30 日間のデータのダウンロードと分析 内部システムまたはサードパーティーのソース (Qualys、Tenable、ServiceNow) からのアプリのインポート	✔ 推奨事項 100 件 /14 日 オンデマンド週次レポート、最大 30 日間のデータのダウンロードと分析 内部システムまたはサードパーティーのソース (Qualys、Tenable、ServiceNow) からのアプリのインポート	✔ 推奨事項 100 件 /14 日 オンデマンド週次レポート、最大 30 日間のデータのダウンロードと分析 内部システムまたはサードパーティーのソース (Qualys、Tenable、ServiceNow) からのアプリのインポート
無制限の App Segments			
AI 活用型のセグメンテーション			
セグメンテーション インサイト			
App Segments インポート（構造化データ ファイルから）			
AppProtection のアドオン	アドオン	アドオン	アドオン
アプリケーション攻撃の可視化			
OWASP Top 10 に対する防御：SQL インジェクション、クロスサイト スクリプティング、環境およびポート スキャン			
ゼロデイ脅威対策			
高リスク ユーザーの監視			

他製品との主な違い

業界初の AI 活用型 ZTNA ソリューションである ZPA は、優れたユーザー エクスペリエンスで高度なセキュリティを実現します。

- **最小特権アクセスのためにゼロから構築：**権限のあるユーザーに、ネットワーク全体ではなく承認されたリソースのみへの接続を許可します。これは従来の VPN では不可能です。
- **見えないアプリ＝攻撃できないアプリ：**プライベート アプリ、ワークロード、デバイスをインターネットから見えなくすることで、アプリの侵害やデータ窃取、ラテラル ムーブメントを阻止します。
- **完全なインライン検査：**プライベート アプリの悪用を特定して阻止し、最も一般的な Web 攻撃を自動的に防止し、業界最高の DLP でデータを保護することで、アプリケーションを守ります。
- **セキュリティを損なうことなくグローバルな事業継続性を実現：**Zscaler クラウドにアクセスできなくなった場合でも、中断の影響を最小限に抑え、ゼロトラスト アクセスを適用して厳格なコンプライアンス要件を満たします。
- **クライアントレス アクセス：**統合 DLP を使用して、サードパーティーに対してブラウザーベースのアクセスを提供します。
- **AI を活用したセグメンテーションでラテラル ムーブメントを排除：**機械学習を使用して、ユーザーとアプリ間の詳細なセグメンテーション、アクセスの可視化、ポリシーの微調整を行い、攻撃対象領域を最小化し、脅威のラテラル ムーブメントを防ぎます。
- **グローバルなエッジの展開：**世界 160 か所以上のクラウド エッジとゼロトラストを本社にまで拡張するローカルのサービス エッジで、優れたセキュリティとユーザー エクスペリエンスを実現します。
- **クラウドネイティブな基盤：**高額なオンプレミスのアプライアンスや複雑なインフラを必要としないクラウド型プラットフォームは、ビジネスの成長に合わせて拡張できます。
- **ユーザー、ワークロード、デバイス向けの統合型 ZTNA プラットフォーム：**業界で最も包括的な ZTNA プラットフォームを使用して、プライベート アプリやサービス、OT デバイスに安全に接続します。
- **拡張可能なゼロトラスト プラットフォームの一部：**完全な SSE フレームワーク上に構築された Zero Trust Exchange でビジネスを保護および強化します。

**Gartner、Magic Quadrant for Security Service Edge、Charlie Winckless、Thomas Lintemuth、Dale Koeppen、2024 年 4 月 15 日

Gartner は、Gartner リサーチの発行物に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。また、最高のレーティング又はその他の評価を得たベンダーのみを選択するようにテクノロジー ユーザーに助言するものではありません。Gartner・リサーチの発行物は、Gartner・リサーチの見解を表したものであり、事実を表現したものではありません。Gartner は、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の責任を負うものではありません。

基本的なコンポーネント

Zscaler Client Connector
ユーザーのノートパソコンやモバイル デバイス上で動作する軽量アプリケーションで、ユーザー トラフィックを最も近い Zscaler Service Edge に自動的に転送することで、セキュリティとアクセス ポリシーがすべてのデバイス、場所、アプリケーションに適用されるようにします。

Zscaler Clientless Access
ユーザーは統合されたブラウザーベースのアクセス (Web、RDP、SSH、VNC)、または管理対象外デバイスでのクライアントレス アクセス用の Zscaler Browser Isolation を使用してアプリ、ワークロード、OT デバイスに安全に接続できます。

ZPA App Connector
軽量の仮想マシンで、データ センターまたはパブリック クラウドに展開されたプライベート アプリの前に配置されます。アプリをインターネットに公開しないインサイドアウト接続で、承認されたユーザーと指定のアプリとの間のセキュアな接続を仲介します。

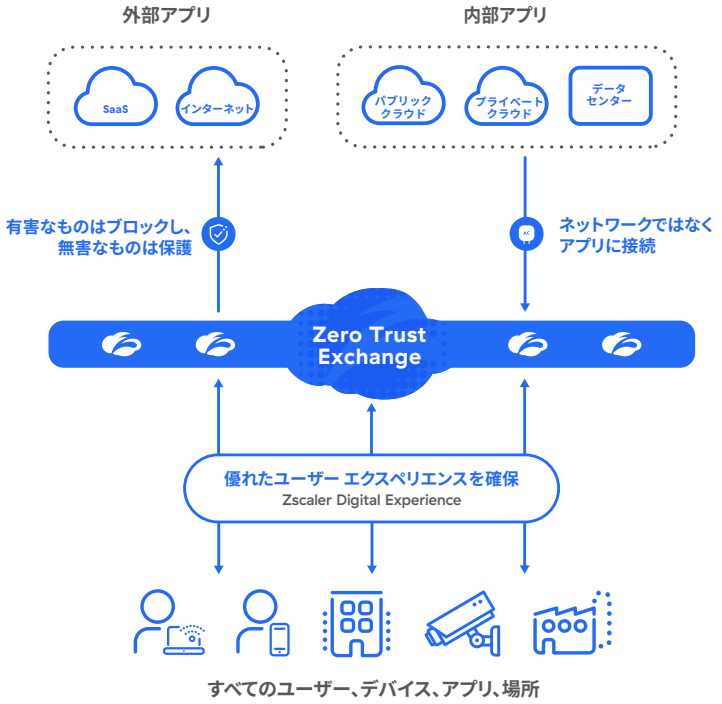
ZPA Service Edges
セキュリティとアクセス ポリシーを施行し、許可されたユーザー (Client Connector およびブラウザー アクセス経由) と特定のプライベート アプリ (App Connectors 経由) 間にインサイドアウト接続を確立します。Public Service Edge は世界 160 か所以上のポイント オブ プレゼンス (PoP) でホストされており、大規模なグローバル組織の何百万人ものユーザーを同時に処理しています。Zscaler が管理する Private Service Edge はオンサイトでホストすることもできるため、オンプレミス ユーザーはローカル ネットワークを離れることなく、オンプレミス アプリケーションに最短経路でアクセスできます。また、ブラック スワン現象の発生時でもミッションクリティカルなアプリケーションへの中断のないアクセスにより、事業継続性を確保します。

包括的な Zero Trust Exchange の一部である ZPA

Zscaler Zero Trust Exchange は、完全なセキュリティ サービス エッジ (SSE) を強化するクラウド ネイティブ プラットフォームで、ユーザー、ワークロード、デバイスを企業ネットワーク上に配置せずに接続します。これにより、ネットワークを拡張して攻撃対象領域を拡大させ、脅威のラテラル ムーブメントのリスクを高め、データ流出を防止できない境界ベースのセキュリティ ソリューションに関連するセキュリティ リスクと複雑さが軽減されます。

ユーザー、ワークロード、OT/ITにゼロトラストを提供するZscaler

わずか数週間で導入し、サイバー保護とユーザー エクスペリエンスを強化



技術仕様

Zscaler のコンポーネント	サポートするプラットフォームとシステム	
Client Connector	iOS 9 以降 Android 5 以降 Windows 7 以降	macOSX 10.10 以降 CentOS 8 Ubuntu 20.04
クライアントレス アクセス	最新の Web ブラウザー： (HTML5 対応)	Chrome Edge Firefox
App Connector	AWS CentOS、Oracle、Red Hat Microsoft Azure	Microsoft Hyper-V VMware vCenter または vSphere Hypervisor Docker ホスト

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 SSE 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.com/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.com/jp