# Forescout eyeControl

## ポリシーベースのコントロールを実施、自動化することにより、攻撃対象領域をプロアクティブに縮小し、インシデントに迅速に対応する

膨大な数のセキュリティツールから通知されるセキュリティ上およびコンプライアンス上の問題が増加しており、ITセキュリティチームはその対処に忙殺されています。

こうしたツールは、絶えずアラートを生成しますが、そのツール自体には何かのアクションを実行する機能はありません。また、残念ながらこれらのツールには、優先順位決定に必要なデバイスコンテキストや、リスク軽減のためのコントロールを実施する自動化機能が不足しています。その結果、高度な技能を持つセキュリティチームは、些末な問題を手動でトラブルシューティングするのに時間を浪費し、プロアクティブにリスクを軽減することや、脅威に対して迅速に対応することに集中できません。

### ポリシーベースのコントロールの実施

Forescout eyeSightからの充実したデバイスコンテキストを備えたForescout eyeControlを利用することにより、セキュリティチームはポリシーベースのコントロールの優先順位決定、実施、自動化を確実に行うことができるようになります。企業はセキュリティ衛生を改善し、攻撃対象領域を縮小するとともに、レスポンスと修復を迅速化して脅威、セキュリティインシデント、コンプライアンスギャップを速やかに軽減することができます。

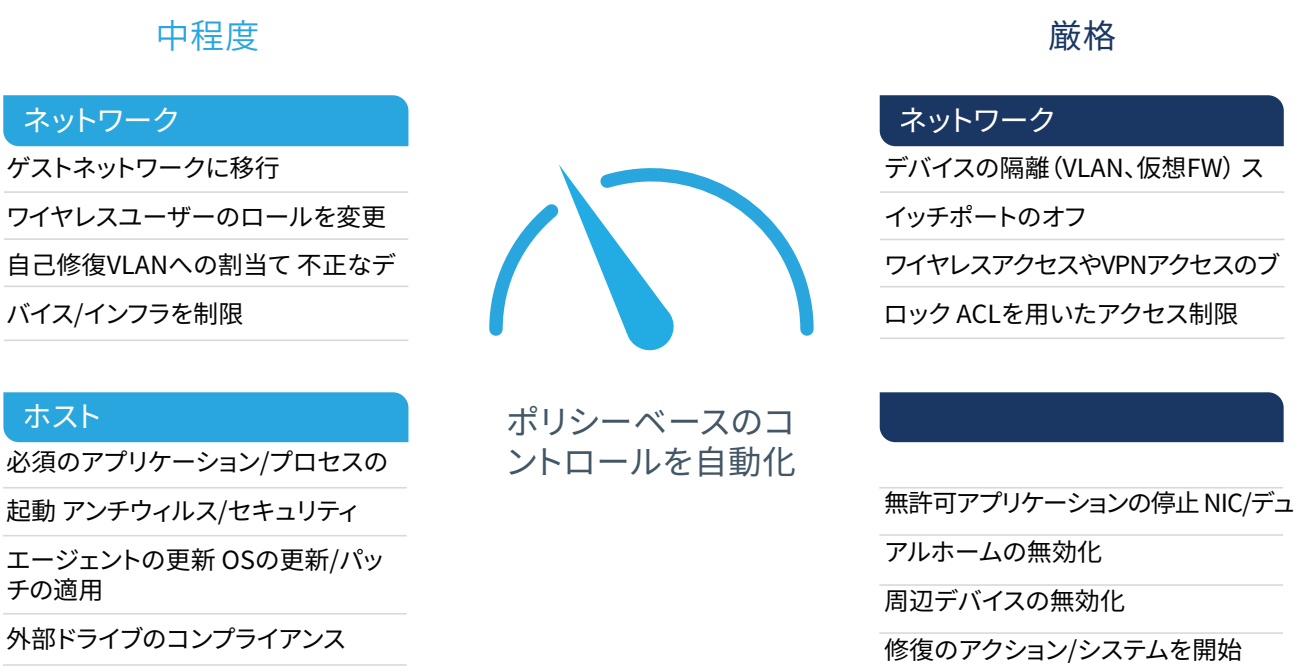
eyeControlを利用することで、セキュリティイニシアティブに応じて、ネットワークアクションとエンドポイントアクションの両方を実施できます。ネットワークアクションをオーケストレーションするため、eyeControlは、異種の物理ネットワークインフラおよび仮想ネットワークインフラ（スイッチ、ワイヤレス、VPN、ソフトウェア定義ネットワーク、クラウドベースネットワーク）とダイレクトに統合されます。エンドポイントアクションはWindows、Mac、Linuxのエンドポイントでエージェントレスに、またはSecureConnector™の利用を通じて実施できます。

eyeControl

### 特長

- 外的脅威から機密データを保護
- 感染したデバイス、脆弱なデバイス、非準拠デバイスによるマルウェアの拡散を防止
- 標的型攻撃によるデータ盗難やネットワークダウンタイム発生を防止
- 従業員、請負業者、顧客へのネットワークアクセスと可用性の確保を支援
- 内部ポリシーと外部規制の コンプライアンス遵守
- 状況に応じた適切なアクションを提供するための、コントロールアクションを自動化

図1ネットワークとエンドポイントでポリシーを実施し、自動化を着実に推進




**コントロールを確実に自動化**

eyeControlでは、直感的に使える柔軟性の高いPolicy Engineを備えているため、ターゲットを絞った緻密なコントロールを適用できます。使いやすい動的スコーピング、ブール論理、ウォーターフォール型ポリシーを用いて、洗練されたワークフローと複合アクションを実装。Policy Graph機能により、正確なポリシー作成、ポリシーフローの分析、アクションを実施する前のポリシーの微調整を容易に行うことができます。

コントロールアクションは、セキュリティチームが手動で開始することもできますし、セキュリティ業務を効率化するため、段階的に自動化を導入することもできます。自動化を基本的で反復的な作業から開始し、徐々により複雑なコントロールに発展させることによって、高度な技術を有するIT人材をこれらの作業から解放し、重要性の高い課題に集中させることができます。このようなアプローチによって、業務の混乱を最小限に抑えながら、ネットワークアクセス、デバイスコンプライアンス、ネットワークのセグメント化、インシデント対応戦略を大幅に改善することができます。

「多くの場合、エンドポイントに対するアクションを自動化することができますが、もし手動の介入が必要になったときでも、必要なのは右クリック1回だけです」– *Haworth*、情報セキュリティシニアアナリスト兼北米プライバシーオフィサー、*Joseph Cardamone*氏

**課題**

- ネットワーク上の非準拠デバイスや無許可デバイスが大きなリスクをもたらしている
- ネットワークがフラットで、十分にセグメント化されていないため、ラテラルムーブメントの脅威にさらされている
- セキュリティ上の脅威やインシデントに、迅速かつ効果的に対応できない
- セキュリティツールを通じて持続的にデバイスポスチャーを実施する能力に制限がある
- 業務が混乱するリスクがあるため、セキュリティコントロールの自動化に制限がある

### ネットワークアクセス制御の実施

ユーザープロファイル（ゲスト、従業員、請負業者）、デバイス分類、セキュリティポスチャーに基づき、エンタープライズリソースへのアクセスをコントロールします。

- ゲストやBYODデバイスのアクセスを差別化
- ネットワークアクセスポリシーを802.1X認証有りまたは無しで実施
- ネットワーク上の不審なデバイス、不正なデバイス、シャドーITデバイスに対するアクション
- 侵入を受けたデバイスや悪意のあるデバイスのネットワークアクセスを制限またはブロック
- コンプライアンス逸脱が解決されるまで、その非準拠デバイスを隔離または分離

「当社がForescoutのプラットフォームを選んだ理由の1つは、このテクノロジーが802.1Xプロトコルに依存していなかったからです。そのため、デプロイメントが非常に簡単です。エージェントをインストールしなくてもよいため、パフォーマンスが上がり、運用もとても簡単です」— *ACCIONA*、ITセキュリティ責任者、*Juan Ignacio Gordon*氏

### デバイスコンプライアンスの改善

コンプライアンス評価、修復コントロールの実施を自動化し、内部セキュリティポリシー、外部基準、業界規制のコンプライアンスを継続的に確保します。

- 各エンドポイントの適切な設定をすること、および重大な設定違反（脆弱パスワードやデフォルトパスワードを含む）の修復開始を支援
- 必要なアプリケーションやセキュリティエージェントの確実なインストール、稼働、最新の状態を維持することを支援
- リスクをもたらす無許可アプリケーション、またはネットワーク帯域幅やリソース生産性に無用な負荷をかける無許可アプリケーションを無効化またはブロック
- リスクの高い脆弱性や欠落している重要なパッチを特定してから、修復アクションを開始
- 必要なセキュリティソフトウェアのインストール、エージェントの更新、セキュリティパッチの適用などの修復アクションをプロアクティブにターゲティング
- AWS、Azure、VMware®を含む クラウドデプロイメントでポリシーを実装し、設定コンプライアンスのコントロールを自動化

「Forescoutのソリューションを利用すれば、指摘事項と修復作業が減ります。その結果、監査が非常にスピーディーになり、何百万ドルも節約できる見込みです」
— ユタ州、情報セキュリティチーフオフィサー、*Phil Bates*氏

### ネットワークの動的なセグメント化の実装

共通のポリシーフレームワークを通じて、ネットワークの動的セグメント化ポリシーを、エンタープライズ内に広がる異なるエンフォースメントテクノロジーを横断して適用します。

- デバイス特性、分類、セキュリティポスチャーに基づき、デバイスをセグメント化グループに動的に割当て
- キャンパスやOTネットワークで、VLAN、ACL、WLANのコントロール、およびタグ付けを介して、セグメント化コントロールを適用
- AWSやVMware NSXなどのパブリッククラウドやプライベートクラウドの環境内で、セキュリティグループ/タグを介して、セグメント化コントロールを適用
- 非準拠デバイスや脆弱なデバイス（特に定期メンテナンス期間中にのみパッチ当てや修復が可能なもの）を別のゾーンに分離し、攻撃対象領域を縮小しつつ、事業継続性を実現
- HIPAA、PCI、SWIFT CSPなどの規制に従い、ゾーンデバイスと、他のネットワークからのクリティカルなデータフローにセグメント化ポリシーを実施

「Forescoutを利用すれば、デバイスの分離やネットワークのセグメント化が可能になるだけでなく、これまで認識されていなかったネットワークを発見することもできます」–大手ヘルスケア企業、副最高情報セキュリティ責任者

### インシデント対応の迅速化

迅速かつ効率的に脅威を抑制し、セキュリティインシデントに対応することで、業務の混乱と事業への損害を最小限に抑えます。

- 抑制または修復されなかった高リスクデバイスを把握
- 接続時にデバイスの侵害指標（IOC）を把握し、平均応答時間（MTTR）を短縮
- 侵入を受けたデバイスや悪意のあるデバイスを分離、抑制し、マルウェアのラテラルムーブメントを回避
- インシデント対応を自動化し、侵入を受けたデバイスの修復ワークフローを開始
- 部門横断的なインシデント対応チームとサイロ化されたテクノロジーに対して、有用なデバイスコンテキスト（デバイスコネクション、ロケーション、分類、セキュリティポスチャー）を提供することにより、MTTRを短縮

「Forescoutを利用しているということは、チームの中に自ら働く脅威ハンターがいるようなものです。1日24時間、当社のグローバルネットワーク全域で脅威を探し回ってくれます。当社は現在、これまで対応できなかった課題に取り組んでいます。これまで数時間かかっていた作業が、今やわずか数分で完了します」
— *HubSpot*、プリンシパルセキュリティエンジニア、*Nick Duda*氏

詳細については、Forescout.comをご覧ください

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