FORESCOUT
Active Defense for the Enterprise of Things™

最新鋭のNAC（ネットワークアクセスコントロール）

無停止型で柔軟な、エージェントレス方式の ゼロトラスト・セキュリティが皆様のEnterprise of Things(EoT)を保護します

キャンパス、端末、ビジター用デバイス、在宅勤務用ラップトップ、IoT、OT、スマートデバイスなど、様々な種類のネットワークに様々なモノが接続する今日のエンタープライズ環境では、ゼロトラスト・アクセスを体系的に実施・維持する必要があります。そのため、以下のような機能を実現する最新鋭のネットワークアクセスコントロール(NAC)プラットフォームが求められています。

- 接続するあらゆるモノの常時識別
- 対象物のポスチャー評価
- アクセスポリシーの適用
- コンプライアンス違反または異常な挙動が見られた場合、コントロールを自動で実施

簡単そうに見えて難しい「ゼロトラスト」

エンタープライズネットワークに接続するあらゆるモノを制御することは、途方もない作業です。IT担当やセキュリティアーキテクトはNACシステムを導入する際、以下のような課題に直面しています。

- 初期のNACソリューションは、業務オペレーションへの支障懸念や複雑な構造により、効果的でない
- 従来型のエージェントでは、エンタープライズネットワークに蔓延するIoT、OTデバイスを認証できない/コントロールできない
- マルチベンダー構成のネットワーク環境では、802.1X認証ベースの制御が機能しない
- ネットワークの定期スキャンでは、なりすましによる侵入その他の突発的な脅威をカバーできない
- ゼロトラスト・アクセスに対応するソリューションは多いが、コストが高すぎる、または手作業プロセスが多すぎる

「Forescoutプラットフォームは一日でデプロイできると聞いていましたが、チームメンバーの様子を見て、皆驚きました。わずか数時間で展開導入が完了したのです!」

MIKE ROLING
ミズーリ州政府
CISO（最高情報セキュリティ責任者）

Forescout: 最新鋭・最高水準のNACソリューション

上記の課題が当てはまる場合、今すぐ当社のNACソリューションをお試しください。以下を通じて皆様のニーズを充足し、期待以上の成果を実現します。

最も包括的な可視性

20種類以上のアクティブ/パッシブ手法を使い分け、拡張エンタープライズネットワークに接続するあらゆるデバイスをリアルタイムで、完全に可視化します。

あらゆる接続デバイスをゼロトラストで制御

エージェントレス方式の常時監視と統合ポリシーエンジンで、皆様のエンタープライズ環境に接続するあらゆるモノを動的にセグメント化し、隔離します。これにより違反による悪影響を抑制します。

ネットワーク環境を止めずにデプロイし、早期に価値を発揮

ソフトウェアを使用しないエージェントレス方式のため、インフラの更改や802.1X認証対応は不要です。このため、数日以内に完全な可視化、数週間以内にコントロールを自動実施できます。

エンタープライズ規模の拡張ネットワークにおける実績

当社のソリューションは多数のFortune 1000掲載企業に採用され、ご満足いただいています。中には200万ものエンドポイントでの導入事例もあり、お客様のネットワークを安全に保つ当社の技術力や信頼性の高さが証明されています。

セキュリティ/IT投資効果を拡大

ほとんどのセキュリティツールは単に、違反にフラグを立てて担当者にアラートを送るだけです。Forescoutプラットフォームにはプラグ&プレイ形式のモジュールが搭載されており、可視化/コントロール機能を以下に応用できます。

- リアルタイムのデバイスコンテキストを社内セキュリティ/IT管理ツールと共有
- ワークフローのオーケストレーション、対応アクションの自動化
- セキュリティポスチャーの継続評価および、自動修復されたデバイスへのコンプライアンス設定

「今日のNACツールは、デバイスや無許可のエンティティ（ユーザー、セグメント、デバイスなど）がネットワークに「接触」しないよう、隔離する際に最適な支援手段です。パッチ適用不備が疑われる未知のアイテムをゼロトラストネットワーク環境から除外するために、Forescoutなどのベンダーが提供する最新のNAC技術を活用してください。[1]」

CHASE CUNNINGHAM
FORRESTER RESEARCH社　プリンシパルアナリスト

識 別

あらゆる接続デバイスを検知、分類してインベントリを作成

Forescoutプラットフォームをご利用になるセキュリティ/IT運用チームは、IP接続デバイスがネットワークにアクセスした瞬間に、リアルタイムで完全に可視化できます。この情報をもとに、正確なリアルタイムの資産インベントリを作成できます。

- 20以上のアクティブ/パッシブ型の検知手法やプロファイリング手法を、皆様の業務環境に合わせて使い分け、ネットワークの継続的な可用性を確保
- Forescout Device Cloudに蓄積された1,200万超のフィンガープリント情報による、忠実度の高い三次元形式のデバイス分類（デバイス機能、OS、ベンダー、機種などの識別情報）
- ロケーション、ネットワーク、デバイスタイプにまたがる、死角のない包括ビュー（802.1X認証有無を問わず）

コンプライアンス

セキュリティポスチャーとコンプライアンスの評価

エージェントベースのセキュリティツールでは、エージェントが欠落/故障したり機能不全になると、管理デバイスをくまなく評価できません。また、セキュリティエージェントに対応していないIoTデバイスを評価することはできないため、攻撃対象領域がさらに拡大してしまいます。Forescoutプラットフォームは、IPベースのデバイスすべてが接続した瞬間から継続的に、ポスチャー評価と修復作業を自動で実行します。

- 管理デバイスの現行セキュリティツールでエージェントが欠落/故障している、または機能不全となっているものを発見し、修復
- デバイスのコンプライアンス違反、ポスチャー変更、脆弱性、脆弱な認証情報、IoC（侵害の痕跡）、なりすまし未遂、その他の高リスク指標をすべて、エージェントレスで検知
- 非管理デバイス（エージェント対応不可のデバイスなど）の評価、継続的監視によるセキュリティコンプライアンス

Forescoutプラットフォームは、信じられないほどの情報を還元してくれます。システムを適切に発見・識別・制御するためのツールとしては他のツールを圧倒的に凌駕しています。今では絶対に欠かせない貴重なツールです。

JOSEPH CARDAMONE
HAWORTH INTERNATIONAL
情報セキュリティ上席アナリスト

接 続

異種混合ネットワーク全体へのアクセスポリシー適用

Forescoutプラットフォームは、デバイスとユーザーの識別情報、デバイスの健全性、リアルタイムのコンプライアンス状況をもとにゼロトラスト・セキュリティを実施します。インフラ上のハードウェアやソフトウェアの更新は不要です。

- ユーザーの役割、デバイスタイプ、セキュリティポスチャーをもとに、エンタープライズリソースへの最小権限アクセスをプロビジョニング
- 無許可、不正、偽装デバイスによる接続を防止
- 有線、無線、VPNインフラ全体での柔軟な統制（802.1X認証有無を問わず）

1. 2019年1月2日付Forrester Research社レポート「The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook」
2. 2019年第4四半期版 Forrester WaveTM「Zero Trust eXtended Platform Providers」

IoT/OTセキュリティに対応する（Forescoutの）プラットフォームとその機能は、群を抜いています。究極の可視化による運用コントロールの最大化こそ、Forescoutのゼロトラスト・アプローチの真髄と言えるでしょう。[2]

FORRESTER RESEARCH

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

FORESCOUT
Active Defense for the Enterprise of Things™

〒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