

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

このForescoutのプラットフォームによって、デバイスの可視性とコントロールのワークフローを、拡張エンタープライズ全体で促進、最適化することができます。このような広がり、とスケールを有し、デプロイメントのあらゆる面を管理する単一の一元管理コンソールがあれば、複数の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、ポリシーの作成と実施の両方を管理することができます。物理アプライアンス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が回避されます。Forescout eyeRecoverによるフェールオーバーやリカバリ方法により、この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されます。



<p>ポリシーの定義</p> <p>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</p>	<p>コントロールの実行</p> <p>各アクションを自動化または開始してリスクを管理</p>	<p>ダッシュボードの共有</p> <p>リスクとコンプライアンスに関するインサイトを同僚やエグゼクティブと共有</p>
<p>インベントリ表示</p> <p>拡張エンタープライズに接続されたすべてのデバイスを表示</p>	<p>ライセンスの管理</p> <p>ライセンスの配布、ソフトウェアアップグレードの管理</p>	<p>デプロイメントの設定</p> <p>Forescoutのデプロイメントをプロビジョニング、設定</p>

図1Forescoutのデプロイメントと運用の全体を一元管理



eyeManage

特長

- < 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を一元化
- < マップ、検索、ドリルダウンの各種方法を備えたデバイスビューから選択
- < 管理IPの分散、ソフトウェアアップグレード、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
- < リスクに関するダッシュボードとレポートを作成し、進捗状況をエグゼクティブと共有
- < 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
- < デプロイされている場所を問わず、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

アプライアンスの管理に加え、eyeManageはデバイスを管理するための中央コンソールとしても働きます。こうした管理機能には、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と管理、ネイティブコントロールアクションの実行などがあります。また、Forescout eyeExtend製品が追加されたことで、eyeManageは他のセキュリティおよびIT管理製品と通信を行い、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でもあります。

アセットインベントリー。各プロセス、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を利用することで、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、ポリシー作成の向上に役立つインサイトを発見できます。Forescout eyeSightの発見機能、分類機能、評価機能によって収集されたデバイスデータは、リストやマップで、あるいはアセットポータルを利用した検索によって表示できます。これにより、以下のことが可能になります。

- セキュリティスタッフがスイッチポートをすばやく探し出し、シャットダウンする
- デバイスのメンテナンスが必要になったとき、IT人員がユーザーを探し出して連絡を取る
- ヘルプデスクスタッフが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させる

ポリシー管理。eyeManageのPolicy Managerでは、インベントリーからの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お客様の事業を保護することができます。そのプロセスを促進するために、ポリシーテンプレートを利用すると以下のことができます。

- ✓ 分類に基づいてネットワークデバイスを検出する
- ✓ 社内デバイス、ゲストのデバイス、無許可デバイスを検出する
- ✓ コンプライアンスを理解し、修復アクションを指導する
- ✓ ネットワークに対する脅威を検出して修復する
- ✓ 無許可の変更を追跡、特定する

モニタリングとリスクインサイト

堅牢なポリシーを構築するために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、ネットワークをモニタリングするSOCチームも、現行のセキュリティを確保するため、コネクテッドデバイスの現況への迅速なアクセスが必要です。同様に重要なこととして、エグゼクティブチームは、規制の遵守状況を取締役会、監査人、顧客に示すことや、最近見つかった脆弱性によるリスクレベルを文書化することが必要です。eyeManageはForescoutのプラットフォームからのデータを収集し、迅速に対応するために必要な知見をチームに提供します。

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が加わることによって、また、進化していく脅威の状況によって絶えず変化しています。コントロールは、動的なポリシーによって、ネットワークおよびそこに接続されたデバイスの現況を常に反映したものになります。セキュリティチームは、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すること、または選択したアクションを自動的に実行するよう選択することができます。

ユーザーに対する制限適用と教育	トラフィックコントロール
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: アクションは自動化または管理者による実行が可能

セキュリティの統合とIT管理の統合。eyeExtend製品を追加すると、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®を追加することにより、これらの製品が共有している情報をポリシーやコントロールアクションに反映させることができます。双方向の統合によって、eyeManageはForescoutのプラットフォームからの情報がこれらのeyeExtend製品に返送されるようにすることができます。こうした情報共有によって、セキュリティ上の問題を迅速に解決し、ITプロセスを効率化できます。

リスクインサイトの可視化。カスタマイズ可能なダッシュボードは、拡張エンタープライズ全体におけるセキュリティ状態やリスクポスターなどのデバイス状況のサマリーを提供します。セキュリティオペレーションチームの平均応答時間短縮のためにビューをカスタマイズすることもできます。

また、ダッシュボードはコンプライアンス目標への進捗状況のスナップショットを提供します。このスナップショットは、透明性の向上やリーダーシップの信頼を目的としてエグゼクティブチームおよび監査人と共有することができます。アセット管理チームは、ダッシュボードを利用して、分散したネットワークや拠点全体のインベントリーの記録をつけることができます。

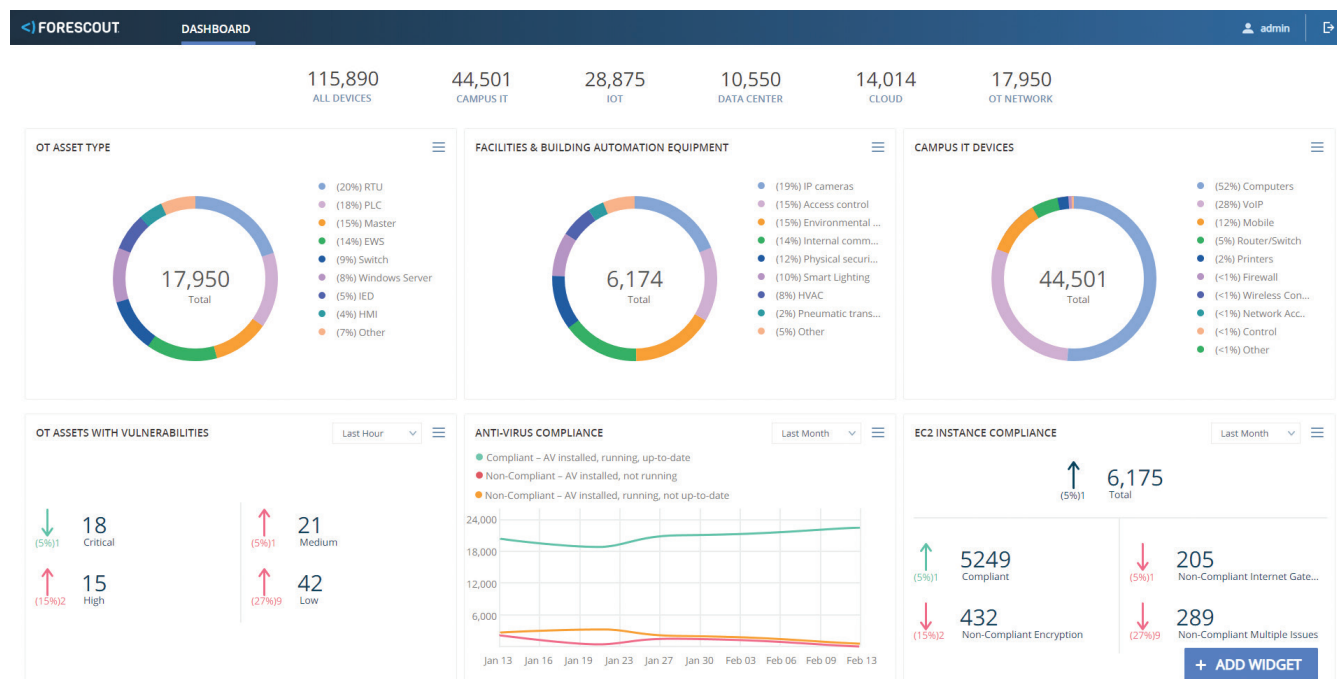


図3: カスタマイズ可能なダッシュボードでは、拡張エンタープライズ全体でのセキュリティ状態やリスクポスターの可視化が可能

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、エグゼクティブ、ヘルプデスク、ITチーム、セキュリティチーム等に完全に情報が行き渡るには、さらに詳細が必要なことがよくあります。eyeManagel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在情報およびトレンド情報が記載されたレポートを提供します。各レポートは、閲覧、スケジュール設定、保存ができ、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言語で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。

広範囲に及ぶデプロイメント管理

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。eyeManage内における規模、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は、大規模で複合的なエンタープライズ環境の厳格な要件を満たしています。

- 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、特に分散化したり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。
- ワンタッチのプロビジョニングおよび拡張。** Forescoutのアプライアンスの設定は、セットアップ時に一元的に行って、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で更新をまとめて適用し、設定をすべてのForescoutアプライアンスにレプリケートすることができます。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引き継ぎます。
- インテリジェントな、IPの検出および配布。** マルチアプライアンスクラスター全体でのIP管理の配布を自動化し、個々のアプライアンスに対するIP範囲の割当て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、ソフトウェアアップグレード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。また、バックアップのスケジュール設定とアプライアンスのリストア開始もできます。さらに、Forescoutのデプロイメントに関連するライセンスは、eyeManageによって割当てられ、最適化されます。
- 障害復旧。** Forescout eyeRecoverを通じて、自動フェールオーバーとデプロイメント回復機能を利用することができます。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のペアの選択、または障害が発生した1つ以上のノード、クラスター、サイト全体からのワークロードのインテリジェントな再割当てに対応した、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。

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

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. は、デラウェア州法人です。当社の商標および特許のリストについては、www.forescout.com/company/legal/intellectual-property-patents-trademarks をご覧ください。他のブランド、製品、サービス名は、それぞれの所有者の商標またはサービスマークである可能性があります。バージョン05_19