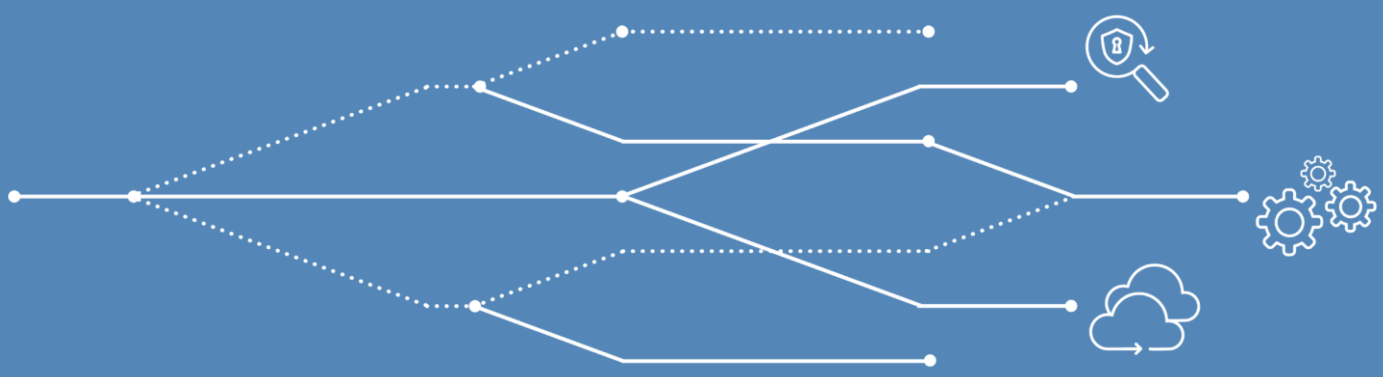


Arista NDR Campus Edition

デジタル変革の取り組みが加速し、組織が対面型の職場に新しい戦略の策定を進めようとする中、キャンパス・ネットワークは大幅に進化しています。今では、ネットワークに接続するエンドポイントのかなりの割合をビルディング・オートメーションやその他の IoT デバイスが占めることが多くなりました。SaaS アプリケーションの導入を主な要因として、そのようなキャンパスからのトラフィックをデータセンターにバックホールすることはまれになり、代わりにインターネットに直接ルーティングするようになっています。このアーキテクチャでは、従来型のネットワーク・セキュリティ・アプローチでこうしたロケーションの多くを把握できません。一方、エージェントベースのソリューションは、保護すべきデバイスとの互換性がありません。そのため、攻撃者のラテラル・ムーブメントや、ランサムウェア、マルウェアを使わない内部脅威、認証情報の悪用に気付かない可能性があります。組織には、それぞれのキャンパス・ロケーションでこのような脅威を効率的に特定でき、そうしたロケーションにおける追加のハードウェア展開やセキュリティ専門知識を必要としない、ネットワークベースの脅威検出・対応ソリューションが必要です。

有線と無線のネットワークの礎を築いてきた Arista は、このようなセキュリティのギャップを埋めるのに最適な立場にあります。

セキュリティをネットワークに組み込むことにより、複数の異なるネットワーク・セキュリティ・オーバーレイが不要になり、Arista のゼロトラスト・ネットワーキング[1] のポートフォリオの他のコンポーネントと併せて、運用コストと複雑さ、および各ロケーションにおける専門家の必要性を低減します。

Arista NDR Campus Edition は、容易に展開できるソフトウェア **AVA Sensor** 拡張を既存の Arista コグニティブ・キャンパス・スイッチに使用します。このセンサーは、Arista CloudVision または Ansible プレイブックを使用して簡単に展開でき、3,000 以上のプロトコルを解析し、レイヤ 2 からレイヤ 7 までのデータを処理するように設計されています。また、暗号化プロトコルを分析して、トラフィックの種類(ファイル転送、インタラクティブ・シェル他)や通信を交わしているアプリケーション、リモート・アクセスの有無などの重要なコンテキストを、データを復号化することなく特定します。**Arista の EntityIQ™** テクノロジーでは、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を自律的にプロファイル化すると同時に、これらの通信履歴をフォレンジックに利用するために保持します。

Arista NDR Campus Edition

EntityIQ™により、組織の管理下にあるかどうかに関係なく、すべてのデバイス、ユーザー、およびアプリケーションを自律的に検出し、プロファイル化できます。

ネットワーク・スイッチに直接展開することで、きめ細かな可視化を実現でき、ハードウェアを追加する運用オーバーヘッドを削減できます。

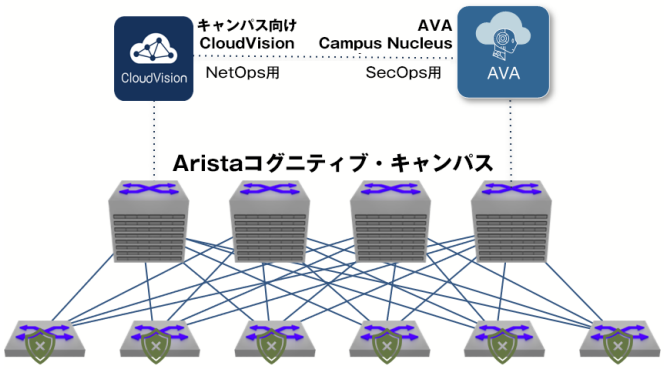
AVA™ AI を利用して、トリアージと調査を自動化し、意思決定支援システムをアナリストに提供できます。

エージェント、手動の設定、または時間のかかるトレーニングを必要としません。

[1] https://www.arista.com/assets/data/pdf/Arista-ZTNO-Solution-Brief.pdf

「Arista NDR は私たちの予想を超えました。接続されたワークスペースを、かつてないほど効果的かつ自律的に保護できるようになりました」

– Rich Noguera 氏、Gap Inc. 前最高情報セキュリティ責任者



コグニティ・キャンパス向け
Network Detection and Response (NDR)

- キャンパス向けに最適化されたNDR Nucleusと、スイッチベースのセンサー、およびオプションのマネージド脅威ハンティングの専門知識
- オーバーレイ・ネットワーク、TAP/SPAN、セキュリティ・ギアのための追加ラック・スペースは不要
- IoT、ラテラル・ムーブメント、内部脅威、ランサムウェアなど、キャンパス環境における脅威検出の盲点を排除
- CloudVisionのセキュリティ専用ダッシュボードを介したNetOpsとSecOpsのワークフロー統合
- NAC、セグメンテーション、ファイアウォール、プロキシ、エンドポイント・セキュリティ、SIEMなどを介したシームレスな修復

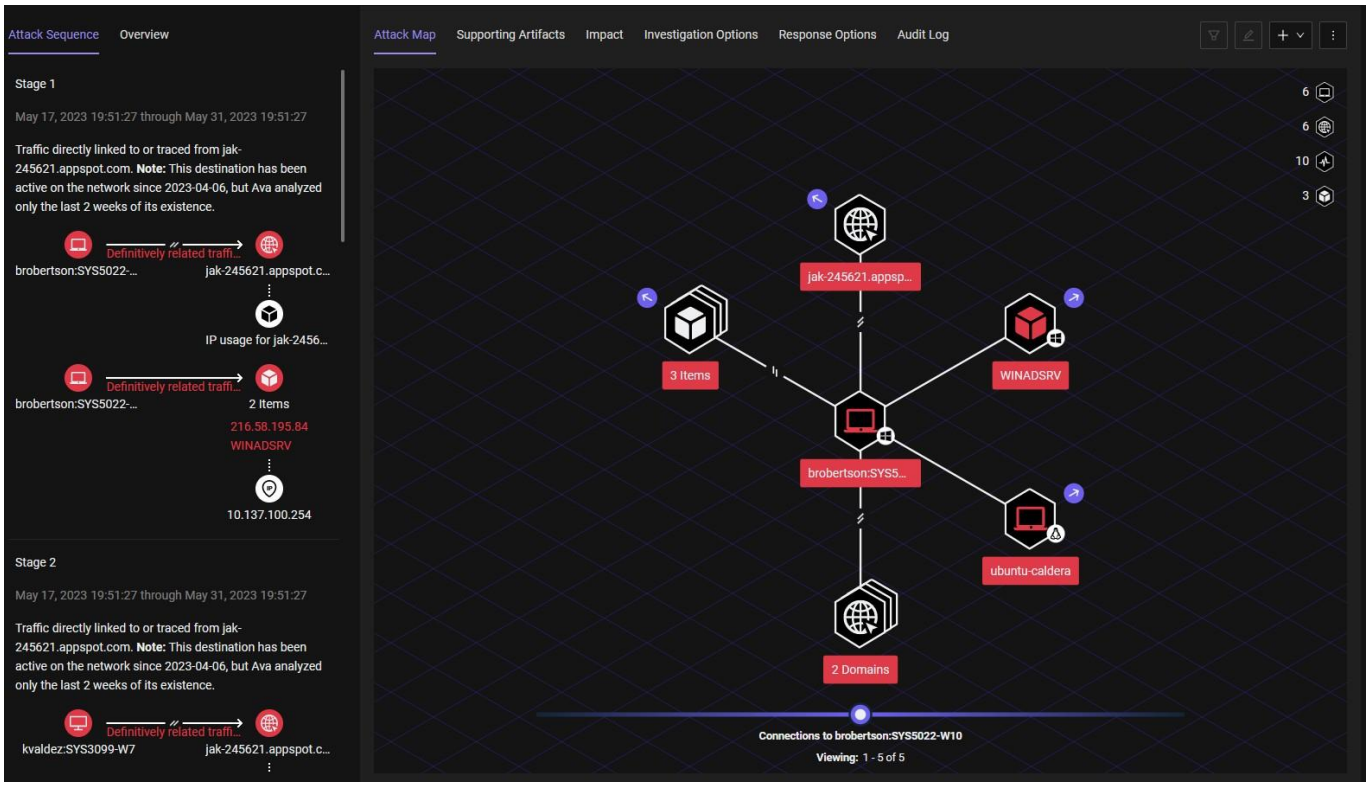
抽出されたアクティビティ・データは **AVA Campus Nucleus** に読み込まれ、複数の検出モデルを組み合わせて悪意のある行為を発見します。複数の機械学習方式を協調させて使うので、単純かつ多大な誤認知や教師なし学習に頼る必要はありません。

Arista の **Adversarial Modeling™**機能では、最高レベルに複雑な攻撃の戦術、技術、および手順(TTP)を見抜くことができます。Arista の脅威研究チームは、Adversarial Modeling を使用して、疑わしいアクティビティに狙いを定めてから有力な証拠を集めて容疑を特定する AI ドリブン・モデルを構築し、保守します。このプロセスは誤検知と検知漏れの両方を削減します。

AVA(Autonomous Virtual Assist)は、Arista の AI ドリブン意思決定支援システムで、脅威ハンティングとインシデント・トリアージを自動化します。AVA は時間、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大量に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するので、アナリストは 1 つの画面で調査と修復のオプションを使って、攻撃の全体像を把握できます。自分で全体像を苦労して組み立てる必要はありません。ここで重要なのは、連合機械学習のおかげで、Arista のお客様は、プライベートなデータを自身のインフラストラクチャに確実に保持しながら、これらの機能を利用できることです。

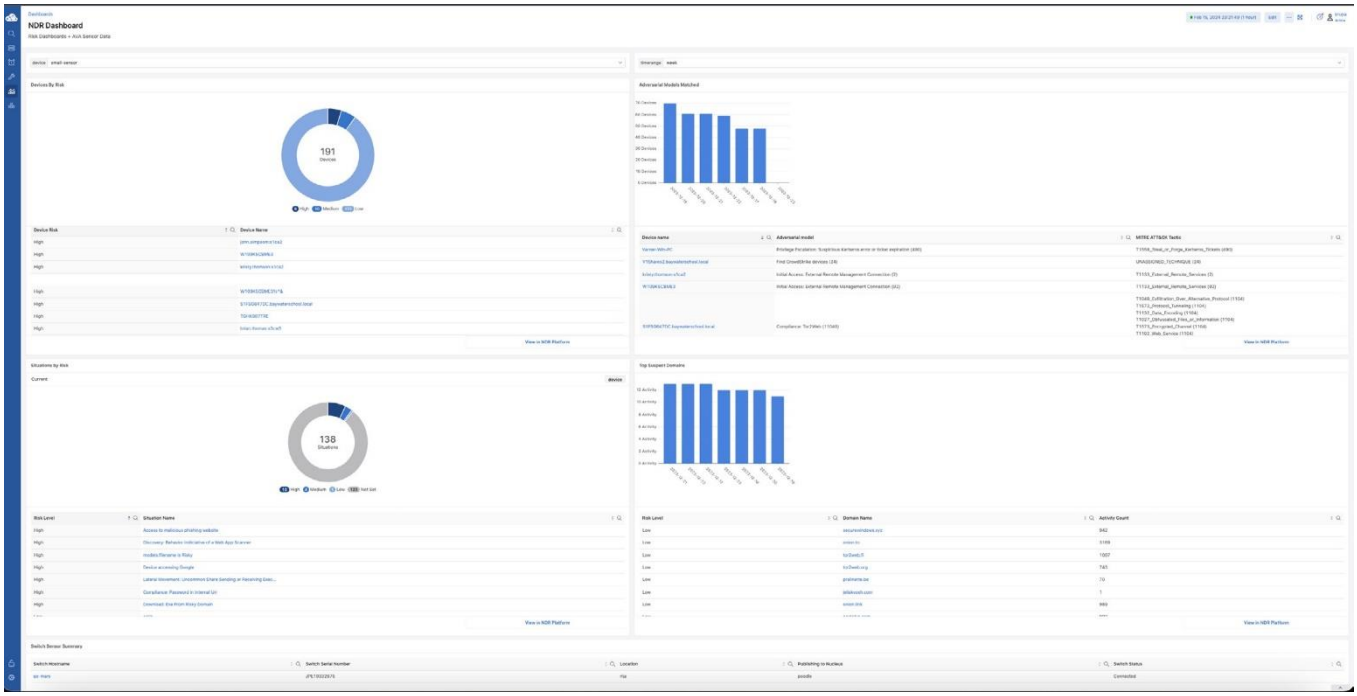
ユースケース

検出	対応	状況認識
内外の攻撃者からの意図や行動に悪意がある脅威を検出し、MITRE ATT&CK フレームワーク・マッピングに基づいてトリアージします。	AVA によってエンティティ、時間、プロトコル、攻撃ステージを相関付けられた、必要な意思決定支援コンテキストを利用して、迅速に調査し、対応します。	契約業者やサードパーティのデバイスも含め、管理対象と管理対象外の IT/IoT デバイスを学習および追跡するプラットフォームにより、キャンパスを包括的に可視化します。



インテグレーション

Arista NDR Campus Edition は、SIEM、エンドポイント検出・対応ツールなどのソリューションや、ファイアウォール/プロキシと統合できます。たとえば、それまで IP アドレスまたは電子メールアドレスしか含まれていない SIEM アラートを頼りにしていたアナリストは、オペレーティング・システム、デバイスの詳細、関連するユーザーが含まれる EntityIQ プロファイル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できます。また、このプラットフォームは、CloudVision や CV AGNI(ネットワーク・アクセス制御)など、Arista のネットワーキングとゼロトラストのソリューションとの緊密なインテグレーションをサポートしています。



モデル番号	DCA-NDR-NCC10
パフォーマンスと容量	
機能	Campus Nucleus
保護されるスループット	最大 10 Gbps
システム要件	
ラック・ユニット	1U
CPU コア数	16
RAM	64 GB
不揮発性メモリ	3.2 TB
ネットワーク	2x 10/25 Gbps SFP 1x アウトバンド管理インターフェイス
電源	2x 800W – 冗長化 / ホットスワップ対応

モデル番号	SS-NDR-G-SWITCH-1M	SS-NDR-G-T1-1M	SS-NDR-G-T2-1M
階層	スイッチ最大 149 台	スイッチ 150～499 台	スイッチ 500 台以上
機能	Sensor のみ	Sensor のみ	Sensor のみ
システム要件			
サポート対象の Arista スイッチ	以下のリンクを参照し、1 つまたは複数のスイッチ・モデルを選択してから[Product Features]で[Campus Features]を選択し、[AVA switch sensor]のチェックマークの有無を確認してください。 https://www.arista.com/en/support/product-documentation/supported-features		

モデル番号	SS-SEC-AMNDR-Switch-1M
階層	このサービスは、30 台以上のスイッチでスイッチごとに利用できます。
機能	Managed Network Detection and Response
システム要件	
サポート対象の Arista スイッチ	このオプションのアドオン・サービスでは、24 時間 365 日対応のエキスパート・チームによる脅威ハンティングおよびインシデント対応を利用できます。 サービスの詳細については、以下のデータシートを参照してください。 https://www.arista.com/assets/data/pdf/Datasheets/Managed-Network-Detection-and-Response-MNDR-Datasheet.pdf

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

2024 年 3 月 6 日