zscaler™

eBook

拠点向けゼロトラストの4つの要件



© 2024 Zscaler, Inc. All rights reserved.

拠点にゼロトラスト アプローチを導入することで、ネットワーク セキュリティを強化できるだけでなく、さまざまな場所のユーザー、デバイス、アプリケーションの接続を合理化できます。

ビジネスを取り巻く環境が流動的になった今、ユーザー、デバイス、アプリケーションのセキュリティ確保が多くの企業で課題になっています。従来、アプリケーションはデータ センター内に存在し、ユーザーからの接続は主にオフィスから行われていたため、接続ニーズは比較的単純なものでした。このような環境では、従来のハブ&スポークおよびファイアウォールベースのアーキテクチャーが効果的に機能していたのです。しかし、人々が働く環境が進化していくにつれ、こうした従来のアプローチでは、脅威に対する適切な保護と最適なユーザー エクスペリエンスの提供が難しくなってきています。

ユーザーの接続元は今やオフィスだけにとどまらず、自宅、カフェ、空港などさまざまな場所に広がっています。さらに、モノのインターネット (IoT) の普及によって、IoT/OT デバイスを通じたセキュリティ リスクが拡大しており、企業のセキュリティ環境はさらに複雑化しています。

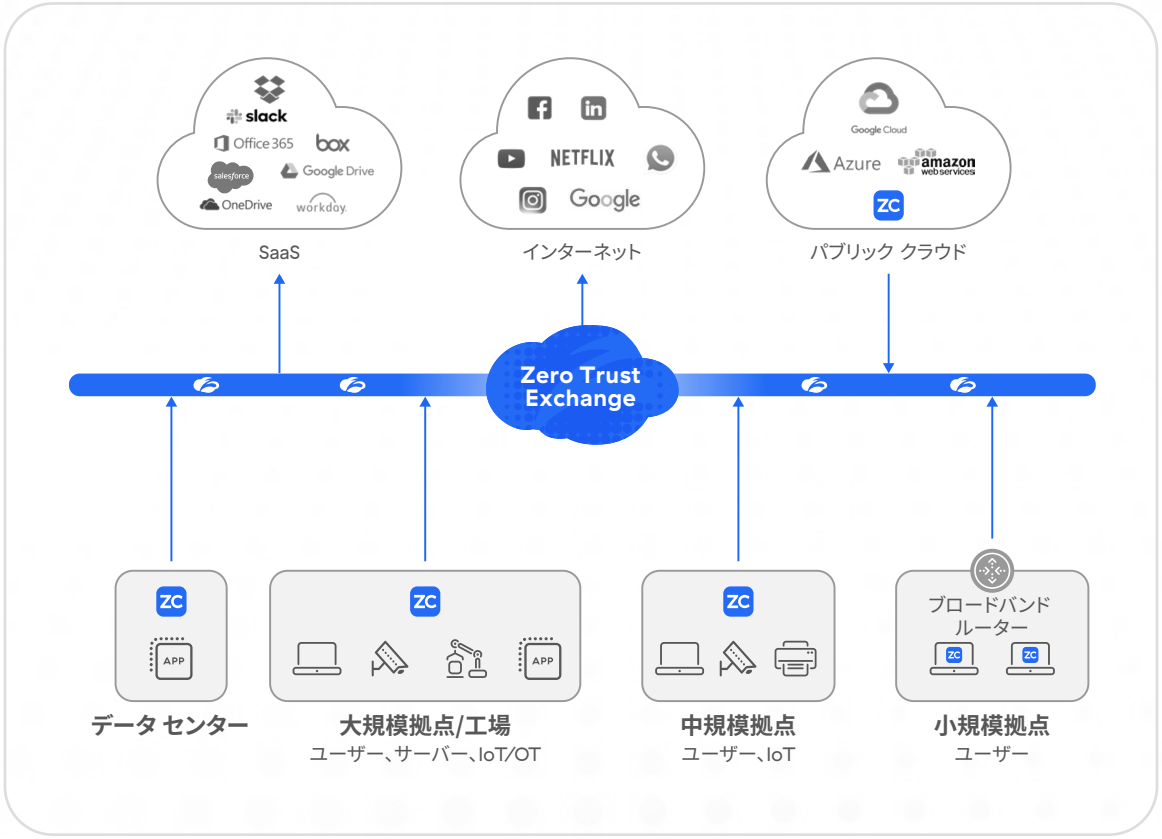


図1:ネットワーク接続にゼロトラストのアプローチを適用する拠点向けゼロトラスト

© 2024 Zscaler, Inc. All rights reserved.

こうした環境の変化を受け、多くの組織がゼロトラストのセキュリティ アプローチを採用し始めています。ゼロトラストの原則 (決して信頼せず、常に検証し、最小特権アクセスを適用すること) は、多くの企業で高度なサイバー攻撃の阻止を可能にしています。ユーザーをネットワーク上に配置し、制限のないアクセスを可能にしてしまう VPN とは異なり、ゼロトラストでは、必要なアプリケーションのみにアクセスを許可します。ネットワーク接続にゼロトラストの原則を適用することで、組織は脅威 (特に拠点から生まれるもの) に対する防御を強化できます。拠点にゼロトラスト アプローチを実装することで、安全な接続と運用の簡素化を実現できるほか、ルーティングの複雑性やユーザー エクスペリエンスの低下を克服しながら、攻撃対象領域を排除し、脅威のラテラル ムーブメントを防止できます。

拠点向けゼロトラスト アーキテクチャーは、支社、工場、小売店舗、データ センターなど、すべての拠点のセキュリティ強化を実現します。拠点向けゼロトラストに求められる重要要件は以下の 4 つです。

ゼロトラストの原則のネットワークへの適用 1

拠点の IoT/OT デバイスの保護 2

SaaS/インターネット トラフィックのクラウドへの直接接続パスの確保 3

オフィス勤務とリモート勤務の従業員に対する一貫したユーザー エクスペリエンスの提供 4

© 2024 Zscaler, Inc. All rights reserved.

「ゼロトラスト」ではない従来の SD-WAN

従来の SD-WAN アプライアンスは、単に企業ネットワークを離れた場所にある拠点に拡張しただけのもので、攻撃対象領域の拡大につながります。脅威のラテラル ムーブメントに対して十分な保護を行えないため、拡張先の拠点内の侵害されたデバイスから、データ センターやパブリック クラウドのビジネスクリティカルなアプリに簡単に通信できてしまいます。従来の SD-WAN の使用は、脅威のラテラル ムーブメントやインターネットベースの攻撃のリスク増加につながります。複数のセキュリティ アプライアンス、セキュリティ ツール、標準的でないポリシーを寄せ集めて使用することで、既知の脅威に対しても未知の脅威に対してもカバレッジに穴が生まれ、セキュリティ リスクは増大します。したがって、拠点の接続アーキテクチャーの安全を担保するには、ゼロトラストの導入に注力し、攻撃対象領域の削減と脅威のラテラル ムーブメントの防止を図ることが不可欠です。

IT プロフェッショナルやサイバーセキュリティの専門家 382 人を対象に調査を行った Cybersecurity Insiders による 2023 年版 VPN リスク レポートでは、VPN がもたらすセキュリティ上のリスクが明らかになっており、VPN によってセキュリティが脅かされる可能性に懸念を示した組織は、「やや懸念している」から「極めて懸念している」まで、合わせて 88%に上りました。

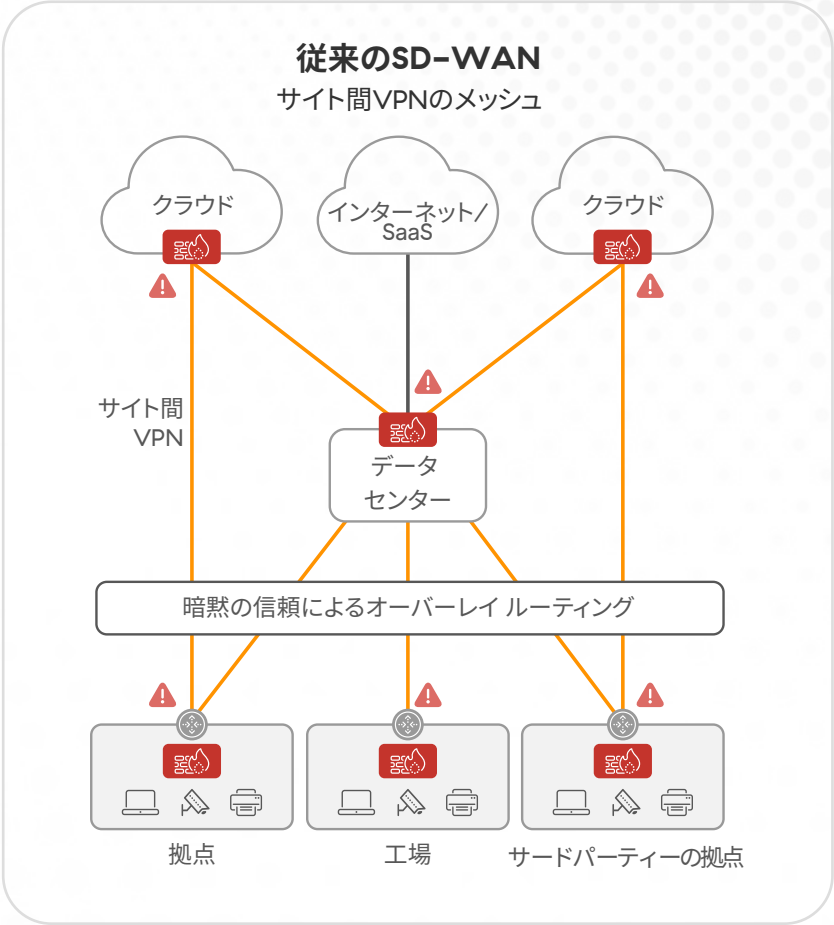


図2:従来のSD-WANは攻撃対象領域の拡大を招くうえ
脅威のラテラル ムーブメントに対して無防備

© 2024 Zscaler, Inc. All rights reserved.



また、VPN の脆弱性を悪用した攻撃を過去 12 か月間に 1 回以上経験した組織は 45% に上り、3 社に 1 社が VPN に関連したランサムウェア攻撃の被害を受けていることがわかりました。このように、VPN に関連した脆弱性を悪用するサイバー攻撃の脅威は拡大しており、現在のアーキテクチャーのセキュリティ課題への対処は急務となっています。

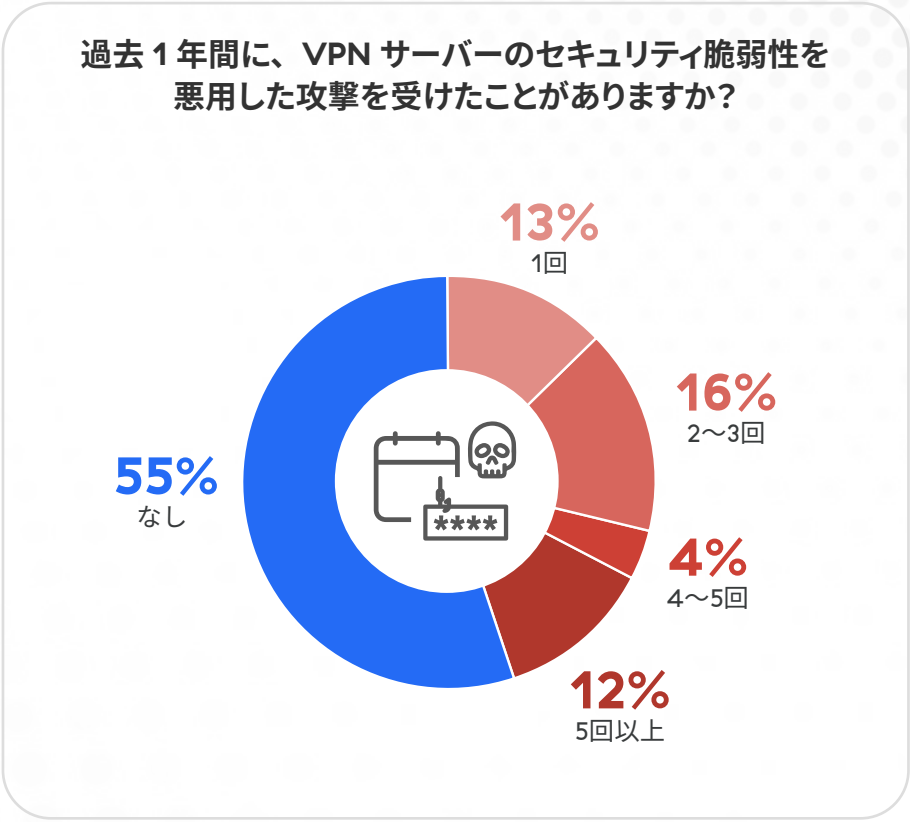


図3: VPNサーバーの脆弱性によって組織のサイバー攻撃被害が増加

© 2024 Zscaler, Inc. All rights reserved.

ファイアウォールやVPN では構築できないゼロトラスト

これまで、データ センターでホストされている重要なアプリケーションへの接続を確立するために、企業はサイト間 VPN を使用していました。しかし、接続先のアプリケーションがクラウドに移行するにつれ、従来のサイト間 VPN アーキテクチャーは効率性を失っていきます。トラフィックは依然としてデータ センターにバックホールされるため、ユーザー エクスペリエンスの低下やパフォーマンスの問題を招くのです。また、VPN トンネルではサイトの管理とセットアップを個別に行う必要があるため、運用の複雑化につながります。そこで、多くの企業の IT 部門が、ハブ&スポーク ネットワークからクラウドへの直接接続アーキテクチャーに移行することで、アプリケーション トラフィックをクラウド セキュリティ プロバイダーに送信し、アプリケーションのパフォーマンス向上を図ろうとしています。

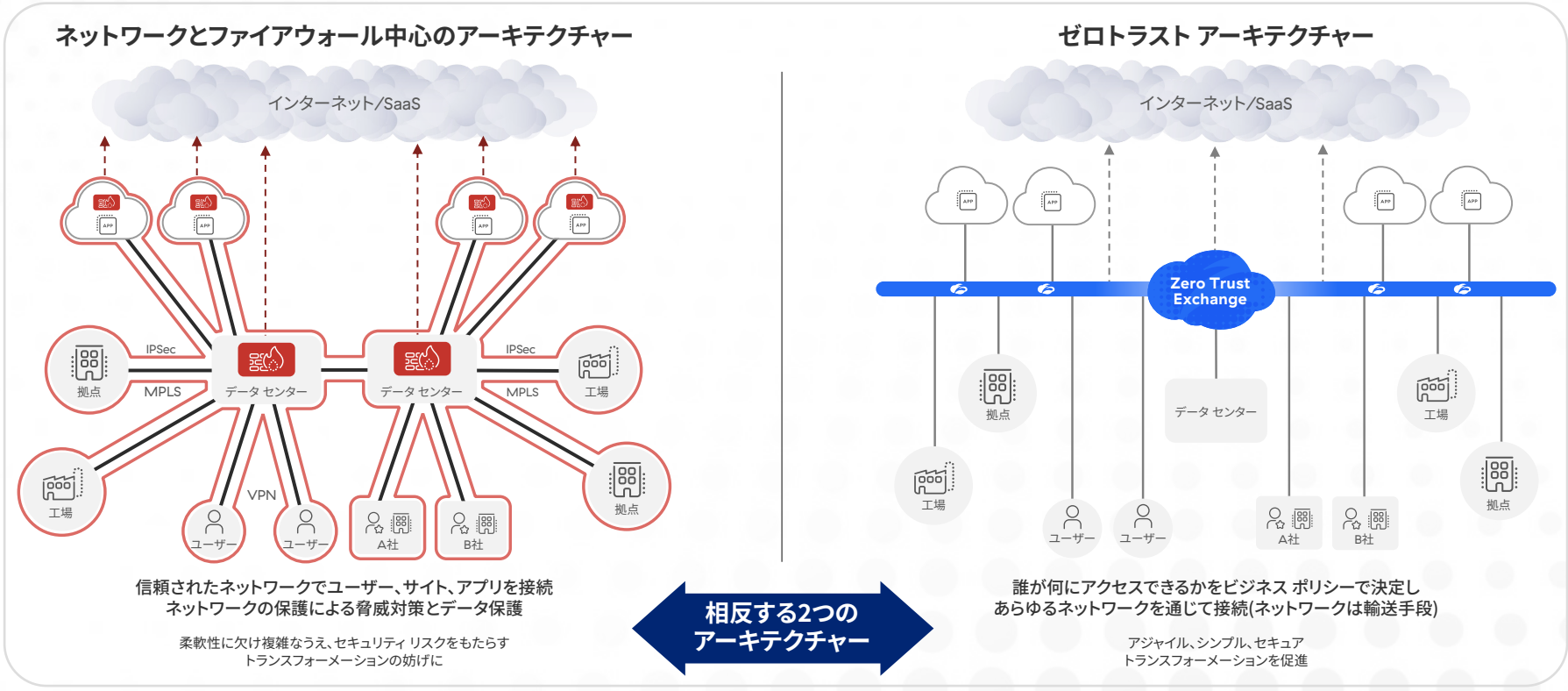


図4: 複雑で柔軟性に欠けるハブ＆スポークのネットワーク(左)とトランスフォーメーションを促進するアジャイル、シンプル、セキュアなゼロトラスト アーキテクチャー(右)

© 2024 Zscaler, Inc. All rights reserved.

拠点向けゼロトラストに求められる4つの重要要件

1 ゼロトラストの原則のネットワークへの適用

サイト間VPN は、拠点、データ センター、クラウド リージョン、サードパーティーに企業ネットワークを拡張します。従来のネットワークは、攻撃対象領域を直接制御できないエンティティーに拡大し、トラフィック フローを黙示的に許可し、脅威のラテラル ムーブメントを可能にします。ネットワークを複数のゾーンに分割し、複雑な管理を必要とする従来のネットワーク セグメンテーションとは異なり、ユーザーとアプリ間およびデバイスとアプリ間のセグメンテーションでは、承認された場合にのみコンテキストに応じたきめ細かなアクセスが提供されます。ゼロトラストの原則に基づくネットワーク基盤は、従来のフラットなネットワークにつきもののリスクを排除し、セキュリティ制御のためのファイアウォール階層化に伴う複雑性の回避に役立ちます。

2 拠点の IoT/OT デバイスの保護

プリンター、テレビ、カメラ、カード リーダー、センサーなど、「スマート」なデバイスの普及に伴い、ほぼすべての組織で IoT/OT デバイスが急増しています。こうしたデバイスは数々のオペレーティング システムを実行しており、さまざまなセキュリティ リスクを抱えているため、依然としてパッチ管理が課題となっています。IT リーダーの多くは、こうしたデバイスについて、詳細なインベントリーはおろか一切の可視性を有していません。しかし、こうしたデバイスは多くの場合、データ センターやクラウド サービス内の重要なアプリケーションに制約なくアクセスできます。IoT デバイスを狙ったマルウェアベースの攻撃は 400% 増加[1]しており、重要な脅威ベクトルとなっています。組織は拠点や工場の IoT/OT デバイスのセキュリティを確保して事業運営を保護する必要があります。

IoT/OT デバイスを狙ったマルウェア攻撃は 2022 年から 400% 増加しており、重要な脅威ベクトルとなっています。

© 2024 Zscaler, Inc. All rights reserved.

3 SaaS/インターネット トラフィックのクラウドへの直接接続パスの確保

クラウドへの直接接続アーキテクチャーでは、世界中のあらゆる場所のユーザーや IoT/OT デバイスを、あらゆるアプリケーションにすばやく接続することが可能です。SaaS やインターネットのトラフィックにクラウドへの直接接続パスを導入することは、ネットワーク パフォーマンスを最適化し、シームレスな接続を確保するために不可欠です。高コストの MPLS リンクを介してデータ センターにトラフィックをバックホールするハブ&スポーク アーキテクチャーは、アプリケーションのパフォーマンス低下を招き、ビジネスの生産性を損ないます。アプリケーションがデータ センターに置かれている場合は、アプリケーション トラフィックを地域のハブにバックホールすることは理にかなっていました。しかし、アプリケーションのクラウド移行が進む今、最も合理的なのは、ユーザーや IoT/OT デバイスのトラフィックを接続先に直接送信する方法です。クラウドへの直接接続アーキテクチャーでは、SaaS アプリケーションとインターネットのトラフィックは最も効率的かつ直接的なルートで接続先に送信されます。この方法には多くのメリットがあり、コストの削減、ユーザー エクスペリエンスの強化、ネットワークの簡素化などにつながります。

今、ビジネス リーダーは、ユーザーや IT 部門にカフェのようなエクスペリエンスを提供することを目指しています。できる限りシンプルな形でビジネス アプリに接続し、アプリケーションが優れたパフォーマンスを発揮できる環境が求められています。

4 オフィス勤務とリモート勤務の従業員に対する一貫したユーザー エクスペリエンスの提供

多くの従業員はリモート ワークかハイブリッド ワークで働くようになりました。そして、この働き方の変化によって、ある重大な問題が浮き彫りになっています。多くのユーザーが、自宅よりオフィスの方が接続品質が低いと不満を訴えているのです。この状況は、IT 部門にとって新たな懸念事項となっています。トラフィックをデータ センターにバックホールする VPN テクノロジーは、ユーザー エクスペリエンスの質や一貫性を損ない、ビジネスへの悪影響や生産性の低下を招きます。

今、ビジネス リーダーは、ユーザーや IT 部門にカフェのようなエクスペリエンスを提供することを目指しています。できる限りシンプルな形でビジネス アプリに接続し、アプリケーションが優れたパフォーマンスを発揮できる環境が求められています。自宅からでもオフィスからでも必要なアプリにアクセスでき、一貫したエクスペリエンスと同等の利便性が担保されていなければなりません。しかし、これは VPN 経由のネットワーク接続では実現できません。競争の激しい今日の世界で存在感を保つためには、オフィス勤務とリモート勤務の従業員に一貫したユーザー エクスペリエンスを提供し、従業員の生産性や創造性を高めることが不可欠です。

吹き出しのテキストを入力してください

© 2024 Zscaler, Inc. All rights reserved.

ゼロトラストの原則を SASE に適用

セキュア アクセス サービス エッジ (SASE) は、ネットワーク サービスとセキュリティ サービスをクラウド型ソリューションに統合し、運用の合理化と複雑性の軽減を実現するとともに、ネットワーク全体への一貫したポリシーの適用を可能にします。SASE は、ゼロトラスト ネットワークと重要なクラウド型セキュリティ サービス (SWG、CASB、FWaaS、ZTNA など) を組み合わせたものです。従来の SD-WAN を基盤に構築された SASE ソリューションは、十分な保護を提供できず、攻撃対象領域の拡大を招き、重要なアプリケーションをインターネット上のさまざまな脅威にさらすものであると認識することが大切です。

さらに、従来の SD-WAN のセグメンテーション機能は断片的で粒度が低いため、脅威を他のシステムに簡単に拡散させ、サイト全体やネットワークのダウンを招く危険性があります。

TechTarget の Enterprise Strategy Group (ESG) は、SASE の現状把握を目的として、北米 (米国およびカナダ) のさまざまな組織の IT およびサイバーセキュリティのプロフェッショナル 390 人を対象とした調査を実施しました。この調査によると、組織の SASE 導入を後押しするユース ケース上位 3 つは以下のとおりです。

1. ネットワーク ポリシーとセキュリティ ポリシーの整合性の確保
2. インターネットの攻撃対象領域の削減または排除
3. リモート ユーザーのセキュリティ強化

この 3 つのユース ケースはいずれも、レジリエントな SASE フレームワークの確立にあたって、ユーザー、デバイス、アプリケーションに安全な接続を提供することの重要性を示しています。SASE の導入に着手する際は、ゼロトラストの原則に準拠したソリューションを第一に考えなければなりません。従来の SD-WAN は、サイト間 VPN やオーバーレイ ルーティングを介してさまざまな拠点を接続すると同時に暗黙の信頼を確立し、侵害されたエンティティーに対しても、重要なビジネス リソースへのアクセスを制限なく許可してしまいます。一方、ゼロトラストの原則に基づいて構築された SD-WAN は、攻撃対象領域を効果的に削減し、脅威のラテラル ムーブメントを防ぐとともに、ユーザーとアプリ間、デバイスとアプリ間、アプリ間の安全な通信の確立に役立ちます。

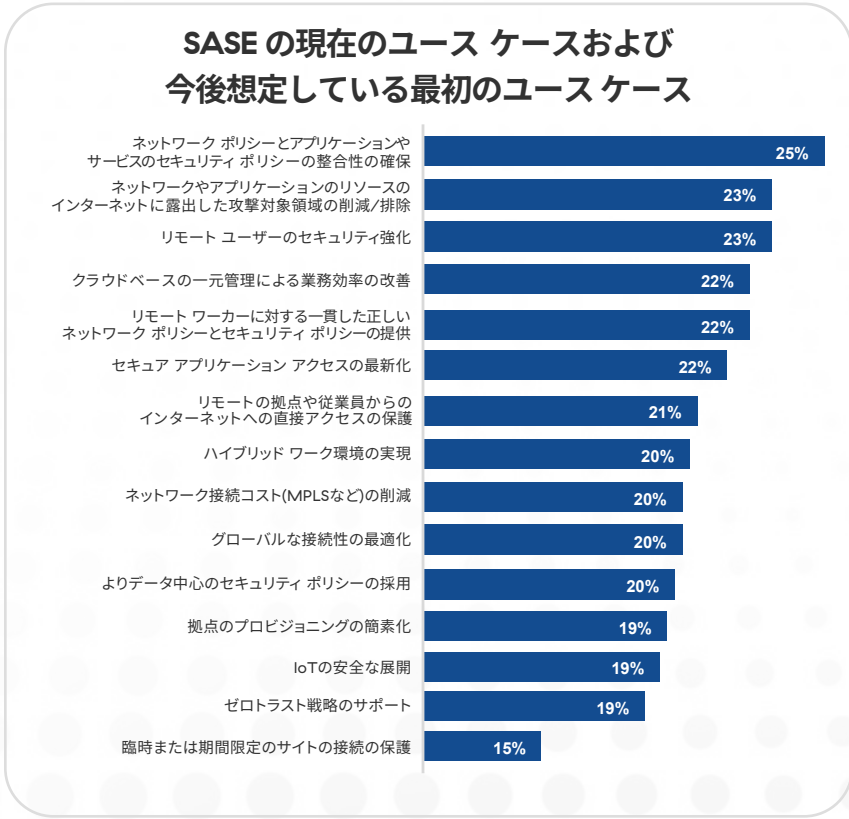


図5: SASEのユース ケースに関するESGの調査結果

© 2024 Zscaler, Inc. All rights reserved.

まとめ

従来の拠点のネットワーク アーキテクチャーは暗黙の信頼に依存しており、攻撃対象領域を最も遠い拠点にまで拡大し、組織全体にわたるサイバー脅威のラテラル ムーブメントを許しています。拠点にゼロトラスト アプローチを採用することで、ネットワーク セキュリティを強化し、さまざまな場所のユーザー、IoT/OT デバイス、アプリケーションの接続を合理化できます。拠点のネットワークをゼロトラストの原則に基づいて設計することで、ルーティングによる複雑性を克服しながら、攻撃対象領域の排除とラテラル ムーブメントの防止を実現し、セキュリティ態勢を改善できます。ゼロトラストの原則を拠点に適用するにあたっては、本書で説明した 4 つの要件を慎重に検討し、セキュリティとネットワーク接続の絶えず変化する複雑なニーズに効果的に対応することが重要です。

参考資料

1. zscaler.jp/press/zscaler-threatlabz-finds-400-increase-iot-and-ot-malware-attacks-year-over-year-underscoring
2. https://info.zscaler.com/2023-vpn-risk-report-jp
3. zscaler.com/resources/industry-reports/esg-sse-leads-the-way-to-sase.pdf

© 2024 Zscaler, Inc. All rights reserved.

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。

© 2024 Zscaler, Inc. All rights reserved. Zscaler™、Zero Trust Exchange™、Zscaler Internet Access™、ZIA™、Zscaler Private Access™、ZPA™、Zscaler Digital Experience、ZDX™、および zscaler.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。

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.jp