Forescout eyeSegment

大規模なネットワークのセグメント化を、確信的に設計、構築、デプロイする

Forescout eyeSegmentは、拡大するエンタープライズ全体における動的ネットワークのセグメント化の設計、計画、デプロイを加速させます。コンテキストを認識したセグメント化ポリシーを作成するプロセスを簡略化し、ポリシーの可視化とシミュレーションを実行してから、プロアクティブな微調整と検証を実施できます。

eyeSegmentは、Forescoutプラットフォームの機能を拡張して、マルチドメイン、マルチユースケースのセグメント化の課題に対応します。これにより組織は、モノのインターネット (IoT) デバイスや運用技術 (OT) を含むすべてのIP接続システムにゼロトラストの原則を採用できます。その結果、拡大するエンタープライズ全体でセグメント化プロジェクトを急速に加速させ、攻撃対象領域を縮小し、横方向の伝播と拡大範囲も制限し、規制、コンプライアンス、ビジネスリスクを軽減します。

課題

- セグメント化プロジェクトを進める自信がない
- フラットネットワーク全体で脅威が横方向に移動する可能性に起因する漏えいのリスク
- デバイス、アプリケーション、およびユーザーに関する不完全なコンテキスト
- ポリシーの無秩序化と、さまざまなテクノロジー全体のコントロールを一貫して実施できない
- ネットワークドメイン全体のセグメント化コントロールにおけるマルチベンダーの運用の複雑さと不整合
- 拡張エンタープライズ全体でネットワークのセグメント化を効果的に設計、構築、デプロイするためのスキルやリソース、ツールが不足している

eyeSegment

特長

- 自信を持ってネットワークセグメント化プロジェクトを促進
- ポリシーの影響を事前に判断し、ビジネスの中断を最小限に抑制
- 業務中断のリスクを軽減
- 単一のポリシーフレームワークを介して、多様な実施テクノロジーとネットワークドメイン全体でコントロールを均一に実施
- コンプライアンスおよび規制要件への適応
- セグメント化プロジェクトの運用の複雑さを軽減
- ゼロトラストアプローチを有効にし、きめ細かなセキュリティコントロールを実装

ハイライト

- ユーザー、アプリ、サービス、デバイスの論理的なビジネス分類を使用して、コンテキスト対応のセグメント化ポリシーを作成
- セグメント化ポリシーを適用する前に、影響をすばやく学習
- セグメント化のハイジーンを継続的に監視、検証
- 拡張エンタープライズ全体のセグメント化ポリシー違反に迅速に対応

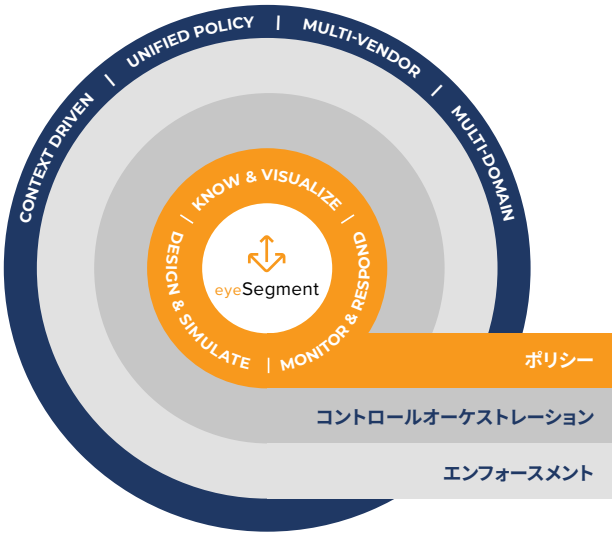

図1: Forescoutは、eyeSegmentを活用した「ポリシーレイヤー」から始める、3層のアーキテクチャをによるエンタープライズ全体のネットワークのセグメンテーションをベストプラクティスとして推奨している

エンタープライズ全体のネットワークのセグメント化を改革

Forescout eyeSegmentは、Forescout eyeSightが提供する包括的なデバイス可視性と詳細なリアルタイムコンテキストに基づいています。ユーザー、アプリケーション、サービス、デバイス間のトラフィックフローと依存関係を可視化し、それからポリシーを設計、シミュレーション、監視して、環境への影響を把握します。Forescout eyeControlおよびeyeExtendを活用して、キャンパス、データセンター、クラウドネットワークの複数のセグメント化エンフォースメントポイントにわたって、ポリシーが調整されます。eyeSegmentは、エンタープライズが大規模ネットワークのセグメント化を確信的に設計、構築、デプロイし、エンタープライズ全体のネットワークのセグメント化を可能にするのに役立ちます。

トラフィックフローを把握して可視化する

Forescout eyeSegmentは、エージェントをデプロイすることなく、エンタープライズネットワーク全体のユーザー、アプリケーション、サービス、およびデバイスの論理分類にトラフィックフローを自動的にマッピングします。これにより、ネットワークトラフィックをリアルタイムで監視し、コンテキストに対応したきめ細かいセグメント化ポリシーを作成できます。典型的なユースケースは、財務部門の従業員のみが異なるドメイン間で実行されているペイメントアプリケーションにアクセスできるようにコントロールを設計することです。もう1つは、レガシーオペレーティングシステムを備えた医療機器に必要な共通サービスを決定し、それらを分離することです。

eyeSegment接続マトリックス機能 (図2) は、トラフィックフローを可視化するのに役立ちます。トラフィックベースラインを作成し、トラフィックデータを長期にわたって維持し、セグメント化ポリシーで定義されているソースゾーンと宛先ゾーン間のリアルタイムフローを表示します。

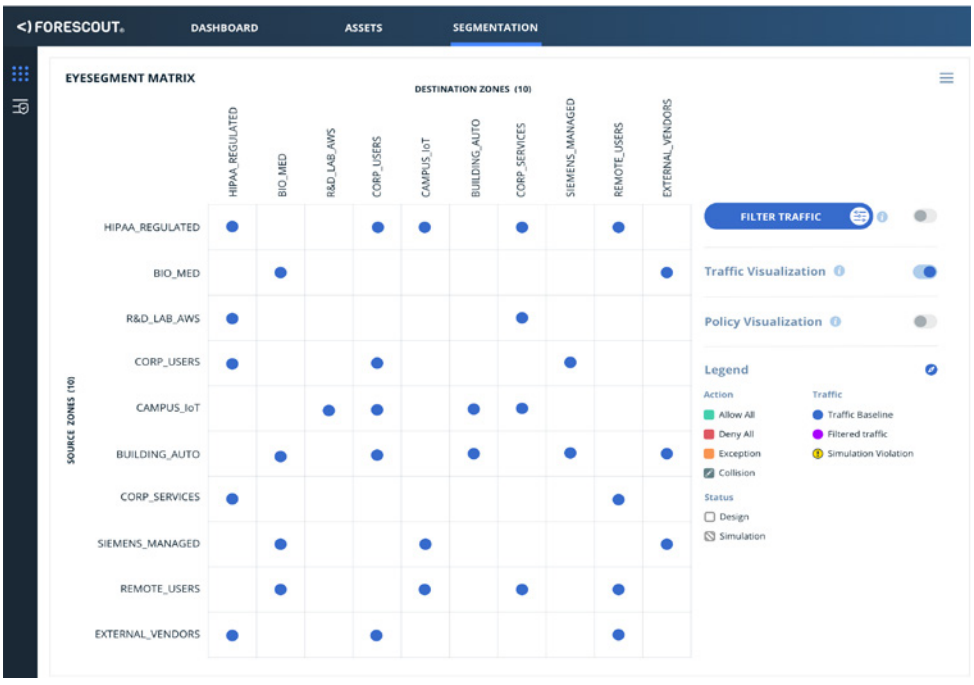

図2: 論理的なビジネストラフィックフローを示すeyeSegment接続マトリックスビュー

セグメント化ポリシーの設計とシミュレーション

Forescout eyeSegmentは、既存の基盤となるテクノロジー全体に適用できる論理的なビジネス分類に基づいて、効果的なセグメント化ポリシーを設計、作成、微調整するのに役立ちます。お客様の環境でポリシーを有効にする前に、ポリシーの実装をプロアクティブにシミュレートして、業務中断の可能性を最小限に抑えます。

統合されたきめ細かなセグメント化ポリシーを構築する

セグメント化ポリシーは、特定のソースゾーンと宛先ゾーン間のすべてのトラフィックを許可もしくは拒否する、または特定のトラフィックのみを許可するルールのセットです。ゾーンは、手動またはポリシーを介して入力できる標準ポリシーグループに基づいています。グループである単一のIPアドレスとForescoutセグメントオブジェクトもゾーンにすることができます。各セグメント化ゾーンは、ソースゾーン、宛先ゾーン、またはその両方として指定できます。

単一のコンソールからセグメント化ポリシーを作成して、さまざまなテクノロジーやネットワークドメインにわたる特定のトラフィックを拒否または明示的に許可できます。各ポリシーは、特定のソースゾーンから特定の宛先ゾーンへのトラフィックに適用できます。デフォルトでは、ソースゾーンから宛先ゾーンへのすべてのトラフィックが許可されます。ポリシーとその例外により、許可されるトラフィックと拒否されるトラフィックが決まります。これにより、個々のサブグループおよびサービスに対して異なるアクションを定義できます。

ポリシーとトラフィックの依存関係を可視化する

ポリシーとトラフィックの可視化を有効にすると、作成されたセグメント化ポリシーとそのステータスを、以下に示すように接続マトリックスで可視化できます。フィルタリング機能を使用すると、特定のポリシーをドリルダウンして、サービスごとにトラフィックをフィルタリングしたり、マトリックスゾーンとソースおよび宛先フィルターの交差部分をフィルタリングしたりできます。

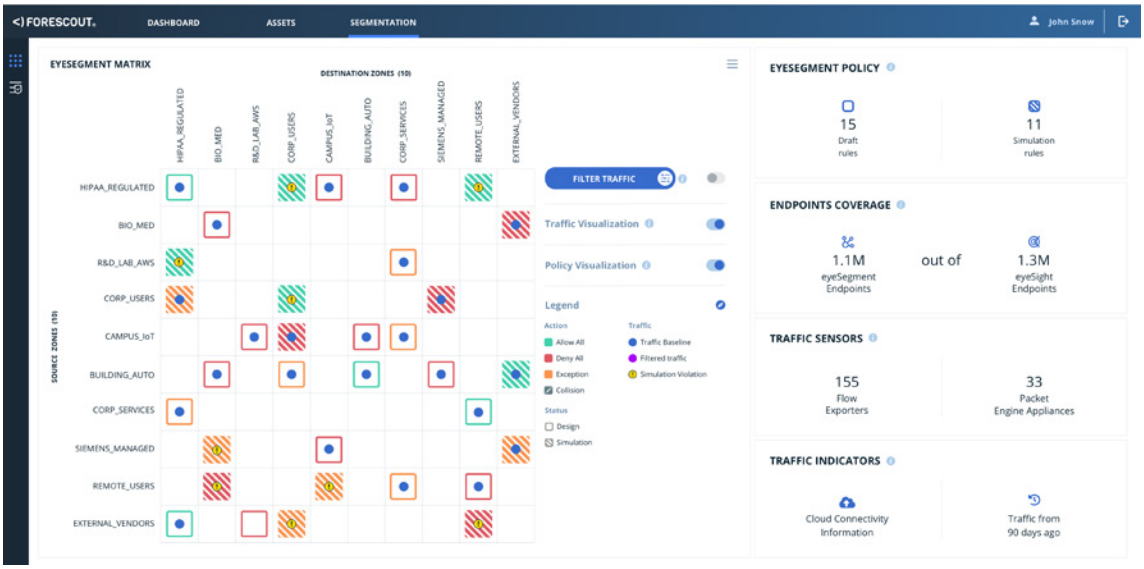

図3: ポリシーの可視化とシミュレーションビュー

監視と対応

eyeSegmentの単一ペインのポリシー管理とダッシュボードを使用すると、異なる送信元ゾーンと宛先ゾーン間のトラフィックフローを一元的に監視できます。基盤となるコントロールから抽出されたセグメント化ポリシーを継続的に監視して対応する機能は、コントロールするための段階的なステップとして、またはインフラストラクチャコントロールが利用できない場合に役立ちます。また、eyeSegmentは、エンタープライズインフラストラクチャコントロールを継続的に監視し、拡大するエンタープライズ全体にコントロールを適用した後も、セグメント化コントロールが実装され、効果的に機能することを保証します。

ユースケース

Forescoutプラットフォームは、幅広いネットワークのセグメント化のユースケースに対応しています。いずれのケースでも、Forescoutプラットフォームの柔軟性は、ビジネス中断のリスクを軽減し、セグメント化プロジェクトに関連する運用コストを最小限に抑えるのに役立ちます。

以下は、一般的なユースケースです。

クリティカルなビジネスアプリケーションの保護	• ビジネスクリティカルなアプリケーションを保護し、コントロールが効果的に実施されていることを確認し、継続的に監視し継続的保護を確保する。さまざまなサービス、アプリケーション、ドメイン全体で適切なビジネス内およびビジネス間のサービスコントロールを維持する • 異なるドメイン間でクリティカルなビジネスサービスへのユーザーアクセスをコントロールする。ビジネスクリティカルなアプリケーションをユーザーによる誤用から保護し、コントロールが効果的に実施されるようにし、実行中の保護を継続的に監視する
クリティカルなITインフラストラクチャへの特権アクセスの適用	• 指定管理者 (ロールベース), IT管理エンドポイントのステータス (暗号化、ドメイン参加など) および安全な通信 (特定のポート/サービス) に基づいて、機密ネットワークデバイス (スイッチ、NGFWなど) およびデータセンター/クラウドワークロード (Active Directory/LDAP、ドメインネームシステム、Oracle Clusterなど) へのIT管理者のアクセスを制限する
エンタープライズIoT/OTデバイス (プリンター、カメラ、VoIP、カードリーダー、HVACなど) の保護	• IoT/OTデバイスからITネットワークを保護する • IoT/OTデバイスを攻撃から保護する
エンタープライズ全体のセグメント化を保証	• 異なるドメイン (キャンパス、データセンター、IoT) 間すべてのエンフォースメントポイントが、他のチームによって管理され、セグメント化ポリシー要件を満たし、意図したとおりに構成されていることを確認する
脆弱なデバイスの抑制	• 脆弱なデバイス (WannaCry、パッチ未適用、サポート終了など) と他のネットワーク間のアクセスを制限する
レガシーアプリケーション/OSデバイスの保護	• レガシーオペレーティングシステムとアプリケーションがインストールされたデバイスを分離することで攻撃対象を縮小する • サポートが終了したオペレーティングシステムを実行しているデバイスに対する脅威のリスクを軽減する

FORESCOUT

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

詳細については、Forescout.comをご覧ください