FORESCOUT
Active Defense for the Enterprise of Things™

OTを止めない、シンプルなゼロトラスト・セグメンテーション

高度なリスク管理と動的セグメンテーションで、拡張OTネットワークを安全に保護

OT（オペレーショナルテクノロジー）やICS（産業用制御システム）ネットワークに接続するOTデバイスを保護する際は、産業用アプリケーションをITネットワークやリモートアクセスユーザーから隔離する、という手法が長年主流でした。しかしOT運用組織が、クラウドSCADA、DCS、先進的な製造実行システム(MES)などの最新技術を駆使してインフラを最新鋭化するなか、これまでのゾーニング戦略ではOT環境の安全性を十分維持できません。

以下は、OT環境における課題の一部です。

- マルウェアや悪意のある攻撃者による攻撃の水平移動リスク、ITの境界を超えるゾーン横断的脅威、リモートユーザーによるサイバー/物理インフラとOTインフラへの影響
- サイバー/物理インフラとOTインフラに影響を及ぼすマルウェア拡散およびゾーン横断的脅威の検知・緩和
- マルチベンダー運用の弊害：拡張OT環境全体でのセグメンテーションコントロールの複雑性、および一貫性の欠如

Forescout：トップクラスのOT対応ソリューション

上記の課題が当てはまる場合は、今すぐ当社ソリューションをお試しください。異種混合のEnterprise of Things (EoT)環境におけるIT、OT、ICSデバイスのゼロトラスト・セグメンテーション簡略化、リスク管理の最適化を支援します。Forescoutプラットフォーム導入により、以下を実現できます。

「2021年までに、産業用IoT(IIoT)プロジェクトの80%*に、OT固有の要件が発生することが見込まれます（現状から40%増*）。」[1]

GARTNER社

「IoTデバイスやネットワーク対応デバイスの技術により、ネットワークとエンタープライズ環境の侵害リスクが増えました。セキュリティ部門は、ネットワーク上のあらゆるデバイスを四六時中、隔離し、安全性の確保およびコントロールを行う必要があります。」[2]

FORRESTER RESEARCH社

forescout.com/platform/eyeSegment　japan-sales@forescout.com　電話番号: 81 50-1746-6455

- IT、OTグループ全体での**ゼロトラスト・セグメンテーションを加速**
- 拡張エンタープライズ環境のあらゆる場所、あらゆる**IT/OT**デバイスの**セグメンテーション状態を**リアルタイムで**瞬時に把握**
- ユーザー、アプリケーション、サービス、機能、ロケーション、デバイス、リスクレベルの論理的な分類にもとづく**トラフィックフローの可視化**
- IT、IoT、OT環境全体での動的セグメンテーションで、**攻撃対象領域を縮小し、コンプライアンス設定を維持**
- エンタープライズ環境全体で一貫性のあるセグメンテーションポリシーを適用することで**IT/OTワークフローを最適化し**、既存資産への投資を有効活用
- **ネットワーク間のアクセスを効率的に管理し**、対応要員を減らして**コンプライアンスリスクとコストを低減**

セキュリティ/IT投資効果の拡大

- 統合セグメンテーションポリシー
- で、IT/OT融合環境のリスク（脅威の水平移動）に対処
- きめ細かいセグメンテーションポリシーの計画、監視、対応アクションにより、OTデバイスに関するリスクに対処
- 既存インフラへの投資を有効活用し、繊細なOT環境で業務の中断をする事なく動的セグメンテーションを実施

「我々の調査対象組織の20%近くが過去3年で少なくとも1件、IoTに対する攻撃を受けています。」[3]

GARTNER社

IT/OTネットワークに最適なリスク管理とゼロトラスト・セグメンテーション

Forescoutソリューションは、OTネットワークを細部にわたり可視化し、あらゆる種類のオペレーショナルリスクとサイバーリスクを効果的に、リアルタイムで管理します。拡張OT環境全体で複数ドメイン、複数ユースケースにまたがるセグメンテーションやリスク緩和の課題に対応し、業務を止めない脅威検知・対応をスピーディーに実施します。

Forescout eyeSegmentは、エンタープライズネットワーク全体のトラフィックフローをユーザー、アプリケーション、サービス、機能、ロケーション、デバイス、リスクレベルの論理的な分類に自動でマッピングし、ゼロトラスト・セグメンテーションの設計と導入展開を支援します。これにより、エージェントのデプロイやインフラの構成変更をせずに、OTトラフィックのベースラインをリアルタイムで作成できます。セグメンテーションポリシー適用前に、影響度をモデル化して評価することもできます。

Forescout eyeInspect（旧SilentDefense）は、特許取得のディープパケットインスペクション(DPI)技術および、ICS固有の脅威インジケーターを豊富に搭載したライブラリ機能で重要インフラを保護します。ネットワーク通信をリアルタイムで監視し、ネットワーク資産、プロトコル、通信内容に関する詳細コンテキスト情報を提供します。eyeInspectは、高度なアラート統合、資産のベースライン作成などの強力な機能を通じて脅威検知とコンプライアンス対応を自動化し、リスク低減とOTセグメンテーションを支援します。

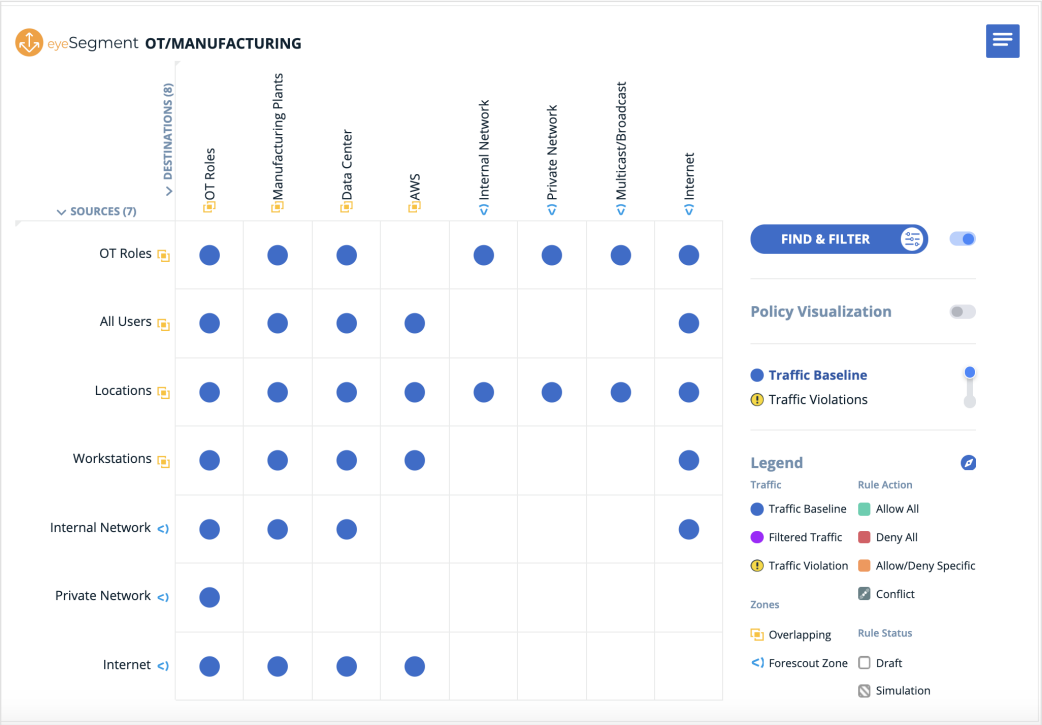

図1：eyeSegmentのマトリックスによる優先順位をもとに、エンタープライズ環境における特定のトラフィックパターンを分析・調査できるため、重要業務に集中していただけます。マトリックス階層のどこからでも、eyeSegmentから瞬時に必要なポリシーを作成できるため、対象トラフィックパターンをセグメント化し、生産システムと業務プロセスを継続しつつ、ビジネスを保護できます。

Forescoutのネットワークセグメンテーションソリューションは、多岐にわたるOTユースケースに対応します。すべてのケースに柔軟に対応し、業務中断リスクを低減し、セグメンテーションプロジェクトに関する運用コストを最小化します。以下は、主なユースケースの一例です。

- OTネットワーク全体でのリスク緩和、コンプライアンス設定の維持、運用コストの低減
- OT環境をリアルタイムで瞬時に可視化し、業務を中断する事なくセグメンテーションポリシーをモデル化
- IT/OTのゼロトラスト・セグメンテーションのスピーディーな実施

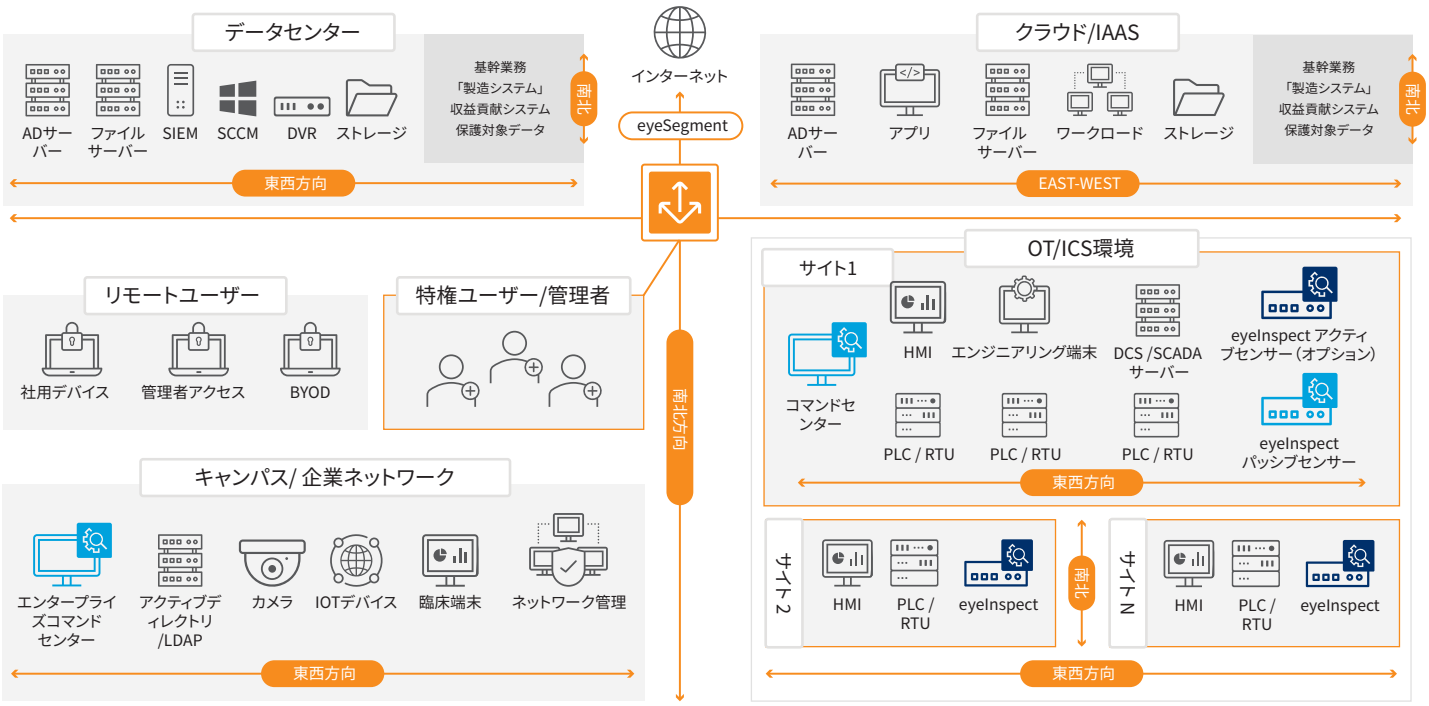

図2：Forescoutソリューションにより、脅威緩和を効率化し、セグメンテーションの状態をリアルタイムで瞬時に把握できます。上のサンプル構成では、eyeSegmentが接続デバイスを医療システムとIT/OTドメインとの間で分割しています。

1. Gartner社による2018年4月の調査「Invest Implications: Cool Vendors in Industrial IoT and OT Security」
2. Forrester Research社が 2020年6月8日に公表した調査「Mitigating Ransomware With Zero Trust」
3. Gartner社による2020年1月の調査「IoT Security Primer: Challenges and Emerging Practices」

Don’t just see it. Secure it.™

EoT(Enterprise of Things)のアクティブ防御を支援します。今すぐお問合わせください。

forescout.com/platform/eyeSegment　japan-sales@forescout.com　電話番号: 81 50-1746-6455

FORESCOUT
Active Defense for the Enterprise of Things™

〒101-0051
フォアスカウト・テクノロジ ーズ株式会社
東京都千代田区神田神保町2-11-15
住友商事神保町ビル2階

詳細はForescout.jpをご覧ください