インターネット、アプリ、データへの安全で信頼性に優れたシームレスなアクセスの提供

データシート

ハイブリッド ワーカーの保護における課題

現代の組織は、急速に進化するデジタル環境の複雑さに対処すると同時に、生産性、俊敏性、セキュリティの間で適切なバランスを確保することを求められており、そのなかで大きな課題に直面しています。

- 従来のファイアウォールやVPNは重大な死角を生み出し、システムは高度なサイバー脅威のリスクにさらされます。
- サイロ化したツールや複数のポイント製品は、運用の複雑化、予算やリソースの浪費を招くうえ、拡張性を確保できません。
- 予期せぬ障害が発生すれば、分散したインフラを活用しながらハイブリッド ワーク環境の事業継続性を確保することができません。

サイバーセキュリティのニーズやコスト圧力が高まるなか、オペレーショナル レジリエンス、リスク管理、従業員の生産性の間でのバランスについて、多くのリーダーたちが頭を悩ませています。ハイブリッド ワーカーはリソースへのシームレスで信頼性の高いアクセスを期待する一方、従来のアーキテクチャーではレイテンシーが発生し、ユーザー エクスペリエンスが低下します。企業が競争力を維持するには、データ保護のための可視性を強化し、運用を効率化するとともに、俊敏性、拡張性、ユーザー エクスペリエンスを重視する形でアーキテクチャーを進化させる必要があります。

あらゆる場所のユーザーにインターネット、SaaS、プライベート アプリへの安全で信頼性に優れた高パフォーマンスなアクセスを提供

Zscalerは、世界最大のクラウド セキュリティ プラットフォームを通じ、クラウドネイティブのセキュリティ アプローチを提供しています。コンテキスト認識型のセキュリティ ポリシーの施行、ラテラル ムーブメントの阻止、リアルタイムでの予防的な脅威検出により、ビジネス リスクを最小化し、重要なリソースを保護します。

ZscalerはAI活用型の包括的なソリューションを提供し、インターネット、SaaSアプリケーション、プライベート リソースへの安全で信頼性に優れた高パフォーマンスなアクセスを実現します。場所やデバイスを問わず、従業員、請負業者、サードパーティーのあらゆるユーザーに対応します。

このソリューションは、ポイント製品を一元的なプラットフォームに統合することで、高額なハードウェアを排除し、運用の複雑さを軽減します。また、高度なAI機能により、リアルタイムの可視性、根本原因分析、プロアクティブなポリシー施行を可能にし、ユーザーのデジタル エクスペリエンスを最適化します。

主なメリット

ビジネス リスクの最小化

ゼロトラストの原則とAIセキュリティ ソリューションの導入によって、攻撃対象領域を削減し、不正侵入やラテラル ムーブメント、データの流出を阻止します。

- クラウドネイティブのプロキシ アーキテクチャーにより、世界最大のセキュリティ クラウドを基盤とするAI活用型のセキュリティ制御を適用しながら、あらゆるポートとプロトコルにわたり完全な検査を提供し、既知の脅威を阻止します。
- インラインのクラウド サンドボックスと不審なWebトラフィックを隔離するZero Trust Browserにより、未知の脅威や検出しにくい脅威を阻止します。
- 悪用可能なハードウェアを排除し、アプリケーションをインターネットから不可視化するとともに、AIを活用したユーザーとアプリ間のきめ細かなセグメンテーションを活用することで、攻撃対象領域を削減します。

エンドユーザーの生産性向上

可視性と制御を通じてデジタル エクスペリエンスを最適化することで、あらゆる場所の従業員やサードパーティーが高速かつ安全でシームレスな形でアプリにアクセスできるようになります。

- Zscalerは全世界160か所のデータセンターを通じて、ポリシーの施行とアクセスの仲介をエッジで処理し、バックホールを必要としません。これにより、レイテンシーを排除し、VPNや従来のファイアウォールよりも優れたパフォーマンスを発揮します。
- すべての場所、ユーザー、デバイス、アプリケーションにわたるエンドツーエンドの可視性を実現し、パフォーマンスを最適化するとともに、コラボレーションを促進します。ネットワーク パフォーマンスに関するインサイト(ISPやラストマイル接続のベンチマーク、Wi-Fiの傾向の監視、ゼロトラスト環境)に加え、アプリケーションの応答時間やCPU、メモリー、ディスク使用量などのデバイス正常性メトリクスも活用します。
- 統合されたインサイトを活用するとともに、AIによって数分で根本原因を特定することで、ネットワーク運用、サポート、セキュリティ部門が場所を問わずシームレスなユーザー エクスペリエンスを提供できるようにします。
- 事業継続性機能により、ブラックアウトやブラウンアウト、まれなブラック スワン障害から組織を保護しながら、ユーザーの生産性を維持し、レジリエンスを確保します。

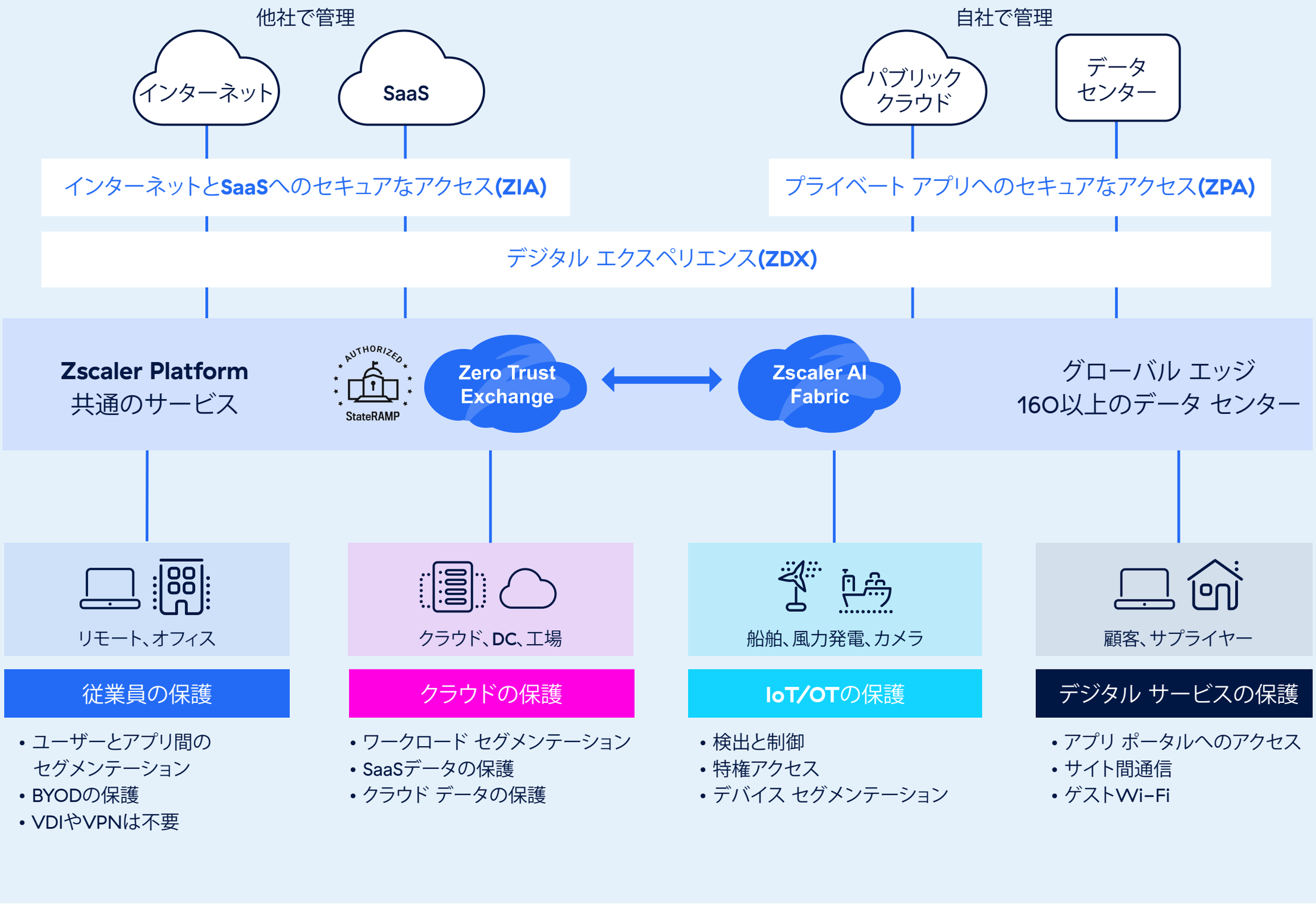
シンプルな運用管理とコスト削減

VPNやファイアウォールといった従来のテクノロジーに付きまとう設備投資や管理負荷を排除し、高速かつ安全なクラウドへの直接接続によってネットワークを簡素化します。また、高度なAI機能により、リアルタイムの可視性、根本原因分析、プロアクティブなポリシー施行を可能にし、ユーザーのデジタル エクスペリエンスを最適化します。

- 単一のアクセス ポリシー セットを構築して、Zscalerの分散型クラウドネイティブ インフラを通じて一元管理し、グローバルに施行します。
- サイロ化されたポイント製品を排除し、ハードウェアと運用のコストを削減します。
- ユーザーフレンドリーな統合コンソールと管理を容易にする生成AIコパイロットを備えた単一の画面を通じて、一元的な可視性を提供します。

ゼロトラスト アーキテクチャーによる組織の強化

ZscalerのZero Trust Exchangeは、ユーザー、デバイス、ワークロード、アプリケーションに包括的なセキュリティを提供する世界最大のセキュリティ クラウド プラットフォームです。このプラットフォームは、最小特権アクセスの原則に基づいて構築されており、ユーザーのアイデンティティーと、場所やデバイス、アプリケーション、コンテンツなどのコンテキストに基づいて信頼を確立し、ユーザーとアプリ間、異なるアプリ間、異なるマシン間の安全で直接的な接続を実現します。



ユース ケース

インターネットおよびSaaSへのアクセスの保護とセキュアWebゲートウェイ(SWG)のリプレース

従来のSWGアプライアンスでは、高速かつスケーラブルでリモート対応のソリューションを必要とする現代の分散した従業員のニーズに対応できません。業界をリードするAI活用型のクラウドネイティブ セキュアWebゲートウェイを活用することで、接続元の場所を問わずインターネットやSaaSへのアクセスを保護します。パフォーマンスを妨げることなく、あらゆるポートやプロトコル、暗号化されたトラフィックをインラインで検査し、高度な脅威をブロックします。AIを活用した脅威インテリジェンスは、インライン サンドボックスと機械学習を活用し、既知と未知の脅威をリアルタイムで阻止します。

アプリケーションへの安全なアクセスの提供とVPNのリプレース

VPNにはいくつかの弱点があり、重大なセキュリティ リスクをもたらします。たとえば、暗黙の信頼が付与され、攻撃者がネットワークへのアクセスに成功した場合にラテラル ムーブメントのリスクが高まることが挙げられます。また、VPNは、組織への侵入経路を攻撃者から検出可能なものにしてしまいます。パブリックIPアドレスによって、VPNの存在と攻撃者に簡単に悪用され得る脆弱性が広く公開されることになります。Zscalerでは、特定のユーザーを許可されたアプリに直接接続でき、アプリケーションをインターネットに公開することがありません。Zscaler Private Accessはゼロトラスト ネットワーク アクセス(ZTNA)を提供し、従来のVPNの不便さ、リスク、非効率性を伴うことなく、プライベート アプリケーションへの安全で高速かつスケーラブルなアクセスを実現します。

サードパーティー アプリケーションへのアクセスの保護とVDIのリプレース

ビジネス パートナーやベンダーにアクセスを提供する方法として、従来のアプローチではVPNやVDIなどの旧式のソリューションが利用されています。VPNは過剰なアクセス権限を付与してリスクの増大を招くことが多く、VDIは非常に高額なうえ管理が難しいという問題を抱えています。Zscalerを利用することで、サードパーティーのベンダー、請負業者、パートナーに対して、セキュリティを損なうことなく、管理対象デバイスまたは管理対象外デバイスから特定のアプリケーションおよびリソースへの安全かつ限定的なアクセスを提供することが可能です。

安全な合併と買収(M&A)の実現

M&A活動では、多くの場合インフラの相違によって組織間でのIT資産の統合が課題となります。インフラの一部には旧式のソリューションが含まれ、アクセスの統合と組織間での安全な接続の確立までに長い時間を要することがあります。また、従来の境界ベースのツールでは、M&A中に急速に変化するビジネス ニーズにも動的に対応できません。一方Zscalerを利用した場合、M&A活動中にセキュリティ リスクを招くことなく、新たに買収した企業のユーザー、システム、アプリケーション間のシームレスで安全な接続を提供し、生産性向上までの時間を短縮することが可能です。

高パフォーマンスのユーザー エクスペリエンスの確保

ハイブリッド ワークには、アプリケーションを信頼性の高い形で利用できることが不可欠であり、接続やインフラの問題は生産性の低下を招きます。ネットワーク運用部門は、ISP、Wi-Fi、ホームオフィス環境のネットワーク パフォーマンスを把握できないことが多く、これが問題の特定と解決を難しくしています。Zscalerはこうした制約を取り除きます。アプリケーションのパフォーマンスを最大化し、摩擦を最小限に抑えることで、常に高速かつシームレスなデジタル エクスペリエンスをユーザーに提供できます。

ソリューションの機能

Zscaler Internet Access:インターネットとSaaSへの安全なアクセスを確保

クラウドならではのスピードと規模を活かした包括的なゼロトラスト脅威対策で、進化する攻撃からユーザーを保護します。また、TLS/SSLで暗号化されたトラフィックをインラインで100%検査し、高度な脅威の侵入やデータの流出を防ぎます。Zero Trust Firewall、Cloud Sandbox、Zero Trust Browserが業界をリードする保護機能を提供し、AIを活用した脅威検出を基盤とする統合プラットフォームを通じて他のポイント ソリューションをリプレースします。

- **ランサムウェアやその他の脅威からの保護:**攻撃対象領域の最小化、不正侵入の阻止、ラテラル ムーブメントの排除、データ流出の防止をすべて実現します。
- **コストと複雑さの軽減:**高速で安全なクラウドへの直接接続でネットワークが簡素化されるため、エッジや拠点のファイアウォールが不要になります。
- **データの保護:**偶発的な外部公開や窃取、二重脅迫型ランサムウェアによる、ユーザー、SaaSアプリ、パブリック クラウドからのデータ流出を防ぎます。
- **ハイブリッド ワークの保護:**従業員、顧客、サードパーティーがWebアプリとクラウド サービスに場所やデバイスを問わず安全にアクセスできるようにし、優れたデジタル エクスペリエンスを提供します。

「Zscalerは、攻撃対象領域を抑えた最新のアーキテクチャーを提供しています。今後の変化に対応する柔軟性を確保しながら、ネットワーク環境をシンプルにしてくれるプラットフォームです。このシンプルさが、変化への迅速な対応を可能にしています」
—AdventHealth、最高情報セキュリティ責任者、Ryan Winn氏

Zscaler Private Access:プライベート アプリへの安全なアクセスを確保

世界で最も展開されているゼロトラスト ネットワーク アクセス(ZTNA)ソリューションにより、高速で信頼性の高い接続を実現します。

- **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。
- **プライベート アプリの侵害防止:**プライベート アプリのトラフィックの完全なインライン検査と情報漏洩防止により、アプリの侵害と情報漏洩のリスクを最小限に抑えます。
- **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、リモート 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。
- **コストと複雑さの軽減:**ユーザー、ワークロード、IoT/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。
- **特権リモート アクセスの実装:**エンド ユーザーの最新ブラウザーからサーバー、ジャンプ ホストおよび要塞ホスト、デスクトップへの接続を保護します。リモート デスクトップ プロトコル(RDP)、セキュア シェル(SSH)、仮想ネットワーク コンピューティング(VNC)を使用した接続に対応し、Zscaler Client Connectorやブラウザー プラグインのインストールは必要ありません。

「ほぼ100%リモート ワークの従業員に対し、ZPAはシームレスなエクスペリエンスと格段に優れた保護を提供し、サポートの負担を軽減してくれます」
—Mercury Financial、CISO、Anthony Cunha氏

Zscaler Digital Experience:
ユーザー エクスペリエンスのプロアクティブな監視と最適化

デバイスからISP、クラウド プロキシ、アプリ、およびその逆方向の通信において、あらゆる場所のユーザーに優れたパフォーマンスを提供できるようにします。VPNやファイアウォール、サイロ化した管理ツールは必要ありません。エンド ユーザーの視点からパフォーマンスを最適化し、アプリ、ネットワーク、デバイスの問題を迅速に修正します。

- **エンドツーエンドの可視化：**ユーザーのデバイスから複数のネットワークを介してアプリやサービス(組織の管理下にないものを含む)に至るまでのメトリクスを収集します。
- **ヘルプ デスクのチケット削減：**AIを活用した根本原因分析により、ユーザーに影響を与える前にITの問題を検出、修正します。
- **複数の監視ツールの統合：**エンドツーエンドの一元的なビューによってモニタリング スタックを簡素化し、コストと労力を削減します。
- **ごく短時間での利用開始が可能：**Client Connectorをインストールしていれば、ZDXを有効化するだけで使用できます。別途何かを展開する必要はありません。

「ZDXを使用することで、ネットワークの問題を数分で切り分け、CSRがインターネット接続の問題に集中できます」
—Careem、CIO兼CISO、Peeyush Patel氏

Zscaler Risk360:
実用的なインサイトによるサイバーセキュリティ リスクの可視化と修復

サイバー リスクを高める主要因、推奨される調査ワークフロー、リスク傾向、同業他社との比較情報のガイダンスのほか、具体的な行動に生かせるCISO向けの概要レポートを提供します。Risk360のモデルは、攻撃の4つの段階をカバーしています。すなわち、外部攻撃対象領域、侵入、ラテラル ムーブメント、情報漏洩です。資産、アプリケーション、ユーザーなど、環境内のあらゆるエンティティーが対象になります。

- **一元的なダッシュボード：**インタラクティブなデータ活用型ダッシュボードでリスクを包括的に確認できるため、大量のツールやスプレッドシートが不要になります。
- **広範な関連付け：**クラウドネイティブ プラットフォームを活用し、従業員のリスクをZscalerのデータと関連付けて可視化します。
- **より詳細なリスク分析：**データ インサイトを基に、ポリシーを活用した実用的な緩和策として推奨事項を提示することで、リスク スコアを改善し、全体的なサイバー セキュリティ態勢を強化します。
- **財務リスクの概要：**リスクを潜在的な財務損失に直接紐付けることで、より良い意思決定や修復の優先順位付けを可能にします。

「Risk360を活用することで、サイバー リスクをより包括的に把握し、修復するための実行可能な方法を知ることができます。リスク管理において非常に貴重なツールであり、リスク エクスポージャーとそれが収益に及ぼし得る影響について、広範かつ詳細な視点を提供してくれます」
—Persistent Systems Ltd、CIO、Debashis Singh氏

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**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**

Zero Trust Everywhere