FORESCOUT
Active Defense for the Enterprise of Things™

eyeInspect
(旧SilentDefense)

エージェントレス

IP接続デバイスやシリアルデバイスをすべて統合したOT資産インベントリをリアルタイムで取得

正確な検知

何千種類ものOT固有の脅威インジケーターと機械学習による高度な異常検知機能を組み合わせて資産ベースラインを作成し、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見極め、緩和策の優先順位を決定

信頼性

セキュリティツールやコンプライアンス統制が機能していることをリアルタイムで保証

効率性

時間のかかるコンプライアンス対応や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

産業用制御システム(ICS)とOT環境におけるリスク低減、コンプライアンスの自動化、脅威分析の最適化

Forescout eyeInspectは、OTネットワークデバイス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かつリアルタイムで管理します。

- 数千種類ものICS/OT固有の脅威インジケーターやクエリーをもとに、許容可能なネットワークの挙動ベースラインを設定
- 何千件ものアラート、何百万件ものログをリスクレベルや原因別に統合
- デバイスの自動分類・評価によるポリシー/規制準拠

可視化

ネットワーク接続と同時にデバイスを可視化

デバイスの出入りを継続的に監視

業務を止めずにリアルタイムの資産インベントリを取得

検知

多種多様なIP対応のシリアルOTデバイスを識別

デバイスとデバイスグループのベースラインを作成

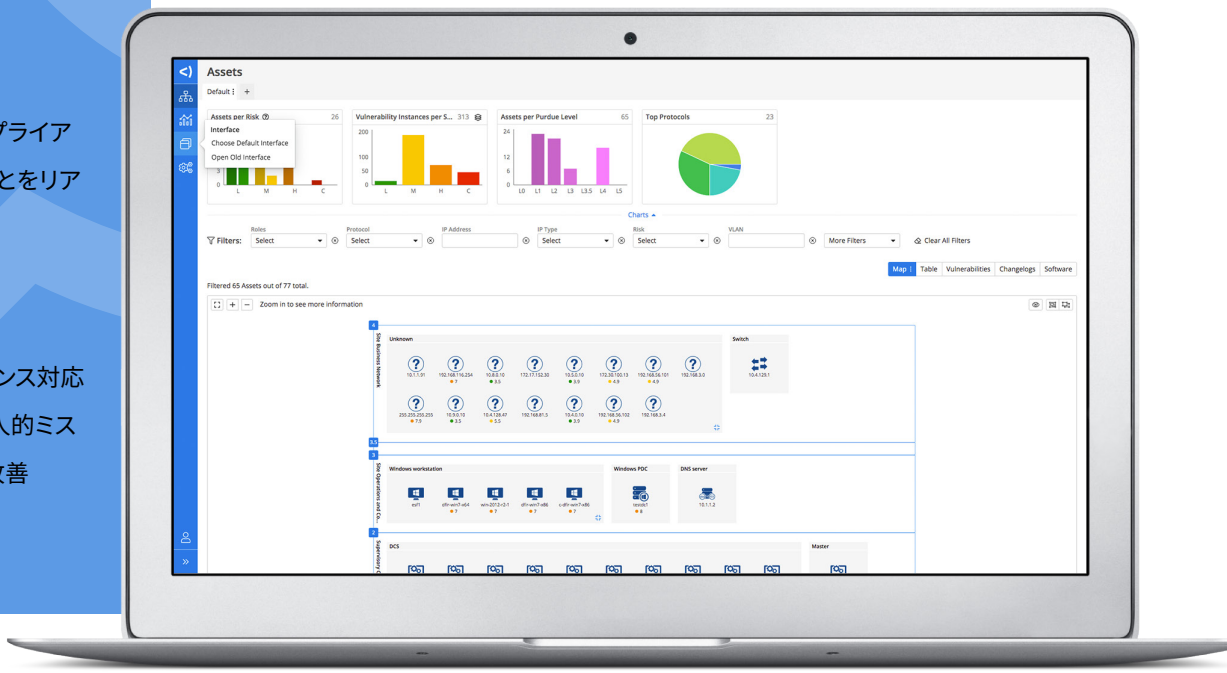
自動分類と継続監視の効率を最大化

対応

コンプライアンス評価の自動化

直感的なスコアによるリスク評価

サイバーリスク、オペレーショナルリスクの状況認識



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

可視化

何千台ものデバイスを単一画面に表示

- 追加接続されたデバイスや不正デバイスを見逃さず、あらゆるものをくまなく可視化
- 正確で詳細な資産インベントリをリアルタイムで取得
- HMI、SCADA、PLC、コントローラー、センサー、メーター、I/OなどのIP対応シリアルデバイスの可視化

検知

インテリジェンスにもとづく脅威検知、リスク管理

- 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）をもとに、既知/未知のサイバー脅威を検知
- 検知したサイバーリスクやオペレーショナルリスクを、緊急度やビジネスへの潜在的影響をもとに優先順位付け
- 準拠違反のデバイスやポリシーをネットワーク全体で検知
- ネットワーク上の変更点（新規デバイス、インフラの変更、通常と異なる操作など）を検知

対応

世界で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

- 明確なスコアに従い、サイバー脅威/オペレーション上の脅威に対応
- 事前定義されたワークフロー、ルール、緩和アクションを自動実行し、アラートに対応
- 資産ベースラインが定義されたルール、パラメータ、レポートをもとに、コンプライアンスの変更内容に対応
- HVAC（空調管理）やアクセス管理をはじめとするビル管理システム(BMS)やビルオートメーションシステム(BAS)のデバイスを可視化
- スイッチ、ルーター、VPS、無線アクセスポイント、コントローラーなど、上記以外の物理インフラやSDNインフラを可視化
- 時間、デバイス、ネットワークロケーション、アラートタイプなどの各種パラメータをもとにアラートやログを可視化

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12コア (intel®) CPU
メモリ容量	32～64ギガバイト
ハードドライブ	500ギガバイト～1テラバイト、シン・プロビジョニング
ネットワークインターフェース	Command Center通信用およびWebアプリケーションアクセス用インターフェース

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

Command Center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台～100台まで）
ハイパーバイザー	VMware ESXi5最小構成		
フォームファクター	19インチ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、2.4 GHz以上の12コア (intel) CPU
メモリ容量	16ギガバイト	32ギガバイト	64～256ギガバイト
ハードドライブ	500ギガバイト	1テラバイト	1テラバイト超
	（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	センサー通信用および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必要条件

	小規模デプロイ（100 Mbpsまで）	中規模デプロイ（500 Mbpsまで）	大規模デプロイ（ 1 Gbps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	過酷環境に対応する小規模ネットワーク	過酷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インチラックサーバー
プロセッサー	64ビット 2または4コア (Intel®) CPU	64ビット 4または6コア (Intel®) CPU　速度：8 GT/s	2.4GHz以上の64ビット 6コア (Intel®) CPU
メモリ容量	4～16ギガバイト	16～32ギガバイト	64～256ギガバイト
ハードドライブ	64～500ギガバイトの産業用PC　（広温度仕様の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

アクティブセンサーの最小要件

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

	単体	仮想環境
プロセッサー	2～4コアCPU	vCPU×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

ハードウェアの詳細条件はこちらをご参照ください：
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では、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/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/実施および自動実行を担う様々な製品をラインナップしています。eyeInspectとForescoutプラットフォームをこれらと組み合わせることで、相乗効果を実現します。

当社のeyeSight、eyeSegment、eyeControl、eyeManage、eyeExtend製品の詳細は、https://forescout.jp/ をご参照ください。

eyeInspectが解決する問題:

散在する異種混合のデバイスネットワークによる**OTの可視性ギャップ**

パッチ対応の不備や、脆弱なアプリの放置による**防御と脆弱性の課題**

アラートの過負荷や緩和策の優先順位ミスによる**オペレーショナル/サイバーリスク**

ポリシーによる防御対応を妨げる**不完全な脅威インテリジェンス**

リソース集約的かつ、違反した場合に多額の罰金リスクにさらされる**コンプライアンス対応タスク**

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/eyeInspect　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