概要

MARSH により CYBER CATALYST℠ に指定された ARUBA ポリシー・エンフォースメント・ファイアウォール

ネットワークがデジタル変換の触媒になると、従来の境界セキュリティの防御では不十分になります。携帯および IoT デバイスは、組織内のあらゆる場所で従業員、パートナー、顧客、およびお客様によって接続されているため、特定の IT アクセス許可に基づいてトラフィックのセグメンテーションを向上させる必要性が高まっています。

IP アドレスを利用した標準的なセキュリティ・ファイアウォール規則と物理的ネットワーク構成はもはや適切ではありません。組織は現在ユーザーのロールやデバイスの種類、場所に関係なく動的に実施される最先端の保護を常に必要としています。

Aruba は、この問題の解決に特に役立つポリシー・エンフォースメント・ファイアウォール (PEF) と呼ばれる包括的なロールベースのアクセス制御ソリューションを初めて開発した企業です。この実績のあるテクノロジーは、アクセスポイントで「ゼロトラスト」境界を提供し、リスク軽減のための Marsh 指定による Cyber Catalyst℠ を稼働させる、唯一のユーザーおよびデバイス中心のファイアウォールです。

潜在的なビジネス上の損失と影響を食い止める

インターネットとクラウドを介したモバイルテクノロジーとトランザクションは現在、組織がビジネスを行い、見込み客に接触する手段において重要な役割を果たしています。残念ながら、これは攻撃対象になります。組織は、適切なセキュリティ態勢、許容可能または回避可能なリスクの区分、そして耐えられる財政上の責任に関して決定する必要があります。

テクノロジー、プロセス、人に加え、サイバーセキュリティ保険は、組織の規模の大小を問わず、サイバーセキュリティの重要な柱となっています。実際、Verizon が最近発表したレポートでは、すべてのサイバー攻撃の約 43% が中小企業 (SMB) を標的にしているということです。
組織は、機密情報の公開に関連する訴訟やランサムウェアによる恐喝のコストにも対処する必要があります。

MARSH プログラムによる Cyber Catalyst℠ とは

Cyber Catalyst℠ プログラムの一環として大手保険会社は、自分たちがサイバーリスク軽減に際して効果的と考えるソリューションを評価および特定します。参加保険会社はアリアンツ、AXIS、AXA の一部門である AXA XL、Beazley、CFC、ミュンヘン再保険、SOMPO インターナショナル、そしてチューリッヒ北アメリカです。マイクロソフトは本プログラムの技術顧問を務めています。

サイバーリスクの軽減に効果があると考えられるサイバーセキュリティ製品およびサービスは、「Cyber Catalyst℠」に指定されます。Cyber Catalyst に指定されたソリューションを採用している組織は、参加保険会社からサイバーセキュリテイ保険契約に関してより手厚い契約条件の対象となる資格を得ます。

ARUBA ポリシー・エンフォースメント・ファイアウォールと HPE サーバー Silicon Root of Trust (SiROT) のいずれも、Cyber Catalyst℠ に指定されています。

ゼロトラスト保護のためのロールベース制御

IP ベースの VLAN を使用して制御する従来のファイアウォールは、ユーザーやデバイスがネットワークに認証されないと有効にならないため、高度な攻撃の魅力的な攻撃対象になってしまいます。
Aruba の PEF テクノロジーは ID やトラフィック属性、その他のコンテキストを使用して、初期接続時にアクセス権限を集中的に適用します。これは重要なのです。なぜなら攻撃者は、毎秒、広く開かれたネットワークに接続し、何千ものマルウェアパケットを解き放ってユーザーの認証情報を取得し、マルウェアの足跡や他の破壊的な活動を拡大するからです。デバイスが接続されてから方策が実施されるまでのギャップを埋めることが不可欠なのです。

Aruba の無線または有線インフラストラクチャを使用する場合、各ユーザーまたはデバイスの ID は、ネットワークまたはそのリソースへのアクセスを許可される前に認証されます。事前に規定された規則に基づいてロールが割り当てられ、許可が与えられます。これにより、ユーザーまたはデバイスが利用できるアプリケーションやデータ、または通信相手が制限されます。たとえば監視カメラの通信相手は、コンテンツをダウンロードするビデオサーバーに限られます。

データの流出やランサムウェアなどの攻撃が検出されると、PEF はユーザーまたはデバイスに関連付けられた権限を、そのロールと認証権限を更新することにより自動的に変更できます。攻撃対応には、帯域幅の削減、隔離、完全なブロックなど、さまざまなアクションが含まれます。攻撃警告は、単純な API 統合に基づいて、組織のセキュリティエコシステム内の特定のセキュリティ製品から発信できます。

PEF は企業内またはクラウド利用の管理機器で管理され、Aruba ネットワークインフラストラクチャと直接連結されているか、またはスタンドアロン・セキュリティ・ゲートウェイを介して連結されています。

組織がゼロトラストのロールベースのアクセス制御を実施できるようにすることで、Aruba ポリシー・エンフォースメント・ファイアウォールは、リスクを効果的に軽減する能力に基き「CYBER CATALYST℠」に指定されました。詳細については、Cyber Catalyst プログラム、Aruba PEF および HPE SiROT に関する次のリソースを参照してください。

その他のリソース

- Aruba ポリシー・エンフォースメント・ファイアウォール
- HPE サーバー
- Marsh による Cyber Catalyst

Cyber Catalyst℠ プログラムでは、大手サイバー保険会社は、自分たちがサイバーリスク軽減に際して効果的と考えるソリューションを評価および特定します。 参加保険会社はアリアンツ、AXIS、AXA の一部門である AXA XL、Beazley、CFC、ミュンヘン再保険、SOMPO インターナショナル、そしてチューリッヒ北アメリカです。 マイクロソフトは本プログラムの技術顧問を務めています。

a Hewlett Packard Enterprise company

AAG_CyberCatalyst_090919 a50000156enw