FORESCOUT
Active Defense for the Enterprise of Things™

eyeControl
ポリシーベースのコントロール実施

無停止でのコントロール
802.1X認証の有無を問わず、様々なデプロイ方法や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
デバイスの健全性評価、自動修復により、エージェントレスでデバイスコンプライアンスを設定

有効性
ゼロトラストによるセキュアなアクセスを実現する統合ポリシーエンジン

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、既存インフラと併用可能

TCOの削減
デプロイ/保守/運用コストを削減し、ROIを早期に実現する無停止型で柔軟なエージェントレス方式（マルチベンダー対応）

異種混合ネットワークにおけるEnterprise of Things(EoT)コントロールの実施自動化

Forescout eyeControlは、異種混合エンタープライズネットワークにおいて、最も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提供します。EoT環境における管理対象/対象外デバイスすべてに、最小権限のアクセスにもとづくゼロトラストポリシーを適用し、自動運用します。ポリシーベースの制御で、デバイスのコンプライアンス設定、攻撃対象領域の機動的な縮小、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ポスチャーにもとづくネットワークアクセス制御

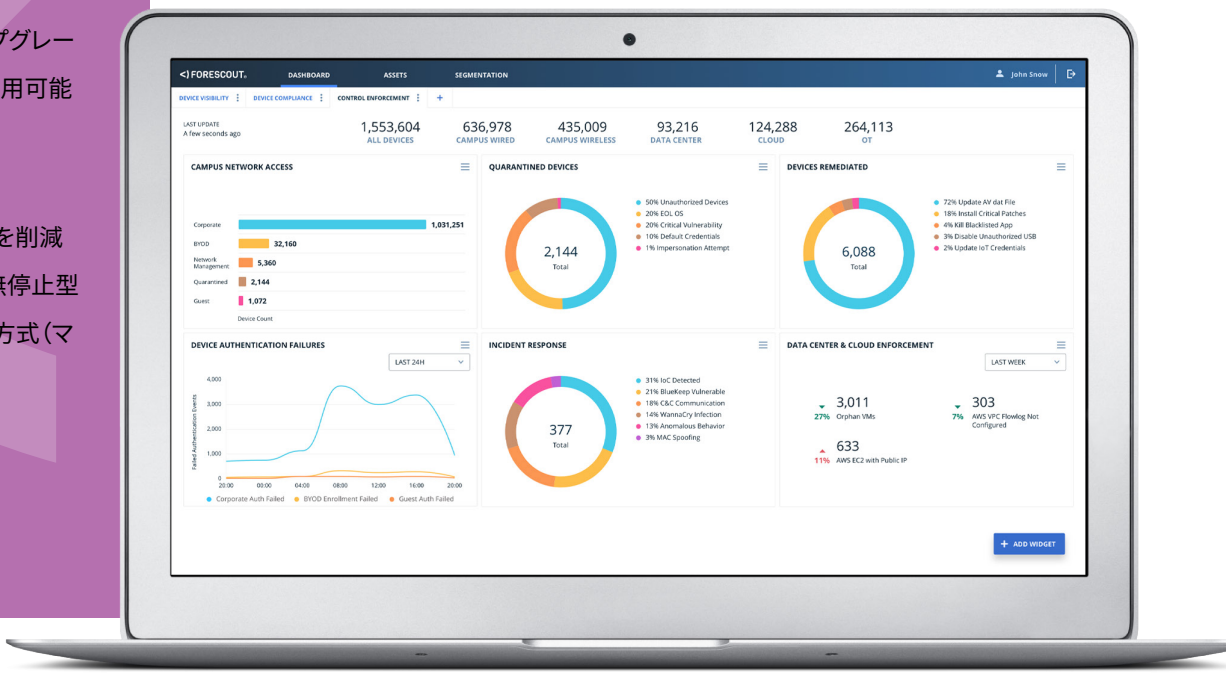
異種混合ネットワークにおけるデプロイ（802.1X認証有無を問わず）

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、基準、規制の準拠

修復やリスク緩和のワークフローを起動

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



forescout.com/platform/eyeControl japan-sales@forescout.com 電話番号: 81 50-1746-6455

コントロールを確実に自動化

ゼロトラストポリシーは、完全なデバイスコンテキスト情報をもとに適用しなければ、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コントロールを確実に実施自動化します。

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、直感的かつ柔軟なポリシーエンジンです。このエンジンはゼロトラストポリシーをベースに、以下を提供します。

- ビジネスロジックやデバイスコンテキストをもとに、デバイスを動的にグループ化/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
- 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、適用アクション実施前の微調整
- 手動で開始したコントロールアクションを徐々に自動化し、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、ポリシー発動時のeyeControl上で実行可能なコントロールアクションの範囲です。

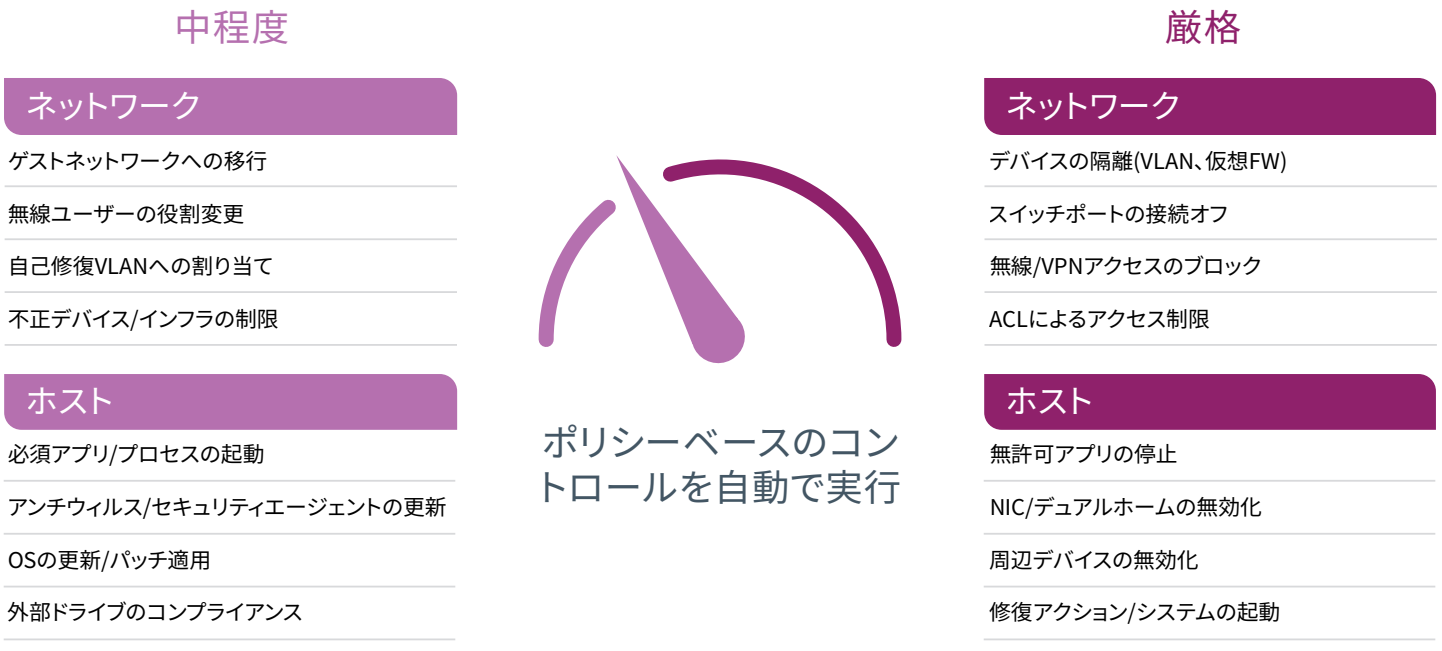


図1：ネットワークとエンドポイントにポリシーを適用し、自動化を段階的に推進

コントロール

セキュアなネットワークアクセス

eyeControlは、柔軟性を最大限まで高めた、異種環境対応で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(NAC)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EoTシステムへ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支援します。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
- 不正/無許可/シャドーIT、なりすましデバイスの特定およびブロック
- コンプライアンス違反の高リスクデバイスを隔離/分離し、修復
- 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実施
- 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

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**

接続デバイスの継続的監視やデバイスポスチャー評価機能の欠如による**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導入の課題**

forescout.com/platform/eyeControl japan-sales@forescout.com 電話番号: 81 50-1746-6455

- 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、構成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。基本的/定常的タスクの自動化により、高スキル人材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
- デバイス接続時に侵害の痕跡(IoC)やリスクを特定し、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素早く隔離し、封じ込めることで、マルウェアの水平拡散を防止
- 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

Don’t just see it. Secure it.™

EoT(Enterprise of Things)のアクティブ防御を支援します。今すぐお問合わせください。

forescout.com/platform/eyeControl japan-sales@forescout.com 電話番号: 81 50-1746-6455

〒101-0051
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

詳細はForescout.jpをご覧ください