ARUBAの概要

有線/無線ネットワーク・エンドポイントの可視性

セキュリティとコンプライアンスを強化するための今日の前提条件

通りかかった誰かのデスクでネットワークに何が接続されているかを目で見ることができたのは過去の時代の話です。BYODや、監視カメラ、IoT（Internet of Things）カテゴリのその他のエンドポイントなどの管理対象外デバイスが登場したことで、IT部門が完全な可視性を維持することは不可能になりつつあります。

課題

従来、接続エンドポイントを特定する際は、多くの場合は総合的なエンドポイント管理ソリューションとエージェントを導入し、複数のエンドポイント・データベースを手動で更新していました。しかし、その多くをユーザーが持ち歩いて使用するBYOD、ゲスト・アクセス配備、有線/無線の不正エンドポイントにIT部門が圧倒されて対応しきれなくなると、これらの方法では目的の結果を得られなくなりました。

IoTデバイスは今後3年間に数十億台がネットワークに接続されるものと予想されています。また、広く報道されている最近のセキュリティ違反の影響もあり、ITの専門家がリアルタイムの可視性とレポート機能を求めているのは確実です。ロケーション、時間帯、エンドポイント・タイプに関係なく、定期的な更新の代わりに継続的な監視とプロファイリングを行うソリューションが求められています。

今日のインテリジェントな可視性ソリューション

ArubaのClearPassファミリは、エージェントを用いないリアルタイムのプロファイリングをスタンドアロン アプライアンスとして、または総合的なポリシー適用ソリューションの一部として提供し、競合他社にはない独自のメリットをネットワークやセキュリティの担当部門に提供します。

どちらを利用した場合でも、AAA対応/非対応の有線/無線ネットワークに接続しているエンドポイントとネットワーク デバイスを、IPアドレスのタイプ（動的/静的）に関係なく継続的に特定でき、エンドポイントの総数と、カテゴリ、ファミリ、タイプごとのデバイス数を総合的なダッシュボードで簡単に確認できます。

ARUBA CLEARPASSのメリット

- エンドポイントの自動検出・分類によるセキュリティおよび監査ニーズへの対応
- ネットワークを出入りするすべてのデバイスの継続的監視
- BYODスマートフォンやIoTなどのデバイスを検出するためのエージェント不要の可視性
- セキュリティとITサービスの多様なソリューションにまで可視性を拡張するコンテキスト属性の共有
- データベース更新の手動による維持に必要な作業の排除
- エンドポイントの数、タイプ、属性の把握によるネットワーク・パフォーマンスとセキュリティの向上

Aruba ClearPass Universal Profiler：完全なNACソリューションの導入準備が整っていない組織や、NACが配備されていないリモート/制限環境向けに設計された、数分間で配備して実行できるスタンドアロン仮想アプライアンスです。あらゆる組織の拡張性ニーズに対応できます。

Aruba ClearPass Policy Manager：総合的なプロファイリング機能、AAA対応/非対応の有線/無線ネットワークでのポリシー適用、ゲスト・アクセス、BYODオンボーディング、エンドポイント評価機能、レポート機能を提供する仮想または物理アプライアンスです。セキュリティおよびユーザー・エクスペリエンス指向のサードパーティ製ソリューションとの統合機能が組み込まれています。

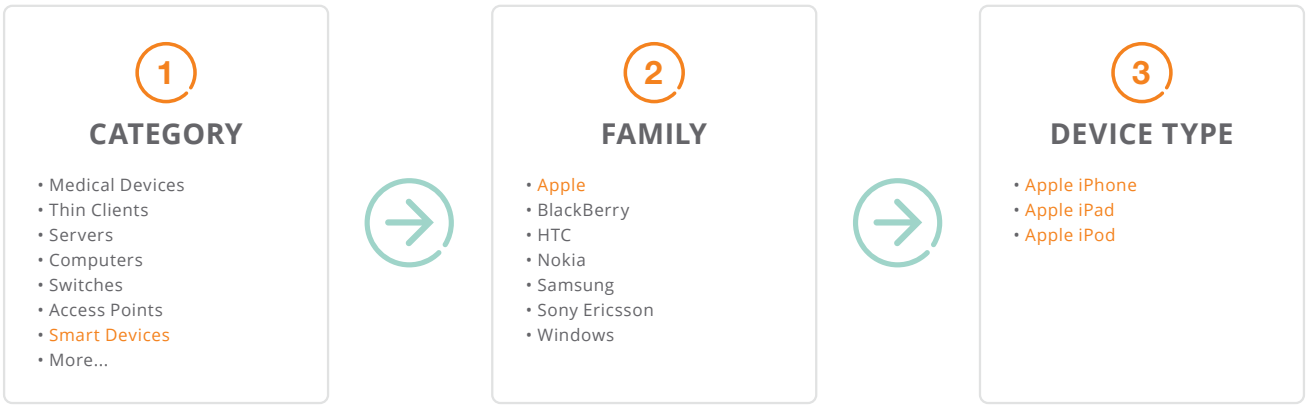

図1：デバイス・カテゴリ、ファミリ、タイプ別の細分性の高い可視性

ClearPassファミリの製品は、エンドポイントの検出、特定、属性プロファイリングを行い、属性からデバイスのカテゴリ、ベンダー、オペレーティング・システム、IPアドレス、ホスト名、所有者などの情報を驚くほど簡単に獲得します。新しい、または未知のIoTデバイスについては、IT部門によるカスタマイズに対応したエンドポイント自動分類機能によって迅速に分類し、可視性やセキュリティ適用のために適切なデバイス・ファミリに割り当てます。

一層の柔軟性のために、ClearPassには標準ネットワークまたはSPANポート監視機能を利用してネットワーク検出を動的に行うオプションが用意されています。これは、大規模エンドポイント配備へのミラーリングのために高額な専用10Gポートを複数必要とするレガシーITネットワーク・アクセス制御ソリューションとは対照的です。

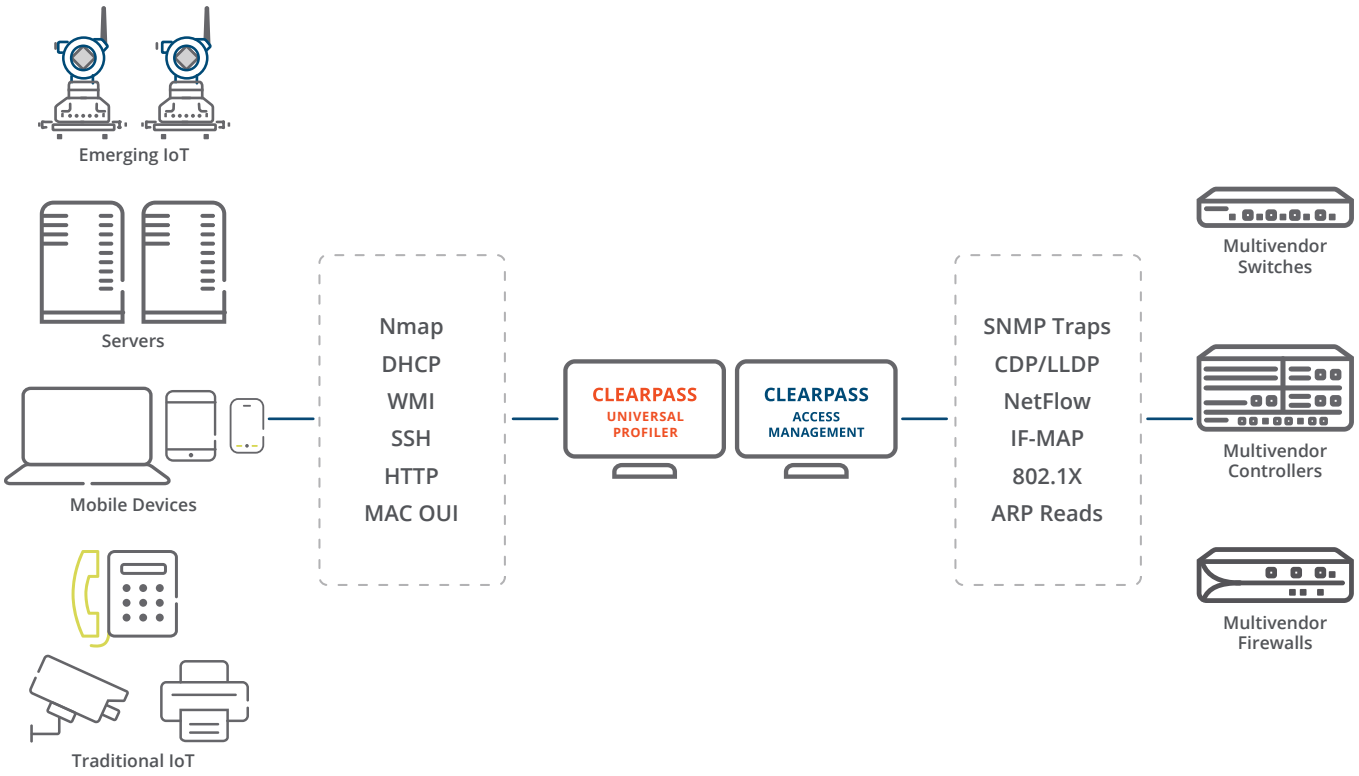

図2：細分性の高い特定およびプロファイリング方式

細分性の高い検出の方式

複数のプロファイリング方式を使用して、細分性の高いエンドポイント属性をデバイスごとに収集します。これは、パフォーマンスに関する潜在的な問題や脅威リスクの特定に役立ちます。向上した可視性とコンテキスト情報に基づくインサイトは、両方のClearPassソリューションの間で共有することも、ClearPass Policy Managerで直接使用してポリシーの最適化に役立てることもできます。ポリシーは、何が接続可能であるかを決定し、IT部門が潜在的な脅威にどれだけ迅速に対応できるかに影響します。

サードパーティ製ソリューションでのエンドポイント可視性の活用

ClearPass API、syslogメッセージング、拡張機能を利用することで、ファイアウォール、SIEM、エンドポイント・コンプライアンス・スイート、ポリシー管理の強化のためのその他ソリューションとの間でエンドポイント属性を簡単に交換できます。これらのソリューションはエンドポイント属性を取り込むと、デバイス・カテゴリごとのルールに基づいてトラフィック・パターンのマッチングを行い、接続の最適化や、疑わしいトラフィックの修正を行います。

詳細情報

ClearPass Universal ProfilerとClearPass Policy Managerの詳細、およびポリシー適用と有線/無線ネットワークの保護の向上のためにすべてのエンドポイントを特定する独自機能については、www.arubanetworks.com/clearpassをご覧ください。