ForeScout

ForeScout

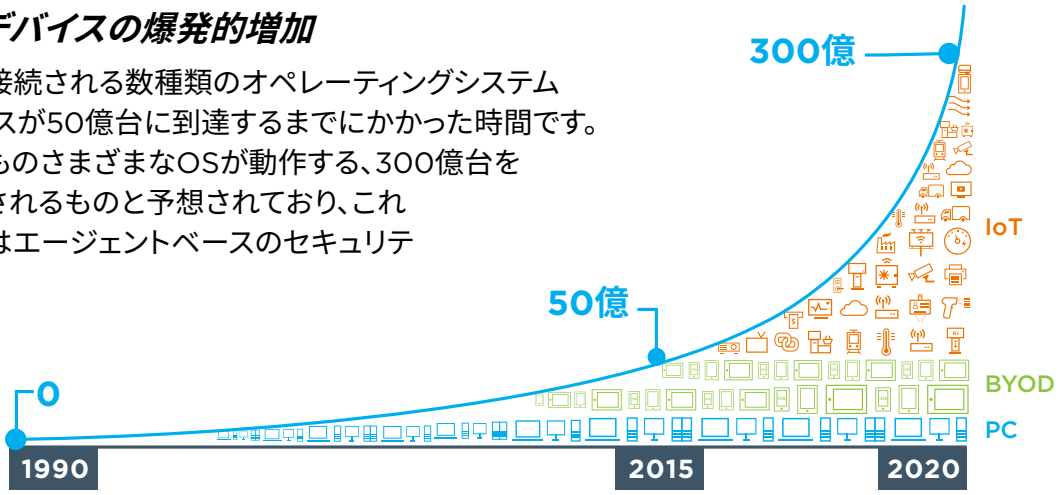
可視化によるセキュリティの革新

監視

課題:

OS基盤およびIoTデバイスの爆発的増加

25年 – ネットワークに接続される数種類のオペレーティングシステム(OS)が動作するデバイスが50億台に到達するまでにかかった時間です。2020年までには数百ものさまざまなOSが動作する、300億台を超えるデバイスが使用されるものと予想されており、これらのデバイスの大多数はエージェントベースのセキュリティ対策ではとても管理しきれなくなるでしょう。ネットワークの「盲点」とそれらに対する攻撃が増え続ける中で、まったく新しいアプローチが必要になります。



ABI Research、2017年

モノのインターネット(IoT)の急成長、新しいOSの登場やモビリティの発展により、アンマネージドデバイスが爆発的に増加している。

ソリューション:

エージェントレスの可視化とコントロール

ForeScoutは、デバイスをリアルタイムで発見、分類、評価、監視するエージェントレスアプローチを開拓しました。このアプローチでは、オンプレミスからクラウドまでネットワーク上に存在するデバイスを可視化し、安全に管理することができます。

実現する方法:

今日のビジネスは画一的で標準的なネットワークで運営されているわけではありません。絶え間なくダイナミックに変化しています。ForeScoutでは、オンプレミスのデバイスからデータセンターやパブリック/プライベートクラウド環境で動作するデバイスまで、ネットワーク全体を可視化する**異種環境における統合セキュリティ**を提供します。ForeScoutの**非常に柔軟**で**ベンダーに依存しない**アプローチは、802.1X、非802.1Xまたはその両方を実行する有線および無線ネットワーク上のCisco、Aruba、Juniper Networksやその他のシステムをサポートします。

セキュリティは、ネットワーク上に何が接続されているかを知ることから始まります。ForeScoutは、管理エージェントや事前にデバイス情報を知る必要なく、会社のインフラ、物理/仮想システム、管理/非管理エンドポイント、IoTおよび不正デバイスを**発見**します。次に、デバイスのウイルス予防策を**評価**し、セキュリティ状態を**継続的に監視**します。

ForeScoutの**アダプティブデータ収集**機能は**機能は管理者が必要とするデータセットをサポート**し、右記の優れたアクティブ/パッシブ技術を活用して詳細な可視化を実現します。ForeScoutソリューションはデバイスおよびアプリケーションをすばやく評価し、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、パッチの適用状況と、セキュリティエージェントの有無を確認します。この情報により、適切なアクセスコントロール、対策、および緩和・修復ポリシーを導入できます。

ForeScoutテクノロジーによるデバイスの詳細な検出手法

1. 一連の接続デバイスに対してスイッチ、VPNコンセントレーター、アクセスポイントおよびコントローラーのポーリングを行い接続デバイスの一覧を作成
2. 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
3. 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
4. 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
5. ネットワークスイッチポートアナライザーポートを監視し、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)
6. ネットワークマッパー(Nmap)スキャンを実行する
7. 資格情報を利用したデバイスのスキャンを実行する
8. NetFlowデータを受信する
9. 外部メディアアクセスコントロールアドレスの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
10. 公開/非公開クラウドの仮想マシンを監視する
11. PoEおよびSNMPを使ってデバイスを分類する
12. 任意のエージェントを使用する

非常に困難なユースケースも解決

IoT (モノのインターネット):

エージェントを利用せずに、ネットワークへの接続時にIoTデバイスを瞬時に検出します。デバイス、ユーザー、アプリケーション、オペレーティングシステムを分類してプロファイルを取得し、デバイスを安全なVLAN (仮想ローカルエリアネットワーク) セグメントに自動的に割り当てて動作を監視します。

ネットワークアクセスコントロール:

ネットワークアクセス時にデバイス、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をリアルタイムで可視化します。問題がある場合はユーザーやITスタッフに通知し、デバイスの制限、ブロック、隔離またはVLANセグメントへの再割り当てなど、適切なアクセスコントロールを自動的に適用します。

ゲストネットワーキング:

訪問者、委託業者、提携パートナーの登録を自動化し、ポリシーに準拠する適切なオンボーディング方法を適用します。デバイスのセキュリティ状態に関する詳細情報を共有し、エンタープライズモビリティ管理ツールおよびエンドポイント保護ツールに準拠する対策アクションを統合的に決定して実施します。

BYOD セキュリティ:

従業員が所有するノートパソコン、タブレット、スマートフォンがネットワークに接続する際に、エージェントレスな可視性を提供します。ネットワークポートの制御に関わる手作業をなくし、アクセスコントロールとエンドポイントコンプライアンスポリシーへの準拠を強化します。

エンドポイントおよび規制コンプライアンス:

ネットワークに出入りするデバイスを監視し、古くなっていて基準を満たしていないセキュリティソフトウェア、オペレーティングシステム、構成設定などのポリシー違反についてユーザーに通知します。自己修復ポータルにユーザーを自動的にリダイレクトします。

安全なクラウドコンピューティング:

敷地内のデバイスと仮想マシンに対する可視性とコントロールをパブリッククラウド、プライベートクラウド環境にまで拡張します。既存のセキュリティオペレーションチームのスキルやプロセスを活用しながら、物理環境および仮想環境の状態を一元的に表示することができます。

コントロール

「デバイスをリアルタイムで発見、可視化、およびコントロールするIoTセキュリティ機構を導入している企業は現在ほんの5%ほどだが、2020年までには25%の企業が備えるようになるだろう」

*—ガートナー、IoTセキュリティにはリアルタイムの発見、可視化、制御が不可欠、*Saniye Burcu Alaybeyi およびLawrence Orans、2016年11月3日

課題:

セキュリティアラートの過多による不十分な対策

ほとんどのセキュリティツールはアラート送信を得意としているものの、対策を講じて強制的に実行する機能が備わっていません。結果として、セキュリティチームは大量のアラートと、手作業によるそれらの評価や解決に追われます。一部のアラートは誤報により無視され、その他のアラートは人手不足により対策が取られないままとなります。

ソリューション:

ポリシーベースのセグメント化および対策

ForeScoutは、デバイス、ユーザーおよびアプリケーションに対するポリシーベースのアクセスコントロールと対策を自動化することによって、特定のリソースへのアクセス制限、ゲストオンボーディングの自動化、エンドポイントセキュリティに準拠していない点を検出し、修正を可能にし、業界規制要件への準拠とさらなる改善を支援します。

実現する方法:

ForeScoutは、幅広いアクティブ/パッシブなアクションを**自動化**し、ポリシーと状況の重大度に基づいて**デバイス接続時のコントロールの実行**を可能にします。ForeScoutでは、ネットワーク上のデバイスが、デバイス動作を規定する一連のポリシーに、準拠していることを**継続的**に確認するためにポリシーエンジンを活用しています。デバイスを周期的にチェックする他社製品とは異なり、ForeScoutのポリシーエンジンは一度の実装で100万台を超えるデバイスの動作**リアルタイム**で監視できます。

ポリシーは特定のデバイスで発生するイベントに基づいてトリガーされます。このトリガーとなり得るものには、ネットワーク許可イベント(スイッチポートへのプラグインやIPアドレスの変更)、認証イベント(RADIUSサーバーで受信またはネットワーク トラフィックで検出)、**ユーザー/デバイス動作の変化**(ウイルス対策ソフトウェアの無効化、禁止されている周辺機器の追加、ポートの開閉)、デバイスの通信方法や利用プロトコルの種類など特定の**トラフィック動作**があります。

通知

- ユーザー/管理者に電子メール送信する
- オンスクリーン通知を送信する
- ウェブページにリダイレクトする
- エンドユーザーの応答をリクエストする
- SYSLOG/CEFメッセージを送信する
- ヘルプデスクチケットを作成する
- ITシステムとコンテキストを共有する

適合

- ゲストネットワークに移動する
- 無線ユーザーロールを変更する
- 自己修復VLANに割り当てる
- 不正デバイスを規制する
- アプリケーション/プロセスを開始する
- ウイルス対策/セキュリティエージェントを更新する
- OSアップデート/パッチを適用する

制限

- デバイスを隔離する
- スイッチポートをオフにする
- 無線またはVPNアクセスをブロックする
- ACLを使用してアクセスを規制する
- 無許可アプリを終了する
- NIC/周辺機器を無効にする
- 緩和・修復システムをトリガーする

ForeScoutは、セキュリティポリシーに基づいて適切なレベルのコントロールを施行できます。

オーケストレーション

課題:

断片化されたセキュリティ

大企業には互いに接続されていない、分断されたセキュリティシステムが数多く存在します。このような縦割り型のアプローチでは、企業全体の連携したセキュリティ対応が阻害されるため、システムの脆弱性を利用した攻撃を受ける危険性が高まります。

ソリューション:

セキュリティの自動化

ForeScoutは、情報共有とポリシーベースのセキュリティ対策に関する動作について、最先端のITおよびセキュリティ管理製品とオーケストレーションを行い、セキュリティワークフローを自動化し、スタッフによる手作業なしで迅速に脅威に対応します。

> **「夜間、スタッフが眠っている間もForeScoutは休まず働き、他のセキュリティソリューションと連携して脅威に直ちに対処してくれている。このような自動化に値段は付けられない。」**
>
> — ミズーリ州、最高情報セキュリティ責任者(CIO)、Michael Roling

実現する方法:

ForeScoutでは根幹となる可視化およびコントロール機能を活用して**縦割り型のセキュリティを統合**するため、これまでのセキュリティに対する投資は無駄になりません。ForeScoutモジュールでは、デバイスのウイルス予防策、脅威、動作およびコンプライアンスに関するデータが頻繁に共有されるため、既存のセキュリティツールおよび分析機能の精度が上がり、よりコンテキストに関連した決定を下すことができます。また、セキュリティインフラに不可欠なコントロール機能を提供することで、**手作業のポリシー施行を自動化**し、**応答を加速**し、抜本的に**セキュリティ状態を改善**します。既存のツールをForeScoutテクノロジーと連携させることで、システム全体のセキュリティオーケストレーションを達成する例をいくつかご紹介します:

標的型攻撃(ATD):マルウェアや、脅威が存在することを示す痕跡(IOC)が検出された場合、主要ATD製品が直ちにForeScoutプラットフォームに通知します。次に、ポリシーに基づいてForeScoutソリューションが感染デバイスを隔離し、緩和・修復措置を取ります。既存および新規のデバイスに対してもIOCの存在を確認するスキャンを行い、結果に応じて緩和措置を開始します。

セキュリティ情報/イベント管理(SIEM):デバイスのネットワーク接続時にForeScoutプラットフォームによってデバイスの検出とプロファイル作成が行われ、SIEMとこの情報を共有することでインテリジェンスを高めます。SIEMは収集されたイベントやログに基づいて対応し、デバイスを評価します。ForeScoutはこの情報をもとに対策を実施し、セキュリティポリシーに基づいてデバイスの許可、拒否、隔離を行います。

ダイナミックネットワークセグメンテーション:主要な他社製ファイアウォール、スイッチおよびルーターとの統合を深化させることにより、ForeScoutのポリシーエンジンがVLANやACL(アクセスコントロールリスト)を自動的に割り当て、デバイスやユーザーを適切なネットワークセグメントに配置または再割り当てします。訪問者、委託業者、特定の従業員およびIoTデバイスをセグメント化することで、ピボット、ラテラル、インサイダー、DDoS攻撃から保護しやすくなります。

オーケストレーションの全機能の一覧については**forescout.com/modules**をご覧ください。提携企業の一部を以下に示します:

amazon web services
Check Point SOFTWARE TECHNOLOGIES LTD
CYBERARK
FireEye
IBM
McAfee
MobileIron
paloalto NETWORKS
QUALYS
RAPID7
servicenow
splunk>
Symantec
tenable
vmware

「ForeScoutのネットワーク アクセスコントロール(NAC)テクノロジーは大きな変革の動力となっている」

— フロスト&サリバン、ベストオブネットワークセキュリティ、2016年

「ForeScoutはJPモルガン・チェースの企業ネットワークに接続される数十万台のデバイスの可視性とコントロールを強化している」

— JPモルガン・チェース、グローバルCISO、Rohan Amin

会社概要

業種:サイバー/IoTセキュリティ

顧客:世界60ヵ国以上の国々の2,000社超の企業や官公庁*

市場:金融サービス、行政および国防、医療、製造、教育、小売、基幹インフラ

創業:2000年

最高経営責任者(CEO):マイケル・ディシーザー

2016 受賞・表彰歴:

- JPモルガン・チェース、変革をもたらすセキュリティテクノロジーのイノベーションアワード殿堂入り
- ガートナー、IoTセキュリティマーケットガイド
- ガートナー、NACマーケットガイド
- フォーブス、クラウド企業トップ100
- デロイト、テクノロジーFast 500™
- ナナライズ、有望なサイバーセキュリティ新興企業9社
- CRN (コンピューターリセラーニュース)、セキュリティ企業第1位
- インク5000、急成長する非公開企業
- SCマガジン欧州、ベストNACソリューション

セキュリティフレームワーク/コンプライアンス要件:

主要なセキュリティ標準化機関およびフレームワークには共通する基本的な原則があります。それはセキュリティは可視性から始まる、ということです。ForeScoutは、企業や官公庁組織による以下の規制へのコンプライアンスをサポートしています:

- Center for Internet Security CSC (クリティカルセキュリティコントロール)
- CDM (継続的な診断と緩和策)
- FISMA (連邦情報セキュリティマネジメント法)
- HIPAA (医療保険の相互運用性と説明責任に関する法律)
- HITECH (経済的および臨床的健全性のための医療情報技術に関する法律)
- ISO/IEC 27001 (国際標準化機構/国際電気標準会議)
- NIST (アメリカ国立標準技術研究所) リスク管理フレームワーク
- PCI-DSS (PCIデータセキュリティスタンダード)
- SCAP (セキュリティ設定共通化手順)
- SOX (サーベンスオクスリー法)

ForeScout®

世界各地の営業拠点:
カリフォルニア州サンホセ(本社)
ダラス
ロンドン
ニューヨーク
シドニー
テルアビブ
ワシントンDC

2016年12月31日現在