

IoT と OT のセグメンテーション

ゼロトラストのセグメンテーション機能をすべてのコネクテッドデバイスに拡張

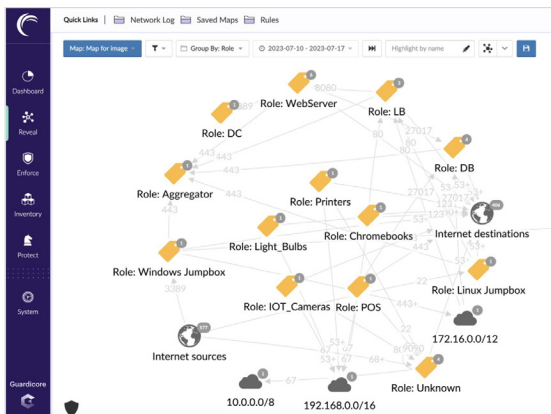
多くのエンタープライズが、成長の促進、効率の改善、そして顧客に対する効果的なサービス提供のために Internet of Things (IoT) デバイスと運用テクノロジー (Operational Technology、OT) の使用を拡大しています。こうしたテクノロジーはビジネス価値を大幅に向上させる可能性があります。その一方で重要な攻撃ベクトルの新たな出現も意味しており、セキュリティチームはこれを防ぐ必要に迫られています。IoT デバイスではハードウェアとソフトウェアの脆弱性が特に発生しやすく、また、多くのレガシー OT システムはコネクテッドな世界のセキュリティ要件を考慮して設計されていません。Akamai Guardicore Segmentation は、こうしたデバイスへのゼロトラスト・セキュリティの拡張を実現します。その結果、攻撃者がデバイスを悪用して、より広範なエンタープライズ IT インフラにアクセスするリスクが軽減されます。

新しいコネクテッドデバイスを継続的に探索




IoT と OT のデバイスの導入は、エンドポイントやその他の従来型エンタープライズデバイスの導入とは大きく異なります。特に重要なのは、IoT と OT のデバイスの導入数が非常に多く、進化する運用上のニーズに応じてデバイスのフットプリントがダイナミックに変化する点です。Akamai Guardicore Segmentation は、接続されているすべての IoT デバイスと OT デバイスを継続的に監視し、探索します。これにより確実に、承認されていないデバイスの通信はブロックし、許可されたデバイスはインベントリー化し保護されます。

すべてのコネクテッドデバイスを識別し分類

Akamai Guardicore Segmentation には、統合されたデバイスフィンガープリンティング機能が含まれています。Akamai の高度なアプローチは、簡単にスプーフィングされるデバイス識別子を上回る機能を提供します。ネットワークのふるまいやその他の信号を分析し、ネットワークに接続されたあらゆるデバイスに対して、信頼度の高いフィンガープリントを開発します。識別されたデバイスは、スケーラブルで抽象的なセキュリティポリシーの作成に使用できるカテゴリに、グループ化されます。



ビジネス上のメリット

- 
 すべてのコネクテッドデバイスの探索、フィンガープリンティング、分類を実現
- 
 専門的な IoT および OT システムなども含めて、単一のインターフェースからゼロトラスト・セグメンテーション・ポリシーを実装
- 
 エージェントベースとエージェントレスのポリシー適用を組み合わせることで全体をカバー



すべてのエンタープライズ資産を同時に可視化

Akamai Guardicore Segmentation によって探索・分類された IoT および OT デバイスは、従来のエンタープライズエンドポイントやアプリケーションワークロードと共に Akamai の Guardicore Reveal マップに表示されます。これは、高度にインタラクティブで視覚的な単一のインターフェースです。これを使用するとセキュリティチームは、あらゆる種類のコネクテッドデバイスについて相互作用の状況を簡単に把握し、ホストベースとエージェントレスの実施手法を組み合わせた効果的なゼロトラスト・セグメンテーション戦略を策定できるようになります。

すべてのデバイスに細分化されたセグメンテーションポリシーを適用

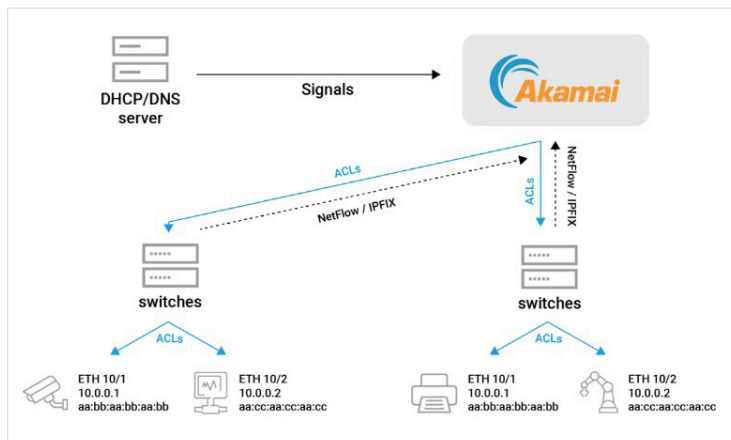
Akamai Guardicore Segmentation は、ゼロトラスト・ポリシーの適用をシームレスに拡張するために、ホストベースのセキュリティソフトウェアを実行できない IoT デバイスと OT システム用に設計されたネットワークベースのセグメンテーションを提供します。そのため、OT デバイスと IoT デバイス、およびその他のネットワークリソース間の通信を制御し、制限することが可能です。これにより、IT 管理システム、専用アップデートサーバー、およびロギングサーバーに対して必要な接続を許可しながら、安全な境界を確立できます。

デバイスが移動しても可視性と制御を維持

Akamai Guardicore Segmentation アーキテクチャは、デバイスが新しいネットワークロケーションに移動しても識別と可視性を維持します。そのため、必要なロケーションベースの適応を含め、適切なゼロトラスト・セグメンテーション・ポリシーが常に適用されます。

仕組み

ネットワークデバイスによって生成されたトラフィックは信号（DHCP、DNS、Netflow、TCP など）を提供します。Akamai Guardicore Segmentation はこうした信号を使用してすべてのデバイスを識別し、分類します。その後、統一されたインターフェースを通じてセグメンテーションポリシーを作成できます。IoT デバイスと OT デバイス、およびホストベースのエージェントを実行できないデバイスのために、セグメンテーションポリシーはネットワークレベルでのアクセス制御ルールの自動実装によって適用されます。



IoT と OT へのゼロトラストの拡張について、詳しくは当社の [Web サイト](#) をご覧ください