FORESCOUT

eyeInspect

OTおよびICS環境におけるリスクを低減し、コンプライアンスを自動化し、脅威分析を最適化

エージェントレス
30以上のアクティブ/パッシブな検出手法により、接続されたすべてのOTおよびICSデバイスを統合した資産インベントリをリアルタイムで取得

正確性
何千種類ものOT固有の脅威インジケータと強力な異常検知機能を組み合わせてネットワークを保護

有効性
プロアクティブなリスク評価・脅威検出により、ビジネスへの影響を測定し、緩和策の優先順位を迅速に決定

効率性
時間のかかるコンプライアンス評価とリスク評価を自動化し、人的ミスを最小限に抑えて効率を改善

Forescout eyeInspectは、OT/ICSネットワークデバイスを細部詳細に可視化し、オペレーショナルリスクとサイバーリスクを効果的かつリアルタイムで管理します。

- 資産リスクフレームワークにより、OTネットワークのサイバーレジリエンスを包括的に把握
- 270を超える産業ネットワークプロトコルのディープパケットインスペクションと資産のベースラインによってデバイスを完全に可視化
- 何千種類ものOT固有の脅威インジケータと強力な異常検知機能を組み合わせてネットワークを保護

可視化
全体をカバーするためにSPANに依存することなく包括的かつパッシブにデバイスを可視化

270以上のITおよびOTプロトコルに対して特許取得済みディープパケットインスペクション(DPI)を実施

検知
セキュリティ分析およびオペレーショナルフォレンジック調査のためにOT資産情報を包括的に収集し、すべての構成変更を記録

アラート調査および対応ツールを使用して脅威の検知、封じ込め、修復を自動化

対応
NERC CIP、EU NIS指令、NIST CSF、IEC 62443、TSA Pipeline Securityなどの主要な標準に対応できるようコンプライアンス対応を簡素化

ダッシュボードによりユーザーのコラボレーションを強化し、アラートの詳細情報によって効率的なインシデント対応を支援

eyeInspectが解決する問題

- **OTの可視性ギャップ**
  各地に散在する異種混合デバイスのネットワークによって発生する
- **防御または脆弱性の課題**
  パッチ適用漏れや脆弱なアプリケーションの放置が原因
- **オペレーショナル/サイバーリスク**
  アラートの過負荷や緩和策の優先順位の設定ミスによって発生する
- **不完全な脅威インテリジェンス**
  ポリシーによる防御を妨げる
- **コンプライアンス対応タスク**
  多くのリソースを使用し、違反した場合に多額の罰金を払うリスクがある

可視化

何千台ものデバイスを単一画面に表示

- 正確なリアルタイムの資産インベントリを、業務を中断することなくパッシブに取得
- HMI、SCADA、PLC、ビル管理システム（BMS）、ビル自動化システム（BAS）などのIP対応のシリアル接続された資産を可視化
- アラートの優先順位を付け、時刻、デバイス、ネットワークロケーション、アラートの種類などの各種パラメータに応じてログを表示

検知

インテリジェントに脅威を検知し、リスクを管理

- 数千種類におよぶICS/OT固有の脅威チェックやIoC（侵害の痕跡）を使用して、既知または未知のサイバー脅威を検知
- サイバーリスクやオペレーショナルリスクを検知し、緊急度やビジネスへの潜在的影響に応じて優先順位付けを実施
- 準拠していない資産やポリシーをネットワーク全体で検知
- 新しいデバイス、インフラの変更、通常とは異なる操作など、ネットワークに対する変更をリアルタイムで検知

対応

最もインテリジェントで拡張性に優れたOTセキュリティソリューションによる対応

- 直感的に理解できるリスクスコアを活用してサイバー脅威/オペレーション上の脅威に対応し、対応の決定を簡素化
- ワークフロー、ルール、修復アクションの自動化により、脅威の発生と同時にリアルタイムでの対応が可能
- 資産ベースラインが定義されたルール、パラメータ、レポートに基づいてコンプライアンスの変更に対応

Enterprise Command Centerの導入条件

	最小要件
ハードウェア/ハイパーバイザー	19インチのラックサーバーまたはVMware ESXi 5の最小構成
プロセッサー	64ビット、2.4GHz以上の4コア(Intel®)CPU
メモリ容量	16～32GB
ハードドライブ	250GB超
ネットワークインターフェース	Command Center通信およびWebアプリケーションアクセス用インターフェース

Command Centerの導入条件

(*) eyeSightライセンスのみの場合のメモリ容量

	小規模デプロイ (センサー5台まで)	中規模デプロイ (10台まで)	大規模デプロイ (11～100台まで)
ハイパーバイザー	VMware ESXi5の最小構成		
フォームファクター	19インチのラックサーバーまたは仮想アプライアンス		
プロセッサー	64ビット、4コアCPU	64ビット、4/6コア (Intel) CPU	64ビット、12コア (Intel) CPU
メモリ容量	16(*)～64GB	32(*)～64GB	64～256GB
ハードドライブ	500GB	1TB	1TB超
	(データ保持期間:90日を想定)		
ネットワークインターフェース	センサー通信およびWebアプリケーションアクセス用インターフェース		

パッシブセンサーの導入条件

	小規模デプロイ (センサー5台まで)	中規模デプロイ (10台まで)	大規模デプロイ (11～100台まで)
ハードウェアモデル(例)	Foxguard® IADIN-FS1	Dell® Embedded PC 5000	Dell® PowerEdge R640
デプロイ内容	過酷な環境に対応する 小規模ネットワーク	過酷な環境に対応する 中規模ネットワーク	大規模ネットワーク、 データセンターの設置
フォームファクター	産業用PC(小型)/DINレール取り付け	産業用PC(中型)	19インチ、1Uラックサーバー
プロセッサー	64ビット、2/4コア(Intel) CPU	64ビット、4/6コア(Intel) CPU、8 GT/s	64ビット2.4GHz以上の6コア(Intel) CPU
メモリ容量	8～16GB	16～32GB	64～256GB
ハードドライブ	64～500GBの産業用PC(広温度域対応のSSD搭載)		
監視インターフェース	最大4つの監視ポート	最大8つの監視ポート	最大8つの監視ポート

Active Sensorの導入条件

パッシブセンサーとの統合
eyeInspectはパッシブセンサーに直接統合できます（小規模、中規模、大規模すべてのデプロイ）

	スタンドアロン	仮想
プロセッサー	2～4コアCPU	vCPU x 4
メモリ容量	RAM (4GB)	RAM (4GB)
ネットワークインターフェース	1枚以上	1枚以上

ハードウェア要件の詳細については、こちらをご覧ください：
https://www.forescout.com/company/resources/command-center-and-sensor-hardware-guidelines/

プロトコル

汎用的OT/ITシステムおよび個別仕様のOTシステムに対応するプロトコル一覧は、
こちらのリンクからご確認いただけます：
https://www.forescout.com/company/resources/eyeinspect-protocols/

オーケストレーション、セグメンテーション、コントロール

Forescoutプラットフォームは、資産管理、デバイスコンプライアンス、ネットワークアクセス、ネットワークセグメンテーション、インシデント対応に関するポリシーの設計および導入、アクションの自動化といった一連の機能により、eyeInspectの価値を拡大します。

Forescoutプラットフォームの詳細については、www.forescout.com/platform/をご参照ください。

FORESCOUT

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
詳細はこちら：Forescout.com