Forescout eyeManage

Forescoutのデプロイメントを拡張エンタープライズ全体で一元管理

Forescoutプラットフォームは、拡張エンタープライズ全体でデバイスの可視性とコントロールのワークフローを促進、最適化します。カバー範囲が広くスケール性に優れ、あらゆるデプロイにワンストップで対応する一元管理コンソールにより、異なる管理ツール間の切り替えが不要になります。Forescout eyeManageは、ネットワーク全体に分散したForescoutのアプライアンスと通信し、デバイスインテリジェンスを収集し、Forescoutの管理下にあるすべてのコネクテッドデバイスを監視できる単一画面を提供します。

eyeManageから各デバイスをコントロールし、リスクとコンプライアンスに関するインサイトを各部門のステークホルダーと共有し、ポリシーの作成や適用を管理することができます。(オンプレミスまたはAWS・Azureクラウド上に)物理または仮想アプライアンスとしてデプロイされるeyeManageはアウトオブバンドでインストールされるため、遅延やネットワーク障害に関する問題を回避できます。また、Forescout eyeRecoverのフェールオーバー/リカバリーオプションを使って、ビジネスクリティカルなアプリケーションの可用性が確保できます。

eyeManage

ポリシーの定義 コンテキストに応じたポリシーを作成してリスクを最小化	**コントロールの実行** 各アクションを自動化または開始してリスクを管理	**ダッシュボードの共有** リスクとコンプライアンスに関するインサイトを部内または経営層と共有
インベントリーの表示 ネットワークに接続されたすべてのデバイスを表示	**ライセンスの管理** ライセンスの配布、ソフトウェア更新の管理	**デプロイメントの設定** Forescoutデプロイメントのプロビジョニング/設定

図1:Forescoutのデプロイメントと運用全体を一元管理

eyeManage

課題

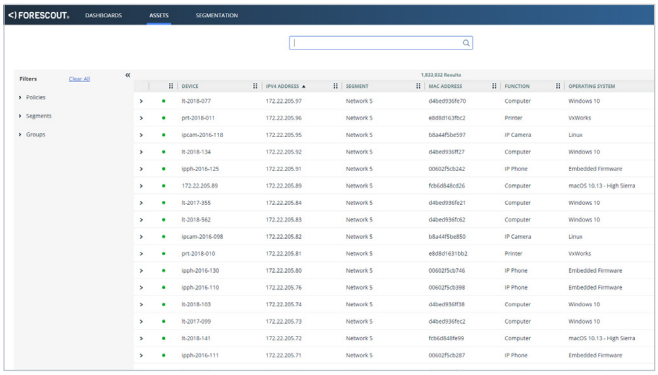
- キャンパス、データセンター、クラウド、IoT、OT間のデバイスインベントリーを一元化
- 一元的アセットビューによる検索・ドリルダウン機能
- IP割り当て、ソフトウェア更新、バックアップを自動化
- 新たなアプライアンスをゼロタッチでプロビジョニングできるため、デプロイメントを簡単に拡張可能
- 事前設定済ダッシュボードにより、可視性・コンプライアンスの進捗状況を経営層とタイムリーに共有
- デバイスポスチャーのリアルタイムスナップショットによって、セキュリティ業務を支援
- デプロイ先のロケーションを問わず、200万デバイスまで対応
- ライセンス管理を拡張エンタープライズ全体で一元化

一元化されたデバイス管理

eyeManageはアプライアンス管理だけでなく、デバイス管理用の中央コンソールの役割（アセットインベントリー情報の検証、セキュリティポリシーの作成/管理、ネイティブコントロールアクションの実行など）も担います。また、Forescout eyeExtend製品経由で外部セキュリティ/IT管理製品とも連携できるため、ネットワークやエンドポイントコントロールをオーケストレーションするためのセントラルハブとしてもお使いいただけます。

アセットインベントリー 各種プロセス、サービス、脆弱性、オープンポート、ログイン中ユーザーなどすべてのリアルタイムアクティビティをインベントリー内で簡単に確認できます。eyeManageをお使いいただくと、ネットワークアクティビティの追跡、コンプライアンス違反の発見、ポリシー作成を精緻化するためのインサイトを得られます。Forescout eyeSightの検出・分類・評価機能によって収集されたデバイスデータをアセットビューに表示し、以下の対応にお役立ていただけます。

- セキュリティ担当者がスイッチポートを迅速に特定/シャットダウンすることで、脅威を排除
- デバイスのメンテナンス時に、IT担当者が対象ユーザーを特定し、連絡
- ヘルプデスク担当者がIPアドレスまたはMACアドレス、およびスイッチポートをリアルタイムでデバイスにリンク



ポリシー管理 eyeManageのPolicy Managerでは、インベントリーに関するインサイトをすぐに利用できるため、詳細かつ緻密なポリシーを作成して事業を保護することができます。ポリシーテンプレートをご利用いただくと、以下の要領でこれらの対応を促進できます。

✓ 分類に基づいてネットワークデバイスを検出
✓ 社内デバイス、ゲスト用デバイス、無許可デバイスを検出
✓ コンプライアンスの状況把握、修復アクションのガイダンス
✓ ネットワークに対する脅威を検出し、修復
✓ 無許可の変更を追跡、特定

セキュリティコントロールの実行 ネットワークは、新たなデバイスタイプ、ソフトウェア、構成、コンプライアンス要件の追加や、脅威の進化によって絶えず変化しています。動的なポリシーを適用することで、ネットワークや接続デバイスの最新状況を常に反映したコントロールが可能となります。セキュリティ部門はeyeManageを使用し、コントロールアクションを必要に応じて自ら開始、または一部アクションを自動実行する、などを設定できます。

ユーザーに対する制限適用と教育	トラフィックの制御
アプリケーションのコントロールと修復	ネットワーク制限
OSのコントロールと修復	デバイスコントロール

図2: アクションの自動実行/管理者による実行を選択可能

セキュリティとIT管理の統合 eyeExtend製品のアドオンにより、さらに多くのコントロールアクションをeyeManageからオーケストレーションすることができます。例えば、eyeExtend for Palo Alto Networks®、またはeyeExtend for Splunk®の追加により、これらの製品が提供する情報をポリシーやコントロールアクションに反映できます。Forescoutプラットフォームが提供する情報を当該eyeExtend製品に確実にフィードバックする「双方向型の統合」による情報共有により、セキュリティ上の問題を迅速に解決し、IT プロセスを効率化することができます。

モニタリングおよびリスクに関するインサイト

堅牢なポリシー作成にあたり緻密なデータを必要とするセキュリティアーキテクトにとって、詳細なビューは不可欠です。しかし経営層にとっては、これらの詳細を積み上げた全体像を取締役会/監査人/顧客に示し、規制への準拠状況を報告したり、新たに発覚した脆弱性によるリスクレベルを文書化することが重要な仕事です。同様に、ネットワークをモニタリングするSOCチームも、コネクテッドデバイスの最新状況にいち早くアクセスし、セキュリティを常時徹底する必要があります。eyeManageはForescoutプラットフォームのデータを拡充し、経営層やセキュリティ部門の迅速な対応を支援するインサイトを提供します。

リスクおよびコンプライアンスに関するインサイトを可視化 事前設定済ダッシュボード（可視性およびデバイスコンプライアンス画面）により、拡張エンタープライズ全体におけるコンプライアンスやセキュリティ状態などのデバイス状況のサマリーを提供します。コンプライアンス目標への進捗状況を示す「スナップショット」を、透明性の向上や経営層への安心材料として経営層や監査人と共有することができます。セキュリティオペレーション部門の平均応答時間を短縮できるよう、ビューをカスタマイズすることもできます。アセット管理部門であれば、分散したネットワークや拠点全体のインベントリーをリアルタイムで表示するダッシュボードを作成することもできます。

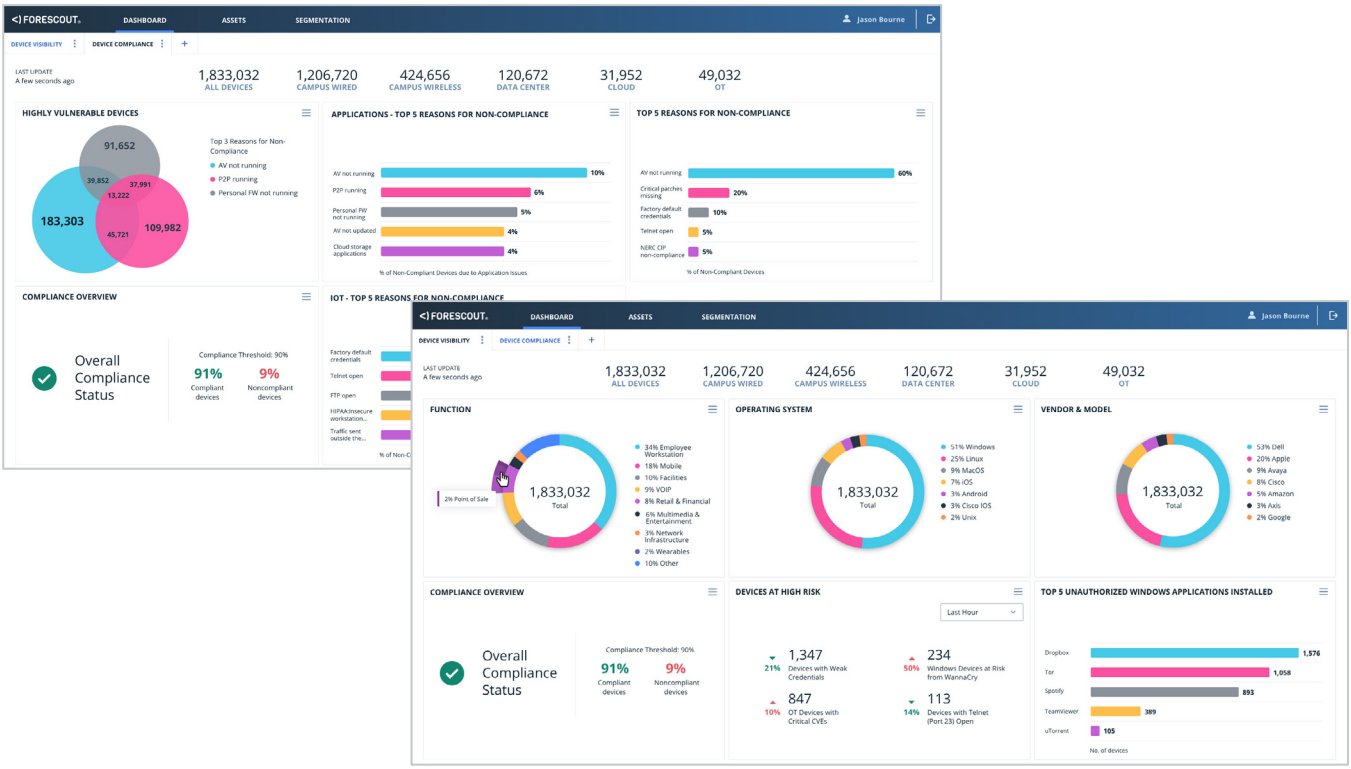


図3:デバイスの可視性/コンプライアンスをリアルタイムで提供するダッシュボードにより、拡張エンタープライズ全体でのセキュリティ状態を見える化

レポート作成の一元化 ダッシュボードでは充実したサマリーが表示されますが、ネットワーク管理者、経営層、ヘルプデスク、ITやセキュリティ部門などに完全な情報を共有するには、さらなる詳細が必要なこともあります。eyeManageは、ポリシー、デバイスコンプライアンスの状態、脆弱性、デバイスの詳細、ネットワークゲストに関する現状およびトレンド情報を反映したレポートを提供します。これらのレポートは閲覧、定期配信、保存が可能なため、一貫性のあるレポートを自動作成できます。お客様のOSがサポートしているどの言語でもレポート作成ができ、作成されたレポートはPDFやCSVの形式で保存できます。

大規模デプロイメントの管理

eyeManageは、デバイス状況とForescoutデプロイメントの管理を単一システムに統合します。スケール性、パフォーマンス、デプロイメントの柔軟性、ライセンス管理機能が充実しているため、大規模で複雑なエンタープライズ環境の厳格な要件を充足できます。

- **200万台のデバイスまで対応** デバイス状況全体を可視化するため、企業にはスケーラブルなプラットフォームが必要です。eyeManageは、柔軟性のある管理機能とデプロイメントアーキテクチャを備えており、物理環境、仮想環境、クラウド環境、およびそれらの混合環境にわたる200万台以上のデバイスで、アクティブなカスタマーデプロイメントを行うことができます。

- **仮想アプライアンスのデプロイメント** eyeManageを仮想アプライアンスとしてデプロイすることにより、特に分散化したリモートサイトにおいて、製品の配布やデプロイメントを簡素化、迅速化できます。eyeManageをVMware®、Hyper-V、またはKVMのシステム上にデプロイすることができます。仮想アプライアンスをAWSやAzureにデプロイし、オンプレミスのフットプリントをさらに縮小することもできます。

- **ワンタッチのプロビジョニングおよび拡張** Forescoutのアプライアンス設定は、セットアップ時に一括実行し、Forescoutデプロイメント全体にプッシュすることができます。また、1回のキーストロークによる一括更新で、設定をすべてのForescoutアプライアンスに複製できます。新たに追加されたアプライアンスは、自動的に既存の設定を継承します。

- **インテリジェントなIP検出および割り当て** マルチアプライアンスクラスター全体でのIP割り当ておよび管理を自動化し、アプライアンス単位でのIP範囲設定に伴う管理オーバーヘッドを削減します。

- **アプライアンスの一元管理** eyeManageでは、ソフトウェア更新ファイルをダウンロードし、お客様のスケジュールに従ってインストールすることができます。バックアップのスケジュール設定およびアプライアンスのリストア実行にも対応可能です。Forescoutのデプロイメントライセンスは、eyeManage経由で割り当て、最適化します。

- **障害復旧** 自動フェールオーバーとデプロイメント回復機能をForescout eyeRecover経由で利用できます。これにより、単一サイトまたはマルチサイト内のForescoutデプロイメントでのサービス継続性が確保されます。eyeRecoverでは、専用のアクティブ/スタンバイ・アプライアンスペアの選択、またはアクティブアプライアンスのフェールオーバークラスター（障害が発生した1つ以上のノード、クラスターまたはサイト全体からワークロードをインテリジェントに再割当て可能）を選択することができます。管理はeyeManageのコンソールから行います。

フォアスカウト・テクノロジーズ
株式会社

〒101-0051 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.com をご覧ください