データ シート

Zscaler Zero Trust Branch

拠点や工場を接続して保護するための、よりシンプルで安全かつ費用対効果の高い方法

ランサムウェア攻撃を助長する複雑な従来のネットワークとセキュリティ アーキテクチャー

従来のネットワークは、現在の分散した働き方やクラウドファーストのアプリ向けに設計されていません。ファイアウォール、VPN、旧来型の SD-WAN を使用すると、以下のようなセキュリティ リスクや運用上の課題が生じます。

- **攻撃対象領域の拡大**

  ネットワークをリモート拠点へ拡張すると、攻撃対象領域が広がります。ファイアウォールや VPN ゲートウェイが攻撃の標的となり、ゼロデイ脅威のリスクも高まります。

- **脅威のラテラル ムーブメント**

  拠点で感染したデバイスが、ネットワーク全体に急速に感染を広げる可能性があります。ランサムウェア攻撃は、わずか 45 分で深刻なシステム停止を引き起こすこともあります。

- **コストと複雑さ**

  ファイアウォール、プロキシ、NAC エージェント、IP ベースのポリシーが複雑に混在することで、運用の複雑さとコストが大幅に増加し、ビジネスの俊敏性が損なわれます。

- **パフォーマンスとユーザー エクスペリエンスの低下**

  トラフィックをデータ センターや複数のセキュリティ レイヤー経由でルーティングすると、アプリケーションのパフォーマンスが低下し、ユーザーの不満を招きます。

Zero Trust Branch

カフェ型の拠点を提供

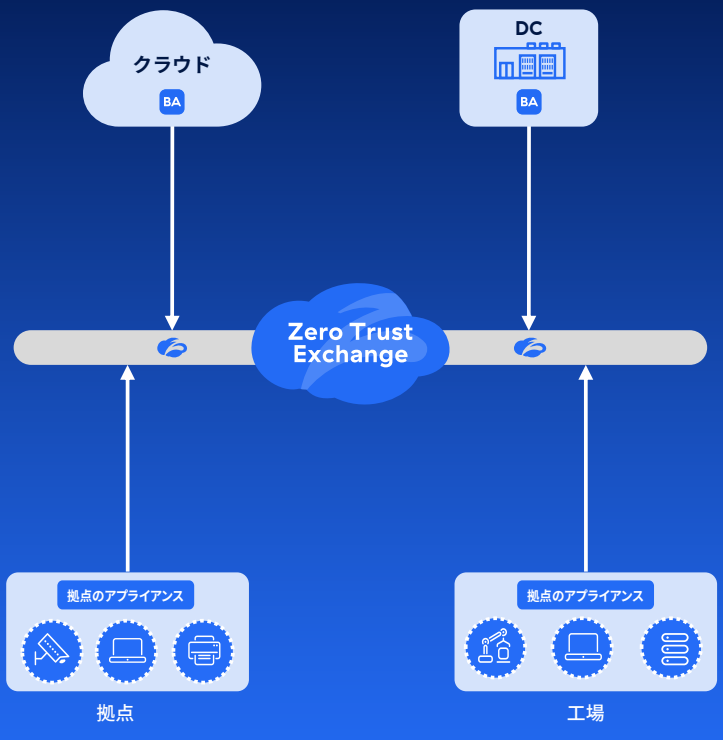
ネットワークをすべての拠点に拡張することなく、ユーザーやデバイスをアプリに接続させます。

ランサムウェアのラテラル ムーブメントを阻止

ユーザーや OT/IoT デバイスをわずか数日でセグメント化します。

ファイアウォールとインフラの支出を 50% 削減

南北と東西のファイアウォール、NAC、高額な専用スイッチ、デバイス エージェントを排除します。



仕組み

Zscaler Zero Trust Branch は複雑な VPN やオーバーレイ ルーティングを使用することなく、拠点、工場、データ センターを安全に接続させ、セグメント化します。このソリューションにより、組織のセキュリティ ポリシーに基づき、ユーザーや IoT/OT デバイスからアプリケーションへのゼロトラスト アクセスが確保されます。先進的な Zscaler Zero Trust Exchange プラットフォームと、拠点や工場に配備された統合型の拠点アプライアンスを組み合わせることで、組織はセキュア アクセス サービス エッジ (SASE) フレームワークを導入し、重要な OT/IoT デバイスのセグメント化とカフェ型の拠点を実現できます。

Zero Trust Branch アプライアンスは ISP 接続を直接終端し、複数の回線にまたがるトラフィック転送を管理することで、高い可用性と回復力を確保します。拠点や工場からのトラフィックは Zero Trust Exchange に安全に転送され、AI を活用した高度なサイバー脅威対策およびデータ保護ポリシーが施行されます。

業界をリードする Zscaler のゼロトラスト アーキテクチャーによって、各拠点は自動的に分離され、マルウェアのラテラル ムーブメントが防止されます。さらに、各拠点内では、Zscaler 独自の「ネットワークオブワン」セグメンテーション技術が、NAC やスキャナー、エンドポイント エージェントを使用することなく IoT/OT デバイスを自動で分類および分離します。自動グループ化と脅威レベルに基づくポリシーにより、影響範囲の最小化、コンプライアンスの簡素化、インシデント対応の自動化がファイアウォールなしで実現します。

デバイスの自動検出と分類機能を活用すれば、ネットワーク管理者は振る舞いベースのアイデンティティーに基づいてデバイスを自動的にグループ化できるため、ポリシー管理が簡素化され、複雑なインベントリー管理が不要になります。

Zero Trust Branch アプライアンスには AppConnector が統合されており、VPN、ジャンプ ホスト、VDI ファームを使うことなく、OT/IoT リソースへのサードパーティーによる特権リモート アクセスを容易に実現できます。

Zero Trust Branch のユース ケース

VPN の代替：サイト間 VPN やオーバーレイ ルーティングの複雑さを排除し、攻撃対象領域の縮小と脅威のラテラル ムーブメントの防止を実現する、よりシンプルかつコスト効率に優れたソリューションを提供します。

IT/OT セグメンテーション：IT システムと OT システム間のラテラル ムーブメントを排除することで、工場、病院、重要インフラを保護します。数か月や数年ではなく、わずか数日でセグメンテーションが実現します。

SD-WAN の刷新：カフェ型の拠点アーキテクチャーを導入し、ランサムウェアのリスクを低減します。ゼロトラスト セキュア アクセス サービス エッジ (SASE) フレームワークによってセキュリティを強化します。

AI を活用したデバイスの検出と分類：エンドポイント エージェント、スキャナー、トラフィック ミラーリングを使用せずに、OT/IoT デバイスを検出して分類し、インベントリー化します。

Zero Trust Branch の機能

カテゴリー	機能
ゼロタッチ プロビジョニング	• 事前定義されたテンプレートによるゼロタッチ プロビジョニング • テンプレートおよびサイトプロファイルに基づく導入方式
トラフィック転送ポリシー	• 柔軟な基準に基づくトラフィック選択：動的グループ、ユーザーおよびマシンのアイデンティティー、5 タプル、または FQDN • トラフィック転送オプション：ZIA、ZPA、またはダイレクト • インテリジェントな経路優先設定：静的、動的、ポリシーベース • サイト間の直接接続に対応

統合型の ゼロトラスト ポリシー	• 統合ポリシー：ユーザーとアプリ間、IoT デバイスとアプリ間、サーバー間 • ロケーションと位置ベースのポリシー • IPS、SSL/TLS 復号、プロキシ、URL フィルタリング、データ保護を含む包括的なセキュリティ検査 • IoT/OT デバイスに対する包括的な保護 • AppConnector によるインバウンド接続
インシデント対応	• Ransomware Kill Switch
インターフェイス	• 複数の L3 LAN ネットワーク • 複数の L3 WAN ネットワーク • 802.1q/VLAN タギング • リンク アグリゲーション (802.3ad) • 専用の管理インターフェイス
高可用性	• VRRP とセッション同期を使用した 2 ノード クラスター • インターフェイスの正常性モニタリング • 構成と状態の同期 • ソフトウェアのヒットレス アップグレード • 稼働中のハードウェアのリプレース
ルーティングとネット ワークのサービス	• 静的ルーティング • 動的ルーティング (BGP、OSPF) • ネットワーク アドレスの変換 (ソース NAT) • DHCP サーバー、リレー / プロキシ • 等コスト マルチパス (ECMP)
デバイス分離	• エージェントレスのデバイス分離 (「ネットワークオブワン」) • 動的マイクロサブネット • MAC アドレスベースのフィルタリング
アプリケーション 認識型のパスの選択	• アプリケーション認識型の動的なパス選択 • 組み込みのリンク モニタリングとフェイルオーバー
ゼロトラスト セグメン テーション	• 自律的なグループ化とポリシー • VLAN 内と VLAN 間のポリシー制御 • デバイス、タグ、ユーザー アイデンティティー、時間、ゾーンに基づいて柔軟に構成できる階層型ポリシー フレームワーク
資産の検出と プロファイリング	• エンドポイントとネットワークの検出 • デバイス フィンガープリンティング • プロファイルベースのデバイスの分類 • ICS と医療のプロトコルのデコード
監視と トラブルシューティング	• リモート デバッグ コンソール • Zero Trust Branch デバイス上でのローカル CLI 対応 • SNMP v2/v3 サポート
一元管理	• シングル サインオン (SSO) と MFA • ログイン イベントと構成変更の監査証跡 • ロールベースのアクセス制御 • 単一の UI で管理できるマルチテナント対応クラウド型プラットフォーム • 包括的な自動化をサポートする OneAPI • 専用のマネージド サービス (MSSP) ポータル
可視性と ログ管理	• すべてのポートとプロトコルにわたるセッションとトランザクションのログを詳細に記録 • ポリシー相関を含むトラフィック マップ • 統合された柔軟なデータ レイク • セグメント内とセグメント間のすべての通信に対するセッション開始ログ
統合	• Microsoft Active Directory • EDR ベンダー – CrowdStrike、SentinelOne • アセット管理 – Armis、ServiceNow、Ordr
Zscaler のデータ センター /POP	• 世界中の 150 以上のデータ センターから提供されるクラウド セキュリティ プラットフォーム • シームレスな PoP フェイルオーバーによる可用性と冗長性を標準搭載

Zero Trust Branch アプライアンス

Zscaler Zero Trust Branch アプライアンスは、拠点や工場への導入に適した物理および仮想のさまざまなフォームファクターで提供されています。

	ZT 400	ZT 600	ZT 800	ZT 8010*
本体 前面				
適した環境	小規模の拠点	小規模から中規模の拠点	拠点、工場	工場、大規模な拠点
CPU	4C	4C	8C	16C
DRAM	32 GB	32 GB	64 GB	128 GB
ストレージ	256 GB	256 GB	512 GB	1 TB
TPM	2.0			
LAN/WAN RJ45 ポート	4 x 1GbE RJ45	6 x 1GbE RJ45	6 x 1GbE RJ45	10 x 1GbE RJ45
LAN/WAN ファイバー ポート	なし	なし	2 x 1Gb SFP	8 x 10G SFP+
USB ポート	1x USB 3.1	2x USB 2.0		2x USB 3.0
コンソール ポート	1 x RJ45			
物理仕様				
ファクター フォーム	デスクトップ	デスクトップ	デスクトップ	ラックマウント – 1U
寸法（幅 x 高さ x 奥行き）	6.61 x 1.26 x 7.20 インチ (16.76 x 3.175 x 18.29 cm)	9.09 x 1.73 x 7.78 インチ (23.08 x 4.39 x 19.76 cm)		17.24 x 1.73 x 12.64 インチ (43.8 x 4.4 x 32.1 cm)
重量	1.98 lbs (0.898 kg)	2.64 lbs (1.197 kg)		18.96 lbs (8.6 kg)
取り付けブラケット	ラックマウント / ウォールマウント（別途オプション）	ラックマウント（標準で付属）		

	ZT 400	ZT 600	ZT 800	ZT 8010*
電源仕様				
電源	DC: 外部 AC 電源アダプター付属			内部：電源
冗長電源	なし			あり (1+1)
標準電力消費	アイドル モード — 12W 最大負荷モード — 20W	アイドル モード — 21W 最大負荷モード — 29W	アイドル モード — 24W 最大負荷モード — 43W	アイドル モード — 107.8W 最大負荷モード — 225.5W
最大電力消費	40W		60W	冗長 PSU: 300W シングル PSU: 350W
電源コード定格	C14 10A			
入力範囲	AC 100~240V@50~60 Hz			冗長 PSU: AC 100~240V @50~60 Hz シングル PSU: AC 100~240V @47~63 Hz
入力電流	1.7Amax		1.8Amax	5Amax
出力定格	11.4 ~ 12.6V			
冷却方法	ファンレス	ファン付き		
環境仕様				
稼働温度	32 ~ 104°F (0 ~ 40°C)			
非稼働時温度	−4 ~ 150°F (−20 ~ 70°C)			
相対湿度	稼働時：5% ~ 90% 非稼働時：5% ~ 95%			
高度	稼働時：5,000 フィート (1,524 m) 非稼働時：50,000 フィート (15,240 m)			

* 近日リリース予定

購入方法に関する注意事項

Zscaler Zero Trust Branch デバイスは、ハードウェアとクラウド サービスを含むサブスクリプションとして提供されます。帯域幅の要件に応じたアプライアンスの選定やサブスクリプション オプションについては、Zscaler 担当者までお問い合わせください。