ForeScout

組織の課題

- ネットワーク上の既知のデバイスや不明なデバイスを一元的に可視化する
- 無許可またはコンプライアンス違反のデバイスから機密システムおよびデータを保護する
- 安全なネットワークアクセスコントロールに必要な人的介入を最小限にする
- 規制要件に準拠する
- 従業員やゲストが自分のデバイスを簡単かつ安全にネットワークにアクセスできるようにする
- BYOD、IoTおよび不正なデバイスを効果的に管理する

技術的な課題

- セキュリティエージェントの有無に関わらず一元的にデバイスを可視化する
- デバイスを発見、評価、監視して異常な動作を検出する
- 組織のポリシーや基準を満たしていないデバイスを特定し、緩和・修復する
- 有線または無線デバイスがネットワークに接続された時に検出する
- 暗号化およびデータ損失防止エージェントが機能していることを確認する
- 無許可のアプリケーションまたは周辺機器がネットワーク上に存在しないようにする

エージェントレスの可視化

接続デバイスを検出する比類なき機能

ネットワーク上に存在する無許可またはコンプライアンス違反のデバイスを検出できなければ、それらに適切に対処することはできません。ForeScout CounterACT® では、デバイスがネットワークに接続した際に瞬時にそれらを検出することができます。ソフトウェアエージェントや、事前にデバイス情報を知っておく必要はありません。このユニークなエージェントレスアプローチにより、マネージドまたはアンマネージド、企業または個人、有線または無線を問わず、デバイスすべてを可視化します。個人所有のBYODデバイスシステム、サーバー、スイッチ、不正ハードウェア、またはIoT(モノのインターネット)デバイスであったとしても例外ではありません。

直面する問題

従来型のセキュリティソリューションでは、エージェントを備えたデバイスに対してのみ検出・評価が可能です。もしすべての接続デバイスにエージェントが実装されており、ITセキュリティにより管理されるのであれば問題ありません。しかし現実には、取引先や請負業者のノートPC、スマートフォンやタブレット、IoTデバイスまたはハッカーの不正エンドポイントなど、検出されない不明なBYODデバイスや従来とは異なるデバイスが、一緒くたにネットワークに押し寄せてきます。すでに世界中のネットワークに存在している数十億ものデバイスと、それに加わるであろう新たな幾十億ものIoTデバイス、そしてネットワークへの不正なアクセスや違反が常に発生している現実を目の前に、ITセキュリティプロフェッショナルの間にはセキュリティに関する当然の懸念が広がっています。

また、大半の従来型エンドポイント管理ソリューションで未解決の別の重要課題として、多くのデバイスがネットワークに出入りすることが挙げられます。これらのソリューションで周期的なスキャンではなくリアルタイムの監視および継続的診断を提供しない限り、無許可デバイスによる重大な損害が発生して、問題が認識された時には手遅れになる事態が生じる可能性があります。

ソリューション

ForeScout CounterACTは、デバイスを可視化するエージェントレスアプローチに基づき、数あるネットワークセキュリティソリューションの中で独自の地歩を築き上げてきました。物理的または仮想的ソリューションで、ネットワークインフラ、BYODシステム、従来のものとは異なるIoTデバイス(ハンドヘルド、センサー、およびマシン)、不正なエンドポイント(無許可スイッチ、ルーター、および無線アクセスポイント)など、IPアドレスを持つデバイスを瞬時に識別します。管理エージェントや、事前にデバイス情報を知る必要はありません。

CounterACTの可視性の範囲

CounterACTは、ネットワークデバイスおよびアプリケーションを識別して評価し、デバイス、ユーザー、所有者、オペレーティングシステム、設定、ソフトウェア、サービス、パッチの適用状況およびセキュリティエージェントの有無を確認するなど、非常に詳細なレベルでデバイスの検出・分析を行います。CounterACTは、ネットワーク上のデバイスのステータスやセキュリティ状態をすばやく特定、評価して、増加し続けるIoTエンドポイントを自動的に分類します。これらすべては802.1Xインフラの有無に関わらず行われます。

さらに、同じく重要な点として、このような詳細な情報がごく短時間で取得可能であることが挙げられます。ネットワークテスト専門機関Miercomによる最近の調査では、テストの対象となったすべてのネットワーク環境において、すべてのエンドポイントがCounterACTによって発見・分類されたことが報告されています。さらに、CounterACTによって500エンドポイントが5秒以内に検出・分類されたことも報告されています。1

これは、検出・分類する機能をほとんど持たず、デバイスのIPアドレスを表示するだけにとどまる従来のネットワークアクセス・コントロールソリューションと比べて、非常に対照的な結果です。

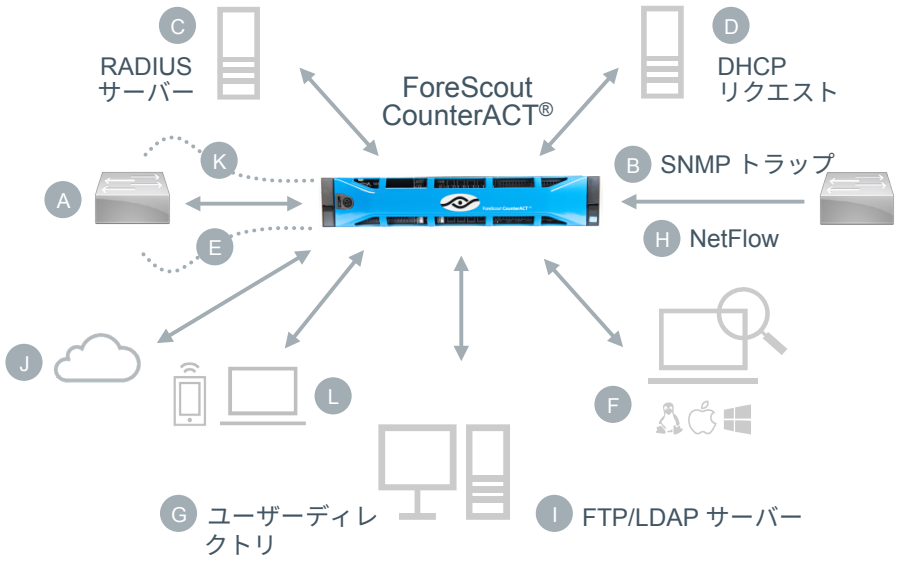
可視性のレベル

- 許可イベント
  - 認証イベント
  - SNMP トラップ
  - DHCP リクエスト
  - スイッチポート変更
  - MAC/IP
  - ネットワークトラフィック
- デバイスの種類および所有権
  - Windows、Macintosh、Linux、モバイル、ネットワークデバイス、IoT、プリンター、VoIP、その他
  - OS の種類
  - NICベンダーなどのハードウェアプロパティ(MACアドレス)
  - スイッチの情報
  - 管理可能(ドメイン/ローカル/SecureConnector)
  - ユーザー情報
  - ディレクトリの情報
  - デバイスの所有権(会社、訪問者/委託先、BYOD)
  - 接続の種類(LAN、WAN、無線、VPN)
  - IPの割り当て(DHCP、固定)
  - 位置情報
- コンプライアンスポリシー
  - 認証アプリケーション導入済み/実行中
  - 不正アプリケーション導入済み/実行中
  - ウイルス対策エージェントステータス(導入済み/実行中)およびデータベースのバージョン
  - パッチ管理エージェントステータス(導入済み/実行中)
  - P2P/IMクライアント導入済み/実行中
  - 任意のポートにおけるデバイス数
  - 企業ドメインのメンバー
  - ネットワークアダプター(デバイスID、名前、アダプターの種類および速度)
  - ファイアウォールステータス(導入済み/実行中)
  - レジストリおよび設定/構成
  - パッチレベル

ForeScoutがデバイスを検出する方法

複数の方法

- A 接続されたデバイスのリストについて、スイッチ、VPNコンセントレーター、APおよびコントローラーのポーリングを行う
- B スイッチおよびコントローラーからSNMPトラップを受信する
- C 組み込みまたは外部RADIUSサーバーへの802.1Xリクエストを監視する
- D 新規ホストがIPアドレスをリクエストする際のDHCPリクエストを監視して検出する
- E ネットワークSPANポートを監視し、HTTPトラフィックやバナーなどのネットワークトラフィックを検出する（オプション）
- F NMAPスキャンを実行する
- G 資格情報を使ってエンドポイントのスキャンを実行する
- H NetFlowデータを受信する
- I 外部MAC分類データをインポート、またはLDAPデータをリクエストする
- J 公開/非公開クラウド内の仮想マシンを監視する
- K PoEおよびSNMPを使ってデバイスを分類する
- L 任意のエージェントを使用する



CounterACTでは、独自開発プロセスを含め、エージェントなしでネットワーク上のエンドポイントを発見して分類するためのさまざまな技法が採用されています。デバイスの詳細情報を取得するため、アンマネージドデバイス上に一時利用エージェント(Dissolvable Agent)をインストールすることも可能です。

高度な可視化とコントロールを他社製ツールにも拡張

ForeScout ControlFabric® テクノロジーに基づくCounterACTはインストールが容易な製品で、通常インフラの変更やアップグレード、エンドポイントエージェントやエンドポイントの再設定を必要としません。CounterACTはネットワークアクセスコントロールで実現出来る機能とレベルを拡張できます。CounterACTのいくつかの機能は、従来のNACが提供する機能をはるかに超えています:

- エージェントレスでの可視化によりネットワークインフラ、BYOD、および従来にはなかったIoTデバイスを含むアンマネージドデバイスを検出可能
- 継続的な監視と評価により、新設デバイス、またネットワークに断続的に接続するデバイスを検出する
- ForeScout ControlFabricアーキテクチャおよびForeScout拡張モジュールにより、コンテキスト情報を共有し、CounterACTの管理機能を幅広いITおよびセキュリティ製品に拡張する

略語用語集:

Dynamic Host Configuration Protocol (DHCP)

File Transfer Protocol (FTP)

HyperText Transfer Protocol (HTTP)

Instant Messaging (IM)

Lightweight Directory Access Protocol (LDAP)

Local Area Network (LAN)

Media Access Control (MAC) address

Network Mapper (Nmap)

Point to Point (P2P)

Power over Ethernet (PoE)

Remote Authentication Dial-In User Service (RADIUS)

Simple Network Management Protocol (SNMP)

Switch Port Analyzer (SPAN)

Virtual Local Area Network (VLAN)

Virtual Private Network (VPN)

Voice over Internet Protocol (VoIP)

Wide Area Network (WAN)

詳細はこちらから

デバイスがネットワークに接続された瞬間に発見して制御し、異なるセキュリティツール間の情報共有および運用のオーケストレーションを行うForeScout製品のユニークな機能の詳細については、**www.ForeScout.com**を参照してください。

ForeScout

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

米国内フリーダイヤル 1-866-377-8771
国際電話番号 +1-408-213-3191
サポート 1-708-237-6591

[1]「An Independent Assessment of ForeScout CounterACT」(ForeScout CounterACTの独自評価)、Miercom、2016年6月