FORESCOUT

eyeControl

ポリシーベースのコントロール適用
様々なネットワーク環境の混在下におけるコントロールアクションの適用・自動運用

無停止でのコントロール
802.1X認証の有無を問わず、様々なデプロイ・アクセスコントロール方法を柔軟に提供

エージェントレス
デバイスの健全性を常時評価・自動修復し、コンプライアンス条件をエージェントレスで適用

有効性
ゼロトラストネットワークアクセスを実現する柔軟かつ統合されたポリシーエンジン

アップグレード不要
ソフト/ハードウェアをアップグレードせずに、既存インフラとシームレスに連携可能

TCOの低減
デプロイ/保守/運用コストを削減し、ROIを早期実現

Forescout eyeControlは、様々なネットワーク環境の混在下において、柔軟かつフリクションレスな(摩擦のない)ネットワークアクセスコントロールを実現します。デジタル環境の管理対象/対象外デバイスすべてに最小権限アクセスにもとづくゼロトラストセキュリティポリシーを適用し、自動運用します。ポリシーベースのコントロールにより、デバイスコンプライアンスの常時徹底、先手を打った攻撃対象領域の縮小、インシデント対応の迅速化を図ることができます。

セキュアなネットワークアクセス

- ユーザー、デバイスの識別情報、セキュリティポスチャーにもとづくネットワークアクセス制御
- 様々なネットワーク環境の混在化におけるデプロイ(802.1X認証有無を問わず)

デバイスコンプライアンスの設定

- セキュリティポリシー、業界基準、政府規制への準拠対応を自動化
- 修復やリスク緩和のワークフローをリアルタイムで起動

インシデント対応の自動化

- セキュリティインシデント対応を自動化
- 脅威を封じ込め、拡散や業務中断リスクを最小化

コントロールを確実に自動化

デバイスを完全に可視化し、コンテキストを取得できなければゼロトラストポリシーを適用しても意味がありません。つまり、あらゆる接続デバイスのユーザーやデバイスの識別情報、セキュリティポスチャー、リスクプロファイルなどをリアルタイムで把握する必要があります。完全に可視化しないままコントロールを実施すると、業務に支障が出たりオペレーションがリスクにさらされます。eyeControlは、eyeSightが提供する豊富なデバイスコンテキストをもとに、ゼロトラストによるセキュリティコントロールを確実に適用し、自動運用します。

eyeControlの中核となるのは、きめ細かいコントロールアクションをピンポイントで適用可能な、柔軟性に優れた統合型ポリシーエンジンです。このエンジンは以下の機能を提供します。

- ビジネスロジックやコンテキストにもとづくデバイスの動的グループ化/スコーピング
- ブーリアンロジックとウォーターフォール型ポリシーを使った複合条件およびアクションによる高度なコントロールワークフローの導入
- ポリシーグラフ(Policy Graph)機能による正確なポリシー作成、ポリシーフロー分析、適用アクション有効化前の微調整
- 手動で開始したコントロールアクションを徐々に自動適用に切り替え、セキュリティ業務の効率を改善

特定のデバイスまたはネットワーク全体で発生するイベントや変更をトリガーにしてポリシーを発動し、リアルタイムで自動評価します。下記の図1は、ポリシー発動時にeyeControl上で実行可能なコントロールアクションの範囲です。

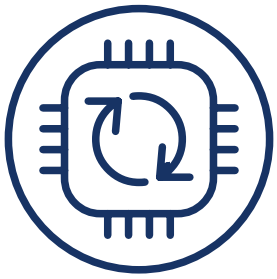
中程度

ネットワーク

- ゲストネットワークへの移行
- 無線ユーザーの役割変更
- 自己修復VLANへの割り当て
- 不正デバイス/インフラの制限

ホスト

- 必須アプリ/プロセスの起動
- アンチウィルス/セキュリティエージェントの更新
- OSの更新/パッチ適用
- 外部ドライブのコンプライアンス徹底



ポリシーベースのコントロールを自動で実行

厳格

ネットワーク

- デバイスの隔離(VLAN、仮想FW)
- スイッチポートの接続オフ
- 無線/VPNアクセスのブロック
- ACLによるアクセス制限

ホスト

- 無許可アプリの停止
- NIC/デュアルホームの無効化
- 周辺デバイスの無効化
- 修復アクション/システムの起動

1:ネットワークとエンドポイントにポリシーを適用し、自動運用の範囲を段階的に拡大

eyeControlが解決する問題

- リスクやコンプライアンスの問題につながる、ネットワーク上の**無許可/不正/なりすましデバイス**
- エージェントベースのツールの更新不備、機能不全による**セキュリティギャップ**
- **セグメント化が不十分なフラットネットワーク**（脅威にさらされやすく、攻撃された際の影響範囲が増大）
- 脆弱なデバイス、重要パッチの適用漏れ、無許可アプリによる**業務中断リスク**
- 侵害された/悪質なデバイスの封じ込めの遅延による、**脅威の水平拡散**
- 接続デバイスの常時監視やポリシー適用の不備による**コンプライアンス違反**
- 異種混合/マルチベンダー環境や有線ネットワークにおける**NAC導入**

コントロール

セキュアなネットワークアクセス

eyeControlは、柔軟性を最大限高めた、異種環境での業務の中断を必要としないネットワークアクセスコントロールソリューションです。有線/無線ネットワーク全体の管理対象/非対象デバイス全体のセキュアなアクセスを実現するほか、監査要件への準拠、攻撃対象領域の縮小、脅威の迅速な緩和を実現します。以下はeyeControlの機能（一例）です。

- ゼロトラスト原則にもとづく、従業員/ゲスト/請負業者/BYODデバイスへのネットワークアクセスプロビジョニング
- シャドーITを含む不正/無許可/なりすましデバイスの特定・ブロック
- コンプライアンス違反の高リスクデバイスを修復完了まで隔離/分離
- 様々なアクセスコントロール手法の活用（802.1X認証有無を問わず）
- ゼロトラストポリシーの統合エンジン経由でポスチャーをエージェントレスで評価し、ネットワークとエンドポイント両方へのアクションを適用
- ソフト/ハードウェアのアップグレードなしで、現行インフラとの相互運用が可能
- 100種類以上の製品モデルをベースに30以上のネットワークインフラベンダーと直接連携

コンプライアンス

デバイスコンプライアンスの設定

セキュリティポスチャーの自動評価、修復コントロールの実施により、社内のセキュリティポリシーや社外基準、業界ルールへの継続的コンプライアンスを徹底します。

- エンドポイントの構成を検証し、重大な違反があった場合は修復を開始
- 管理デバイスのセキュリティエージェントが欠落/故障している場合、該当デバイスを特定し、修復
- ネットワーク帯域幅や生産性に悪影響を及ぼし、潜在リスクを伴う無許可アプリケーションの検知/無効化
- 脆弱性や、重要パッチの適用漏れがある高リスクデバイスを特定し、修復アクションを開始
- Windows/Mac/Linux/IoT/OTデバイスへの修復アクション、リスク緩和アクションをエージェントレスで実施
- AWS、Azure、VMwareなどのクラウド実装環境におけるポリシー適用および、設定コンプライアンスコントロールの自動実行

自動化

スピーディーなインシデント対応

迅速かつ効果的に脅威を抑制し、セキュリティインシデントに対応することで、業務の中断やビジネスへの影響を最小化します。

- 基本的/定常的タスクの自動化により、貴重なリソースが定型タスクから解放され、優先順位や影響度が高い業務や課題対応に集中可能
- デバイスの侵害の痕跡(IoC)やリスクをリアルタイムで特定し、平均応答時間(MTTR)を短縮
- 侵害されたデバイスや悪質デバイスを自動的に隔離し、封じ込めることで、マルウェアの水平拡散を防止して潜在的な影響範囲を縮小
- インシデント対応を自動化し、対象デバイスの修復ワークフローをリアルタイムで開始
- 有用なデバイスコンテキスト(デバイス接続状況、ロケーション、分類、セキュリティポスチャー)を、多部門にまたがるインシデント対応チームと縦割りシステム全体で共有することで、MTTRを短縮

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、eyeConrol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。

FORESCOUT

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
詳細はこちら: Forescout.com