組織の課題

- 全体的なネットワークセキュリティの向上
- 外部の脅威から機密データを保護
- 従業員、契約ベンダー、お客様によるアクセスは妨げない
- 内部ポリシーおよび外部規則の順守
- 既存のセキュリティ投資の価値を維持

技術的な課題

- エージェントソフトウェアを持たない不明なデバイスをネットワーク上で検出
- デバイスの種類、場所、ユーザーID、役割、およびコンプライアンスレベルの識別
- 非対応または感染したデバイスによるマルウェア拡散の防止
- 標的型攻撃によるデータ盗難やネットワークダウンタイムの防止
- ユーザーの介入なしに、状況に応じて適切な措置を自動的に講じるNACソリューションを探す
- セキュリティコントロールの効果を評価し、規則のコンプライアンス状況を表示

ネットワークアクセスコントロール

デバイスのネットワークアクセス時にリアルタイムの可視化とコントロールを実現

ForeScout Technologies, Inc.は、毎日種類と数において劇的に増加しているネットワークアクセスデバイスのコントロールと管理を行うユニークなソリューションを提供します。当社の旗艦製品ForeScout CounterACT®は、リアルタイムの可視化機能を備えており、認証済みおよび無許可のデバイスを瞬時に検出して、状況に応じてアクセスをコントロールできます。

直面する問題

今日の企業ネットワークにはパソコン、タブレット、スマートフォンから産業用制御システム、仮想サーバー、ワイヤレスアクセスポイント、クラウドベースのアプリケーションに至るまで、従来のデバイスや従来とは異なる多種多様なデバイスおよびエンドポイントが接続されます。さらに、BYOD*、IoT*、ハイブリッドIT環境、高度なハッキング技術が広まるにつれ、デバイスに関連する問題の範囲が広がることは疑いようもありません。それで、ネットワークアクセスコントロール(NAC)ソリューションでは、企業所有のデバイスだけでなく従業員所有のデバイス、また既知のデバイスだけでなく、大幅に増加する傾向にある無許可の正体不明なデバイスによるアクセスを管理しなければなりません。

包括的かつ高度にインテリジェントなNACセキュリティソリューションの必要性を強調するいくつかの事実を以下に示します:

- 2020年までに260億台のネットワーク接続デバイスが使用される[1]
- モバイルアプリの75%は基本的なセキュリティテストに不合格[2]
- 2014年に発生したデータ漏洩の98.7%は外部からのハッキングが原因[3]

IT管理者またはセキュリティシステム管理者は、ネットワークへの接続を試行している、またはすでにログオンしているデバイスやシステムが組織のセキュリティ基準に適合しているかどうかを知っておかなければなりません。

ForeScoutのソリューション

ForeScout CounterACT®は、ネットワークにアクセスした瞬間にデバイスを可視化する機能に基づいて、総合NAC機能およびその他の機能を提供します。CounterACTは継続的にネットワークをスキャンし、既知の会社所有のデバイスだけでなく、従業員所有のデバイスや不正なエンドポイントなど不明なデバイスの活動を監視します。さらに、ポリシーに基づく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自動化して強化できます。ForeScout CounterACTには、可能な最大限の範囲においてユーザーエクスペリエンスを保ち、ビジネスオペレーションを継続させるための幅広い種類の自動コントロールが用意されています。

CounterACTのインテリジェンスと機能の基盤は、以下の3点に要約できます:

監視 CounterACTは、ソフトウェアエージェントや従来のデバイスに関する知識を要することなく、デバイスがネットワークに接続した際に瞬時に検出するユニークな機能を提供します。CounterACTは、マネージドデバイス、個人所有のデバイスやその他のエンドポイントに対して継続的にモニタリングし、デバイス、ユーザー、アプリケーションおよびオペレーティングシステムのプロファイルを作成して分類します。

コントロール CounterACTはデバイス状態とセキュリティポリシーに基づいて、ネットワークアクセスを許可、拒否または制限できます。またCounterACTは、悪意のある、または高リスクのエンドポイントを評価して緩和・修復措置をとることで、組織全体のリスクとなりえるデータ侵害およびマルウェア攻撃の脅威を軽減します。さらに、ネットワーク上のデバイスを継続的にモニタリングして、セキュリティポリシーに基づいてコントロールすることで、業界標準や規制に対するコンプライアンスが劇的に効率化されます。

オーケストレーション CounterACTは、ForeScout ControlFabric®アーキテクチャにより、70種類を上回るネットワーク、セキュリティ、モビリティおよびIT管理製品**と統合できます。リアルタイムでセキュリティ情報を複数のシステム間で共有し、統一されたネットワークセキュリティポリシーを強化する能力により、システム全体への脅威に対する対応を自動化し、脆弱性を軽減します。さらに重要なこととして、既存のセキュリティツールのROI(投資対効果)を高め、ワークフローの自動化によって時間を節約できます。

ForeScout CounterACTは、エンドポイント、その位置、所有者および内容に関するコンテキストの詳細を収集します。以下のことを保証できます:

- ネットワーク上に無許可のデバイスまたは未認可のアプリケーションがないこと
- 認証済みのデバイスで最新のオペレーティングシステムが使用されている、最新のアンチウィルスソフトウェアがインストールされ実行されている、脆弱性に対して適切なパッチが適用されていること
- 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
- ユーザーは無許可アプリケーションまたはネットワーク上の周辺機器を実行できないこと

エンドポイントが組織の基準に適合していない場合、CounterACTは、電子メールによる不適合の通知や、ソフトウェアアップデートなどの必要措置、徹底した隔離やアクセス阻止など、さまざまなポリシーベースの施行および緩和・修復措置アクションを自動的に開始します。ゲストアクセスの管理、システムの位置検索およびネットワークポートの開閉に関連する操作をユーザーが行う必要はありません。ネットワークアクセスはポリシーに基づいてコントロールされます。

ForeScoutは、世界60か国にわたる2,000社超の企業**に対し、最高レベルのセキュリティ基準や規制のコンプライアンスに適合し、使いやすく展開しやすい、インテリジェントで費用効果の高いネットワークアクセスコントロールを提供しています。CounterACTは仮想または物理的なアプライアンスとして販売しており、ほとんどの場合、いずれもネットワーク設定を変更せずに既存のインフラに導入できます。CounterACTアプライアンスは物理的に帯域外でインストールできるため、待ち時間やネットワーク障害による問題を回避することができます。膨大な数のエンドポイントを、一元化されたコンソールから動的に管理できます。

詳細については
www.ForeScout.com
をご覧ください。

ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 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
Fax 1-408-371-2284

1 ガートナー・リサーチ、http://www.gartner.com/newsroom/id/2636073
2 ガートナー・リサーチ、2014年9月 http://www.scmagazine.com/gartner-75-percent-of-mobile-apps-will-fail-security-tests-through-end-of-2015/article/372424/
3 Privacy Rights Clearinghouseリサーチ、http://www.securityweek.com/data-breaches-numbers

*BYOD(私的デバイス活用)、IoT(モノのインターネット)
**2016年1月時点