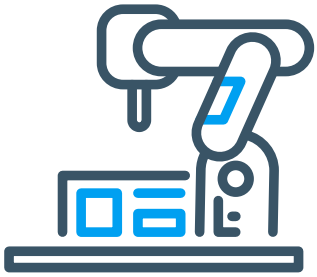


OTサイバーセキュリティ

OT/ITが融合された環境における オペレーショナルリスクと セキュリティリスクの低減

情報技術（IT）、モノのインターネット（IoT）、制御・運用技術（OT）環境の統合とデジタルトランスフォーメーションにより、これまで隔離されていたOTおよび産業用制御システム（ICS）ネットワークの複雑性や脆弱性が増しています。OT/ICS環境で稼働するデバイス資産の数が飛躍的に増加していることも、こうした変化に拍車をかけています。

これまでOTネットワークは社内のITシステムや外部サービスとの接続が遮断された「エアギャップ」環境であったため、サイバー脅威が運用に支障を来たすリスクはほぼ皆無でした。しかし今日の製造現場には、何百ものデジタルシステムや相互接続機器が存在します。これらは業務にとって有益であると同時に新たなリスクへの入り口となっています。

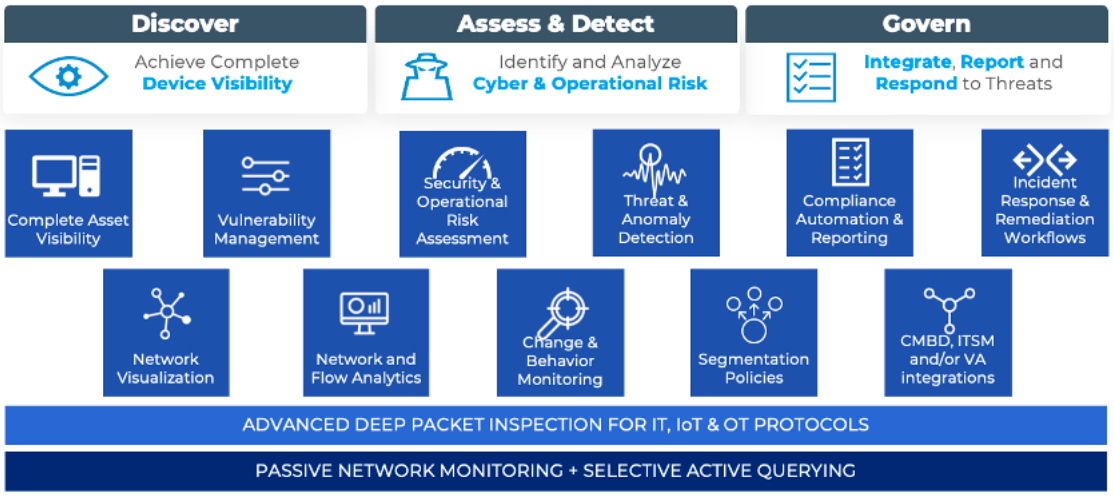
重要インフラや製造業への攻撃は大々的に報道されますが、大半のハッカーはIT/ IoTデバイスを介してネットワークに侵入してからラテラルムーブメントを行います。多くの場合、こうした事態への懸念からOTシステムの停止や遮断という措置が取られる事となります。

生産性への支障という点では、外部からの攻撃よりも、日々起こっている様々な要因（ネットワークやプロセスの設定不備、運用ミス、リソース消費の急増などの異常事態）の方がはるかに高い確率で発生しているものと思います。ネットワークが複雑化し、世界各地で優秀なセキュリティエンジニアが逼迫する今、緩和策の各ステップを洗い出して優先順位を付けたり、先手を打ってサイバーリスクを低減したりすることは困難となってきています。

産業環境においてデジタルシステムへの依存が高まる中、組織はダウンタイムを回避し、法令遵守を確保するために、資産の発見、評価、ガバナンスに関する包括的なアプローチが必要となってきています。これにより、サイバー脅威を検知し、運用やセキュリティのインシデントにつながる前に対処することが可能になります。

OT環境でデジタルトランスフォーメーションを実現するには、相乗効果を生み出す手段、つまり途切れることのないサイバーセキュリティ対策の各ステップを自動化できる総合プラットフォームが必要となってきます。

Forescoutプラットフォームは、すべてのOT、IoT、IT資産の発見、評価、ガバナンスを自動化し、サイバーリスクと運用リスクを低減します



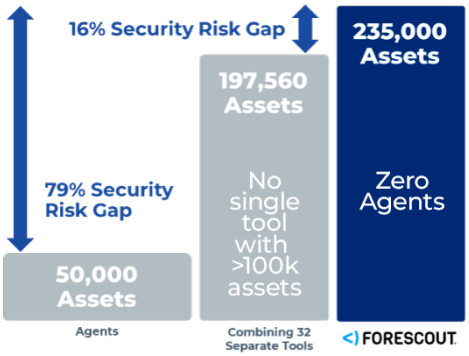
OT/ICS資産の全てを継続的に発見しインベントリを作成

盤石なセキュリティ対策の第一歩は、すべての資産がどこにあり、どのようなコンプライアンス状態であるかをリアルタイムに正確に把握することから始まります。重要インフラや製造現場のデジタル化が急速に進む一方、これらは複数の大規模拠点の敷地内に分散していることが多いため、OT/IoT/IT環境の資産の状態を正確に把握して管理することがますます困難になりつつあります。さらに産業機器は独自のプロトコルを採用し、通常のデバイスに比べて脆弱なため、単純な手法では該当する機器および関連プロセスを識別することが困難です。

OTデバイスは繊細であり、安全性に関する規則、製品の互換性、産業プロセスにおける各種要件など様々な要素を検討しなければならないため、IT/IoT環境と同様の識別手法では効果が出ない恐れがあります。とくに、OTデバイスで重要インフラを制御しているような場合、ダウンタイムやサービスの停止は許されません。そのため、業務を妨げないパッシブ方式での監視やエージェントレス方式の手法が求められます。

ForescoutはOT/ICSネットワーク全体を100%可視化し、あらゆるネットワーク上のサイバー資産を常時くまなく識別して、運用事故やセキュリティインシデントに発展する前にサイバー脅威を検知します。OTネットワーク/デバイス種別に対する詳細な資産管理と監視では、細部にわたる情報を収集するために30以上のパッシブ/アクティブ方式の識別手法を用いてデバイス名および配置場所を特定し、サイバーポスチャーの状態を判定して異常を検知します。これには、300以上のIT/OT/IoTプロトコルを網羅するディープパケットインスペクション（DPI）を活用すると同時に、OT/ ICS環境の特定エンドポイント（産業用コントローラ、ネットワークインフラなど）に対するアクティブクエリを選択的に実行し、ポートミラーリングだけでは到底実現できない精度でデバイス可視性を提供します。

Energy Company



大手エネルギー企業のお客様事例：当初の可視化範囲はエージェント搭載可能なデバイス5万台のみでした。その後32種類のセキュリティ製品を導入し、そこからの断片的な情報で20万弱のデバイスが識別されました。エージェントレス方式のForescoutを採用した結果、合計23万5千台のデバイスを特定することができ、当初のエージェント方式と比べセキュリティリスクギャップ（死角）が79%もあったことが判明すると共に、情報の一元化も図れました。

- **60万ドル以上のコスト節減（3年間での投資効果）**
- **すべてのデバイスを1週間で識別**
- **資産インベントリ作成により、5ヵ月以上の工数を削減**

Forescoutの特長

あらゆる資産をリアルタイムでくまなく発見：30以上のパッシブ/アクティブ/ハイブリッド手法を駆使してOT/ICSネットワーク全体であらゆるデバイスタイプを包括的にカバーし、ポートミラーリング機能を大幅に凌駕する可視性を実現します。

- **パッシブ監視**：300以上のOT/IoT/ITプロトコルを網羅するDPI技術で、すべてのデバイスの振る舞いを細部にわたり監視し、業務を妨げることなくOT/ICSの脆弱性を特定します。
- **アクティブクエリによるエンドポイントの発見**：OT/ICSに特化した30種類以上のアクティブクエリを実行し、OT/IoT/ITの汎用デバイスを特定して重要情報を抽出します。これにより資産インベントリに必要なデータを拡充し、手動での監査を削減します。Windows/Linux/Macエンドポイント向けに、詳細なセキュリティコンプライアンスクエリを用いて拡張可能です。
- **ネットワーク連携**：ネットワークインフラとの連携により、ネットワークに接続されたデバイスを瞬時に特定して接続場所を把握することで、効率的な資産管理を実現します。

サイバーリスクとオペレーショナルリスクを継続的に評価

個々の組織で稼働しているデバイスの種類は多岐にわたるため、リスクとコンプライアンスの状態を評価する際は様々な手法を駆使して情報を連携しながら進める必要があります。企業のセキュリティ部門は通常、数十種類ものリスク診断製品を使ってあらゆるニーズに対応しています。しかし、これらのツールを監視し、その詳細を一つの信頼できる情報源に統合しているのは誰の役目でしょうか？

Forescoutは、お客様組織のデジタル環境全体にわたるサイバー資産（繊細なOT/ICSデバイスを含む）を常時特定してリスクを緩和する唯一のプラットフォームです。このプラットフォームは既存のセキュリティツールへの投資効果を高め、それらが適切に展開され、正しく構成され、正常に機能していることを確保し、ツール間のコミュニケーションを統制します。

Forescoutでは産業制御システム（ICS）に関する脅威ライブラリを随時拡充しています。これをICS特有の侵害の痕跡（IOC）と脆弱性（CVE）のデータベースと併用することで、業務を止めずにパッシブ方式で脅威を特定し、ネットワークに接続するすべてのデバイスのリスクを評価しています。定期更新されるライブラリには、数千種類にのぼる挙動チェック項目や脅威インジケータが含まれており、資産所有者であるお客様組織を高度なサイバー攻撃、ネットワークの設定不備、運用ミスなどのリスクから保護します。

自社のセキュリティポスチャーの妥当性が証明されない限り、現実的な脅威の有無にかかわらず予期せぬダウンタイムに直面するリスクは残ります。デバイスコンプライアンスを立証できないままOTを運用している組織がサイバー攻撃を受け、内部に侵入されてしまった場合、慎重を期すためにOTシステムの遮断という予防措置を取るでしょう。しかしForescoutはお客様のデジタル環境を常時評価して修復するため、サイバーインシデント発生期間中もシステムの稼働状態を保てるという副次的メリットを享受できます。

セキュリティリスクおよびオペレーショナルリスクのスコアを活用しノイズを排除

Forescout独自のアセットリスクフレームワークは、2種類のリスクスコアをデバイスごとに算出し、サイバーセキュリティリスクとオペレーショナルリスクの両面からデバイスの状態を評価します。これらのスコアは、対象デバイスに関するイベント検知、感染が疑われるまたは不審な振る舞いを見せるデバイスとの近接性、通信リンク、既知の脆弱性などの詳細な項目にもとづくリスクレベルに応じて継続的に更新されます。Forescoutの多面的なリスクスコアは、OTエンジニアやセキュリティ担当者による意思決定および必要な措置の優先度判定に役立つ判断材料となります。

Forescoutの特長

資産の構成管理：OT資産情報の自動収集および構成変更を記録し、セキュリティ分析、規制に対する報告、運用フォレンジクスに活用します。これにより、運用の中断を回避します。

リアルタイムでの脅威検知とインシデント対応：14年以上にわたるOT/ICSの脅威リサーチが反映されたICS専用脅威指標はMITRE ATT&CK® for ICSと連携し、設定不備や運用ミスに起因する脅威から高度なサイバー攻撃まで様々な脅威を検知します。

コンプライアンス対応の簡素化：パワフルなダッシュボードおよび分析・レポート作成ツールで、NERC CIP、EU NIS Directive、NIST CSF、IEC 62443をはじめとする主要基準への準拠対応を簡素化します。

OT/ICS資産のガバナンスをプロアクティブに管理し、攻撃対象と侵害の影響を継続的に最小化

資産のガバナンスとは、迅速な緩和や修復に必要なオプションを数多く取り揃えるだけでなく、利用可能なあらゆるインテリジェンスを駆使して適切なオプションを使用すべきかを把握することが求められます。ワークフローの自動化によるチケットの作成や、OTエンジニアへの設定ミスの確認などは、あまり厳格度が高くないオプションです。より厳格なオプションとしては、修復の自動実行、ネットワークアクセス制御、動的セグメンテーション、複数製品にまたがるオーケストレーションなどが含まれます。

脆弱性が発覚すると通常は、最初の修復手段としてパッチを適用します。しかしミッションクリティカルなOTデバイスは、その性質上パッチ適用が困難であることは周知の事実です。パッチを適用するにはシステムを停止してから再起動しなければならないためダウンタイムが発生します。高炉設備など、安全上の理由で素早く停止できないプロセスや設備もあります。パッチ適用に代わる一般的な修復手段は、脆弱なOTデバイスをネットワーク上の他の領域から隔離し、望ましくない振る舞いが発生しないかどうかを監視することです。

Forescoutは、SIEM/SOCにおけるインシデントレスポンスや動的セグメンテーションなどのワークフローを自動対応し、高リスクなネットワークを保護すると共に、ミッションクリティカルな制御・運用機器のオンライン接続状態を維持します。自動対応はForescoutプラットフォームが直接、または相互連携先の外部セキュリティツールが実行します。Forescoutを介して既存のセキュリティエコシステムを相互接続させることで、縦割り状態で稼働する個別ソリューションの効果を高めることが可能です。

ダウンタイムゼロ？可能です。

運用上のダウンタイムや業務の中断が発生すると、たちまち安全性や売上に影響が及んでしまいます。Forescoutは、厳格度が中程度～高レベルまでの緩和措置を柔軟に適用するため、OT/ICSシステムに脆弱性が存在する場合でもセキュリティを確保しながら稼働を継続できます。

Forescoutの特長

製品同士の連携：ITSM、SIEM、テレメトリシステム、ファイアウォール、認証サーバーなど、複数のIT/セキュリティ製品にまたがる情報を共有し、ワークフローを自動化することで、デジタル環境全体の状態をより正確に把握できます。

ネットワークアクセス制御：重要資産へのアクセス許可に先立ち、外部技術者やリモート勤務社員のデバイスが社内ネットワークに接続した時点でセキュリティポスチャーを検証します。

拡張性：デプロイ形態を柔軟に選択できます。既存のネットワークインフラ、SIEM/SOC、資産管理ツール、各種セキュリティツールともシームレスに連携可能です。

FORESCOUT

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com