継続的な診断と緩和策

情報資産について許容できる一貫したレベルの機密性、完全性および可用性を保証するため、行政機関のIT部門は増加する規制、指令、および規格に準拠する必要があります。主な目的は、侵入の阻止(機密性)、秘密情報の保護(完全性)、サービス妨害攻撃への露出の緩和(可用性)です。

CDM(継続的診断および対策)プログラムとは、サイバー攻撃から行政機関のネットワークおよびシステムを防御するためのダイナミックなアプローチです。CDMにより、連邦政府機関および官公庁にサイバーセキュリティのリスクを継続的に識別する機能とツールが提供され、潜在的なインパクトに基づいてリスクに優先順位を設定できるため、サイバーセキュリティ担当者は最初に最も重要性の高い問題から処理できます。米国議会は、リスクに基づく費用対効果の高い十分なサイバーセキュリティを確立し、サイバーセキュリティ担当の人員を効率よく割り当てるためにCDMプログラムを設立しました。

CDMプログラムの「継続的」とは、24時間365日ということではなく、情報の価値や想定されるリスクレベルに基づき、一定の間隔で評価を繰り返すことを意味しています。連邦政府刊行物では、セキュリティコントロールの変動、保護対象機能や識別済みの弱点がシステムに与えるインパクトのレベルに基づいて、評価の頻度を決定するガイドラインが設けられています。ガイドラインでは、CDMセキュリティプログラムで応答の許容可能レベルの評価と監査に使用する指標としてDIL(検出間隔レイテンシ)を定義しています。

CDM順守に関する課題

CDMでは受動的な対処と文書化によるアプローチではなく、能動的で、データ中心、リスクベースの対処が求められています。プロセスとデータの統合は組織、データ、およびシステムの境界を超えなければならないため、一般にセキュリティインフラに対する大幅な変更が必要とされます。CDMフレームワークでは、データ収集、資産管理およびリスク管理プロセスは定期的ではなく、継続的に、環境全体で行われます。IT組織にとって最大の技術的課題は、継続的なデータフローの統合と相関に関するものです。

IT環境の情報が更新された場合、CDMシステムには、しきい値を上げ、ネットワークポリシーやコントロールアクションを調整することにより、継続的フィードバックのループで情報を取り込んで応答することが求められます。さらにCDMでは、米連邦政府の上級セキュリティ担当者による連邦政府のセキュリティの健全性およびリスク管理情報の可視性を向上させる点で支援すべく、多大な費用のかかるセキュリティ運用を合理化させることも求められています。効果的な導入においては、継続プロセスからデータを収集し、複数のコンテキスト要因を関連付け、ふさわしい場合はアクションを自動化し、残る問題に優先順位を付けて表示する必要があります。

CounterACTセキュリティプラットフォーム

ForeScout CounterACTセキュリティプラットフォームは、CDMの基礎として、マネージド、アンマネージド、さらに従来のものとは異なるデバイスのリアルタイムの監視、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。具体的には以下のとおりです。

監視

- エージェントを要することなく、ネットワークへの接続時にデバイスを瞬時に検出
- 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、分類
- マネージドデバイス、BYODおよびIoTエンドポイントを継続してモニタリング

コントロール

- デバイス状態および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
- 高リスクや悪意のあるエンドポイントを評価して修復
- 業界標準・規制に対するコンプライアンスを向上

オーケストレーション

- 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

ハイライト

リアルタイムの可視化。エンドポイントがネットワークに接続する際に、自動化された、リアルタイムの可視性を実現します。IPアドレスを使用しない、ステルス性の高いスニファーデバイスも検出できます。

アクティブな資産管理。デバイス、ハードウェア、オペレーティングシステム、アプリケーション、パッチレベル、プロセス、オープンポート、周辺機器、ユーザーなど、ネットワークのリアルタイムインベントリーを生成します。

ポリシーベースのアクセスコントロール。スイッチポートのセキュリティを保護するため、ネットワークアクセスを802.1X認証あり、または802.1X認証なしのユーザーとデバイスに制限します。

継続的モニタリング。エンドポイントのセキュリティおよびコンプライアンス状態を、ネットワークへの接続前後においてリアルタイムで評価します。エンドポイントの設定に関する違反、悪意のある行動を検出し、違反の重大性に基づいて応答を調整します。

緩和・修復措置の自動化。エンドポイント設定や保護システム、パッチ、アップデートの自動更新、アプリケーションまたは周辺機器のインストール、アクティベーション、または無効化など、不適合エンドポイントに対する緩和・修復措置を自動化します。

HBSS統合。ホストベースセキュリティシステム(HBSS)エージェントがない、または不具合があるエンドポイントの検出、および緩和・修復措置の自動化により、状況認識およびインシデント応答を向上させます。HBSSが評価するコンプラアインス基準に基づいて、ネットワークアクセスを許可、拒否または制限します。

コンプライアンスレポート機能。ポリシーコンプライアンスのレベルを表すリアルタイムのレポートを作成します。設定時間までスキャンを待機するのではなく、ホストがネットワークに接続する際にコンプライアンスに関するスキャンを開始することで、DIL(検出間隔レイテンシ)を低減します。

導入要件

CDMを導入する組織は、リアルタイムの資産検出および脆弱性管理、自動化された、インテリジェンス主導の応答メカニズム、企業管理システムへの継続的なデータフィードバックに投資しなければなりません。さらに、システムは既存のITフレームワークに簡単に導入できる必要があります。

リアルタイムの資産検出および脆弱性管理システムについては、オペレーティングシステムまたはフォームファクターから独立した、ネットワークのシステムを検出し、プロファイルを作成するため、受動的および能動的な検出、モニタリング技術を組み合わせて活用しなければなりません。受動的な検出技術では、トラフィックをモニタリングしてアクティブなデバイスを監視します。能動的な検出技術では、ネットワークを検査してアイドル状態のデバイスを検出します。これら両方の技術を活用することで、IT資産の完全かつ一貫した可視化が実現します。ネットワークでデバイスのインストールや再設定が行われると、その瞬間に変更を検出でき、デバイスに対する評価を実行できます。最後に、資産管理システムにはネットワークのエンドポイントのセキュリティ状態や脆弱性を評価する機能が含まれていなければなりません。

自動化された応答システムについては、資産検出および脆弱性管理システムからのデータを取り込み、この情報とエンドポイントの動作について認識されている情報に基づいて、組織へのリスク緩和のための一連のインテリジェントな応答を生成しなければなりません。応答はポリシーコンプライアンス違反の重大性やエンドポイントの動作に基づいて適切なものにする必要があります。たとえば、応答システムでは次のようなアクションを実行できる必要があります:

- アラートを担当者または適切なIT管理チームに送信する
- エンドポイントの緩和・修復措置を自動的に行う、または他社システムによる措置をトリガーする
- ネットワークアクセスを制限する
- ネットワークアクセスをブロックする

資産データおよび自動コントロールアクションは、システム全体の効率と効果を向上させるために、CDMシステムの他の部分にもフィードバックとして共有される必要があります(図1を参照)。たとえば、組織のセキュリティ情報/イベント管理(SIEM)システムとCDMシステムをリンクさせることで、SIEMシステムによって生成されるコンプライアンスレポートの正確性を保証できます。

また、アンチウィルス、パッチ管理およびモバイルデバイス管理(MDM)システムなどのエージェントベースのシステムがネットワークのアンマネージドエンドポイントの存在を認識できるようにするため、CDMシステムから情報を提供することも必要です。

最後に、CDMシステムはすばやく簡単に導入できる必要があります。たとえば、次のような要件を満たす必要があります:

- ネットワークを再構築せずに既存のネットワークインフラに導入可能
- 既存のネットワークインフラとの統合が可能
- インライン導入またはその他の単一障害点に依存しない
- エンドポイントエージェントの追加インストールを必要としない

ハイライト(続き)

モバイルおよびワイヤレスコントロール。スマートフォンやタブレットなどのモバイルデバイスを検出し、セキュリティコントロールを実施します。ワイヤレスネットワークインフラとの統合により、ワイヤレスコンプライアンスを強化します。

業務を中断しない導入。CounterACTはフェーズドアプローチにより段階的に導入できるため、業務の中断を最小限にとどめて導入成果を高めます。

IT相互運用性。ディレクトリサービス、パッチ管理、エンドポイント保護、脆弱性評価、SIEMおよびMDMシステムなどの既存のITインフラとの統合を活用します。

CDMの基礎となるForeScout CounterACT®

ForeScout CounterACT®は、CDMの要件を満たし、お客様のCDMソリューションにおいて中心的な役割を果たすことができます。CounterACTにより、ネットワークに接続されるスマートフォン、タブレット、ノートパソコン、その他の会社所有または個人所有のモバイルデバイスを含むエンドポイントはリアルタイムで可視化され、コントロールできるようになります。

CounterACTは、複数の検出技術を組み合わせた受動的・能動的反応測定技術を使用して、エンドポイントを正確に分類します。CouterACTのエージェントレスソリューションは、マネージドまたはアンマネージド、既知または不明かにかかわらず、さまざまな種類のエンドポイントと連携できます。

CounterACTでは、お使いのLAN/WAN環境にあるエンドポイントのセキュリティ状態を評価できます。通常、既存のエンドポイント管理システムではアンマネージドのBYODデバイスを認識できないため、この機能は特に重要です。CounterACTは、マネージドデバイス(ドメイン接続コンピューター)にエージェントを追加することなく、デバイスのセキュリティ状態を評価できます。これは、CounterACTシステムの迅速な導入および簡単な運用に役立つ非常に重要な要素となっています。アンマネージドのBYODデバイスについては、軽量な削除可能エージェントをインストールすることで、セキュリティ状態を評価できます。このエージェントは、Windows®、MacOSおよびLinuxをサポートしており、ユーザーがネットワークに接続してシステムに登録する際に自動的にデプロイされます。エージェントの有無にかかわらず、CounterACTは必須ソフトウェア、ソフトウェアおよびパッチのバージョン、デバイス設定、エンドポイントの脆弱性のモニタリングを含め、さまざまなコンプライアンスチェックを実行できます。CounterACTは最先端のネットワーク、セキュリティ、ホストベースのセキュリティシステムおよび識別プラットフォームと統合し、エンドポイントのリアルタイムの詳細情報とセキュリティ状態の情報を提供します。

ForeScout CounterACTには、エンドポイントのセキュリティ状態に応じて、緩和・修復措置として幅広いアクションが用意されています。CounterACTでは、適合しないホストに対して自動的に更新を行うようアンチウィルスサーバーに指示を出したり、デバイスのオペレーティングシステムを更新するようパッチ管理システムに指示を出したり、さらに無許可のソフトウェアを無効にしたりすることができます。加えて、CounterACTはSIEMシステムによるエンドポイント設定の詳細情報の提供、アクセスとコンプライアンス違反の関連付け、およびインシデント応答のスピードアップにも役立ちます。CounterACTには、ポリシーコンプライアンスの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するビルトインのレポートが含まれています。

CounterACTは仮想または物理的なアプライアンスとして販売されており、ほとんどの場合、いずれもインフラを変更することなく、またネットワーク業務に遅延を生じさせることなく、既存のネットワークにシームレスに導入できます。CounterACTアプライアンスはインラインではない形でインストールされるため、ネットワークの遅延や中断のリスクなしに、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。

ForeScout CounterACTではITリスク管理で実績あるアプローチを採用しています。ネットワークにアクセスするデバイスの識別、コントロール、緩和・修復措置(希望する場合)、そして継続的なモニタリングを通じて、コンプライアンスとネットワークの保護を保証します。CounterACTのコンプライアンスエンジンにより、セキュリティポリシーに適合しないデバイスまたはユーザーが検出され、ピアツーピア(P2P)アプリケーション、USBドライブ、スマートフォンを使用するなど、リスクのある活動またはその他の無許可の活動を行っているユーザーを追跡します。適合しないコンピューターやユーザーについては、不適合の理由やデバイスの位置など詳細情報とともにメインコンソールに表示されます。

最後に、CounterACTは、コンプライアンススキャナーを統合してイベントベースのスキャン機能を追加することで、IT担当の責任者が許容できるDIL(検出間隔レイテンシ)指標の設定を支援しています。この統合によりホストがネットワークに接続した際に、CounterACTからコンプライアンススキャナーがトリガーされます。このイベントベースのスキャンを追加することで、DIL指標が大幅に改善します。ForeScout CounterACTは、Tennable® Nessus、BeyondTrust® Retina、Qualys®など、さまざまな最先端のVA(脆弱性評価)スキャナーと統合でき、その他製品との統合も現在開発中です。

複雑性を軽減して効率を高める

これまでITセキュリティを担当する責任者はリスクごとに特定の技術ソリューションを用いて対応する傾向にありました。規制要件は専門のコントロールで対応し、短期的に許容できるレベルのセキュリティおよびコンプライアンスを達成していました。今日では、互いに独立するセキュリティソリューションは複雑性が高まり、複雑性によりリスクが上昇し、管理する人件費も増加することが知られています。ITコントロールが相互に接続していないことは、IT部門がリスク管理を効率化させる上で大きな課題となっています。また、これにより状況認識レベルが低下し、すばやい脅威の検出やリスク緩和・修復措置に必要な情報の取得が制限されます。

ForeScout CounterACTは、この問題の解決に役立ちます。CounterACTは既存のシステムを統合して、複雑性を排除して大幅な効率化を実現する、応答性と正確性の高い継続的モニタリングシステムを構築できるように設計されています。結果的にシステムによるリアルタイムの可視化が実現し、エンドポイントの精査、継続的なモニタリングおよび緩和・修復措置の自動化、他のセキュリティ管理システムとの統合、迅速な展開およびトータルコストの削減が可能になります。

図1: Desired State — ForeScout CounterACTは、ネットワークをリアルタイムで可視化し、既存の業務およびセキュリティインフラで双方向の情報共有を行います。

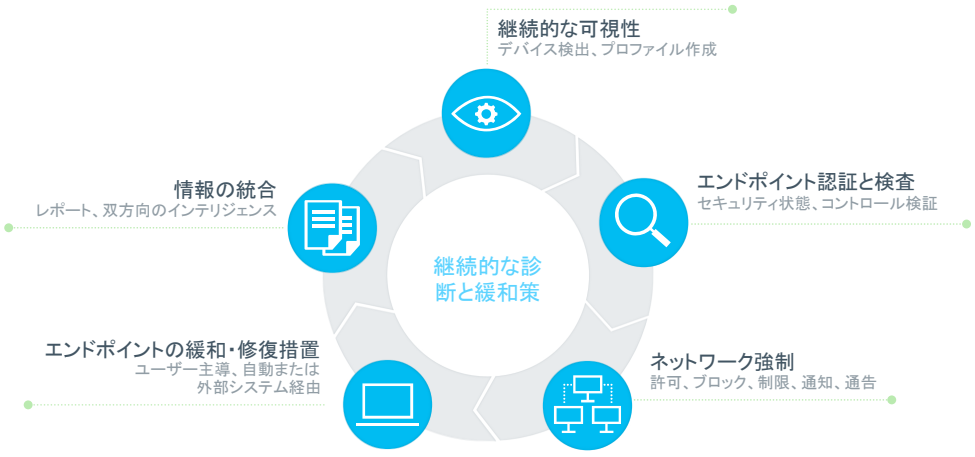

図2: ForeScoutのインテリジェントなセキュリティ自動化プラットフォームにより、リアルタイムの可視性と自動コントロールが提供されます。

継続的診断および緩和・修復措置の条件[1]		ForeScout CounterACT
資産検出および分類	ネットワーク上の無許可またはアンマネージドのハードウェア、およびネットワーク上のIT資産に含まれる無許可またはアンマネージドのソフトウェア設定を検出します。	CounterACTでは、リアルタイムでネットワークデバイスが検出され、ハードウェアおよびソフトウェア資産の包括的なデータベースが管理されます。このインベントリーは、さまざまなハードウェアまたはソフトウェアの属性で検索でき、整理できます。インベントリーレポートも生成可能です。
評価	エンドポイントのセキュリティ状態を評価し、正確でタイムリーなソフトウェアインベントリーを作成することは、ソフトウェアの脆弱性やセキュリティ構成設定に対する状況認識および効果的なコントロールを支援する上で欠かすことができません。	CounterACTでは、お使いのLAN/WAN環境にあるエンドポイントのセキュリティ状態を評価できます。通常、既存の管理システムではアンマネージドのBYODデバイスを認識できないため、この機能は特に重要です。CounterACTでは必須ソフトウェア、ソフトウェアおよびパッチのバージョン、デバイス設定、エンドポイントの脆弱性のモニタリングを含め、さまざまなコンプライアンスチェックを実行できます。他のホストベースのエージェントやツール、および脆弱性スキャナーと統合され、詳細なコンプライアンス情報を取得できます。
認証およびアクセスコントロール	無許可のネットワーク接続/アクセスを防止、削除および制限し、攻撃者が内部および外部のネットワーク境界を利用してさらに機密な場所へのネットワークアクセスを取得したり、ネットワーク上の動的または静的なデータにアクセスしたりすることを防ぎます。アカウントのアクセス、セキュリティ関連の行動、資格および認証情報を管理します。	CounterACTは、無許可デバイス(ネットワークへの接続後に不適合になる場合も含む)へのアクセスをブロックまたは制限できます。CounterACTはイベント駆動型のシステムで、エンドポイントのオペレーティングシステムの設定に変更が生じた場合は再評価を行います。
緩和・修復措置の自動化	攻撃対象領域を少なくし、システムの脆弱性が残る部分に到達するのに必要な労力を増やすため、弱点を最小限に抑えるよう意識的にシステムを設計し、基準に適合するシステムを構築することにより、システムの脆弱性が利用されることを防止します。	コンプライアンス違反が検出された場合、CounterACTは、アラート発行またはITスタッフへの通知、緩和・修復措置の自動実行、不適合エンドポイントの隔離やブロックなど、違反の重大度に基づいた応答を実行できます。また、パッチ管理など他社システムとインターフェースすることも可能です。
状況認識	エンドポイント状況を正確でタイムリーに把握することは、ネットワークにおける組織に関するあらゆるセキュリティ問題の状況認識、効果的なコントロール、報告を支援するうえで欠かすことができません。	CounterACTは、ネットワークのエンドポイントを識別し、エンドポイントライフサイクル管理製品、資産管理システム、データベース、SIEM、VA、アンチウィルス製品など、他のセキュリティ管理システムと統合して、総合的な状況認識を可能にし、エンドポイントのリアルタイム情報とセキュリティ状態を把握できるようにします。また、SIEMシステムによるエンドポイント設定の詳細情報の提供、アクセスとコンプライアンス違反の関連付けも支援します。

[1]参照元「継続的診断および緩和・修復措置の条件」
https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=f154da08471898c2e7a9ab05595c3df6

ForeScout ControlFabric®アーキテクチャ

ForeScout CounterACTとお使いのCDMソリューションとの統合は、他のITシステムとの統合と同様、ForeScout ControlFabricアーキテクチャを活用して実現されます。ControlFabricはオープン統合テクノロジーで、ForeScout CounterACTと他のソリューション間で情報を交換し、さまざまなセキュリティ問題の緩和・修復措置を効率化します。詳細についてはwww.forescout.com/controlfabricをご覧ください。

ForeScout にご相談ください

ご興味のあるForeScoutソリューションについてお知らせください。無償でオンサイト評価を実施いたします。

ForeScoutについて

ForeScout Technologies, Inc.は「可視化」によってセキュリティを革新します。ForeScoutでは、最新デバイスを含め、さまざまなデバイスがネットワークに接続した瞬間に監視するユニークなソリューションを、Global 2000企業および行政機関に提供しています。さらに重要なのは、ForeScoutではこれらのデバイスをコントロールし、異なるタイプのセキュリティツール間で情報共有や操作のオーケストレーションを行うことにより、インシデント対応を促進できることです。従来のセキュリティシステムとは異なり、ForeScoutソリューションではソフトウェアエージェントまたは従来のデバイスに関する知識を必要としません。当社のソリューションは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管理製品を統合することで、縦割りセキュリティの問題を解決し、ワークフローの自動化および多大なコストの削減を実現します。ForeScoutソリューションは、60を上回る国々で2,000社超の企業にご利用いただいており、お客様のネットワークセキュリティやコンプライアンスへの取り組みの改善を支援しています。*

詳細についてはwww.forescout.comをご覧ください。

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

*2016年1月時点