ForeScout CounterACT®

マネージド、アンマネージド、さらに従来とは異なるデバイスのリアルタイムのモニタリング、コントロールおよびポリシーベースの緩和・修復措置を提供します。

ForeScout CounterACT®は、ネットワークエンドポイントおよびアプリケーションがネットワークに接続した瞬間に動的に認識して評価するエージェントレスなセキュリティアプライアンスです。CounterACTでは、ユーザー、所有者、オペレーティングシステムだけでなく、デバイス設定、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が確認されます。次に、これらのデバイスで必要な緩和・修復措置が実行され、コントロールおよび継続的モニタリングが提供されます。

CounterACTでは、会社所有のエンドポイント、個人が所有するBYOD(私的デバイスの業務利用)エンドポイント、従来のものとは異なるデバイスに対してこれらのアクションが実行されます。ソフトウェアエージェントまたはデバイスに関する情報は必要ありません。CounterACTは既存の環境にすばやく導入でき、ほとんどの場合、インフラの変更やアップグレード、またはエンドポイントの再設定は必要ありません。

お客様がCounterACTを選ぶ理由

異機種環境のサポート。一般的なネットワークインフラ、オペレーティングシステム、エンドポイントソフトウェアおよび他社のセキュリティソリューションで機能します。

エージェントレス。認証とネットワークアクセスコントロールにはエンドポイントエージェントは必要ありません。

優れた可視化機能。他のソリューションでは難しい、以下のデバイスを監視可能:

- デスクトップ、ラップトップ、サーバー、ルーター、スマートフォンおよびタブレット
- 有線/ワイヤレスLANおよびプリンター
- プロジェクター、産業用制御システム、医療機器、製造機械、POSデバイスなどのIoTデバイス

自動コントロール。以下のアクションを自動化可能:

- デバイスの状態とセキュリティポリシーに応じて、ネットワークアクセスを許可、拒否または制限する
- 悪意のある、または高リスクのエンドポイントを隔離して、緩和・修復措置を実施

迅速なTime to Value。すばやく導入し、数時間内にネットワークを可視化します。

ポリシーの施行。ネットワークアクセスコントロール、エンドポイントコンプライアンスおよびモバイルデバイスセキュリティを強化します。

生産性。担当スタッフに煩わしい手作業を生じさせることなく、ユーザーおよびデバイスに適切なネットワークアクセスを付与します。

信頼性。不正なインフラを識別して削除することで、ネットワークの安定性を向上させます。

コスト削減。ゲストアクセスのためのネットワークポートの開閉に必要とされる人件費を削減できます。

コンプライアンス。ポリシー違反の識別、エンドポイント不具合の緩和・修復措置、規制コンプライアンスの評価を自動化します。

ネットワークセキュリティのリスクと盲点

従来のネットワークセキュリティでは、ファイアウォールおよび侵入防御システムを使用して外部からの攻撃を防ぐことに焦点が置かれていました。ただし、これらのセキュリティツールはセキュリティインシデントや侵害の大幅な増加の原因である、膨大な内部からの脅威に対してはまったく無力です。以下の脅威に対処する必要があります:

- **訪問者:** 訪問者や契約ベンダーが自分のコンピューターを会社に持ち込みます。インターネットへのアクセスを必要としており、契約ベンダーであればその他のリソースへのアクセスも必要かもしれません。制限なしのアクセスを付与してしまうと、ネットワークが攻撃のリスクにさらされることになります。
- **ワイヤレスおよびモバイル(BYOD)ユーザー:** 従業員が個人用のスマートフォン、タブレット、またはノートパソコンを会社のネットワークに接続する場合があります。十分にコントロールしないと、これらのデバイスによってネットワークが感染したり、データを喪失したりする原因となるかもしれません。
- **IoT(モノのインターネット)デバイス:** IP化されたプロジェクター、サーモスタット、照明コントロール、セキュリティカメラなど、従来にはなかったタイプのアンマネージドデバイスが幅広く使用されるようになったことで、攻撃の対象が広がりました。
- **不正なデバイス:** 従業員は善意から安価な有線ハブ、部署ごとのサーバー、ルーター、およびワイヤレスアクセスポイントを追加して、ネットワークを不安定にし、脆弱性を生じさせることがあります。
- **マルウェアおよびボットネット:** ネットワークが侵害されるとネットワーク接続デバイスが「ピボット攻撃」に利用され、外部者がネットワークをスキャンして、データを盗むことがあります。
- **コンプライアンス:** 誤って設定されたエンドポイントおよび仮想マシンに、不適切な設定やソフトウェアが含まれていることがあります。さらに、悪意のあるユーザーまたはマルウェアによって意図的に無効にされ、セキュリティコントロールが停止される可能性もあります。

見えないものは防げない

可視性が制限されていると、セキュリティに盲点が生じます。多くのエンドポイントセキュリティシステムでは、デバイスを監視、管理するため、デバイスに最新のエージェントがインストールされていることが必要です。通常、ITセキュリティの責任者には、アンマネージドBYODエンドポイントや毎日ネットワークで増加するIoTデバイスの存在の可視性がまったくありません。

ForeScout CounterACT®のしくみ

ForeScout CounterACTは、IPアドレスが割り当てられたネットワークデバイスを監視してコントロールし、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ユニークな機能を提供しています。具体的には以下のとおりです。

監視 CounterACTアプライアンスは、インラインではない接続方法でネットワークにデプロイされます。その後、ネットワークトラフィックを継続的にモニタリングし、ネットワークインフラと連携して、デバイスがネットワークにアクセスした瞬間に識別します。CounterACTには、IPアドレスが割当てられた多数のエンドポイント、ユーザーおよびアプリケーションを監視するユニークな機能があります。実際、CounterACTの高度なテクノロジーは、他社製品では認識できないデバイスも検出することを可能にしています。

CounterACTの機能はそれだけではありません。検出後、CounterACTは受動的または能動的な反応測定技術を活用して、ネットワーク上のエンドポイントを分類します。CounterACTではデバイスの種類、位置、ユーザー、デバイスがドメインのメンバーかどうか、その他の基本的情報を識別できます。また、管理者用の資格情報を使って会社所有のデバイスを問い合わせ、デバイスのセキュリティ状態に関する詳細情報を取得できます。

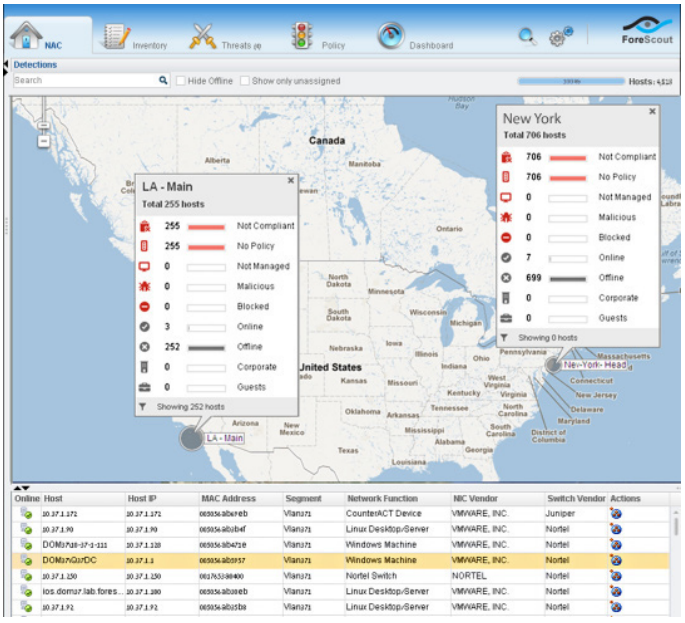

図1: ForeScout CounterACTは、ネットワーク上のデバイスに関する概要および詳細情報の両方を提供できます。

コントロール。 CounterACTによってエンドポイントにセキュリティ上の問題が検出された場合、高度なポリシーマネージャーが問題の重大度に応じてさまざまな対応を自動的に実行できます。軽微な違反の場合は、エンドユーザーに警告メッセージが送信されます。自分のデバイスを持ち込む従業員や契約ベンダーは、自動化オンボーディングポータルにリダイレクトされます。重大な違反については、デバイスのブロックや隔離、セキュリティエージェントの再インストール、エージェントまたはプロセスの再起動、エンドポイントによるオペレーティングシステムパッチの取得トリガー、その他の緩和・修復措置アクションが実行されることがあります。

アナリスト、顧客、パートナー企業に選ばれたCounterACT

- ForeScoutは、その実行能力とビジョンの完全性に基づいて、ガートナーのネットワークアクセスコントロールのマジック・クアドラント**で4回連続「リーダー」に選出されています
- SCマガジン「ベストNACソリューション」、2015年6月
- SCマガジン「ベストバイ」、2014年10月

> 「当社には、業務を中断するリスクを侵すことなく迅速に展開できるNACソリューションが必要だった。加えて、Aruba®やCisco®の製品が混在するITインフラをサポートする必要もあった。ForeScout CounterACTはこれらの要件をすべて満たすだけでなく、既存のFireEye®およびArcSight®セキュリティツールとの優れた統合能力など、ほかにも多く優れた機能を提供していた。さらに、複数の自動化セキュリティチェックやコンプライアンスコントロールを最も効果的な方法で実現することから、当社ではCounterACTを当社情報セキュリティ部門の「スイス・アーミーナイフ」と呼んでいる」
>
> **ー アリ・クトルハン・アクタス氏、情報セキュリティ/リスク管理部門主任、KKB**

ControlFabricアーキテクチャの価値

ControlFabricアーキテクチャは、ForeScout CounterACTの機能と、他社ネットワーク、セキュリティ、モビリティ、およびIT管理製品を結びつける接着剤の役割を果たします。縦割り型セキュリティの壁を打ち破り、次を実現します:

- システム全体のセキュリティ管理を統一
- 作業効率向上を達成
- 脅威に対する対応を加速
- セキュリティへの投資効率をアップ
- ネットワークセキュリティとコンプライアンス順守の姿勢を大幅に向上

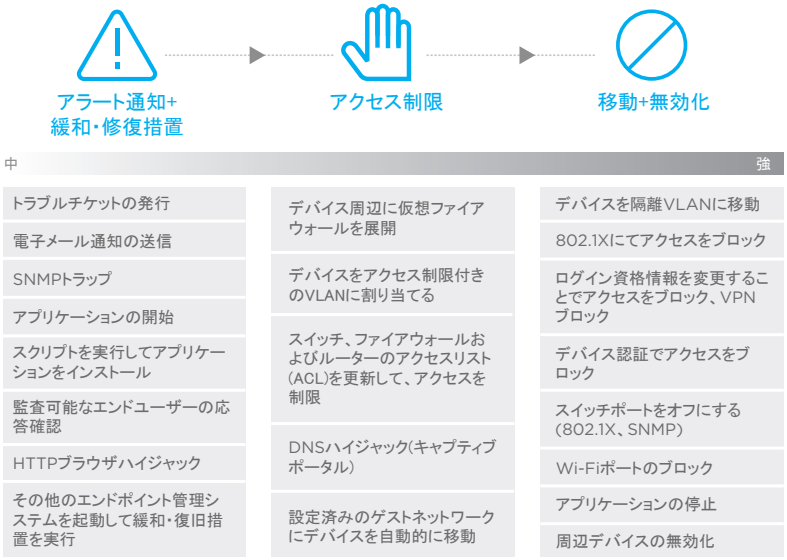

図2: ForeScout CounterACTでは、幅広いコントロールアクションを実行できます。

オーケストレーション。 CounterACTは、ForeScout ControlFabric®アーキテクチャを利用して、既存のセキュリティおよびシステム管理ツール間での情報共有や運用のオーケストレーションを行います。ControlFabricアーキテクチャでは、これはカスタム統合またはプラグアンドプレイのソフトウェアモジュールにより実現されます。ForeScoutテクノロジーパートナーと共同開発されたForeScout基本および拡張モジュールにより、70を超える最先端のネットワーク、セキュリティ、モビリティおよびIT管理製品*にCounterACTのパワーが適用され、以下の機能が提供されています:

- コンテキストの詳細情報をITセキュリティおよび管理システムと共有
- 共通のワークフロー、ITタスクおよびセキュリティプロセスをシステム間で自動化
- セキュリティリスクやデータ漏洩を緩和・復旧するため、システム全体の応答を加速

機能

全般

インラインではない形でのデプロイ: インラインではない形で既存のネットワークにデプロイされるため、ネットワーク遅延や障害が発生するリスクはありません。

可視性: 資産インベントリー機能により、リアルタイムの多次元の可視性とコントロールが提供され、ユーザー、アプリケーション、プロセス、ポート、外部のデバイスなどを記録してコントロールすることができます(図1を参照)。

オープンな相互運用性: CounterACTは、メジャーなスイッチ、ルーター、VPN、ファイアウォール、エンドポイント、オペレーティングシステム(Windows®、Linux、iOS、OS X、およびAndroid)、パッチ管理システム、アンチウィルスシステム、ディレクトリおよびチケット発行システムと連携します。インフラを変更したり、機器をアップグレードしたりする必要はありません。

レポート機能: 完全に統合されたレポートエンジンが、ポリシーコンプライアンスレベルのモニタリング、監査における規制要件の適合、リアルタイムインベントリーレポートの作成を支援します。

スケーラビリティ: 100万台を超えるエンドポイントが存在するお客様のネットワークで導入実績があります。CounterACTアプライアンスは、お使いのネットワークの規模に合わせて提供されます。

認定: ミリタリーグレードの性能と品質を提供するCounterACTは、以下の認定を受けています:

- USMC Authority to Operate (ATO)
- U.S. Army CoN (Certificate of Networthiness)
- UC APL (Unified Capabilities Approved Product List)
- Common Criteria Evaluation Assurance Level (EAL) L4+

業務を中断しない導入: ユーザーやデバイスに支障は生じません。自動コントロールへの移行は段階的に進め、最も問題のある箇所から始めて段階的に適切なアクションを選択することができます。

ポリシー管理: 企業にとって適切なセキュリティポリシーを作成します。ビルトインのポリシーテンプレート、ルールおよびレポートがあらかじめ用意されているため、設定と管理はすばやく簡単に完了します。

ControlFabricアーキテクチャ: ControlFabric®アーキテクチャにより、他社ベンダーとの優れた相互運用性とオープン統合アーキテクチャが提供されます。

エンドポイント

エージェントレス: エージェントなしに、ネットワークアクセスを識別、分類、認証、コントロールします。CounterACTにエンドポイントに対する管理用の資格情報がある場合、エージェントなしでエンドポイントの精査を実行します。BYODなど、CounterACTに管理用の資格情報がないエンドポイントの場合は、CounterACTに同梱のSecureConnectorエージェントを無償で活用して精査を実行できます。

エンドポイントコンプライアンス: 企業ネットワーク上のエンドポイントが、アンチウィルスポリシーに適合しており、適切なパッチが適用されていて不正なソフトウェアが含まれていないことを保証します。CounterACTは、ポリシー違反の識別、エンドポイントのセキュリティ不具合の修復、規制準拠レベルの評価を自動的に行います。

脅威の検出: ネットワークへの接続と切断を繰り返すデバイスもあるため、継続的モニタリングにより一回限りの脆弱性スキャンよりもタイムリーで正確な詳細情報を取得できます。

不正なデバイスの検出: 無許可のスイッチやワイヤレスアクセスポイントなど、不正なインフラを検出します。CounterACTでは、機密情報を盗むことを目的とした、ステルス性の高いパケットキャプチャデバイスなど、IPアドレスを持たないデバイスも検出できます。

アクセス

ゲストの登録: 社内ネットワークセキュリティを侵害させることなく、ゲストのネットワークアクセスを許可します。複数のゲスト登録オプションから、組織のニーズに合わせてゲスト承認プロセスをカスタマイズできます。

ロールベースのアクセス: CounterACTは、ユーザーにロールを割り当てる既存のディレクトリを利用して、正しいデバイスを使う正しいユーザーが正しいネットワークリソースにアクセスできるようにします。

柔軟なコントロールオプション: 厳格なコントロールを採用してユーザーの業務を中断する従来のNAC製品とは異なり、CounterACTでは、状況に応じて応答を調整できる、幅広い適用オプションが提供されています。低リスクの違反については、エンドユーザーに通知を送信するか、セキュリティの問題の緩和・修復措置を自動実行することにより、処理中もユーザーの作業効率を維持することができます(図2を参照)。

802.1X認証あり、またはなし: 802.1X、またはLDAP、Active Directory®、RADIUS®、Oracle®、Sunなど、その他の認証テクノロジーを選択できます。ハイブリッドモードでは複数のテクノロジーを同時に使用でき、これにより大規模かつ多様な環境へのNACソリューションの導入を速めることができます。

ビルトインRADIUS: ビルトインRADIUSサーバーによって802.1Xの展開が簡単になります。または、CounterACTをRADIUSのプロキシとして設定することで、既存のRADIUSサーバーを活用することも可能です。

スケーラブルなモデル

CounterACTは、100万台を超えるエンドポイントが存在するお客様のネットワークで導入実績があります。物理的および仮想アプライアンスに関する一連のオプションにより、お客様のビジネスの特定のニーズに対応することができます。複数のアプライアンスを必要とする大規模ネットワークであっても、CounterACT Enterprise Managerで一元管理できます。各CounterACTアプライアンスには、ネットワークデバイスの無期限ライセンスが一定数含まれています。ライセンス許諾ポリシーの詳細については、www.forescout.com/licensingをご覧ください。

管理およびコントロールの一元化

CounterACT Enterprise Managerは、物理または仮想アプライアンスとしてデプロイして、CounterACT実装の管理とコントロールを一元化することができます。CounterACTの活動およびポリシーを監督し、各アプライアンスにおける悪意ある活動に関する情報だけでなく、CounterACTによる識別、通知、制限および緩和・修復措置に関する情報も収集します。これらの情報はCounterACTコンソールにて表示、報告することができます。

詳細については
www.ForeScout.com
をご覧ください。

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

*2016年1月時点。
**ガートナー、「マジック・クアドラント - ネットワークアクセスコントロール」、ローレンス・オレンス&クラウディオ・ネビア、2014年12月10日。ガートナーは、ガートナー・リサーチの発行物に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。また、最高のレーティングまたはその他の評価を得たベンダーのみを選択するように助言するものではありません。ガートナー・リサーチの発行物は、ガートナー・リサーチの見解を表したものであり、事実を表現したものではありません。ガートナーは、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の保証を行うものではありません。