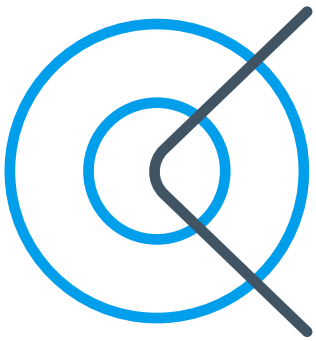
FORESCOUT



eyeSight

接続デバイスの現状をデジタル環境全体で正確に把握

エージェントレス
セキュリティポスチャーやリスクポスチャーを含む、ネットワークに接続されたデバイスをリアルタイムで一元的に把握することができます。

正確性
あらゆるデバイスを分類して、プロアクティブなセキュリティポリシーとコンプライアンスポリシーを作成するためのコンテキストを取得

有効性
コンプライアンスポスチャーやサイバーリスクエクスポージャーの測定、レポートの作成といった定型タスクを自動化し、人的ミスを最小限に抑制

効率性
セキュリティツールやコンプライアンスコントロールが適切に機能していることをリアルタイムに確認

Forescout eyeSightは、ネットワーク機器との連携により、すべての接続デバイスに対する卓越したインサイトを提供します。

- 30種類以上のアクティブ/パッシブ手法によって包括的な資産インベントリを取得し、デジタル環境全体にわたりカバレッジギャップを明らかにすることで、攻撃対象領域をリアルタイムに可視化
- デバイスの分類を自動化するとともに、弊社のセキュリティー調査部門であるVedere Labs提供の脅威インテリジェンスにより既知のリスクや脆弱性などの包括的なプロファイルを作成
- 新興脅威に対しては、クラウドベースの機械学習を活用してForescout Device Cloud（300億以上の個別のデータポイントを有するForescout独自のデバイスインテリジェンスソース）を継続的に増強することで対応
- エージェントをインストールせずに、デバイスのステータス、リスクポスチャー、ポリシーコンプライアンスを継続的に評価（IoT/IoMT/OTデバイスの保護に不可欠な機能）
- コンプライアンスポスチャーやサイバーリスクエクスポージャーのレポート作成を自動化することで、人的ミスを最小限に抑え、重要課題の対応に時間をさくことが可能に

検出
ネットワークに接続されたデバイスを即時に認識
デバイスの一時的な接続と切断を継続的に監視
資産インベントリをリアルタイムに取得し可視性のギャップを明確化

分類
さまざまな種類のIT/IoT/IoMT/OTデバイスを識別
Device Cloudを活用してデバイスコンテキストを包括的に把握
自動分類の有効性、カバレッジ、スピードを向上

評価
セキュリティエクスポージャーとコンプライアンスギャップを特定
内部規則と外部規制の遵守状況を評価
サイバーリスクとオペレーショナルリスクの状況を把握

eyeSightが解決する問題

- **可視性ギャップ**
  チームのサイロ化や
  セキュリティツールの乱立による
- **オペレーショナルリスク**
  ミスが起こりやすい手作業
- **不完全なデバイス インテリジェンス**
  セキュリティポリシーの適用を
  阻害する
- **セキュリティーギャップ**
  エージェントベースのツールが
  更新されていなかったり、
  機能していない
- **検出不可能な不正デバイス**
  MACスプーフィングなど
- **コンプライアンス違反**
  定期的なスキャンの隙間を
  狙ったように発生する

検出

リアルタイムの詳細な検出

デジタル環境のあらゆる面を完全に可視化することで、死角をなくしリスクを最小化します。

- スイッチ、ルーター、無線アクセスポイント、コントローラーなどの物理／SDNインフラ
- ラップトップ、タブレット、スマートフォン、BYOD/ゲストシステム、在宅勤務用デバイス
- キャンパスネットワーク、データセンター、支店、リモートサイト、エッジネットワークのIoTデバイス
- Amazon Web Services/Microsoft Azure/VMware環境のパブリック／プライベートクラウドインスタンス
- HMI、SCADA、PLC、ビル管理システム（BMS）、ビル自動化システム（BAS）などのオペレーショナルテクノロジー（OT）システムや産業コントロールシステム
- 輸液ポンプ、診断装置など、病院や医療提供ネットワーク（HDO）のIoMTデバイス

環境に合わせた検出／監視手法のカスタマイズ

有線、無線、VPN、仮想/SDNのすべてにわたり、30種類以上のアクティブ/パッシブ監視手法を柔軟に活用することで、アクティブスキャンの影響を受けやすいデバイスの停止等を回避します。

インフラに対するアクティブ監視手法

ネットワークインフラポーリング

SDN統合
- Meraki
- Cisco ACI

パブリック／プライベートクラウド統合
- VMware
- AWS
- Azure

ディレクトリサービスのクエリ（LDAP）
Webアプリケーションのクエリ（REST）
データベースのクエリ（SQL）
eyeExtendオーケストレーション

資産に対するパッシブ監視手法

SNMPトラップ

SPANトラフィックFlow分析
- NetFlow
- Flexible NetFlow
- IPFIX
- sFlow

DHCPリクエスト
HTTPユーザーエージェント
TCPフィンガープリント
プロトコル解析
RADIUSリクエスト

資産に対するアクティブ監視手法

エージェントレスWindowsインスペクション
- WMI
- RPC
- SMB

エージェントレスmacOS/Linuxインスペクション
- SSH

NMAP
SNMPリクエスト
HTTPリクエスト
Forescout SecureConnector®

分類

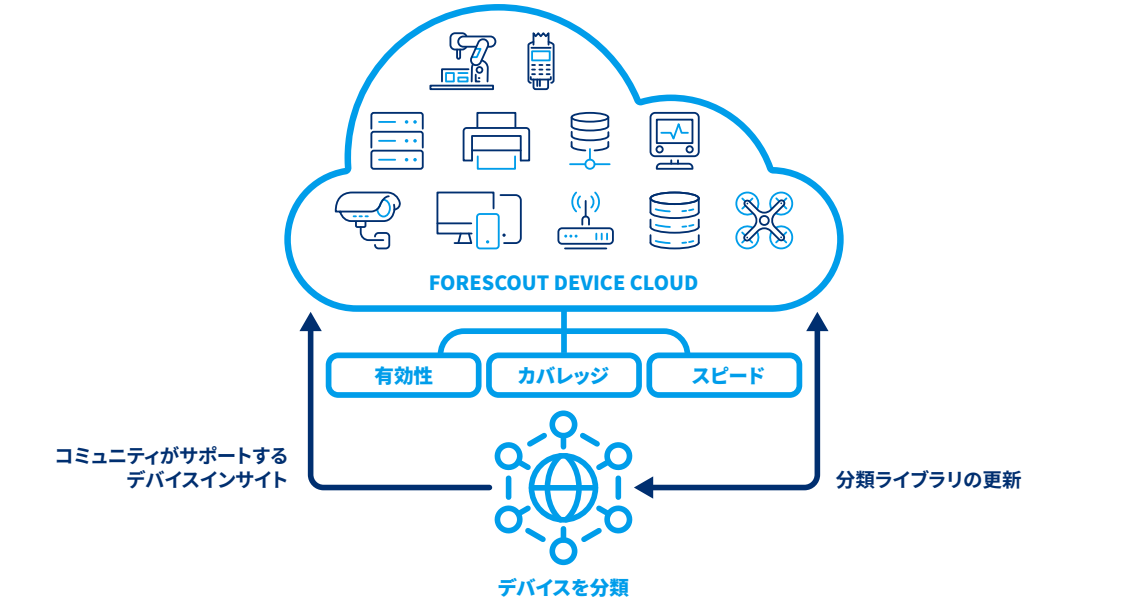
インテリジェントな自動分類

包括的なデバイスコンテキストがない状態でセキュリティポリシーを実装すると、望ましくない結果を招いて業務を危険にさらす可能性があります。Forescout独自のDevice Cloudは、5,000万台以上のデバイスから収集したデバイスインテリジェンスの世界最大規模のリポジトリであり、あらゆる接続デバイスについて包括的なコンテキストを自動的に提供します。Forescoutの多次元分類法により、デバイスの機能と種類、オペレーティングシステムとバージョン、ベンダーとモデルを特定できます。特定可能な対象は以下のとおりです。

- 1,900種類以上のオペレーティングシステムバージョン
- 7,700種類以上のデバイスのベンダーとモデル
- 400社以上の大手医療機器メーカーの医療機器
- 製造、エネルギー、石油・ガス、公共事業、鉱業などの重要なインフラ業界で使用されている、何千種類もの産業用制御システムおよびオートメーションデバイス

Forescout Device Cloudを活用した自動分類

資産インテリジェンスの世界最大規模のデータベースであるDevice Cloudを活用すれば、あらゆる組織の資産リスクを極めて包括的かつ正確に把握できます。



機能	オペレーティングシステム	ベンダーとモデル
> タブレット > 無線AP > プリンター > VoIPサーバー > PoSレジ > X線機器 > HVACシステム	> Windows > Windows Server > OS X > iOS > CentOS > Android	> Apple iPad > Apple iPhone > Apple AirMac > 3M Control System > GE Water Processor > Hitachi Power System > Hoana Medical

評価

エージェントレスのポスチャー評価

eyeSightはデバイスの検出を継続的に行い、設定、ポスチャー、リスク指標を即時に評価することで、そのデバイスがコンプライアンス要件やセキュリティポリシーに準拠しているかどうかを把握します。ポリシーにより以下のようなコンプライアンス状況を評価することで、リスクをより適切に定量化できます。

- セキュリティソフトウェアがインストールされ、適切に機能し、最新のパッチで更新されているか？
- ビジネスを運用するために重要なデバイスか？
- 非承認アプリケーションを実行している、または設定基準を満たしていないデバイスはないか？
- デフォルトまたは脆弱なパスワードを使用しているデバイス（特にIoT、IoMT、OTのシステム）はないか？
- 正規のデバイスに偽装したものなど、不正なデバイスは検出されていないか？
- 最新の脅威に対して特に脆弱な接続デバイスはないか？

監視

コンプライアンスに関するインサイトの提供

直ぐに利用可能なダッシュボードからは、実用的なインサイトが得られ、デジタル環境全体におけるリスクの特定、優先順位付け、プロアクティブな緩和を行えます。ダッシュボードはカスタマイズが可能で、セキュリティアナリストやSOCチームを以下の機能でサポートします。

- ポリシーの全体または一部について、リスクとコンプライアンスの改善状況を評価
- 脆弱なデバイスや侵害されたデバイスを特定し、焦点を絞ったインシデント対応を迅速化
- コンプライアンス状況の経時変化を追跡
- リスクとコンプライアンスに関するデータを、経営陣や監査役向けにパーソナライズして共有が可能
- ポリシーや属性による資産の迅速な検索/フィルタリング

セグメンテーション、オーケストレーション、エンフォースメント

Forescoutプラットフォームは各種サイバーセキュリティ機能の自動化によりeyeSightの価値をさらに高めネットワークアクセスコントロール、動的ネットワークセグメンテーション、ゼロトラストセキュリティの基盤を可能性にします。

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

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