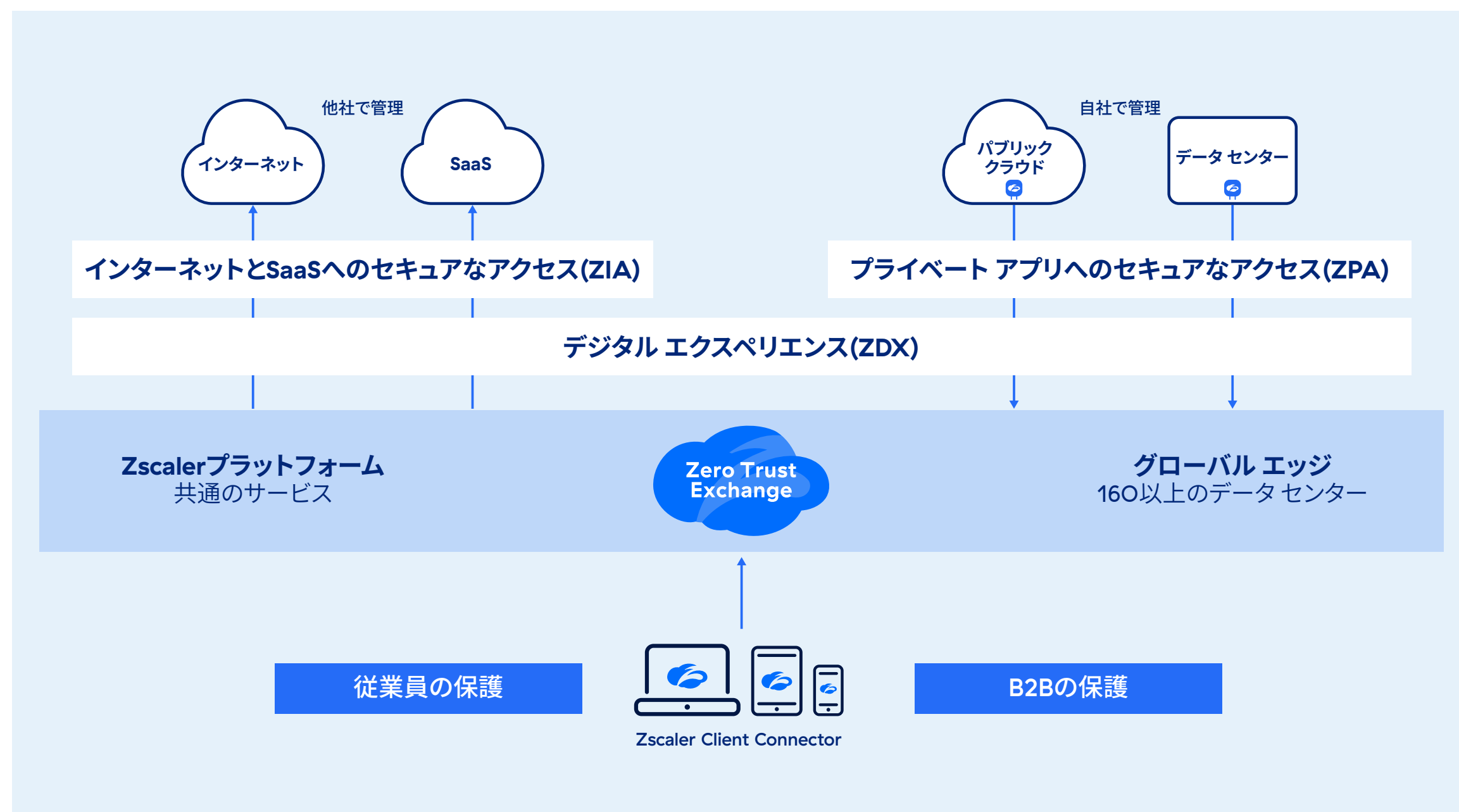


Zscaler Client Connector



すべての宛先への高速で安全なアクセスを
あらゆる場所やデバイスから実現

データ シート

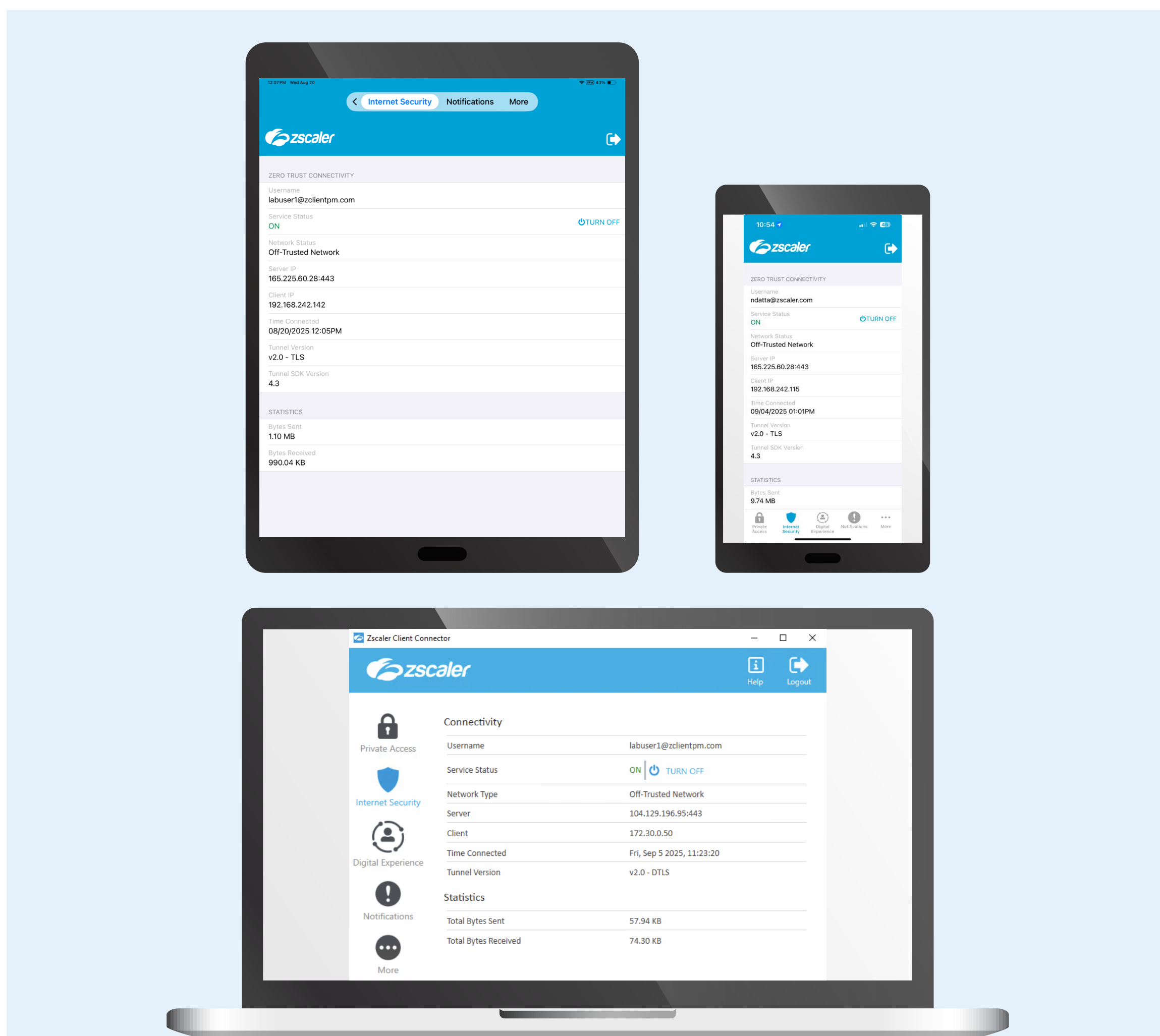


働き方が大きく変わった今、現代の従業員はさまざまな場所で作業し、多様なデバイスを介してクラウド アプリや世界中のリソースにアクセスしています。この新しいハイブリッド ワーク環境では、IT リソースへの高速かつシームレスなアクセスが不可欠ですが、同時にデータの安全性も確保する必要があります。成功を目指す組織には、生産性の高いユーザー エクスペリエンスの維持とグローバルに分散したエンドポイントの保護の両立が求められます。この課題に対応するために、多くの IT 部門が Zscaler とそのエンドポイント エージェントである Client Connector を活用しています。

以前は、ユーザーもアプリもオフィス内で管理されていたため、ネットワーク中心のセキュリティや接続ソリューションを使うのが一般的でした。しかし現在、オフィス外の従業員が IT 部門の制御下でないネットワークを使用してオフィス外のアプリにアクセスしています。このトラフィックをデータセンターにバックホールして保護しようとすると、遅延が発生し、生産性が損なわれます。さらに、バックホールは、ユーザーを企業ネットワークに接続するため、ユーザーが過剰な権限を悪用したり、ネットワーク上の他のリソース間を水平移動したりするリスクを生み出します。また、攻撃対象領域を拡大し、[他のセキュリティ上の問題を引き起こす要因](#)にもなります。

これらの課題を解決するのがゼロトラスト アーキテクチャーです。Zscaler は、これを世界最大のクラウド セキュリティ プラットフォームである Zero Trust Exchange 経由でサービスとして提供しています。Zero Trust Exchange はインテリジェントな交換機として機能し、ネットワークではなくビジネス ポリシーに基づく Any-to-Any のゼロトラスト通信を提供します。そして、ユーザーの IP アドレスではなくコンテキストベースで IT リソースへの最小特権アクセスを確保します。これは、世界 160 か所以上の拠点のエッジで実行されます。そのため、IT 部門はユーザーの場所やデバイスによらず優れたデジタル エクスペリエンスを確保しながら、脅威やデータ漏洩を阻止できます。

Zscaler Client Connector は、Any-to-Any のゼロトラスト通信を実現するうえで重要な役割を果たしています。この軽量で多機能なエンドポイント エージェントは、ユーザーがどこにいても、インターネットや IT リソースにスムーズかつ最小限の権限でアクセスできるようにします。また、セキュリティと接続を強化する豊富な機能を備え、従来のポイント製品や専用エージェントの必要性を排除します。



Zscaler Client Connectorのメリット

Client Connector のメリットは、以下の 7 つのカテゴリに分類できます。詳細については、このデータ シートの末尾の表をご参照ください。



あらゆる宛先へのゼロトラスト通信

組織は異なる宛先へのアクセスを保護するために、専用のソリューションやエージェントを使い分ける必要がなくなります。Client Connector は、Web、SaaS、プライベートアプリなど、あらゆる宛先への最小特権のゼロトラスト アクセスを提供します。この仕組みは、Gartner が提唱する **SSE** と **SASE** のビジョンとも整合しており、複数のエージェントによるデバイスのパフォーマンス低下を回避することができます。



あらゆるデバイスに対応するゼロトラスト通信

宛先へのアクセスだけでなく、あらゆるデバイスでのアクセスも保護する必要があります。これは、従業員がデスクトップやノートパソコン、タブレット、スマートフォンなどの多様なデバイスと複数のオペレーティング システムを使用しているためです。Client Connector はあらゆるデバイスを保護し、従業員の安全性と生産性を確保します。



コンテキスト対応のインテリジェントなセキュリティ

IT リソースへのアクセスを管理するうえで、アイデンティティだけでは不十分です (アイデンティティは盗まれる場合があり、正規のユーザーであっても不用意に組織に損害を与える可能性があります)。そのため、コンテキストとリスクに基づいてアクセスを管理する必要があります。Client Connector はデバイスのセキュリティ態勢に関するインサイトを提供し、それを元に適応性の高いインテリジェントなアクセス制御を可能にします。



エンドユーザー デバイスのデータ保護

あらゆる漏洩経路を保護する Zscaler の包括的なデータ セキュリティ ソリューションの一部として、Client Connector はエンドポイン

ト DLP を提供します。これにより、別途管理が必要なポイント製品を必要とすることなくリムーバブル ストレージ、ネットワーク共有、パーソナル クラウド ストレージの同期、エンドポイントでの印刷を保護します。



環境内に潜む脅威の検出

ステルス性の高い攻撃者は組織の環境内に潜み、悪意のある行為のために偵察を行うことがあります。Client Connector は、アプリのブックマーク、Cookie、セッション、パスワードなどを模倣したリアルなデコイで攻撃者をおびき寄せるデセプション テクノロジーを採用しています。デコイにアクセスされると、精度の高いアラートが生成されます。



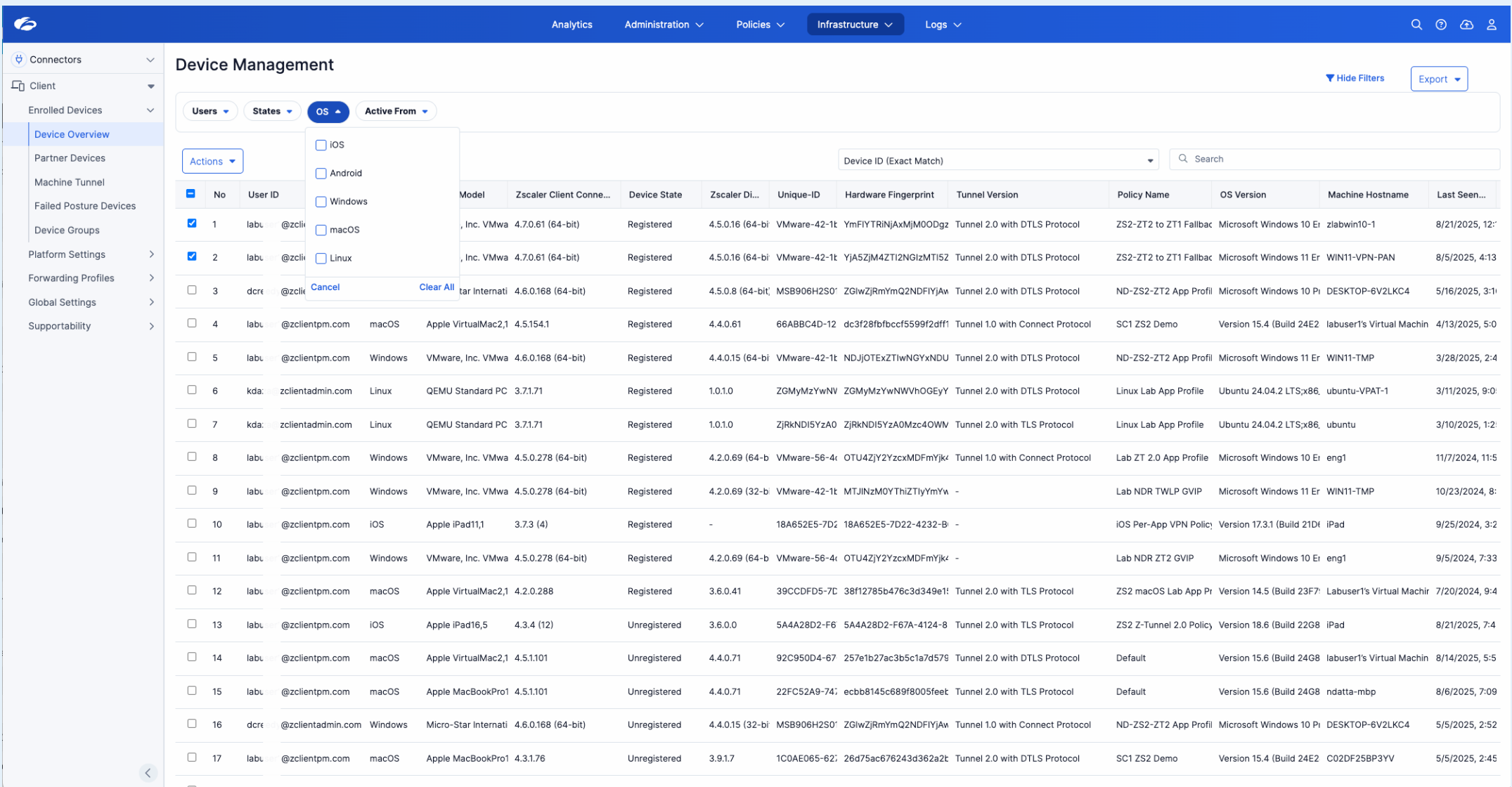
優れたユーザー エクスペリエンスと生産性

トラフィックをバックホールさせる従来のツールとは異なり、Client Connector はトラフィックを最短経路で宛先へ誘導します。また、Zscaler Digital Experience (ZDX) にデバイスのイベントや状態の可視性を提供し、管理者がユーザー接続の全体像を把握できるようにします。これにより、ユーザー エクスペリエンスの問題解決が加速し、ユーザーと管理者の業務効率が向上します。



クラウドベースの効率的な管理

Zscaler の統合 UI である Experience Center で Client Connector を管理することで、運用効率が飛躍的に向上します。Experience Center により、転送とセキュリティ、アップグレードとロールバックを管理するための継続的なポリシーとライフサイクル管理が可能になります。また、統合されたダッシュボードやレポート機能も提供されます。管理者は、Zscaler プラットフォーム全体に対応する単一の API である OneAPI を介してタスクを自動化することもできます。





ZSCALER CLIENT CONNECTOR モジュール

Zscaler Internet Access	ZIA は、インターネットへのアクセスを保護しながら、きめ細かな脅威対策機能を施行する Zscaler のソリューションです。また、セキュア Web ゲートウェイ (SWG) の Magic Quadrant で 10 年間リーダーと評価されています。
Zscaler Private Access	Zscaler Private Access は、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とリスクを軽減するコンテキスト対応型のポリシーにより、プライベート アプリケーションにアクセスするすべてのユーザーにシームレスなゼロトラスト通信を提供します。
Zscaler Digital Experience	Zscaler Digital Experience は、ユーザー エクスペリエンスをエンドツーエンドで可視化するとともに、パフォーマンスの問題をすばやく検出してトラブルシューティングや解決を効率化します。この仕組みにより、管理者とエンドユーザー双方の生産性が向上します。
Zscaler Endpoint DLP	Zscaler Endpoint Data Loss Prevention (DLP) は、Zscaler Data Security ソリューションの一部であり、データ セキュリティのコストと複雑さを軽減しながら、デバイス データに必要な可視性と制御を提供します。
Zscaler Deception	Zscaler Deception は、IT 環境全体にリアルなデコイ資産を展開して隠れた攻撃者を誘導し、精度の高いアラートを生成することで、脅威をより迅速に検出、阻止できるようにします。

CLIENT CONNECTOR の機能と詳細

包括的なオペレーティング システムのサポート	<p>デスクトップとシン クライアント：</p> <ul style="list-style-type: none">• x64 および ARM64 上の Microsoft Windows 11、Windows 10• Intel および Apple Silicon 上の Apple macOS Tahoe (26)、Sequoia (15)、Sonoma (14)• Linux デスクトップ (RHEL、CentOS、Fedora、Ubuntu、Debian、openSUSE、Arch Linux、Maya OS)• ChromeOS 上の Google Android• eLux および IGEL OS <p>モバイル：</p> <ul style="list-style-type: none">• Apple iOS 17、18、26• Google Android 10、11、12、13、14、15、16
シングル ユーザーとマルチユーザーの VDI のサポート	<ul style="list-style-type: none">• Windows 365 Cloud PC、Azure Virtual Desktop• AWS Workspace• Citrix の仮想アプリおよびデスクトップ• Omnissa Horizon および Horizon Cloud <p>VDI 用 Client Connector でサポートされるマルチセッション VDI 環境</p>



幅広いトラフィックのサポート	<ul style="list-style-type: none">すべてのポートとプロトコル (Z-Tunnel 2.0)Web トラフィックのみ (Z-Tunnel 1.0)クライアント間のトラフィックサーバーとクライアント間のトラフィック
トンネル輸送	DTLS 1.2、TLS 1.2、HTTP CONNECT
暗号化	<ul style="list-style-type: none">相互 TLS 認証制御チャネル接続のための SSL ピンニングFIPS140 準拠
最適な DC 選択	自動選択 ポリシーベース：地理的位置情報、優先 DC、レイテンシー、トラフィックの宛先
レイヤー 3 プロトコルのサポート	IPv4 および IPv6
柔軟な接続方法	<ul style="list-style-type: none">ユーザーが開始オンデマンドマシントンネルを使用したログイン前のサポート常時オンiOS でのエンタープライズ VPN プロファイルまたはアプリごとの VPN プロファイルのサポートiOS でのデュアルトンネル サポート (エンタープライズ VPN とアプリごとの VPN プロファイル) のサポートAndroid の仕事用プロファイルのサポート
展開とライフサイクルのオプション	<ul style="list-style-type: none">Intune、Workspace ONE、JAMF Pro、MobileIron、MaaS360、SCCM などの MDM や UEM、その他のソリューションを使用した展開Active Directory (AD) で Microsoft GPO を使用した展開Zscaler からの直接ダウンロードを使用した手動展開クラウド管理によるリリース更新とロールバックのサポートSSL インспекション用の信頼されたルート CA 証明書のシームレスな配布API ベースのポリシーとデバイス管理
業界標準のユーザー プロビジョニング	<ul style="list-style-type: none">System for Cross-Domain Identity Management (SCIM)SAML 2.0 ベースのジャストインタイム プロビジョニング緊急ユーザー アクセスのためのジャストインタイム プロビジョニングマシンキーベースのデバイス自動プロビジョニングデバイストークンベースのユーザー / デバイスの自動プロビジョニングSCEP ベースの証明書プロビジョニング *Microsoft AD または LDAP ディレクトリー サーバーの同期ホスト ユーザー DB へのユーザーの手動追加や一括アップロード



サポートされている認証オプション	<ul style="list-style-type: none">• SAML 2.0• Kerberos• 証明書とスマート カード• 多要素認証 (MFA)• FIDO2 準拠のハードウェア トークンのサポート• ログイン前のサポートのためのマシンキーベースのデバイス認証• トークンベースのユーザー / デバイス認証• パスワード• ステップアップの認証サポート• ブラウザーベースの認証
シングル サインオン	<ul style="list-style-type: none">• Windows 向けのシームレスな SSO• Kerberos SSO• macOS と iOS 向けの Microsoft Enterprise SSO プラグイン• Apple Enterprise SSO フレームワークのサポート• OKTA SSO 拡張機能のサポート
ポリシーベースのユーザー制限	<ul style="list-style-type: none">• 改ざん防止のサポート• ユーザーのログアウト、クライアントの終了、サービス停止の制限を制御するための OTP とパスワードの制限
サポートされている言語	英語、フランス語
エンドユーザー通知	<p>デスクトップと OS 通知のサポート：</p> <ul style="list-style-type: none">• 利用規約の通知• サービス ステータス• ソフトウェアのアップデート• 認証と定期的な再認証• インラインのデータ セキュリティ イベント• エンドポイント DLP 通知とワークフロー• インターネットとプライベート アプリのアクセス ポリシー イベント通知• 高度な脅威対策• Zscaler Zero Trust Firewall、IPS、DNS のセキュリティ通知• Zscaler Digital Experience Co-pilot の通知サポート
組み込みのトラブルシューティングのツール	<ul style="list-style-type: none">• 暗号化されたログの自動取得• 手動でのログ エクスポート• 自動および手動のパケット キャプチャーのサポート• サービスの監視と管理の自動化のサポート

広範囲のセキュリティ態勢のサポート	<ul style="list-style-type: none">ファイル パスレジストリー キーと値証明書の信頼CRL 付きクライアント証明書サーバー検証済みのクライアント証明書ファイアウォールのステータスフル ディスクの暗号化AD ドメイン参加ステータスEntra ドメイン参加ステータスプロセス チェックCarbon Black によるリアルタイム検出クライアント出力 IPMicrosoft Defender によるリアルタイム検出	<ul style="list-style-type: none">CrowdStrike によるリアルタイム検出CrowdStrike ZTA デバイス OS スコアCrowdStrike ZTA センサー スコアウイルス対策ソフトの検出OS バージョンの確認JAMF エージェントの検出JAMF リスク レベル不正な変更所有権の変数Zscaler Client Connector リリースバージョン
その他の機能	<ul style="list-style-type: none">ディザスター リカバリーと事業継続性のサポートネットワーク ロックダウンのオプションを備えた組み込みのキャプティブポータル処理ローカル LAN のブロック機能を備えた Client Connector エンドポイントのファイアウォール管理デバイス隔離のサポート信頼されたネットワークの検出と切り替えの自動化No Default Route (NDR) 環境のサポート	

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™ プラットフォームは、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](https://twitter.com/zscaler) をフォローしてください。

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ および zscaler.com/jp/legal/trademarks に記載されたその他の商標は、米国および/または各国の Zscaler, Inc. における (i) 登録商標またはサービス マーク、または (ii) 商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。



Zero Trust
Everywhere