アリスタのクラウド・ネットワーキング向け ゼロトラスト・セキュリティ

エッジレス、マルチクラウド、マルチデバイスのコラボレーションに基づくハイブリッド作業モデルが普及したことで、グローバル境界や企業の脅威対策のあり方は大きく変化しました。ハイブリッド作業モデルの成長に伴い、企業データを取り巻く攻撃対象領域と新しい脅威は日々増え続けています。さらに、BYOD、IoT デバイス、クラウド・アプリの利用が一般化し、企業の管理対象外のアセットが大幅に増え、真の攻撃対象領域が見えにくくなっています。

このパラダイム・シフトを受けて、ネットワーク・インフラの中枢部分にセキュリティを組み込む大企業が増えています。セキュリティをネットワーク・レイヤに実装すれば、運用コストと複雑さを軽減すると同時に、幅広い攻撃対象領域から入り込む脅威を効果的に追跡し、適切に対応できます。

本ホワイトペーパーでは、アリスタのゼロトラスト・セキュリティ・アーキテクチャについて説明します。NIST 800-207 に基づくアリスタのアプローチは、状況認識、セグメンテーション、ポリシー適用、継続的な診断および監視を実現し、今日の複雑な脅威に対する効果的な防御策を提供します。

目次

アリスタのゼロトラスト・セキュリティの概要

ゼロトラスト・ネットワーク方式によるセキュリティは、堅牢なサイバーセキュリティ・エコシステムを構築しようとする現代の組織にとって最優先の課題です。ゼロトラスト・セキュリティでは、明示的な信頼性という前提に基づき、エンタープライズ・ネットワーク上のあらゆる活動を、どのデバイス、アプリケーション、ユーザーがどのリソースにアクセスする場合でも、完全に可視化し、制御します。この方式では、信頼されていないネットワークに従来のファイアウォール経由で接続しているネットワークの内部を信頼しません。また、ネットワーク・ロケーションに対する暗黙の信頼をなくし、代わりにすべてのデバイスとアプリケーションで悪意ある活動を継続的に監視し、迅速に対応します。アリスタのゼロトラスト・ネットワーキング・アーキテクチャは、NIST の 800-207 フレームワークのガイダンス[1]に沿って作成され、以下の柱によって支えられています。

ゼロトラストのフレームワーク

- 状況認識 → すべてのアセットとワークロードを可視化
- ポリシー適用 → アクセスを必要な接続だけに制限
- 継続的な監視 → 何者も信頼せず、継続的に検証

ゼロトラストの前提

- 認証の成功だけでは不十分
- 単純なフィンガープリントではなくデバイスとユーザーを可視化
- クライアント・エージェントが多数のIoTデバイスを持つことはできない

具体的な実装はセキュリティ管理者の固有の要件によって異なりますが、アリスタのパートナーとのインテグレーションや、業界最高水準の Arista スイッチ、CloudVision のネットワーク自動化とテレメトリ、アリスタのネットワーク脅威検知・対応（NDR）プラットフォーム、Arista DANZ Monitoring Fabric（DMF）を利用します。注目すべきは、アリスタのソリューションがオープン規格を採用しており、すべてのネットワークが複数ベンダーの製品で構成されている点です。

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

あらゆるネットワークに対応したゼロトラスト

アリスタは、柔軟でセキュアなネットワークの構築を構想段階から支援します。アリスタのゼロトラスト・ソリューションは、ネットワーク全体のセキュリティ態勢をリアルタイムで可視化して対応する統合アーキテクチャを提供するため、いくつかのネットワーク監視ツールやセキュリティ・ツールは不要になります。アリスタの他にない特長は、このような機能をキャンパス、データセンター、クラウドなど多様なネットワークに提供できることです。

データセンター向けのゼロトラスト

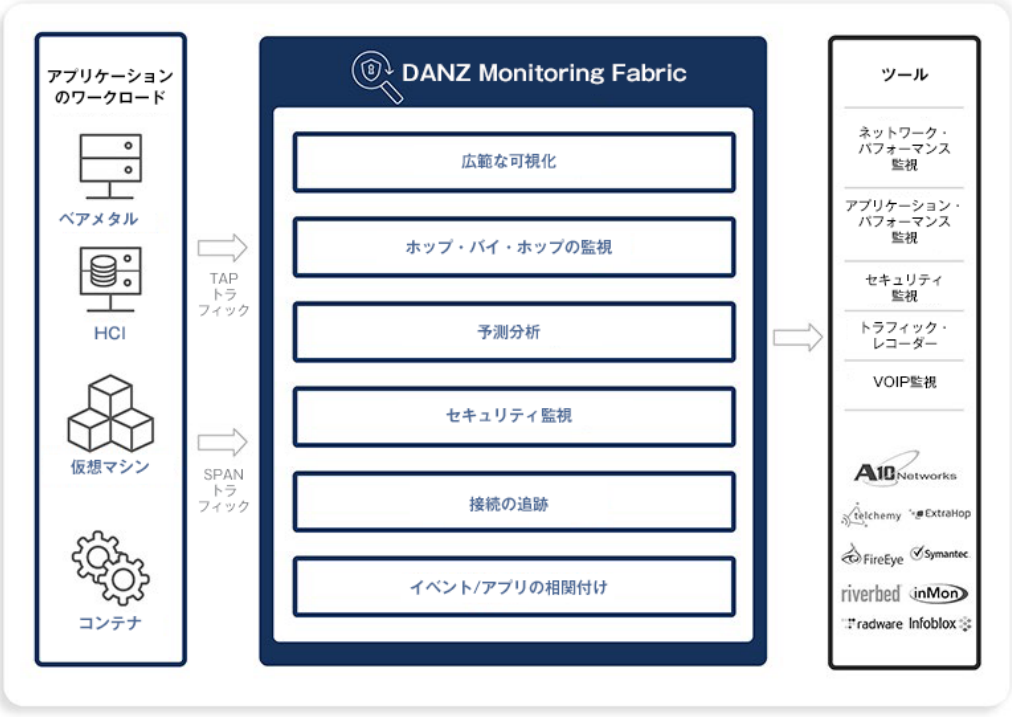
このソリューションは、DANZ Monitoring Fabric（DMF）のネットワーク・パケット・フィルタリング、転送、ストレージの機能と、AVA を活用した Arista NDR プラットフォームの高度なネットワーク脅威検知・対応（NDR）機能を組み合わせたものです。DFX（DANZ Forensic Exchange）は、ネットワーク、デバイス、ワークロード、アプリケーション、ユーザー単位での可視化を可能にするとともに、自律的な脅威ハンティング、脅威検出、対応を実現します。さらに、完全にプログラム可能な API 対応の機能を備えており、特定のトラフィックを選んで監視したり、企業のデータセンターやアプリケーション特有の脅威を警戒するカスタムの脅威ハンティング・モデルを作成したりできます。

DANZ Monitoring Fabric を使用したゼロトラスト・データセンターの展開

ゼロトラスト・セキュア・ネットワークを展開するには、状況分析と継続的な診断およびリスク緩和（CDM）のために、フローまたはパケット情報の収集と分析を続ける必要があります。従来のやり方では、パケット情報を収集するにはスイッチ単位でパケットをミラーリングします。ネットワーク・パケット・ブローカー（NPB）もよく使われますが、その大部分は独自技術によるもので、組織全体を監視するための拡張は難しいことが実証されています。

DANZ Monitoring Fabric（DMF）は、組織全体にわたる広範な可視化とセキュリティを実現する次世代 NPB です。DMF を利用することで、IT オペレーターはすべてのトラフィックを広範囲にわたって監視し、ミラーリングできます。さらに、DMF は詳細なホップ・バイ・ホップの可視化、予測分析、スケールアウト型のパケット・キャプチャを提供します。

DMF ダッシュボードは、モニタリング・ファブリック全体を制御し、リアルタイムおよび過去のコンテキストに対するネットワーク・パフォーマンス監視を簡素化します。



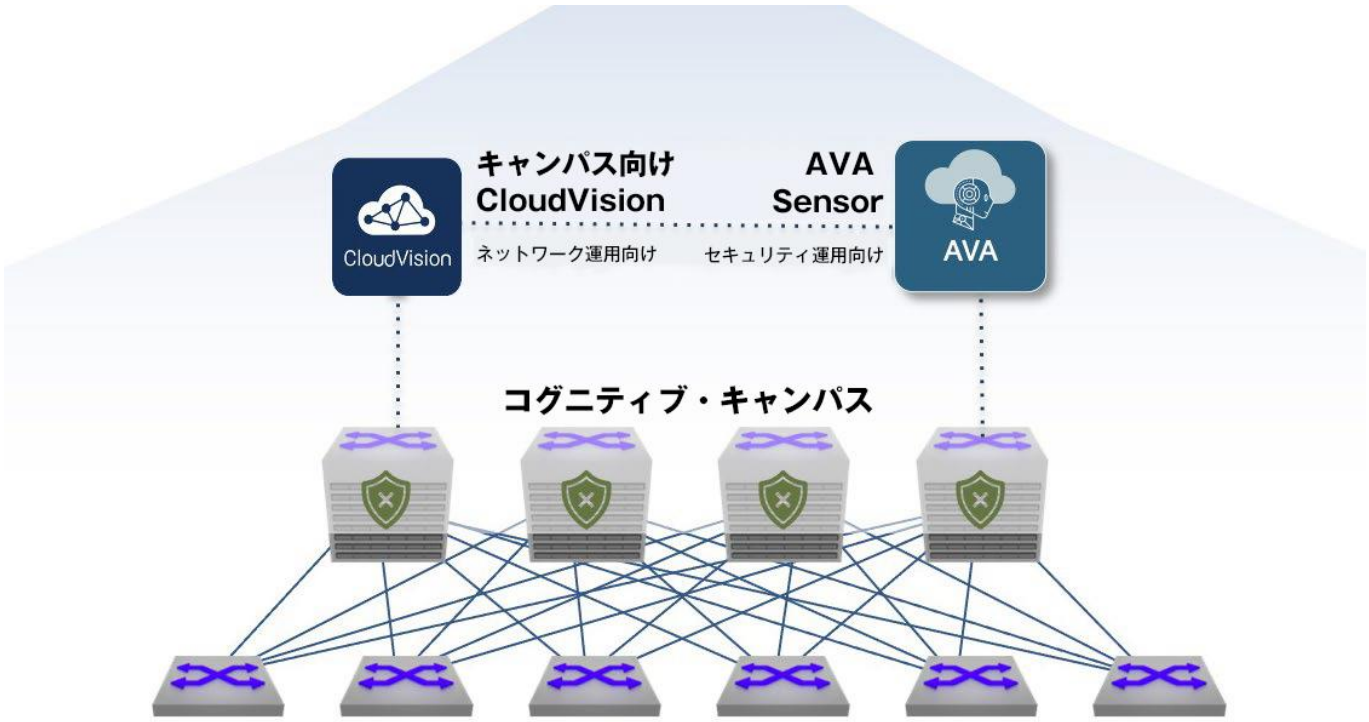
DMF Analytics Node は、DMF と連携してフロー分析を行います。この直観的なユーザー・インターフェイスは、疑わしいトラフィックや異常動作をピンポイントで警戒します。これにより、未知のホストや、ビジネスと関係ないホストからの大量のフロー、セキュリティ・チームとコンプライアンス・チームに承認されていない Web サイトへのトラフィックなどが特定されます。この機能は、ゼロトラストの意思決定を促進するのに特に役立ちます。

DMF Analytics Node は、DMF Recorder Node と連携してパケットレベルでの可視化を実現し、さらに詳細な分析と再現を可能にします。これらの機能は、セキュリティ管理者がハイブリッド・ネットワークの問題を可視化、検出、修正するための強力な手段になります。

コグニティブ・キャンパス向けのゼロトラスト

アリスタのゼロトラスト・キャンパス・ソリューションでは、AVA Sensor をスイッチに埋め込みます。これにより、ディープ・パケット・インスペクションによる独自のセキュリティ分析ソリューションをキャンパス・ネットワーク・ファブリックに組み込むことが可能になります。

アリスタの AVA Sensor がスイッチ・レイヤに埋め込まれているため、さらに多くのネットワーク・セキュリティ・コンポーネントを導入しなくても、キャンパス上のさまざまなエンタープライズ・アプリケーション、エンドポイント、IoT デバイス、ユーザーに対する強力なトラフィック分析、脅威検出、対応を行えます。また、Arista NDR が組織の既存スイッチング・インフラで提供する脅威ハンティング機能は、可視化できるキャンパスの範囲を広げ、人手による現在のセキュリティ・ワークフローを最適化しつつ、修復を自動化できる統合セキュリティ・ソリューションを実現します。



AVA Sensor を使用したゼロトラスト・コグニティブ・キャンパスの展開

ネットワーク管理者は、Arista CloudVision と Arista NetDL（ネットワーク・データ・レイク）で提供されるリアルタイムのストリーミング・テレメトリとネットワーク全体の状態データからメリットを得られます。一方で、Arista NDR を使うセキュリティ・チームは、コンテキストに応じた不可欠なデータ、履歴のフォレンジック、AI ドリブン型の脅威ハンティング機能を利用して、検出までの時間と修復までの時間の両方を短縮できます。

AVA Sensor は、ハードウェア、仮想、クラウド・ワークロード、スイッチなど、さまざまなフォーム・ファクタで提供されます。このセンサーは、ネットワーク・トポロジ、負荷、帯域幅、コストを念頭に置いて設計されています。さらに、このソリューションで適切なディープ・パケット・インスペクション・データをキュレーションし、分析エンジンへのデータの転送を最適化することで、ピーク時のパフォーマンスを損なわずに、新しいネットワークにセキュリティを組み込むことができます。

アリスタ・ネットワークスの高品質で信頼できるシングル OS のアプローチに慣れているお客様が、今度はネットワーク・セキュリティでも、一元化された統合型アプローチを利用できます。アリスタは、次の手法でネットワーク・アーキテクチャにセキュリティを組み込んでいます。

- 最新のキャンパス・インフラ全体にわたる各種エンティティ（デバイス、ユーザー、アプリケーション）の包括的なコンテキストを入手し、可視化する
- これらのエンティティにもたらされる脅威や、エンティティから生じる脅威を検出する
- ネットワーク上のエンティティの場所を自動的に特定し、アクセスを隔離・分離することによって、これらの脅威に対応する

ゼロトラスト・アーキテクチャの柱

1.状況認識でネットワーク上のすべてのリソースを把握

NIST の ZTA アーキテクチャの基本原則は、すべてのリソースとプロセスを可視化することです。リソースの定義は幅広く、さまざまなデータ・ソース、コンピューティング・サービス、ユーザー、IoT デバイスも、リソースの一種です。各リソースの状態データには、ソフトウェア・バージョン、ロケーション、日時、観測された動作、デバイス分析などを含めることができます。そのため、ゼロトラスト・モデルに移行しようとする組織は、まずリソース、権限、ビジネス・プロセスについて詳細な知識を持つ必要があります。この知識に基づいてアクセス権限ポリシーを定義し、そのポリシーをセグメンテーションなどの手段を通じて適用します。

セグメンテーションの例を考えてみましょう。 グループベースのモデルでは、さまざまなエンドポイントを動作グループに分類し、グループ間およびグループ内の通信を規制するポリシーを定義します。たいていのネットワークでは「実稼働」、「実稼働前」、「パブリック」など少数のグループだけで十分ですが、きめ細かいセグメンテーションを行うためにもっと多くのグループを必要とするネットワークもあります。グループの数がどうであれ、セグメンテーションの第一歩は、接続しているエンドポイントと通信パターンを把握することです。

さらに、既知の不具合の影響を受けやすいエンドポイントやネットワーク・インフラ、たとえば PSIRT（製品セキュリティ・インシデント対応チーム）などの既知のソフトウェアの不具合や脆弱性によって特定されるものを判別し、高リスク・グループに分類する必要があります。状況認識の戦略には、ネットワーク・インフラの脆弱性や、エンドポイントのセキュリティ態勢を理解することが欠かせません。デバイスの識別と同様、エンドポイントのセキュリティ態勢の分析に必要なきめ細かさのレベルは顧客固有の要件によって異なりますが、たとえば OS のバージョンや、接続している周辺機器（リムーバブル・ストレージ・デバイスなど）、動作中のプロセス、インストールされているアプリケーション、メモリ使用率などを含めることができます。

状況認識には多くのコンポーネントがありますが、必ずしもすべてのコンポーネントがすべてのお客様に必要なわけではありません。アリスタは、状況認識のために多様な可視化テクノロジーを提供し、他のベンダーと戦略的パートナーシップを築き、相互運用性を確保するためのオープンな規格を追求します。

2.ポリシー適用でゼロトラストのアクセス制御を実現

ゼロトラスト・セキュリティの 2 つ目の柱は、ポリシー適用コントロールです。信頼性アルゴリズムによる実行時の判断に基づいてのみ、アクセスが提供されるようにします。アリスタは、データセンター、キャンパス、クラウド・ネットワークなど、クライアントのマルチドメイン環境に適した多様なセグメンテーション・コントロールをサポートします。

従来の最も単純なセグメンテーションの形は、ポートベースのアクセス制御リスト（PACL）や、Routed ACL（RACL）を使用する VLAN または VXLAN、あるいはクライアントの通信を規制する VRF です。もちろん、ネットワーク・エッジでは外部接続からの保護、データセンターでは水平型接続の保護のために、ファイアウォールが使用されます。言い換えると、セグメンテーションの概念は新しいものではありません。1990 年代前半以来、管理者はクライアントとワークロードを VLAN や VRF セグメントに分類してきました。

少数のセグメンテーション・ゾーンだけを必要とする多くのネットワークでは、今後も VLAN や VRF などの使い慣れたセグメンテーション手法で十分です。アリスタのゼロトラスト・モデルでは、管理者がユーザーやデバイスの詳細を可能な限り把握し、きめ細かく動的なセグメンテーションを行う必要があります。セグメントが増えると、セキュリティ・グループと IP アドレスを関連付けるだけでも運用上の負担が大きくなります。たとえば、VLAN または VRF のアーキテクチャでは、新しいセグメントを追加する際に、既存のサブネットを 2 つの小さいサブネットに分割し、分割前のサブネットに接続していたデバイスの IP を割り当て直すことが必要になる場合があります。このようなネットワークの変更は扱いにくく、混乱をもたらします。標準的な PACL にも、特に TCAM（Ternary Content-Addressable Memory）でのハードウェア・リソースの拡張に関して、独自の課題があります。

ゼロトラスト・フレームワークで、特に IoT や OT が進んでいる環境でキャンパスおよびデータセンター・ネットワークのきめ細かなセグメンテーションを行うには、また別のアプローチが必要です。基本的に、セキュリティ・セグメンテーション・グループは、ネットワーク IP 構造から独立して定義する必要があります。たとえば、よく知られた Mirai ボットネットから組織を保護するために、管理者が防犯カメラ用とネットワーク化されたデジタル・ビデオ・レコーダー（DVR）用、さらに物理的セキュリティ管理者用に異なるグループを定義したいとします。各ポリシーのカメラに対しては、DVR およびセキュリティ管理者との通信のみを許可します。別のカメラとの通信については、たとえ同じサブネット上に存在するカメラであっても、許可してはなりません。なぜなら、建物が複数ある場合に、昔ながらの L3 ネットワーク設計ではカメラが複数のサブネットにまたがることが可能だからです。セキュリティ管理者とネットワーク管理者は、セグメントやその関連ポリシーを簡単に、つまり IP アドレス構造や他のネットワーク・フォワーディング構造から独立して定義できる必要があります。

3.AI ドリブン型の継続的な検出および監視

デバイスまたはユーザーがネットワーク上に存在するからと言って、信頼できることにはなりません。アリスタのゼロトラスト・アーキテクチャは継続的な監視を実行して、境界内外で発生する悪意ある行為を識別します。そして、Arista NDR によって明らかになった脅威とリスク・スコアを使用し、前述の適用コントロールでセグメンテーションの判断を行います。たとえば、リスクにさらされているエンドポイントを「高リスク」のセキュリティ・グループに移動して、アクセスを制限することができます。

インシデント対応は、NIST 800-207 フレームワークに直接含まれるものではありませんが、効果的なゼロトラストや、継続的な診断およびリスク緩和に関連します。この領域に自力で対応できる組織もありますが、多くの組織は必要に応じて専門家の力を借りたいと思っています。そこでアリスタは、世界で有数の侵害行為に長年対応してきた専門家の経験を活かした、マネージド・ネットワーク脅威検知・対応（MNDR）ソリューションの提供を開始しました。アリスタの MNDR ソリューションは、攻撃対象領域を包括的に理解してから、オンプレミス、クラウド、IoT、オペレーショナル・テクノロジーなど、すべてのインフラにおける脅威を検出し、監視することで、セキュリティ・プログラムの成熟度を大幅に向上させます。このソリューションは、受賞歴を誇るアリスタの NDR テクノロジーと、長年にわたる専門知識や高度なインシデント対応手法を組み合わせたものです。

アリスタは、侵害を受けた後の組織の対応を支援する、さまざまなインシデント対応サービスも提供しています。侵害によるダメージが後を引く主な原因は、侵害されたという事実よりも、侵害への対応の仕方にある、というのが最近の考え方です。

アリスタは、高度なスキルを持つ人材を維持し、堅牢な調査プロセスと対応プロセスを備えつつ、管理対象外のデバイス、IoT、クラウドといった技術的課題にも対応することの難しさを認識しています。しかも、これらは予防的なインシデント対策を難しくする要因の一部にすぎません。アリスタの MNDR チームが提供するリテーナーには、事前合意済みの法的条件と料金、適切なプロセス、エンドポイントおよびネットワークでの対応テクノロジー、オンデマンドで利用できる専門知識が含まれます。これによって時間を節約し、侵害後数分以内に本当に必要な専門知識を入手するとともに、金銭的損失やイメージ悪化といった攻撃の影響を封じ込めることができます。

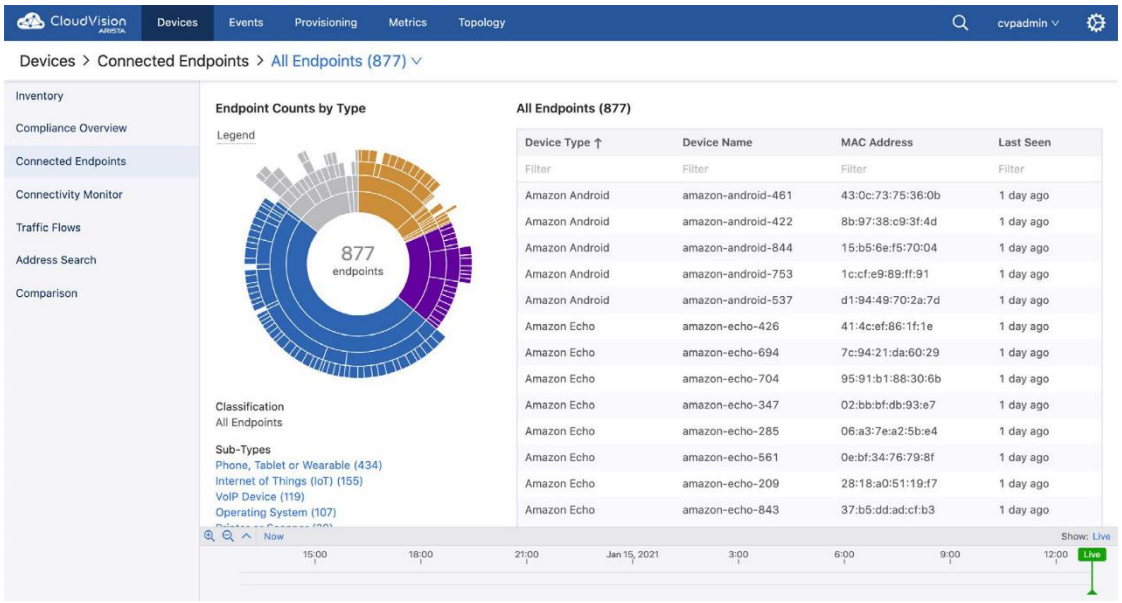
アリスタを利用したゼロトラスト・ネットワークの構築

1.Arista CloudVision、Arista NDR セキュリティ、アリスタのパートナーを活用して、接続済みのエンドポイントを把握

802.1X や他のエージェントベースのテクノロジーによるデバイス認証を行っていない IoT デバイスがある場合は、ネットワークベースの分析を利用してデバイスのプロファイル作成や認証を行うことが特に重要です。802.1X をサポートしているユーザーや他のデバイスについては、証明書と認証情報を利用して、接続プロセスの一環としてデバイスを認証します。大部分のセキュリティ・アーキテクチャでは、エージェントベースの技術とネットワークベースの技術を組み合わせてデバイスを識別します。

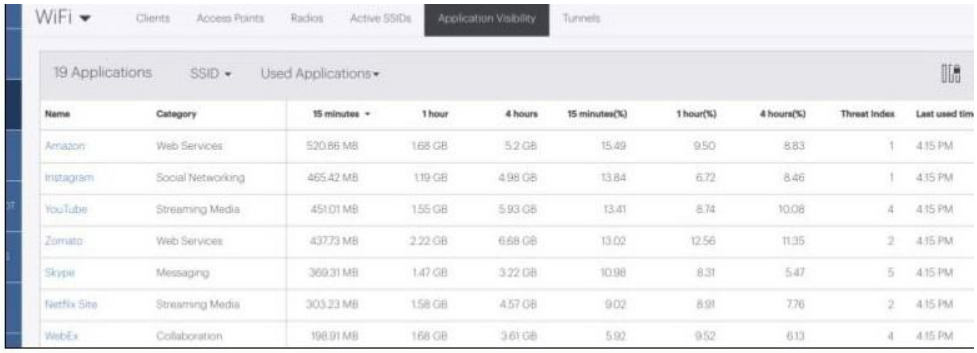
1.1 Arista CloudVision デバイス・アナライザ

Arista CloudVision デバイス・アナライザは、DHCP 分類情報を使用して、接続しているエンドポイントのプロファイルを作成します。以下のデバイス・アナライザのスクリーンショットは、ネットワーク内に 877 のデバイスがあることを示しています。デバイスは Android 携帯、タブレット、Amazon Echo などのさまざまなグループに分類され、IP/MAC アドレスや接続しているスイッチの情報と共に表示されます。



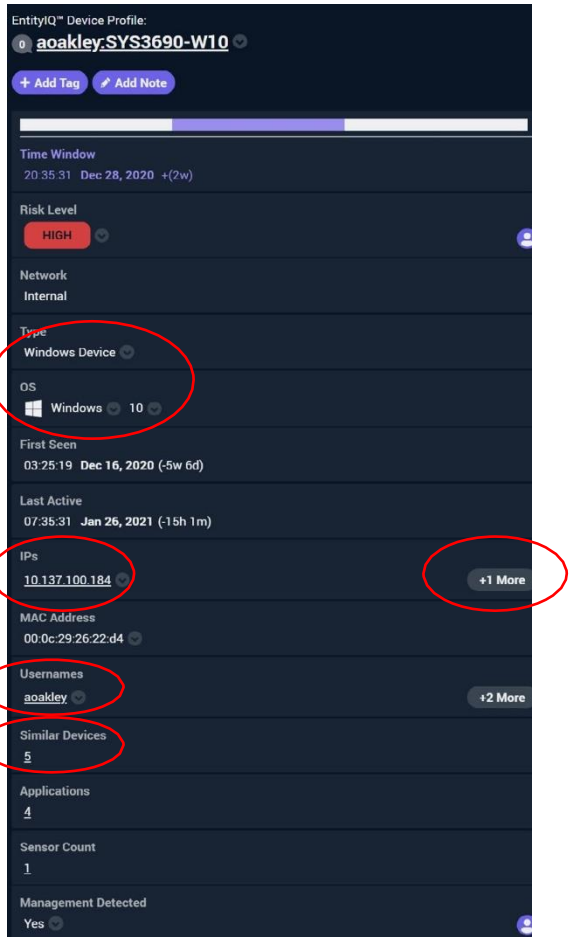
1.2 Arista CloudVision Wi-Fi

CloudVision Wi-Fi は、ワイヤレス・デバイスにも使用できます。このソリューションはパケット情報を利用して、デバイスのタイプだけでなく、使用中のアプリケーションも判断します。以下の CloudVision Wi-Fi のスクリーンショットには、Amazon や Instagram など、さまざまなアプリケーションが表示されています。アプリケーションは、Web サービスやソーシャル・ネットワーキングなど複数のカテゴリに分類されています。以下に示すように、CloudVision Wi-Fi はこの種のテレメトリを利用して、特定のアプリケーションを実行しているエンドポイントを即座に識別できます。



1.3 EntityIQ

EntityIQ は AI ベースのセキュリティ・ナレッジ・グラフを使用して、動作に基づくデバイス識別を行います。このグラフは、1 つのネットワーク接続だけで、エンタープライズ・ネットワーク上のデバイス、ユーザー、アプリケーションをエージェント不要で識別し、プロファイルを作成し、追跡します。すべてのパケットが Arista NDR にミラーリングされ、従来の IP アドレス・ルックアップにとどまらず、複数の軸に沿った分析が行われます。デバイスは共通の動作に基づいてピア・グループに分類され、ネットワークをまたいで移動したときや、IP アドレスが変更されたときにも追跡されます。たとえば、暗号化トラフィックの TLS ヘッダーを分析したり、SMB や Kerberos などのプロトコルを詳細に解析してデバイスやユーザーを識別したり、DHCP/DNS トランザクションを監視して、IoT デバイスからオペレーショナル・テクノロジーまで、ネットワーク上のあらゆるものを識別したりできます。以下のスクリーンショットに示すように、EntityIQ はそのデバイスが Windows 10 デバイスであること、主に aoakley が使用していること、最近 3 つの異なる IP アドレスが割り当てられていたことを判断できます。



1.4 サードパーティの NAC

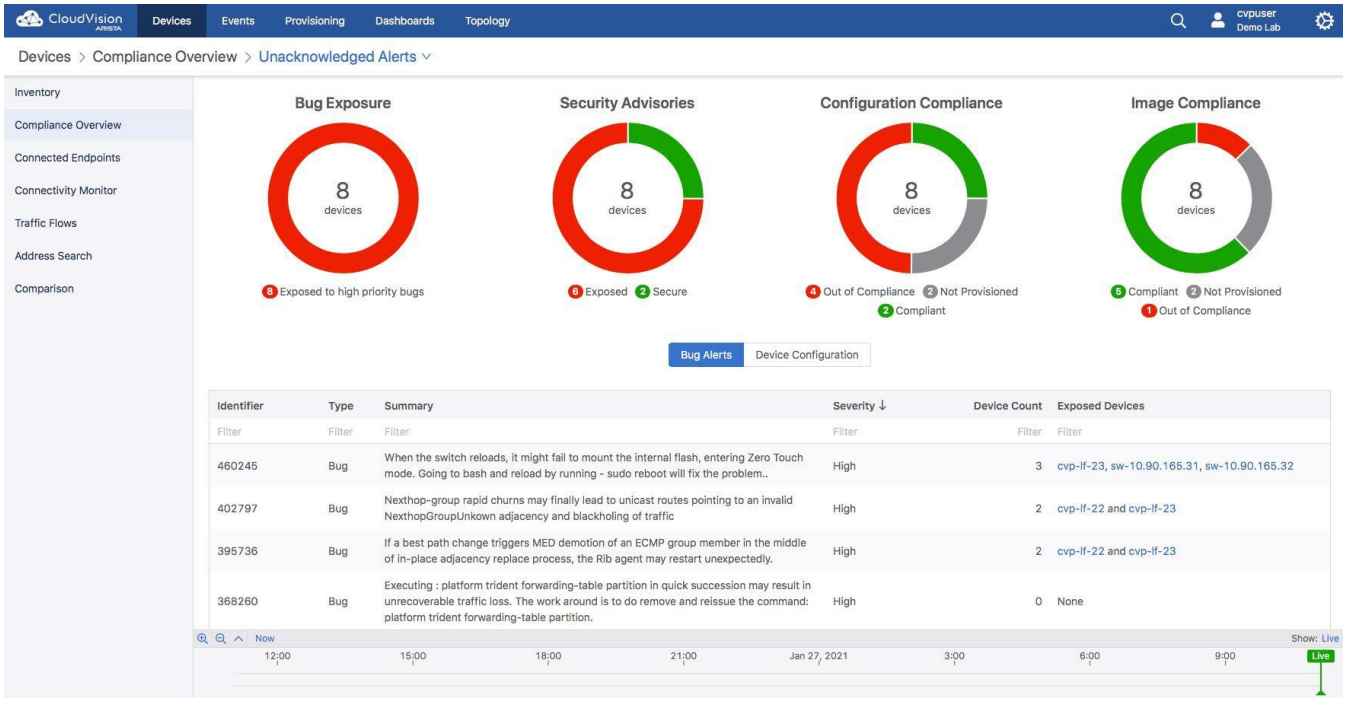
従来の NAC 製品も、接続しているエンドポイントの識別と分類に利用できます。アリスタは、Aruba ClearPass、Cisco ISE、Forescout など、すべての主要 NAC プロバイダと相互運用性があります。NAC 製品は、802.1X または MAC ベースの認証（MBA）によってデバイスを認証する RADIUS サーバーでもあります。IoT デバイスの認証には、DHCP、DNS、ユーザーエージェント、SNMP などのフィンガープリント技術がしばしば利用されます。

2. CloudVision を使用したネットワーク・スイッチの可視化

接続しているエンドポイントのデバイス・アナライザによるプロファイル作成と分類に加え、CloudVision はスイッチのパフォーマンス、ネットワーク・コンプライアンス、フロー分析処理を可視化できます。

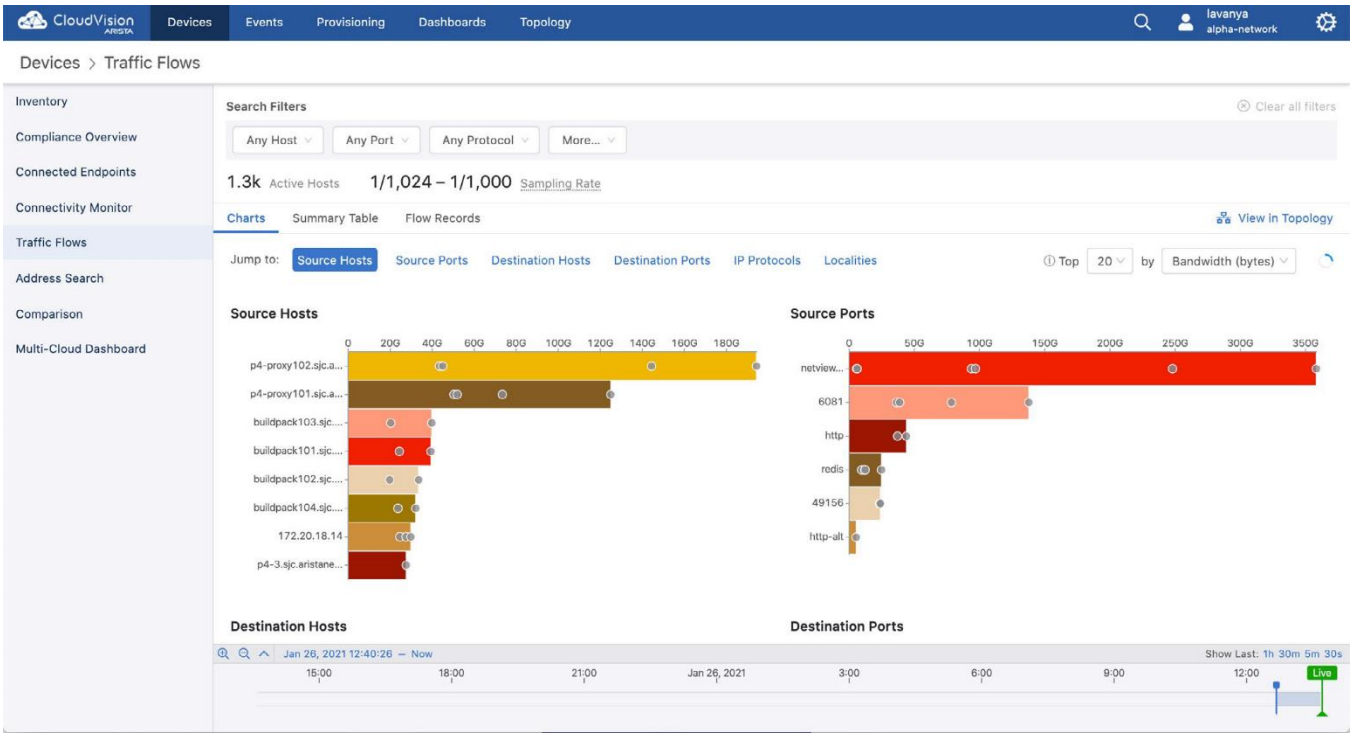
2.1 ネットワーク・コンプライアンス

ネットワーキング・デバイスが業界の PSIRT アドバイザリに対して脆弱でないと保証することは、セキュアなネットワークに不可欠です。これは ZTA の信頼性アルゴリズムの重要な要素です。CloudVision のシンプルなコンプライアンス・ダッシュボードは、ネットワーク内で観測された PSIRT セキュリティ・アドバイザリをレポートします。また、関連するソフトウェアの不具合に対する既知の脆弱性や、管理対象のスイッチに対するアウトオブバンドで無許可の構成変更もレポートします。



2.2 フロー分析

CloudVision は、sFlow や IPFIX 経由で受信したサンプリングまたは非サンプリングのフロー情報を分析し、協調に関するやり取りやフローのトラフィック・パターンのクエリ機能を提供します。この情報は、ZTA を設計し、ネットワークを継続的に監視しつつ、ビジネス・プロセスについて理解するのに役立ちます。これについては、本ホワイトペーパーの次のセクションで詳しく説明します。以下の図は、使用されている上位 20 件のホストとポート番号を表示するシンプルなクエリです。他のクエリには、特定のホストと宛先の組み合わせについてのトラフィック量が含まれています。

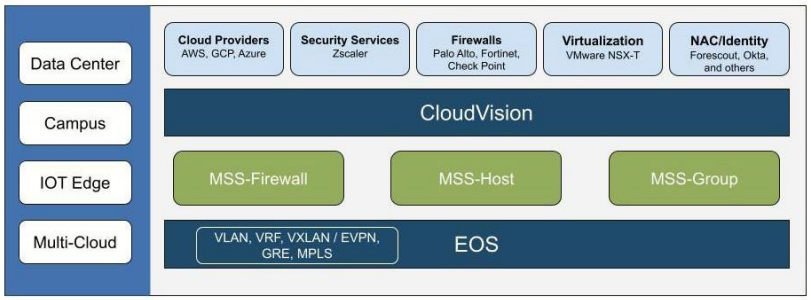


3.Arista Macro-Segmentation Service（MSS）

Arista Macro-Segmentation Service（MSS）ソリューション・セットは、VRF、VXLAN、PACL など従来のモデルをサポートしつつ、最先端セグメンテーション・オプションを提供します。

3.1 マルチドメインの MSS-Group サービス

アリスタは、MSS ソリューション・セットの一部として、マルチドメインの MSS-Group セグメンテーションを導入しました。MSS-Group は、インターフェイスやサブネット、物理ポートではなく、セキュリティ・セグメント・グループに認証ポリシーを適用します。



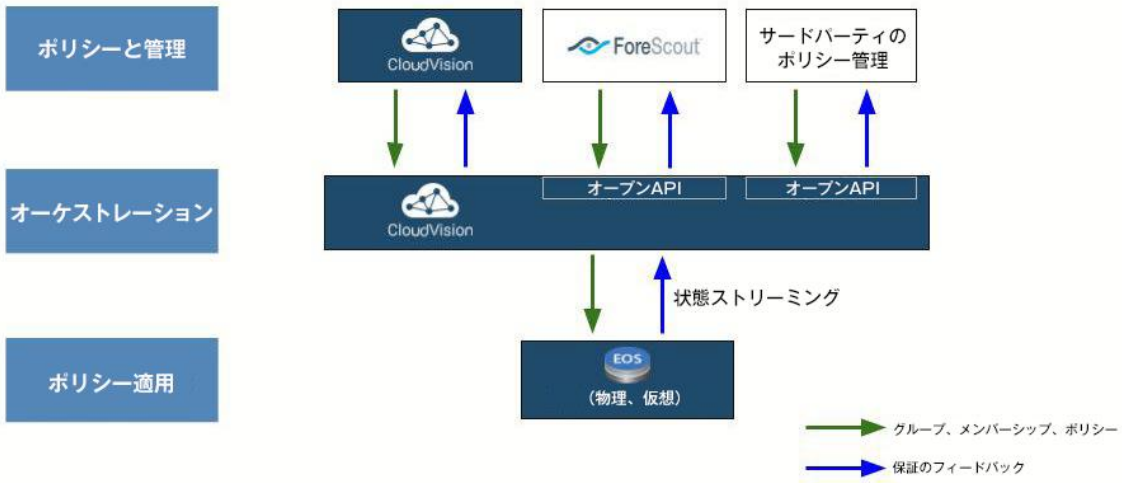
IP アドレスまたは IP サブネットは、管理者が定義したセキュリティ・セグメント・グループに分類されます。グループごとにポリシーが適用され、セグメント・グループ間とセグメント・グループ内の両方の通信を定義します。

たとえば、よく知られた Mirai ボットネットから組織を保護するために、管理者が防犯カメラ用とネットワーク化されたデジタル・ビデオ・レコーダー（DVR）用、さらに物理的セキュリティ管理者用に異なるグループを定義したいとします。管理者は MSS-Group を利用し、定義済みのセグメント・グループ「DVR」とは協調できるが、互いを含むその他すべてのメンバーとは通信できない「カメラ」というセグメント・グループをポリシーごとに定義できます。ポリシーはセグメント・グループ単位で定義されるので、IP アドレスと関係なくセグメンテーション・ルールのポリシーを作成できます。

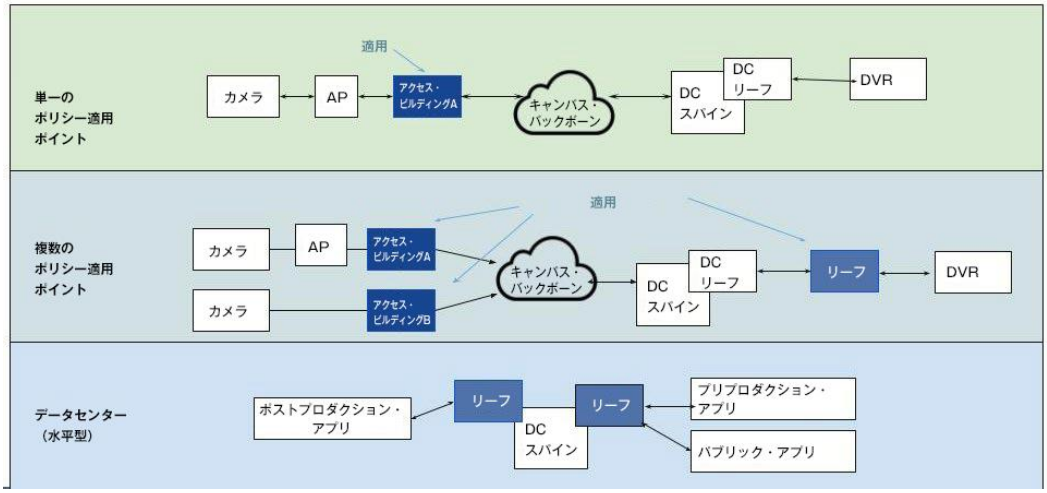
Arista スイッチのハードウェアには、セキュリティ・セグメントを作成し、セグメント間にポリシーを適用する機能が組み込まれています。スイッチは、各セグメントに属するホストやサブネットを定義するメンバーシップと、特定のセグメントが通信できる他のセグメントを定義する（同じセグメントの他のメンバーと通信できる場合を含む）ポリシーを使用し、どのようなセグメント・グループを作成する必要があるかに基づ

いて構成します。スイッチはさまざまな方法で構成できます。スイッチの台数が少ない場合には、アリスタの標準 CLI や EAPI などで十分です。

ネットワーク全体に展開するスイッチは、オーケストレーション・レイヤを使用してプロビジョニングしなければなりません。オーケストレーション・レイヤは CloudVision の機能の 1 つで、MSS-Group のポリシー適用を実行するすべての Arista スイッチに、一貫性ある構成をプッシュします。オーケストレーション・レイヤは、ポリシー・レイヤからグループのメンバーシップとポリシー情報を受け取ります。ポリシー・レイヤは論理レイヤで、やはり CloudVision の機能に含まれる場合があります。管理者は、静的グループ・セグメント・ポリシーとメンバーシップを CloudVision 内でプログラムできます。



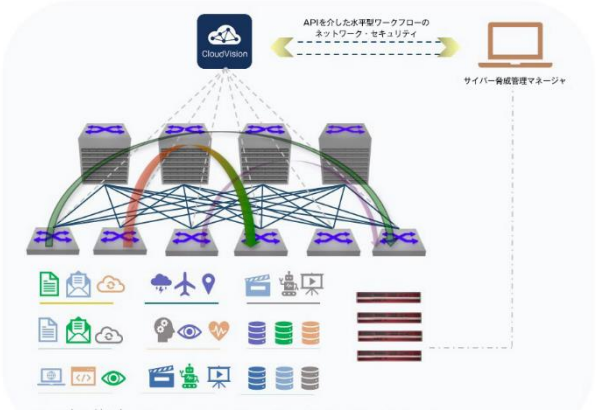
MSS-Group ソリューションが最も強力になるのは、CloudVision が動的識別レイヤと統合されているときです。Forescout などのパートナーは、CloudVision で利用できる API を活用し、デバイスのフィンガープリント、動作、802.1X 認証、およびその他のメカニズムに基づいて、さまざまなデバイスを論理グループに分類できます。Forescout は、API を利用して各デバイスと関係するセキュリティ・セグメンテーション・グループを関連付け、CloudVision 内で適切なセグメンテーション・ポリシーを適用することができます。すると、MSS-Group 対応の各種スイッチに合わせて、必要なポリシーを CloudVision がオーケストレーションします。新しいデバイスがネットワークに参加したり、セグメンテーション・グループのメンバーシップが変更されたりすると、Forescout はその変更内容で自動的に CloudVision を更新します。CloudVision は、各種スイッチからヒット数やセグメント破棄情報を収集します。この情報は、CloudVision の分析レポートに使用されたり、Forescout に転送されて Forescout のレポートに使用されます。

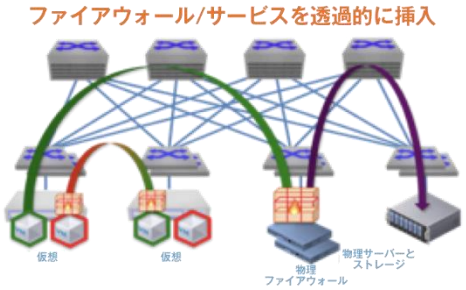


MSS-Group のセグメンテーション・アーキテクチャは、市販されている他のソリューションとは異なり、独自のイーサネット・タグやプロトコルに依存しません。そのため、上流でも下流でもあらゆるベンダーのスイッチを使用できます。 アリスタの MSS-Group 対応スイッチは、ポリシー適用が必要なあらゆる場所に展開できます。 スイッチを流れるすべてのパケットに対して適用するポリシーを作成できます。MSS-Group はアクセス・レイヤに展開することが理想的ですが、以下の図は、MSS-Group を利用して構成した 1 台のスイッチで通信フローの端から端までポリシーを適用する方法を示しています。もちろん、ポリシー適用ポイントは必要に応じて追加できます。

3.2 MSS Firewall サービス

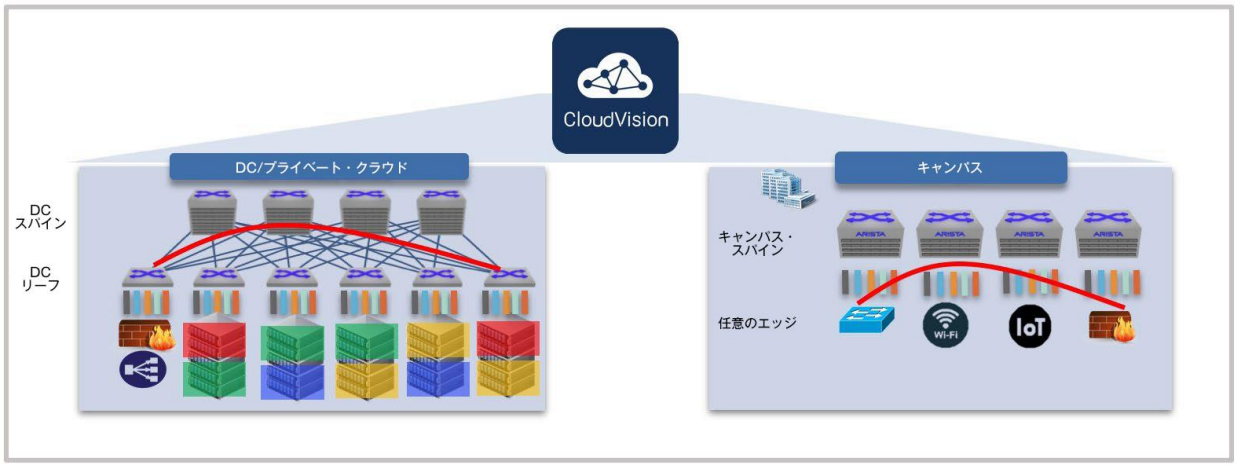
MSS Firewall は MSS の一種で、管理者が Fortinet、Palo Alto Networks、または Check Point の論理ファイアウォールをトラフィック検査用のデータ・パスに動的に挿入できるようにします。CloudVision は、サポート対象のファイアウォール・コントローラと接続します。管理者は、そのファイアウォール・コントローラ内でトラフィック検査ポリシーを定義します。そのファイアウォール・コントローラが、定義されたポリシーを CloudVision に伝達します。Arista CloudVision は、ネットワーク内のすべての状態データを保存する、NetDB と呼ばれるネットワーク全体のデータベースを保守します。NetDB は、すべてのワークロードがネットワーク内のどこにあるかを認識します。また、ネットワークに追加、移動、削除された新しいデバイスやワークロードについて、リアルタイムで学習します。ファイアウォール・コントローラからトラフィック検査ポリシーについて学習した CloudVision は、NetDB 内にあるスイッチの位置情報を利用して、適切なスイッチを構成します。CloudVision は、特定のトラフィックをファイアウォールにリダイレクトするようにスイッチをプログラムできます。あるいは、選択したトラフィックを破棄または転送して、ファイアウォールを回避するように ACL をプログラムできます。





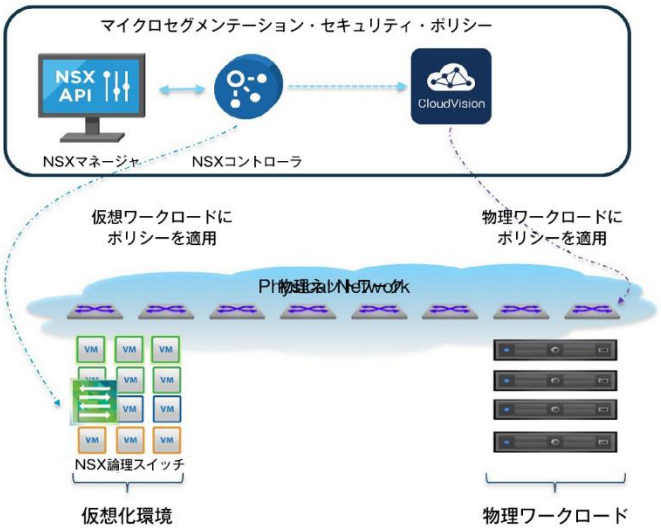
以下の図は、ネットワーク内のあらゆる場所にあるワークロードの特定のトラフィックを単一の物理ファイアウォールで検査できる仕組みを示しています。大規模なデータセンターでは、ファイアウォールを 1 台のサービス・ラックに一元化し、オンデマンドで、またはファイアウォール・ポリシーに基づいて、あらゆるワークロード間のパスに挿入することができます。 MSS Firewall は標準ベースのフォワーディングを使用して、複数のサービス・デバイスをトラフィックのパスにまとめます。この機能は、ネットワークが複数ベンダーのデバイスで構成されている場合でも完全に機能します。

当初、MSS Firewall はデータセンターのトラフィックをセグメント化するために開発されましたが、現在はキャンパスの垂直型トラフィックのセグメント化にも利用されています。キャンパスのユースケースでは、MSS Firewall がセキュアなアプリケーションへのトラフィックを制限し、サービス拒否（DOS）攻撃から保護します。 選択したアプリケーションに接続しているすべてのフローはファイアウォール・サービス・ノードに転送され、ファイアウォールで定義されたポリシーごとに詳細な検査が行われます。同様に、デバイスを信頼する前、または件名にリスクがあると見なされる場合、MSS Firewall はさらなる検査を追加できます。



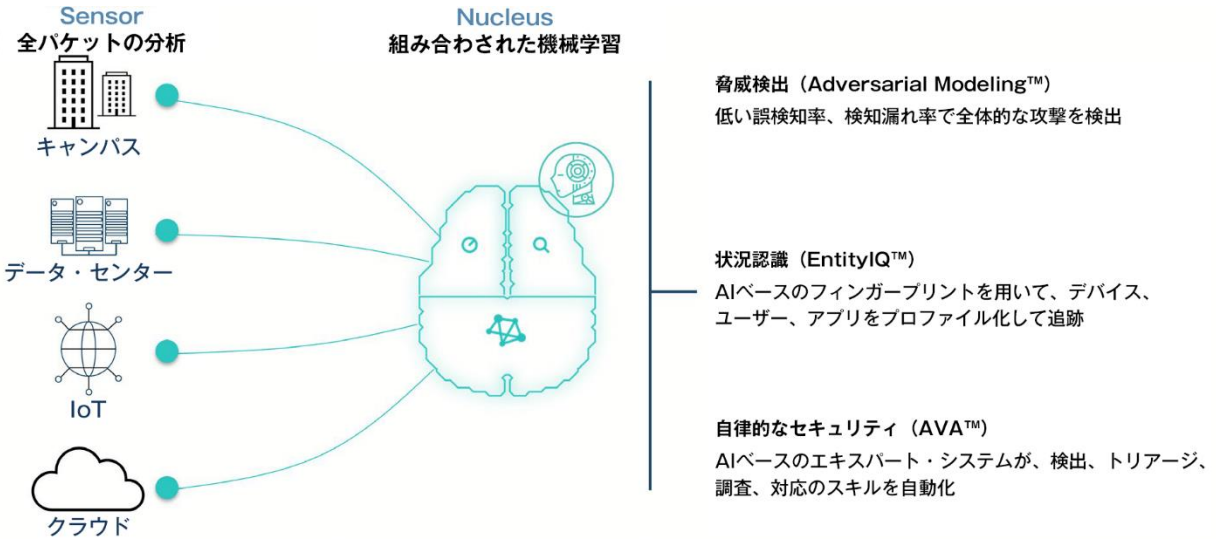
3.3 MSS Host サービス

アリスタと VMware は相互の提携に基づき、VMware のマイクロセグメンテーション・テクノロジーと Arista MSS Host を統合しています。このソリューションにより、単一の管理ドメインで VM と物理ワークロードの両方を管理できます。ネットワーク・エッジで物理ワークロードにセキュリティ・ポリシーを適用することで、均一性と一貫性が確保されます。稼働時には、Arista MSS Host が VMware NSX コントローラに登録され、ポリシーを受け取ります。CloudVision は、単独の Arista スイッチまたはスイッチ・ペアを、物理ワークロードと仮想ワークロード間のやり取りを許可または拒否するように適切にプログラムします。これによって、新しいセキュリティ・ポリシーが作成されたときや、既存のポリシーが変更されたときに、セキュリティ・ポリシーを動的に同期することができます。MSS Host ソリューションにより、組織は統一ポリシーを大規模に導入してすべてのアセットを保護し、全体的なリスクを軽減したり、俊敏なサービス・デリバリーを実現したりできます。



4.Arista NDR

Arista NDR は、キャンパス、データセンター、IoT、クラウドのワークロード・ネットワークにまたがる詳細なネットワーク分析を基盤として構築されています。Arista NDR は、他のネットワーク脅威検知・対応（NDR）ソリューションと異なり、3,000 以上のプロトコルを解析し、暗号化トラフィック分析の実行など、レイヤ 2 からレイヤ 7 までのデータを処理します。前述のとおり、EntityIQ はこの情報を使ってデバイス、ユーザー、アプリケーションなどのエンティティのプロファイルを自律的に作成すると同時に、このような通信内容を履歴のフォレンジックに利用するために保存します。その後、AVA Nucleus が機械学習の組み合わせを用いて、隠されていた悪意ある行為を見つけ出します。



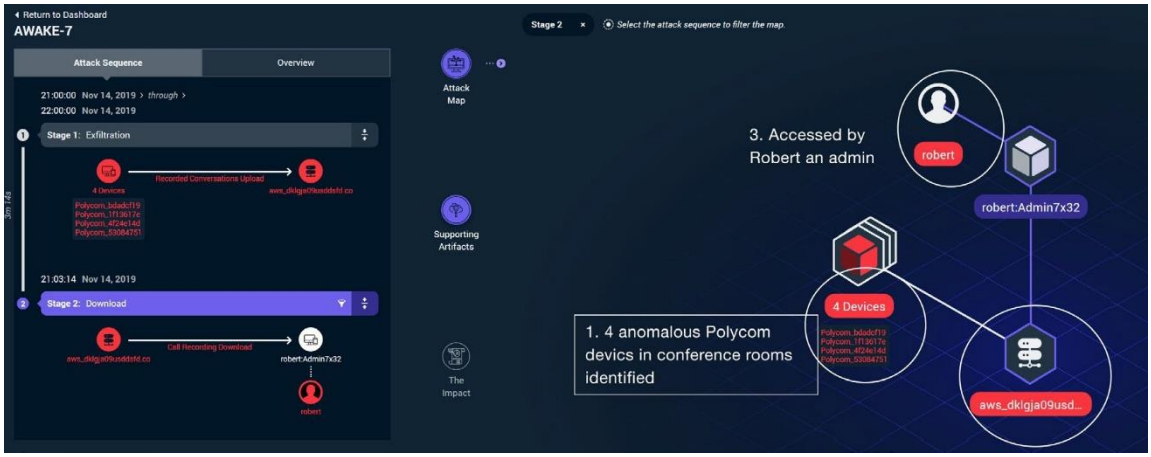
4.1 Adversarial Modeling

Adversarial Modeling 機能によって、複雑な攻撃の戦術、技術、および手順（TTP）を表現するボキャブラリーを提供し、さまざまなプロトコルで長期間にわたり発生している場合でも、このような動作パターンを識別して、複数のネットワーク・アセットに影響を与える自律的な脅威ハンティングを実現できます。

4.2 Arista AVA

世界初の AI ベースのセキュリティ・エキスパート・システムである Arista AVA（Autonomous Virtual Assist）は、自律的な脅威ハンティングとインシデント・トリアージを実行します。AVA は人工知能、オープンソースのインテリジェンス、人の知識を利用して、自律的に、時間、エンティティ、およびプロトコルから複数の点を多次元的に結び付けることで、意味のないアラートを生成するのではなく、エンドツーエンドの状況をエンドユーザーに提供できるようにします。さらに、1 つの画面で攻撃の全体像を可視化し、調査と修復のオプションを提示する意思決定サポート・システムが、アナリストにメリットをもたらします。自分で全体像を苦労して組み立てる必要はありません。

このスクリーンショットは、Arista NDR の機能を説明するものです。この実用的なケース・スタディでは、他の Polycom デバイスとは異なる振る舞いをしている 4 台の Polycom デバイスが、プラットフォームによって識別されました。これらのデバイスは、EntityIQ によって「IP 電話」というラベルが付けられ、4 つの会議室に関連付けられています。さらに、これらの電話は、AWS にホストされているサーバーと予期せぬ通信を行っています。それとは別に、IT 管理者（匿名化されたケース・スタディでは「Robert」）が AWS サーバーにアクセスしています。Arista NDR はこれらの異質なイベントをまとめ、悪意ある活動を識別しました。この例では、Robert が 4 つの会議室にある Polycom 電話経由のやり取りを録音し、そのデータを AWS サーバーにアップロードしました。その後、Robert は録音データを不正な目的で取得しました。AVA が悪意ある行為を識別すると、コンテキストに応じた対応メカニズムがトリガーされ、デバイスの分離とゼロデイ脅威の解決が行われます。



4.3 アリスタのサードパーティ・インテグレーション

Arista NDR は、既存のソリューションと連携でき、業界最高水準の SIEM（Splunk など）や、ビジネス・インテリジェンス（Microsoft Power BI など）、チケッティングおよび分析機能（ServiceNow など）、エンドポイント検出機能（CrowdStrike など）、セキュリティ・オーケストレーション・ツール（Palo Alto Networks の Cortex XSOAR など）との連携を通じて、その機能を強化できます。また、ワークフローや統合をカスタマイズするための完全な API もサポートしています。たとえば、SIEM が統合されると、それまで IP アドレスまたは電子メールアドレスが含まれるアラートを頼りにしていたアナリストは、関連するユーザーと役割、オペレーティング・システムとアプリケーションの詳細が含まれるデバイス・プロファイル、フォレンジックな脅威タイムライン、およびキャンペーン分析用のデバイスのリストが使えるようになります。同様に、エンドポイント統合によって、1 回のクリックで侵害デバイスを隔離したり、エンドポイントのフォレンジック・データを取得することが可能になります。

まとめ

攻撃はますます高度化し、従来のマルウェアベースの脅威よりも巧妙で、よく知られたフィッシングやエクスプロイトなどの手法に依存しない攻撃も現れています。2021 年には、ランサムウェアに関連するデータ・リークが 82%増加しました。

実際、ハイブリッド・ネットワークが世界中で採用されるに伴い、サイバー攻撃者は状況の変化に適応し、より広範囲に罠を仕掛けるようになっています。

セキュリティ・チームはまず、「環境は侵害され、境界は侵入を受ける」と考えなければなりません。この考え方の下で、想定される侵害状態に耐えられるよう、ネットワークやシステムを設計する必要があります。これが、AI ドリブン型のセキュリティ・モデルとセグメンテーションや可観測性を組み合わせた、アリスタのゼロトラスト・ネットワーキング・アーキテクチャの前提となっています。

[2] CrowdStrike、2022 Global Threat Report

アリスタネットワークスジャパン合同会社

〒100-0004　東京都千代田区大手町 1-7-2　東京サンケイビル　27F
Tel:03-3242-6401

西日本営業本部
〒530-0001　大阪市北区梅田 2-2　ヒルトンプラザウエストオフィスタワー　19F
Tel: 06-6133-5681

お問い合わせ先

Japan-sales@arista.com

www.arista.com/jp

2022 年 2 月