Forescout eyeSight

各デバイスを常時発見、分類、評価することで、状況を把握してリスクを軽減する

CIOは、増加するネットワークに接続されたシステムの安全性、特にIoTデバイスやOTデバイスの安全性を確保する責任を負っています。このデバイス数（種類）の急増により、ネットワークに接続されたすべての物理デバイスと仮想デバイスの可視化を求める切迫感が業界内で強まってきています。なぜならば、見えないものを守ることはできない™からです。こうしたデバイスには、従業員、請負業者、顧客、さらには善意の運用スタッフによって接続されたマネージドデバイス、アンマネージドデバイス、不明なデバイスなどがあります。また、これらのデバイスがネットワーク上のどこにあろうとも、すなわちキャンパス、データセンター、プライベートクラウド、パブリッククラウド、さらにはOT/ICSのいずれの環境にあろうとも、それらを適切に検出、プロファイリング、把握する必要があります。

拡張エンタープライズ全体でデバイス可視化

図1キャンパス、IoT、データセンター、クラウド、運用技術(OT)の全体で詳細な可視化を実現

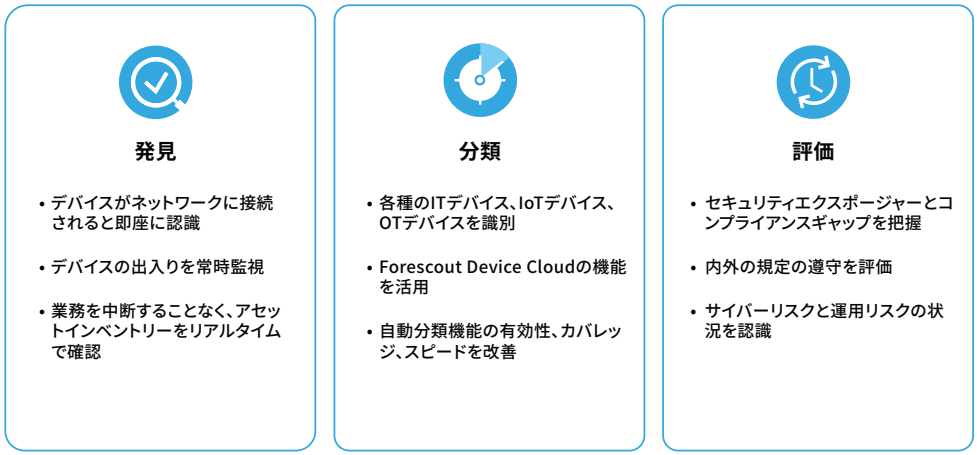
Forescout eyeSightを利用すれば、クリティカルな業務プロセスを中断することなく、デバイス状況全体に関する比類ないインサイトを得ることができます。Forescout eyeSightは、まず拡張エンタープライズネットワーク上にあるあらゆるIP接続デバイスを発見します。しかし、デバイスの発見は、完全な可視化への単なる最初のステップに過ぎません。適切なポリシーを作成し決定をコントロールするには、包括的なコンテキストが不可欠です。接続デバイスを発見した後、次にeyeSightは、こうしたデバイスを自動分類してから組織のポリシーに照らして評価します。これら3つの機能、すなわち発見、分類、評価の強力な組み合わせにより、必要なデバイス可視化を実現し、適切なポリシーとアクションを推進することができます。

eyeSight

特長

- ネットワークに接続されたデバイスの一元化されたリアルタイムインベントリーをエージェントレスで実現
- デバイスを正確にプロファイリングし、プロアクティブなセキュリティとコンプライアンスポリシーを構築するために必要なコンテキストを獲得
- 不正なデバイス、脆弱なデバイス、非準拠デバイスを特定および、それらからのリスクを限定するためのポリシーを構築
- 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働いていることをリアルタイムで確認
- 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を効率的に測定して報告
- 共通タスクの自動化によりヒューマンエラーを最小限に抑え、効率性を向上

図2eyeSightで利用できる必須の可視化機能



デバイスを常時、エージェントレスで発見

IoTデバイスやOTデバイスを起因とする、可視性に関する独特の課題が生じています。こうしたデバイスは膨大な数にのぼるため、規模を原因とする課題が生じます。なぜなら、手動によるデバイスの発見が現実的にもはや不可能だからです。さらに、これらデバイスの多くは、エージェントがサポートされておらず、また、システムや業務の中断を引き起す可能性のあるアクティブプロービングやスキャン技術の影響を受けやすくなっています。全部で20を超えるアクティブおよびパッシブ監視技術（図3を参照）を活用しているeyeSightを利用することで、以下のデバイスが自動的に発見され、想定しうる可視性ギャップを回避することができます

- キャンパスネットワーク上のラップトップ、タブレット、スマートフォン、BYOD/ゲストシステム、IoTデバイス
- データセンター内の仮想マシン、ハイパーバイザー、物理サーバー
- パブリッククラウドとプライベートクラウド上のAWS、Azure、VMwareのインスタンス
- 運用技術（OT）ネットワーク上の医療用、産業用、および建設用オートメーションデバイス
- 物理ネットワークインフラおよびソフトウェア定義ネットワークインフラ（スイッチ、ルーター、VPN、無線アクセスポイント、コントローラーなど）

こうした各発見機能の組み合わせにより、オペレーションリスクを最小化し、可視化できないブラインドスポットをなくします。その結果、拡張エンタープライズ全体における包括的かつ持続的なデバイスインベントリーを構築できます。

図3アクティブおよびパッシブ発見技術

インフラスを対象とするパッシブ技術	エンドデバイスを対象とするパッシブ技術	エンドデバイスを対象とするアクティブ技術
SNMP トラップ	ネットワークインフラポーリング	エージェントレスでのWindowsの検査 • WMI • RPC • SMB
SPANトラフィック	SDN統合 • Meraki • Cisco ACI	エージェントレスでのmacOSおよびLinuxの検査 • SSH
フロー解析 • NetFlow • NetFlow flessibile • IPFIX • sFlow	パブリック/プライベートクラウド統合 • VMware • AWS • Azure	NMAP
DHCPリクエスト	ディレクトリサービスの照会（LDAP）	SNMPクエリ
HTTPユーザーエージェント	ウェブアプリケーションの照会（REST）	HTTPクエリ
TCPフィンガープリンティング	データベースの照会（SQL）	SecureConnector®
プロトコル解析	eyeExtendオーケストレーション	
RADIUSリクエスト		

課題

- サイロ化されたチーム、セキュリティツール、およびプロセスが原因となり、可視性ギャップが生じている
- エラーを誘発する人手作業が原因となり、運用リスクと事業リスクが生じている
- デバイスインテリジェンスが不完全であるため、防御できるポリシーを構築するためのコンテキストを、ITにほとんど提供できない
- セキュリティツールがインストール、設定され、適切に動作しているかどうかを検証することができない
- 検出されない不正なデバイスによって、無用なセキュリティリスクやコンプライアンスリスクが生じている
- 旧式のポイントインタイムスキャンがコンプライアンスポスチャーにおける信頼性の欠如をもたらしている

インテリジェントな自動分類

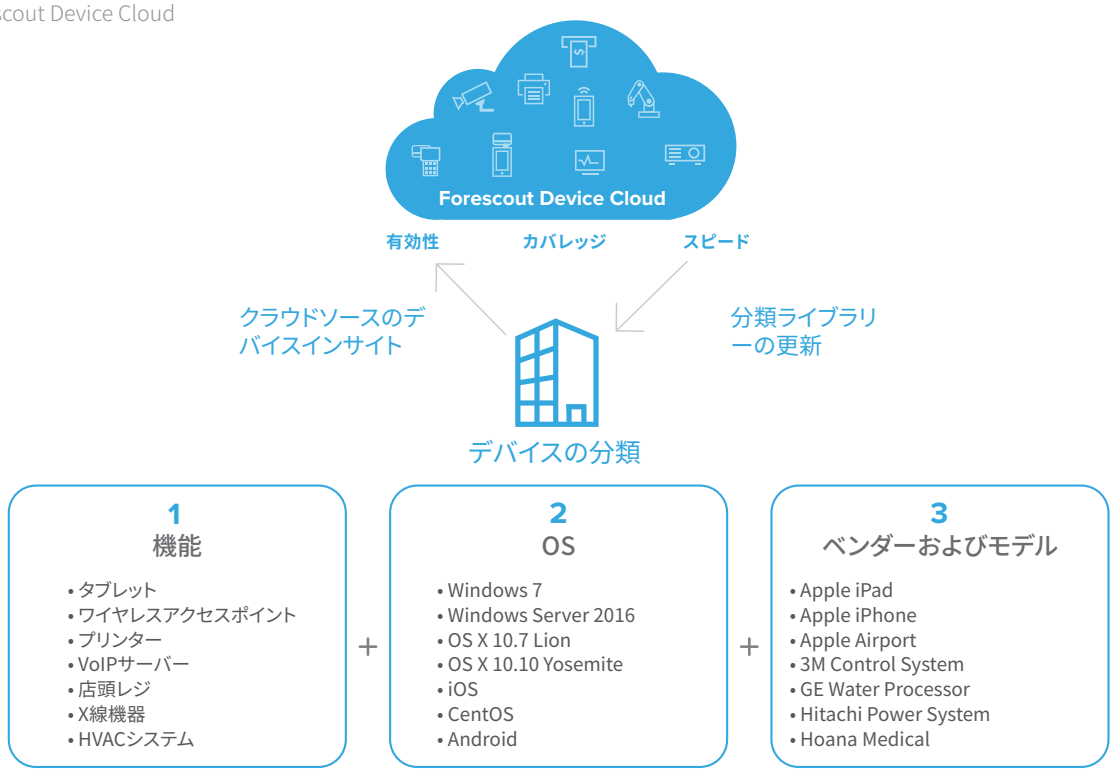
緻密なポリシーを作成するには、すべてのデバイスの完全なコンテキストを獲得することが重要です。デバイスごとに最適な保護方法と管理方法を決定するには、そのデバイスの運用上のコンテキストと目的を把握する必要があります。デバイスが増加、多様化したことにより、こうしたコンテキストを人手で収集するのはほぼ不可能であり、また、適切なコンテキストなしでポリシーを作成すれば、業務をリスクにさらすことになります。eyeSightは、多次元分類法を利用してデバイスの機能と種類、OSとバージョン、ベンダーとモデルを特定することにより、従来のIoTデバイスやOTデバイスを自動分類します。合計100以上のITプロトコルとOTプロトコルに対してディープパケットインスペクションを実施することにより、IoTデバイスやOTデバイスの種類についての詳細なインサイトを獲得します。

eyeSightは以下のものを自動分類します

- 500以上の各OSバージョン
- 5,000以上のデバイスベンダーおよびデバイスモデル
- 350以上の主要医療テクノロジーベンダーのヘルスケアデバイス
- 製造、エネルギー、石油・ガス、公共事業、鉱業等の各重要インフラ産業で利用されている何千もの産業用コントロールデバイスと自動化デバイス

Forescout Device Cloud によってeyeSightの自動分類機能が充実します。そのため、この充実したコンテキストソースは、デバイスの増加とその多様性のスピードに対応できるものになります。Forescout Researchでは、当社デバイスクラウド*内にある800万台以上の実世界デバイスからのインテリジェンスを活用し、新たなプロファイルを頻繁に発表することにより、お客様のデバイス状況全体における分類の有効性、カバレッジ、スピードを改善しています。

図4Forescout Device Cloud



デバイスポスチャーの評価

デバイスを分類することにより、デバイス機能に関する運用上のコンテキストを得ることができます。すなわち、そのデバイスが何であるのかがわかります。しかし、完全なコンテキストを得るには、各デバイスの健全性やウイルス予防策を測定するための別の視点が必要です。

eyeSightは、ネットワークを常時監視し、接続された機器の設定、状態、セキュリティポスチャーを評価することにより、そのデバイスのリスクプロファイルを確認するとともに、そのデバイスがセキュリティおよび規制に関するコンプライアンスポリシーに準拠しているかどうかを判定します。eyeSightは以下のような重要項目を判定します。

- セキュリティソフトウェアが、インストールされているか、動作しているか、最新のパッチよって更新されているかどうか。
- 無許可のアプリケーションを実行しているデバイス、または設定基準に違反しているデバイスがあるかどうか。
- デバイスでデフォルトパスワードや脆弱パスワード（IoTデバイス特有のリスク）が使用されているかどうか。
- 不正なデバイス（なりすまし技術によって正規デバイスを偽装しているものを含む）が検出されたかどうか（また、こうしたデバイスがネットワークに接続されているかどうか）。
- コネクテッドデバイスのうち、最近の脅威に対して特に脆弱なものはどれか。

デバイスインテリジェンスの力

eyeSightによる発見、プロファイリング、自動分類、評価によって実現されたデバイスの可視化は、Forescoutコンソールに即座にわかりすく表示されます。これにより、カスタマイズ可能なダッシュボード上で概略的なインサイトを確認し、リスクとコンプライアンスに関する目標に向かって業務を進めながら、進捗状況のスナップショットを共有することができます。これらの動的ビューによって、チームは以下のことを実施できます。

- 特定のポリシーがどの程度うまく実装されたのかを評価する
- 違反があった場合、脆弱なデバイスを特定してインシデント対応を迅速化する
- 特定のコンプライアンス要件への遵守状況を経時的に追跡する
- リスク、コンプライアンスに加え、潜在的脆弱性についての、エグゼクティブや監査人向けのビューを作成する
- 特定のポリシー、デバイスタイプ、ロケーション等に関係するトラブルシューティングの問題点について掘り下げて調べる

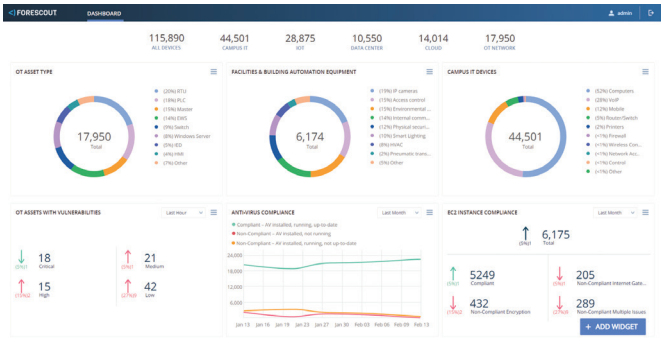


図5複数の関係者に必要なコンテキストを提供できるようダッシュボードをカスタマイズ

また、eyeSightによるデバイス可視性は、通知アクションやAPIを介し、各部門のIT関係者間で共有することもできます。eyeExtendの製品群は、このデバイスコンテキストを他の主要なIT製品およびセキュリティ製品と共有しており、これによりワークフローを自動化し、システム全体のレスポンスをオーケストレーションします。

eyeSightから得られるクリティカルなデバイスコンテキストがなければ、企業はコントロールポリシーを確信をもって実装することができないでしょう。なぜならば、不十分なデバイスインテリジェンスに基づいてアクションを実施すると、業務運営をリスクにさらす恐れがあるからです。

eyeSightを利用することにより、緻密なポリシーを作成、実装するために必要な詳細なインサイトを得ることができます。また、アセット管理、デバイスコンプライアンス、ネットワークアクセス、ネットワークのセグメント化、インシデント対応開始のアクションを自動化するための詳細なインサイトも得られます。その後、Forescout eyeControl製品とForescout eyeExtend製品を利用して、ポリシーベースの効果的なコントロールと、アクションのオーケストレーションを確信をもって実現できます。

詳細については、Forescout.comをご覧ください

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