ビジネスにおける課題

- 安全にIoTの先進技術を導入する
- 技術運用チームによる安定した確保する
- 情報システム部門に対してセキュリティおよびコンプライアンスを提供する
- 知的財産および機密データを保護する
- 企業または業界に関連する規制要件に準拠する
- 既存のネットワークセキュリティへの投資を活用する

技術的な課題

- 管理エージェントのない不明なデバイスをネットワーク上で検出する
- デバイスの識別情報を検証する
- デバイスを分類して所有者を判別する
- デバイスを評価、監視して異常な動作を判別する
- 感染またはコンプライアンス違反のデバイスによるマルウェアがネットワークに拡散するのを防ぐ

> 「2018年までに企業の3分の2がIoTセキュリティ侵害を経験すると予想されます」
>
> **ー IDC チーフアナリスト Frank Gens**

IoT（モノのインターネット）

従来のセキュリティ製品では検知できないIoTデバイスを検出・コントロール

前回のセキュリティ監査で、ネットワーク上にあるデバイスを特定できませんでしたか? OT(オペレーショナルテクノロジー)は、ITと同じネットワークを共有していますか? プリンターやHVACデバイスがPCのように動作し始めているか知りたいと思いますか?

直面する問題

エージェントレスでの可視化を提供する最先端のIoTセキュリティソリューションが導入されない場合、ネットワーク上のIoTデバイスは目に見えない(そして将来的には望まれない)存在となります。現在、ほとんどの企業でビデオ監視システム、プロジェクター、マルチコピー機およびプリンター、工業制御およびHVACシステムが一般的な存在となっています。ネットワークに接続することでこれらのデバイスの能力と価値はさらに高まりますが、セキュリティが破られた場合などは、あっという間にハッカー達のお気に入りのターゲットとなってしまいます。

増え続けるデバイスの「モノ」には一つの共通する特徴があります。それは、デバイスに搭載されている軽量オペレーティングシステムでは、従来のセキュリティツールで実施されるデバイスの検出と管理機能を提供するソフトウェアエージェントがサポートされない、という点です。

業界アナリストがIoTの驚異的な成長について議論している一方で、企業のITスタッフはより切実な悩みを抱えています。ネットワーク上にすでに存在するエージェントが導入されていないデバイスを特定するということです。以下の事実を考えるとデバイスの可視化不足が懸念されます:

- IDCアナリストは、2018年までに企業の3分の2がIoTセキュリティ侵害を経験すると予測。[1]
- 2020年までに企業ネットワークに接続される新規デバイスのうち、従来の方法で管理可能なものは10%未満。[2]
- 2020年までに208億台の「モノ」がインターネットに接続されると予測。[3]

ガートナーの「2017年および2018年IoTテクノロジートップ10」ランキングでセキュリティが1位を占めたことも当然と言えます。[4]

「OTの分断 = ITのセキュリティホール」となる理由

少し前まで製造ライン、環境管理、工業制御システムやセンサーなど、重要インフラで利用されるOT(オペレーション・テクノロジー)はネットワークから隔離され、分断されていました。これらの指揮統制タイプのネットワークはレガシーオペレーティングシステムや自社開発のネットワークテクノロジーで使用されており、通常デバイスのセキュリティを犠牲にしてシステムパフォーマンスや可用性を優先していました。この「隠蔽によるセキュリティ(Security through Obscurity)」と呼ばれるアプローチはもはや通用しません。

1 IDCのグローバルテクノロジーの予測、2016年
2 ForeScoutの分析
3 ガートナーによると2016年には2015年より30%増の64億台の接続された「モノ」が使用される見込み、ガートナーリサーチ、2015年11月
4 *2017年および2018年、IoTテクノロジートップ10*、ガートナーリサーチ、2016年2月

IoTアプリケーションおよびその導入効果の例。

施設管理
暖房/冷房/照明制御、防火およびビルセキュリティ。
リソース利用の最適化と予防保守によりコストを削減します。

ヘルスケア
遠隔デバイス監視、現状把握および在庫管理。
診療を効率化し、診断精度を向上させ、医療費/保険料を削減します。

石油/ガス
探査から精製流通までのインフラをインターネットに接続。
事業/流通コストを削減し、プロセスを最適化し、プロアクティブな保守を実現します。

製造
スマートセンサー、在庫管理およびデジタルコントロールシステム。
需要の変動に迅速に対応し、プロセスを自動化して効率を最適化します。

公共部門
デジタルガバナンス、スマートシティおよびインターネット接続インフラ。
市民に対する利便性を高め、公共の安全を確保し、交通の流れをスムーズにして街路灯のコストを削減します。

小売業
インターネット接続された在庫、CRM/カスタマーロイヤリティ、在庫管理システム。
在庫管理を最適化し、顧客インサイトを改善して、マーケティングをパーソナライズします。

サプライチェーン
リアルタイムの在庫管理、追跡、出荷、およびロジスティクス。
プロアクティブに問題を解決し、業務効率を向上させます。

電力・ガス事業
インターネット接続メーターおよびスマートグリッド。
メーター読み取りを自動化し、稼働率/生産効率を改善します。

IP接続の経済的な優位性により、すぐに分断された業務ネットワークの利点はかき消され、外部にもつながるITネットワークへの接続によって大きなセキュリティ上の課題が生じています。かつては分断されたネットワーク上に存在していた脆弱なデバイスが、多くの企業ネットワーク上にも存在するようになった一方、これらのデバイスには管理エージェントが存在しないことで、セキュリティチームはデバイスを保護することはおろか、その目録を作成することもままなりません。

IoTイノベーションおよび企業ネットワーク

IoTデバイスのほとんどは消費者ではなく企業により利用されています。実際、ネットワーク接続デバイスの79%は企業/製造、ヘルスケア、小売業に関連しています。[5] これらのデバイスでは情報取得/共有、機能の自動化ができるように設計されており、IPベースのネットワーク接続を実現するための基盤は整っています。ただし、最低限のシステムリソースと独自のオペレーティングシステムで動作しているため、管理エージェントを組み込むことができず、従来型のセキュリティ管理システムからは見ることができていません。これらのデバイスが有線および無線の企業ネットワークに出入りしているにも関わらず、積極的に受け入れている企業や官公庁において安全性を確保する方法や、さらされているリスクについてはほとんど考慮されていません。

ForeScoutのソリューション

ネットワークに新たに接続するデバイスの大多数はアンマネージドIoTエンドポイントです。ForeScoutは、以下の3つの点で企業によるIoTデバイスのセキュリティ確保を支援しています:

可視化 ForeScout CounterACT®は、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。ソフトウェアエージェントは必要ありません。さらに、デバイスの検出と分類を行い、識別情報を検証します。この重要な機能は、エンドポイントのコンプライアンス状態を改善し、IoTセキュリティおよびコンプライアンス・ポリシーを定義するために欠かすことはできません。加えて、CounterACTはIoTデバイス、ポートおよび接続状況を継続的に監視します。

コントロール ネットワーク上の各IoTデバイス、その所有者と目的について把握すると、CounterACTによってさまざまなネットワークアクセスコントロールオプションが提供されます。非対応デバイスへのアクセスを制限し、異常な動作が発生したデバイスについてはインターネットアクセスをブロックし、隔離するとともに、セキュリティ上の懸念についてデバイスの所有者に通知できます。特定のデバイスを特定のネットワークセグメントまたはVLANに隔離する場合は、CounterACTによってそのプロセスはさらに簡素化されます。

オーケストレーション CounterACTが導入されていない場合、他社の管理ソリューションからアンマネージドデバイスやIoTエンドポイントを見ることはできません。ForeScoutでは、ForeScout拡張モジュールを通じて、CounterACTのエージェントレスの可視性とコントロール機能を主要ネットワーク、セキュリティ、モビリティおよびIT管理製品にも拡張します。マルチベンダーセキュリティのオーケストレーションを行うユニークな機能により以下の操作が可能になります:

- 複数システム間でコンテキストや制御情報を共有して、ネットワークセキュリティポリシーを一元的に適用する
- システム全体で脅威に対する対応を自動化して、脆弱性のある個所を減らす
- 現行のセキュリティツールのROIを向上させ、ワークフロー自動化で時間を節約する

5 インフォグラフィックで読み解くIoT - インテル

> 「ホワイトハッカーは、病院のロビーから患者がチェックインするキオスク端末のセキュリティを突破しピボット攻撃をかけて、血液サンプルや薬のデータを改ざんできることを実証している」
>
> **― フォーブス、2016年2月23日**

IoTユースケース

IoTが極めて高価値で幅広く採用されていることから、多数のセキュリティベンダーがIoTセキュリティ機能を標榜しています。多くの宣伝にも関わらず、実際のユースケースはなかなか見つかりません。ForeScoutが現在対応している実際のユースケースのいくつかをご紹介します。

企業ネットワークでIoTデバイスの安全を確保

今日の企業ネットワークには、エージェントレスIoTデバイスおよびアンマネージドBYOD/CYODデバイスが接続されています。これらのデバイスは一つ一つが潜在的なネットワーク攻撃または偵察ポイントとなります。感染したIoTプリンターをForeScoutで検出、監視、ブロックする方法について一つの例を示します。このシナリオは、防犯カメラ、HVAC/照明制御、モニター、プロジェクターなど、企業で使われているその他の多くの接続デバイスにも当てはまります。

1. IoTデバイスがネットワークに接続されます。
2. CounterACTはデバイスを検出してプリンターとして分類します。
3. 感染したプリンターが企業ファイルサーバーにアクセスを試みます。
4. 他社製SIEM（セキュリティ情報/イベント管理）ソリューションが変則的な動作を検出します。
5. CounterACTは感染したプリンターをネットワークからブロックして隔離し、IT部門がデバイスを安全にネットワークから取り除き、フォレンジック分析を実行できるようにします。

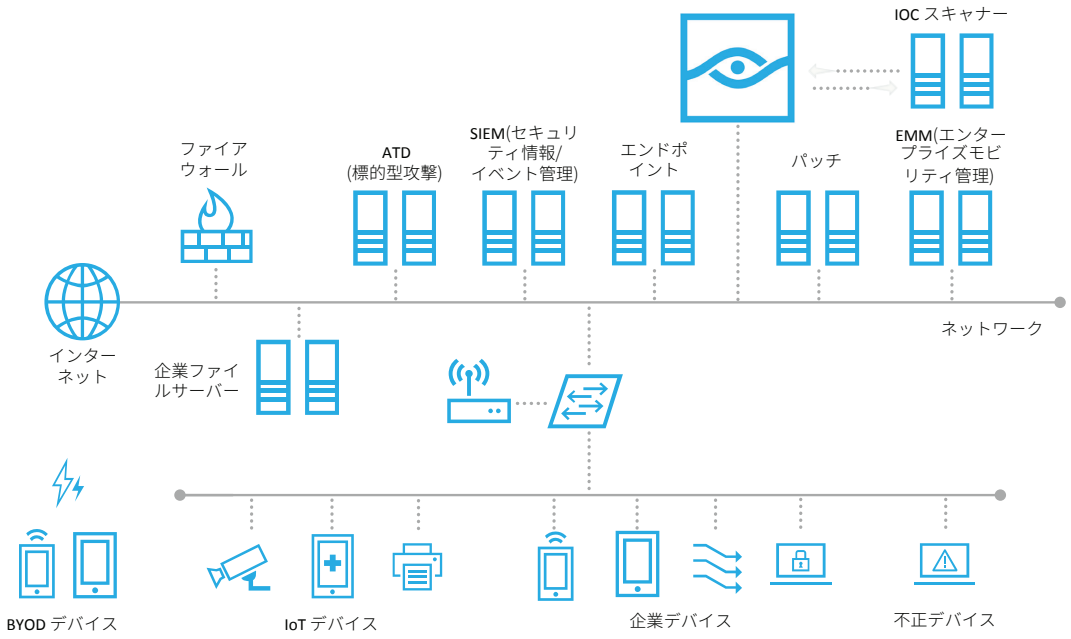

図1: ForeScoutのエージェントレスなIoTセキュリティプロセスにより、可視性とコントロール、そしてSIEMを含む他社ソリューションとのオーケストレーションが提供されます。

> 「IoTから最大の付加価値を得られるであろう分野には、製造、ヘルスケアプロバイダー、保険、銀行および証券業界が挙げられる。」
>
> **ー ガートナーによる発表、2014年9月11日**

IoT医療デバイスを発見・分類

CounterACTのカスタムポリシーエンジンは既知の特性に基づいて、ネットワーク接続デバイスの発見を可能にします。さらに、CounterACTの臨床デバイス分類ポリシーでは、225社に上るメーカー製の数千もの医療デバイスを自動的に特定できます。新しいデバイスの分類は継続的に追加されており、ネットワーク接続されている医療デバイスに関する正確でリアルタイムの目録を提供することで、ヘルスケアITチームの貴重な時間を節約するとともに、FDAおよびHIPAAの要件に対するコンプライアンスを支援します。

デバイスの発見と分類に加え、CounterACTでは無許可のUSBメモリースティックやその他の周辺デバイスを検出してブロックすることもできます。多くの医療デバイスには管理者が手動でファームウェアを更新するためのUSBポートが備わっているため、これは重要なセキュリティの検討事項となります。

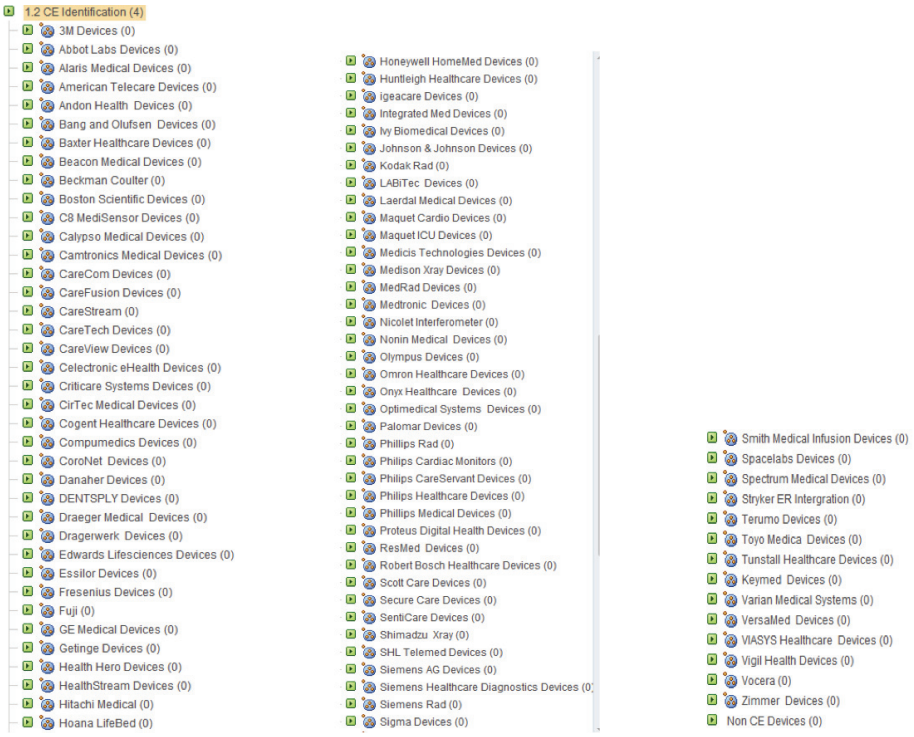

図2: CounterACTはすばやく正確に数千もの医療デバイスを発見して目録を作成し、重要な臨床ケアエンドポイントを監視して、ポリシーを施行します。プロファイリングモジュールは現在すでに利用可能か、重要インフラ向けコンポーネントを含む他の業界向けに開発中です。

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