

eyeSegment

業務を止めないゼロトラストのセグメンテーションを、あらゆる場所のあらゆるデバイスに

セグメンテーションの健全性確保

接続中のあらゆる資産の「現状」と通信パターンをリアルタイムで把握

最小特権によるアクセス制御

最小特権のアクセス権を付与したゼロトラスト・セグメンテーションの統合ポリシーを作成し、デジタル環境における脅威の拡散を防止

有効性

柔軟なセグメンテーションポリシーでサイバーリスクを低減し、被害範囲を縮小して基幹業務プロセスへの支障を防止

運用の複雑性を低減

IT、セキュリティ、ネットワーク、エンジニアリング部門の協働によるセグメンテーションの促進

エンフォースメントの自動化

セグメンテーションの自動エンフォースメントにより、時間とコストを節減、導入済みの現行ネットワークインフラへの現行資産の有効活用

Forescout eyeSegment は、貴社のデジタル環境全体にわたる動的セグメンテーションの設計・計画・導入展開を簡素化します。また、セグメンテーションを迅速に実行することにより、攻撃対象領域や攻撃による影響範囲 (Blast Radius) を縮小し、規制や事業リスクを緩和します。

Forescout プラットフォームの中核コンポーネントである eyeSegment をご利用いただくことで、ゼロトラストにもとづくセキュリティ対策およびデジタル領域全体でのサイバーセキュリティ対策の自動化が可能となります。



検知・可視化

トラフィックフローをもとに、対象環境上のデバイスやユーザー、アプリケーション、サービスを論理的に分類



設計・試行

論理セグメンテーションのポリシー作成・修正・試行サイクルを通じて、ポリシー効果を事前検証



監視・対応

セグメンテーションの健全性をリアルタイムで監視し、デジタル環境全体でのポリシー違反に素早く対応

ネットワークセグメンテーションによる企業全体の抜本改革

Forescout eyeSegmentは、Forescoutプラットフォームの包括的なデバイス可視化およびコントロール機能を活用し、キャンパス、データセンター、クラウドネットワーク全体の様々なエンフォースメントポイントでポリシーベースのセグメンテーションを自動実行します。大規模なネットワークセグメンテーションを確実に設計、構築、デプロイし、ネットワークアクセスにおける真のゼロトラスト化を実現できます

- ▶ エンフォースメントに先立ち、ポリシーを可視化・試行することで、プロアクティブな微調整と検証を徹底
- ▶ Forescout プラットフォームを広範囲に活用し、複数ドメインや利用環境にまたがるセグメンテーションの問題に対処
- ▶ 現行のインフラを有効活用

eyeSegment マトリックス (下図) を活用しシステム環境内の特定トラフィックパターンだけを分析・調査することで、重要業務に専念できます。マトリックス階層のどこからでも、対象トラフィックパターンへのセグメンテーションを実施し、業務プロセス継続を行い、効果的な eyeSegment ポリシーを瞬時に作成・監視できます。



トラフィックフローの把握・可視化

IPアドレスをもとにデバイスやアプリケーション、ユーザー、サービスを論理的に分類します。



ポリシーの設計・試行

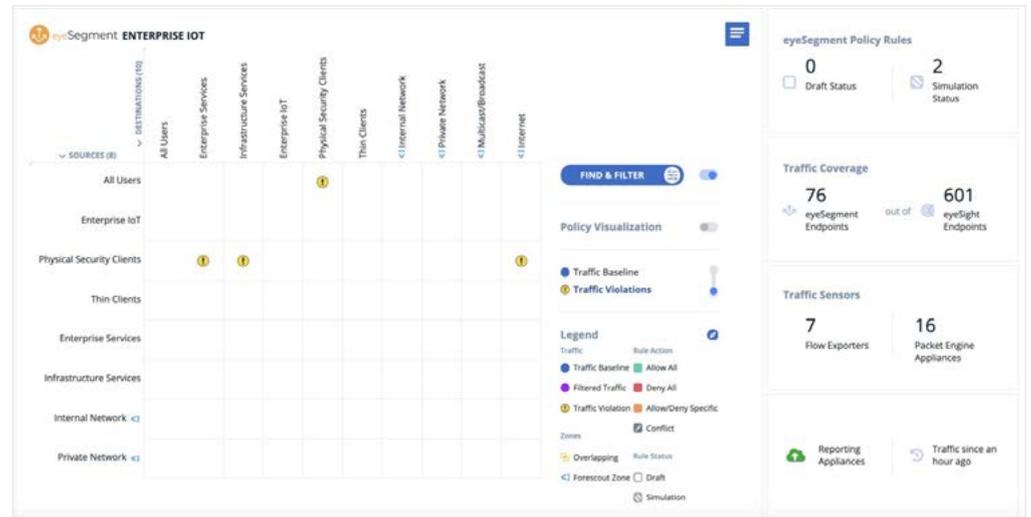
論理的な業務分類とリスクスコアをもとに、効果的なセグメンテーションポリシーを設計・作成し、調整を行います。

The screenshot displays the eyeSegment POLICY interface. It features a table with columns for Rule Name, Source, Destination, Action, Services, Status, and Comment. The table contains several policy rules, including 'Physical Security CL...' and 'Any to Physical Secu...'. A legend at the bottom right indicates risk levels from Level 0 to Level 4.

RULE NAME	SOURCE	DESTINATION	ACTION	SERVICES	STATUS	COMMENT
Physical Security CL...	Physical Security CL...	- Any -	Deny		Simulation	Physical Security Clie...
	IP Cameras Segmentation Groups	DHCP Segmentation Groups	Allow	bootps/67 (UDP), bootpc/68 (UDP)		
	IP Cameras Segmentation Groups	DNS Segmentation Groups	Allow	domain/53 (UDP)		
	IP Cameras Segmentation Groups	Digital Video Reco... Segmentation Groups	Allow	rtsp/554 (TCP)		
Any to Physical Secu...	- Any -	Physical Security CL...	Deny		Simulation	Any to Physical Secur...
	Physical Security U... Segmentation Groups	IP Cameras Segmentation Groups	Allow	https/443 (TCP)		

監視・自動化・対応

ベンダーやネットワークドメインが混在する環境に統合ポリシーを適用・監視し、業務を止めることなくポリシー違反をリアルタイムで特定します。business operations.



検出・評価・ガバナンス

デバイスの100%可視化、コンプライアンス準拠の維持、ネットワークセグメンテーションおよびゼロトラストの強固な基盤を実現する Forescout プラットフォームが、eyeSegment の価値をさらに高めます。

詳細は、www.forescout.com/products をご覧ください。