ソリューション概要

ARUBA CLEARPASS POLICY MANAGER

有線/無線ネットワークのアクセスを可視化し、セキュリティを確保

IT 部門がセキュリティを確保し、厳格なポリシーと完全に閉じられたエコシステムで管理を行っていた時代は とうの昔に過ぎ去り、今日では、IT 環境とユーザー所有のデバイスが境界セキュリティの内外で接続されています。

ノートパソコン、スマートフォン、タブレット、およびモノのインターネット (IoT) デバイスが職場で広く使用され、データを保護するには、ネットワーク上のデバイスを特定することから始めなければならない今日においては、ポリシーの適用を自動化して、特定のユーザーとデバイスのみに接続を許可するとともに、リアルタイムの脅威保護でセキュリティを確保し、内外の監査とコンプライアンスの要件に対応する必要があります。

また予測が正しければ、有線 / 無線ネットワークにおける IoT デバイスの利用が増えることで、IT 部門の重点課題は変化するものと思われます。大部分の組織は、無線ネットワークや無線デバイスのセキュリティを確保する一方、会議室、IP 電話、およびプリンターエリアの有線ポートについては何の対策も講じていません。そして IoT デバイスに関しては、十分なセキュリティ属性が得られず、外部の管理リソースからのアクセスを必要とすることがあるため、有線アクセスが新たなリスクとなっています。

制御の維持に苦心する IT 部門は、基盤となるインフラストラクチャのプログラミングを迅速に行い、既知か未知かを問わず、あらゆる IoT およびモバイルデバイスのネットワークアクセスを制御するための適切なツールセットを必要としています。今日のアクセスセキュリティソリューションは、プロファイリング、ポリシーの適用、ゲストアクセス、BYOD の導入などをサポートし、IT 部門の負荷を軽減して強力な脅威保護機能を提供するとともに、ユーザーエクスペリエンスを向上させるものでなければなりません。

NACに対する考え方に変化をもたらすモビリティとIoT

IT ドメインの境界は今や企業を囲む 4 つの壁の外側へと広がり、多くの組織は、セキュリティを犠牲にすることなく時間や場所を問わない接続を実現することを目標に掲げています。IT 部門がビジネスやユーザーエクスペリエンスに影響を与えることなく可視性と制御を維持するには、まず 3 段階の計画を立てる必要があります。

1. 使用されているデバイス、デバイスの台数、デバイスの接続元、およびサポートされるオペレーティングシステムの特定。これにより基盤が構築され、変更やデバイスの使用状況に関する情報を継続的に取得できるようになるため、長期間にわたって必要な可視性が得られます。
2. ユーザー、デバイスの種類、または場所を問わず、適切なユーザーおよびデバイスアクセスを提供する、正確なポリシーの適用。これにより、期待通りのユーザーエクスペリエンスが実現します。スマートフォンや監視カメラなどのデバイスの種類を問わず、組織は進化を続ける今日のデバイスとその用途に対応する必要があります。
3. 動的なポリシー制御とサードパーティのシステムまでをカバーする実運用環境の脅威防御によるリソースの保護。これは計画の最後の段階で、ネットワークにおける真夜中の異常な動作に対応するには、トラフィックをブロックし、デバイスの接続ステータスを変更する一元的なアプローチが必要です。

組織においては、既存の課題と予期せぬ課題に対応するための計画を立てなければならず、ユーザーがリモートでの作業、または新しいスマートフォンの購入を決定したときに、常に IT 部門やヘルプデスクのスタッフに対応を依頼するのは現実的ではありません。NAC はもはや、既知のデバイスにアクセスする前にアセスメントを行うためだけのものではないのです。

1つの場所ですべてを確認して管理

ClearPass のポリシー /AAA ソリューションは、組み込みのデバイスプロファイリング機能、Web ベースの管理インターフェイス、およびリアルタイムのアラートを含む包括的なレポート機能を提供します。収集したすべてのコンテキストデータは、アクセスの方法やデバイスの所有権にかかわらず、ユーザーやデバイスに適切なアクセス権限を付与するために使用されます。

また、組み込みのプロファイリングエンジンにより、デバイスのカテゴリ、ベンダー、OS バージョンなどを含むリアルタイムのデータが収集されるため、無線 / 有線ネットワーク上で何台のデバイスが接続されているのかを推測する必要がなくなるうえ、きめ細かい可視化によって、監査に合格したり、パフォーマンスとセキュリティのリスクの原因を特定したりするのに必要な情報を得ることができます。

THE POWER OF CLEARPASS EXCHANGE

スタンドアロンの ClearPass Universal Profiler を導入すれば、全面的にポリシーを適用できる状態にない組織や 最初に ClearPass が配備されることのないリモートエリアにおいても、同様にプロファイルを可視化することが可能です。

IT 部門はテンプレートベースのポリシー適用により、ユーザーの役割、デバイスの種類、MDM/EMM データ、認証のステータス、場所、曜日などを活用した、有線 / 無線中心のポリシーを作成でき、こうしたポリシーを作成すれば、従業員、学生、医師、ゲスト、経営幹部、およびそれらの人物が持ち込むことを決定したデバイスの種類に合わせたルールを容易に適用することが可能です。

ClearPass OnConnect は、組織が AAA に対応していない多数の有線ポートをロックダウンできる組み込みの機能です。この機能によってデバイスの構成が不要になり、スイッチに必要なコマンドラインの入力も 1 回で済みます。また、有線と無線に関する標準的な AAA/802.1X のメソッドもサポートされます。

そしてこれにより、サイロ化した AAA、NAC、およびポリシーソリューションでは実現できない、一貫したポリシーの適用とエンドツーエンドのアプローチが可能になります。1 つのポリシーサービスで Microsoft Active Directory、LDAP 準拠のディレクトリ、ODBC 準拠の SQL データベース、トークンサービス、および内部のデータベースセットを含む、複数の ID ストアを利用できる ClearPass は、レガシーソリューションと一線を画しています。

IT部門の関与を必要としないデバイスのプロビジョニング

BYOD 環境への個人用デバイスの導入の管理は、IT 部門やヘルプデスクのリソースの負荷を増大させ、セキュリティの問題をもたらすことがあります。

ClearPass Onboard により、ユーザーはセキュアなネットワークで各自が使用するデバイスを構成できます。また、デバイス固有の証明書を使用することで、ログイン認証情報を 1 日に何回も入力する必要がなくなるため、利便性が向上し、セキュリティも強化されます。

IT チームは、デバイスを導入できる人物、それらの人物が導入できるデバイスの種類、および 1 人あたりのデバイスの台数を定義しますが、組み込みの認証局により、内部 PKI を構築したり、定義後に IT リソースを利用したりする必要がなくなるため、IT 部門はこれまでより迅速に個人用デバイスをサポートできます。

シンプルかつ迅速なゲストアクセス

BYOD においては、従業員のデバイスだけでなく、有線または無線ネットワークアクセスが必要なデバイスを使用する訪問者も重要で、IT 部門は、デバイスを指定のポータルにプッシュするとともにアクセス認証情報の設定を自動化し、社内のトラフィックを切り離すセキュリティ機能を提供する、シンプルなモデルを必要としています。

従業員、受付係、イベントコーディネーター、およびその他の IT 部門以外のスタッフは、ClearPass Guest を使用することで、その日限りの一時的なネットワークアクセスアカウントを簡単かつ効率的に作成し、任意の数のゲストに提供できます。また、MAC のキャッシングにより、ゲストはゲストポータルで何回も認証情報を入力することなく、1 日を通して簡単に接続を確立することが可能です。

これ以外にも、自己登録によって従業員の負荷が軽減され、ゲストが各自で認証情報を作成できるほか、印刷したバッジ、SMS テキスト、またはメールでログイン認証情報が提供されます。認証情報は一定の期間 ClearPass に保存することが可能で、指定した時間または日数が経過した時点で自動的に期限が切れるように設定できます。

デバイスの稼働状況に基づいてアクセスを決定するタイミング

認証プロセスでは、特定のデバイスが企業のウイルス対策、スパイウェア対策、およびファイアウォールのポリシーに沿っていることを確認するために、それらのデバイスのヘルスアセスメントが必要になることがありますが、自動化により、企業ネットワークへの接続の前にユーザーにウイルス対策スキャンを実行させることができます。

ClearPass OnGuard は、ポスチャーベースのヘルスチェックを実行して、幅広いコンピューターのオペレーティングシステムやバージョンにわたる脆弱性を排除する機能を内蔵しています。使用しているエージェントが常駐型であるか非常駐型であるかどうかにかかわらず、ClearPass では無線、有線、または VPN インフラストラクチャ上の問題のないエンドポイントを一元的に識別できます。

セキュリティの強化に貢献する高度なヘルスチェックには、次のようなものがあります。

- ピアツーピアのアプリケーション、サービス、およびレジストリキーの処理。
- USB ストレージデバイスや仮想マシンインスタンスが許可されているかどうかの確認。
- ブリッジ接続したネットワークインターフェイスとディスク暗号化の使用の管理。

サードパーティソリューションの有効活用

ClearPass Exchange では、ファイアウォール、MDM/EMM、MFA、ビジター登録、SIEM ツールなど、広く普及しているサードパーティソリューションを使用して、セキュリティの脅威を自動的に防御したり、サービスを強化したりすることが可能です。また、組織において ClearPass に含まれるコンテキストインテリジェンスを活用することにより、デバイス、ネットワークアクセス、およびトラフィック検査 / 脅威保護レベルでセキュリティと可視性を確保できます。

共通言語の (REST) API、Syslog メッセージ、および ClearPass Extensions と呼ばれる組み込みのレポジトリを使用してワークフローと意思決定を自動化すれば、タスクが簡素化されて組織が保護され、複雑なスクリプト言語や面倒な手動による構成が不要になります。また統合を迅速化する Extensions により、パートナーは拡張機能をアップロードして、共通のお客様に新しいサービスをリアルタイムで提供できます。

ClearPass Exchange を活用すれば、ネットワークで以下のような処理を自動的に行うことが可能です。

- デバイスのジェイルブレイクのステータスをはじめとする MDM/EMM データにより、デバイスがネットワークに接続可能かどうかを確認する。
- ファイアウォールでユーザー、グループ、および特定のデバイス属性に基づいてポリシーを正確に適用するとともに、ClearPass を活用して動作が異常なデバイスを修正する。
- すべての接続デバイスの認証データを保存するように SIEM ツールをセットアップする。
- 多要素認証を使用して本当にネットワークやリソースに接続していることを証明するようユーザーに求める。

また、ネットワークイベントを通じて、双方向でアクションをトリガーすることにより、ファイアウォール、SIEM、およびその他のツールから ClearPass に情報を提供し、デバイスで対策を講じさせることも可能で、たとえば、ユーザーがネットワーク認証に複数回失敗した場合、ClearPass からデバイスに直接通知メッセージをトリガーするか、そのユーザーをブラックリストに登録し、ネットワークへのアクセスを禁止できます。

場所を問わない業務用アプリケーションへの安全なアクセス

日々の作業用アプリケーションへのログインは、迅速かつ簡単に行えなければならないことから、ClearPass は SSO と ClearPass Auto Sign-On 機能をサポートしています。すべてのユーザーが一度アプリケーションにログインする必要があるシングルサインオンとは異なり、Auto Sign-On では有効なネットワークログインを使用して、ユーザーにエンタープライズモバイルアプリケーションへのアクセスが自動的に提供されるため、デバイスで必要なのはネットワークログインか有効な証明書のみとなります。

また、ClearPass はシングルサインオンが使用される ID プロバイダー (IdP)、またはサービスプロバイダー (SP) として使用することも可能です。

Bonjour、DLNA、およびUPnPサービス

DLNA/UPnP、またはApple AirPlayやAirPrintを使用するプロジェクター、TV、プリンター、およびその他のメディアアプライアンスは、Aruba Wi-Fi インフラストラクチャを使用して複数のユーザー間で共有できますが、ClearPass を導入すれば、それらのデバイスの検索と共有が容易になります。

たとえば、タブレットからプレゼンテーションを表示したいと考えている教師には、教室で使用できるディスプレイのみが表示され、キャンパスの別の場所にあるデバイスが表示されることはありません。また、ポータルからディスプレイを使用できるユーザーを選択し、学生が勝手に使用しないようにすることも可能です。

この他にも、たとえば医療の分野では、医師が iPad を使用して、病院内のあらゆる場所にある大きな画面にデジタル PACS 画像を簡単に投影できるため、患者とのコラボレーションがこれまでより容易になります。

適応性に優れたセキュリティとサービスの基盤

今日のモバイルユーザーにシームレスなエクスペリエンスを提供し、IoT テクノロジーを迅速に導入するには、IT に関する数多くの新しい課題に対応しなければならず、時間や場所を問わない安全な有線 / 無線アクセスを実現するには、計画の策定、適切なツール、および強力な基盤が必要です。

一貫性のある単一のソリューションでデバイスの特定、ポリシーの制御、およびワークフローと脅威保護の自動化をサポートし、こうした課題を解決する ClearPass を使用すれば、リアルタイムのコンテキストデータを取得して関連付けることで、オフィス、キャンパス、または球場などのあらゆる環境に適用可能なポリシーを定義できます。

また、ClearPass に加えられた最新の機能強化により、IoT の導入、モバイルデバイスやモバイルアプリケーションの認証の強化、およびより詳細なセキュリティインシデントの可視化に関連する、ネットワークセキュリティの新たな課題に対応することも可能です。自動化された脅威保護とインテリジェントなサービス機能を活用すれば、現場において極力 IT 部門の手を借りることなく、各デバイスにネットワークアクセス権限を正確に付与できます。

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | 電話: 1.408.227.4500 | ファクス: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com