OT/IoT 向け Zscaler Zero Trust Device Segmentation

ラテラル ムーブメントの阻止、攻撃対象領域の縮小、オペレーションの安全性の向上

ソリューションの概要

現在の課題

国家支援型の脅威アクターによる、米国の重要インフラへのサイバー攻撃に関する注意喚起や警告が急増しています。2024 年 2 月 7 日、連邦捜査局 (FBI)、サイバーセキュリティ インフラストラクチャー セキュリティ庁 (CISA)、国家安全保障局 (NSA) は政府機関に向けて合同で警告を発し、交通システムや石油天然ガス パイプライン、水処理プラント、電力網などの重要インフラを混乱させようとしている脅威アクターについて言及しました。この警告は、空港、航空機運航会社、鉄道のセキュリティを確保するために TSA が講じた同様の措置や、最近の DOE サイバーセキュリティ ベースライン、および CIP-015-1 のほぼ最終的な NERC 更新を補完するものです。

OT/IoT テクノロジーは、スピードとトランザクションの効率性を第一に考えるように設計されており、セキュリティへの対応は後回しになっているのが実状です。OT/IoT は現在、サイバー犯罪者の格好の攻撃対象となっており、Zscaler ThreatLabz の調査でも、これらを対象とした攻撃が前年比で 400% 増加していることがわかっています。中でもランサムウェア攻撃は最も頻繁に発生しており、侵害全体の 61% が OT に接続された組織を標的にしています。

必要な対策

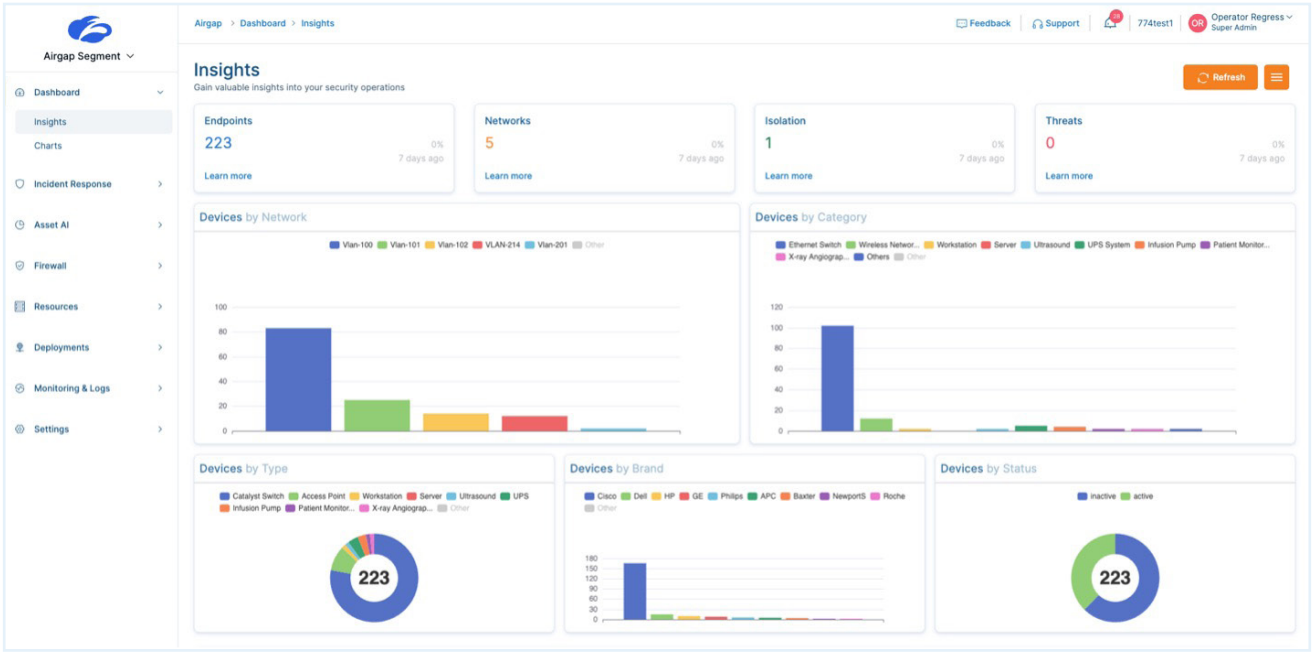
EPA、CISA、FBI はシステム オペレーターに対し、サイバーセキュリティを強化するための指針としてゼロトラストを採用するよう求めた大統領令に従い、取り組みを実施することを強く推奨しています。

以下の項目はこの推奨事項の中でも特に重要な要素です。Zscaler Zero Trust Device Segmentation を採用することで、これらの領域にすぐに対処できます。

- インターネットへの露出の削減
- 脆弱性への露出の削減
- ネットワーク セグメンテーション
- ログの収集
- 許可されていないユーザーによる接続の禁止
- 悪用されるリスクがあるインターネット上のサービスの廃止
- OT/IoT からインターネットへの接続の制限
- 関連する脅威の検出
- OT/IT 資産のインベントリーの作成

Zscaler のソリューション

ネットワーキングの基本とされてきたセグメンテーションは、アクセス制御リスト (ACL) やファイアウォールなどのツールを使用して、North-South (クライアントとサーバー間) トラフィックを管理してきました。しかし、OT マイクロセグメンテーションでは、デバイスとワークロード間を水平方向に流れる、より脆弱な East-West トラフィックに焦点が移ります。共有 VLAN は旧式のスイッチング アーキテクチャーを採用しており、デバイス同士が相互に認識して通信できるため、マルウェアが拡散しやすい脆弱な環境が生まれます。残念ながら、クラウド ワークロード向けに開発されたエージェントベースのソリューションでは、OT で一般的な旧式のヘッドレス マシンをセグメント化できません。また、従来の ACL ベースのアプローチは依然として非常に複雑です。



Zscaler Zero Trust Device Segmentationのダッシュボード

Zscaler は、旧式のヘッドレス システムを含むすべての IP エンドポイントを「1 つのネットワーク セグメント」に分離します。そして、すべての脅威のラテラル ムーブメントを阻止するエージェントレス ソリューションで、VLAN 内のセグメンテーションの課題を解消します。これにより、複雑な ACL や既存のインフラの変更が不要になり、最もきめ細かく効果的なセグメンテーションが可能になります。

ユース ケース

エージェントレスのデバイス セグメンテーションの代表的なユース ケースとして、以下が挙げられます。

LAN マイクロセグメンテーション

ゼロトラストを LAN に拡張するには、East–West トラフィックをセグメント化します。これにより、内部の攻撃対象領域が縮小し、重要な OT/IoT ネットワークにおける脅威のラテラル ムーブメントが排除されます。NAC やファイアウォールベースのセグメンテーションは一切必要ありません。

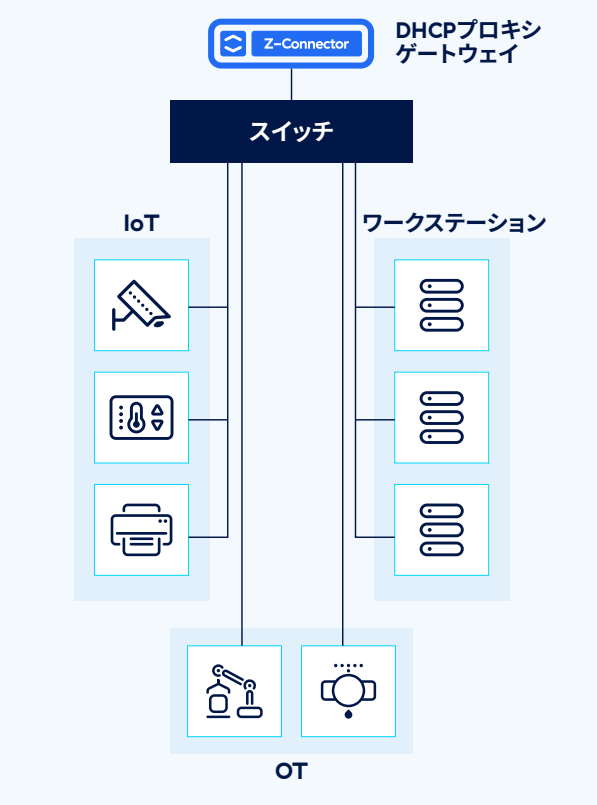
ネットワークにゼロトラスト セグメンテーションを実施する方法は以下のとおりです。

- すべてのデバイスを 1 つのセグメントに自動プロビジョニングする (/32 を使用)
- 不正なデバイスが MAC を装ってネットワークに侵入するのを防ぐために、デバイス、ユーザー、アプリのトラフィック パターンを分析して自動的にグループ化する
- ユーザーとデバイスのアイデンティティーとコンテキストに基づいて、East–West トラフィックのポリシーを動的に施行する

IT/OT セグメンテーション

Zscaler Zero Trust Device Segmentation は、ランサムウェアの機能を止めるキル スイッチとして機能し、業務を中断することなく、重要でないデバイス通信を無効化して脅威のラテラル ムーブメントを阻止します。このソリューションは、IoT デバイスや OT システム、エージェントをインストールできないデバイス上のランサムウェアなどの高度な脅威を無力化します。

- 任意のデバイス上の既知の MAC アドレスを自動的にグループ化し、ポリシーを施行する (例：管理者以外のカメラへの RDP アクセスを拒否)
- 不明な MAC アドレスを自動的に分離し、デバイスが侵害された場合の影響範囲を制限する
- 資産管理システムと統合し、安全なアクセス制御ポリシーを確保する



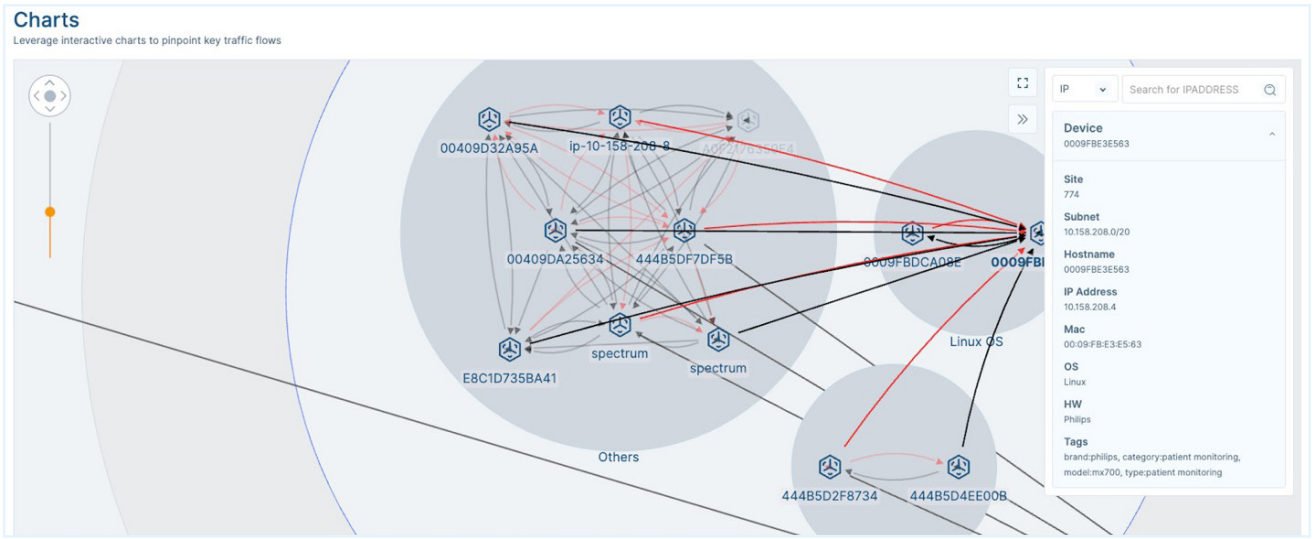
各デバイスを 1 つのセグメントに分離する、
自動化された IoT/OT セグメンテーション

デバイスの自動検出と分類

OT/IoT トラフィックの大部分はローカル ネットワーク内にとどまるため、East-West トラフィックを継続的に可視化することが重要です。ネットワーク管理者は、デバイスの自動検出と分類により、複雑なインベントリー管理なしで、IoT/OT システムのパフォーマンス、稼働時間、セキュリティをより適切に管理できます。

以下を行うことで、ネットワークとデバイスを効果的に可視化できます。

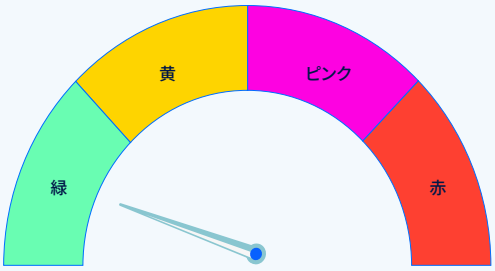
- エンドポイント エージェントなしで、OT/IoT デバイスを検出して分類し、インベントリーを作成する
- トラフィック パターンとデバイスの振る舞いをベースライン化し、許可されたアクセスと許可されていないアクセスを特定する
- パフォーマンス管理と脅威マッピングに活用できる、ネットワークに関する正確な情報を取得する



デバイス検出のダッシュボード

インシデント対応の自動化

Zscaler Ransomware Kill Switch では、ユーザーが選択した方法で攻撃対象領域を削減できます。事前に設定された重大度を選択すると、脆弱な既知のプロトコルやポートが段階的に制限され、製造ラインや病院フロアなどのネットワーク全体へのアクセスが即座に無効化されます。脅威に合わせて調整するだけで業務の生産性を維持できるため、侵害の混乱の中で不確かな推測をする必要がなくなります。



平均修復時間を大幅に改善

リスクの高い
アクセスをブロック

ラテラル
ムーブメントを阻止

重要資産への
アクセスをブロック

Zscaler の技術専門家によるデモ

当社の技術専門家とのデモを依頼して、重要インフラを保護する Zscaler ソリューションの詳細をご確認ください。