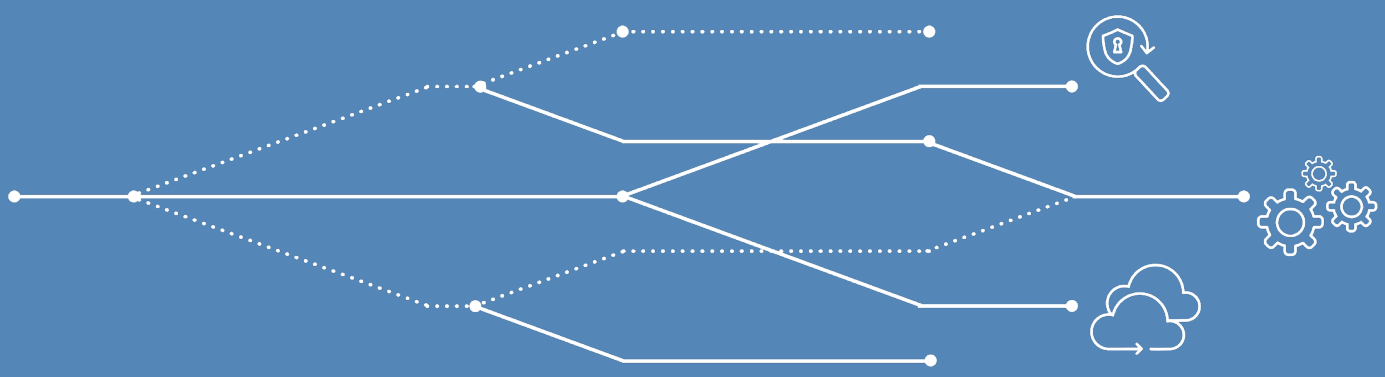


Arista NDR

攻撃の手口がマルウェアだけでなく、サプライチェーンへの脅威、インサイダー攻撃、環境寄生型攻撃へと進化しているため、従来型のセキュリティソリューションの対応が手詰まりに陥っています。それと同時に、ネットワークの世界でも、非管理型 IoT、クラウド・インフラストラクチャ、契約業者やサードパーティのデバイス、シャドーIT などの新しい変化が現れています。新しいネットワークがますます重要性を増し、企業の境界を越えて広がっているため、連鎖的な攻撃対象領域に対処し、サイバーセキュリティ戦略を統合して総合的な可視性と制御を提供することが、組織にとって不可欠となっています。

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・レイヤに実装することで、ネットワーク・セキュリティ技術を何層も重ねる必要がなくなるため、運用コストと複雑さを軽減できます。このアプローチにより、幅広い攻撃対象領域の脅威を効果的に追跡し、適切に対応できます。

Arista NDR プラットフォームは、データセンターやキャンパス、IoT、クラウド・ワークロード・ネットワーク、SaaS アプリケーションなどの「新しいネットワーク」に展開された AVA Sensor による高度なネットワーク分析を基盤に構築されています。これらのセンサーは、Arista スイッチ内蔵型、スタンドアロン・ハードウェア、仮想またはクラウドなど、多様なフォーム・ファクターで提供されます。

Arista NDR は、他のネットワーク検出対応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、レイヤ 2 からレイヤ 7 までのデータを処理します。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。アリスタの EntityIQTM 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 にしかない機能

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。

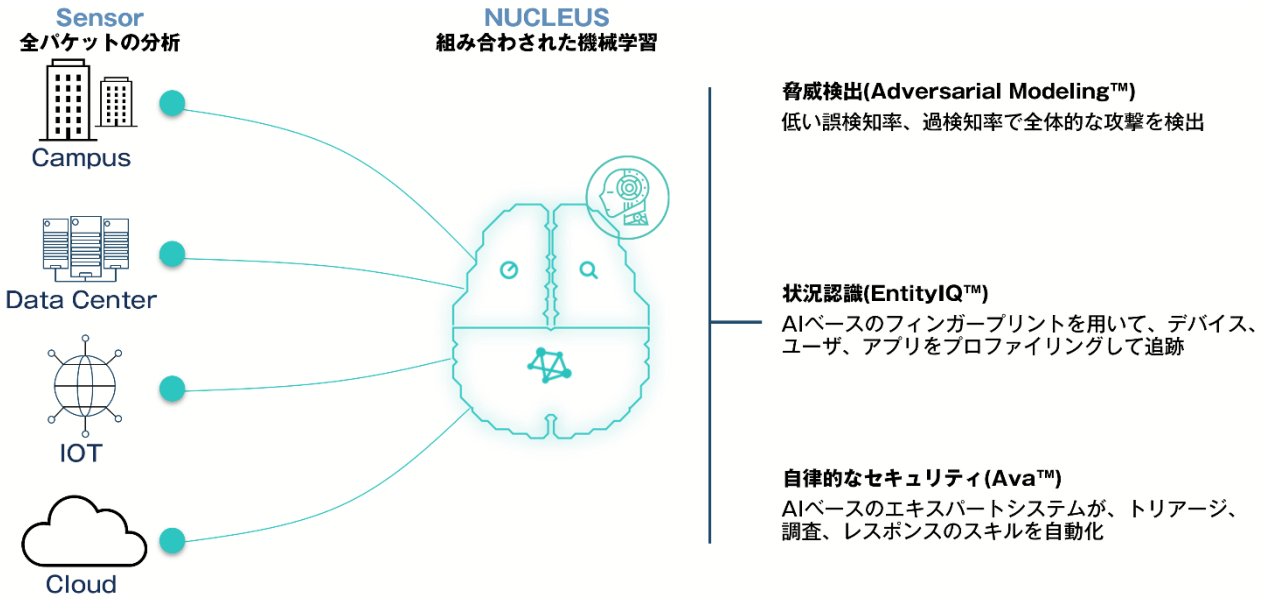
AI を使って暗号化トラフィックを可視化して、ネットワーク・アプリケーション、リモート制御、ファイル転送などを特定できます。

内部の脅威、認証情報の悪用、ラテラル・ムーブメント、およびデータ流出などの攻撃を暴く Adversarial Modeling™を提供できます。

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、意思決定サポート・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。



抽出されたアクティビティ・データは **AVA 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。AVA Nucleus は、完全にオンプレミスで利用することも、Arista クラウドで SaaS 機能として利用することもできます。

Arista の **Adversarial Modeling™** 言語では、最初に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し拡張可能な AI ドリブン・モデルを使うことで、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。このモデル化言語は、豊かなデータ分析機能と攻撃の TTP を表現するボキャブラリーを提供できるので、比較的経験の浅いアナリストでも高度な脅威を検出できます。AVA Nucleus は、シングル・サインオンのロールベースのユーザー・エクスペリエンスを提供するだけでなく、拡張性、通知、および自動応答と修復のための他の IT およびセキュリティソリューションとの統合のための完全な API も備えています。

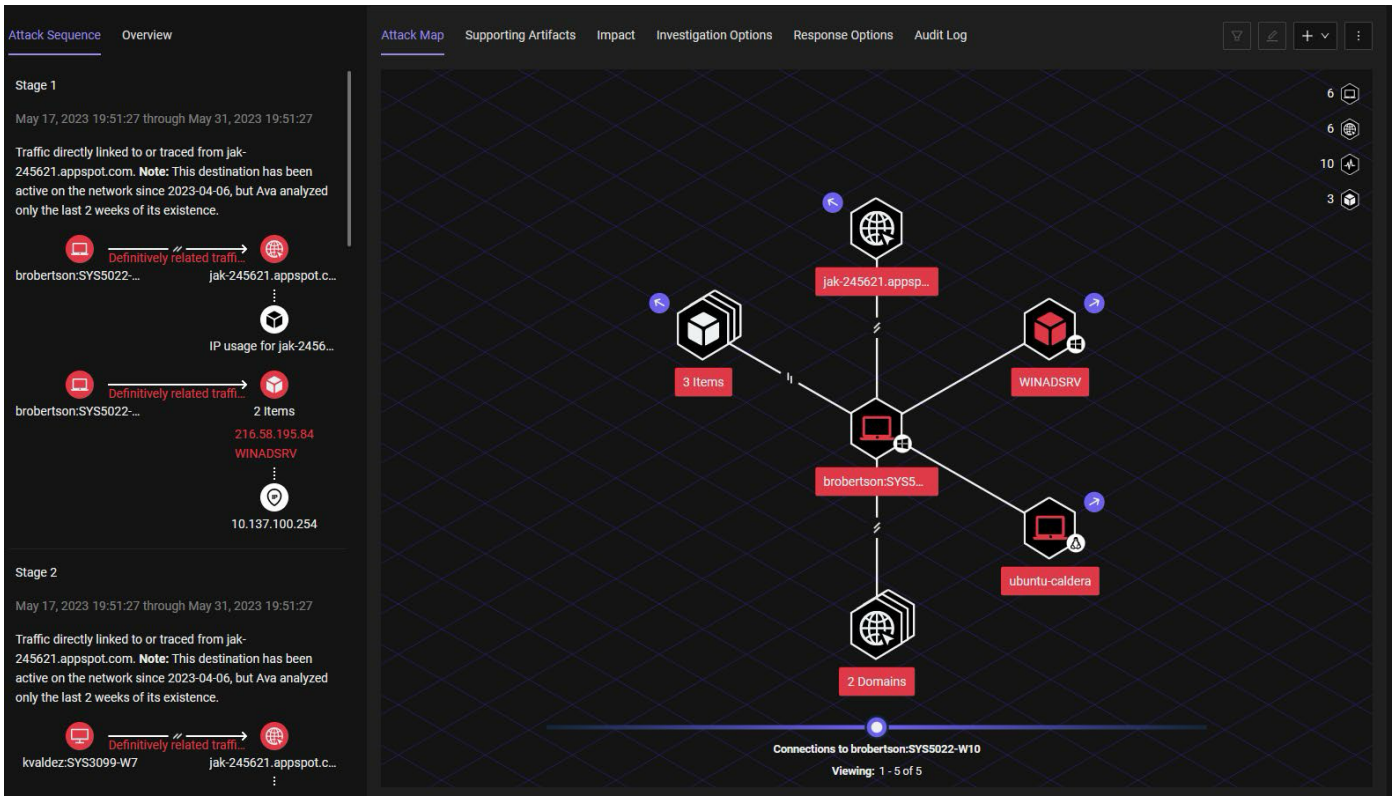
AVA（Autonomous Virtual Assist）は、Arista の AI ドリブン意思決定支援システムで、脅威検出とインシデント・トリアージを実行します。AVA は時間、エンティティ、およびプロトコルから複数の点を多次元的に結び付けることで、意味のないアラートを大量に生成するのではなく、エンドツーエンドの**状況**をエンドユーザーに提供するので、アナリストは 1 つの画面で調査と修復のオプションを使って、攻撃の全体像を把握できます。自分で全体像を苦労して組み立てる必要はありません。ここで重要なのは、連合機械学習のおかげで、Arista のお客様は、プライベートなデータを自身のイ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。

「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、Gap Inc. 前最高情報セキュリティ責任者

ユースケース

検出	対応	状況認識	脅威検出
AI を活用して内外の攻撃から意図や行動に悪意がある脅威を検出して優先度を決定し、これらの攻撃を MITRE ATT&CK フレームワークにマッピングします。	AVA はエンティティ、時間、プロトコル、および攻撃ステージからフォレンジックにインシデントを相関付け、「状況」を明らかにし、迅速な脅威対応に必要なすべての意思決定支援データを提供します。	Arista NDR は、オンプレミス、クラウド、または SaaS、あるいは管理対象と管理対象外（契約業者やその他のサードパーティ）の区別なく、IT、OT、または IoT の環境でエンティティを学習し、追跡します。	豊かなデータセットとクエリ機能で、強力な脅威検出ワークフローを提供します。AVA は人間のアナリストから 1 つのヒントを受け取り、短時間でキルチェーン全体を自律的に検出できます。



インテグレーション

Arista NDR プラットフォームは、業界最高水準の SIEM、ビジネス・インテリジェンス、チケッティングと分析、エンドポイント検出、およびセキュリティ・オーケストレーション・ツールを既存のソリューションに統合し、それらを強化します。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できます。

展開モデル

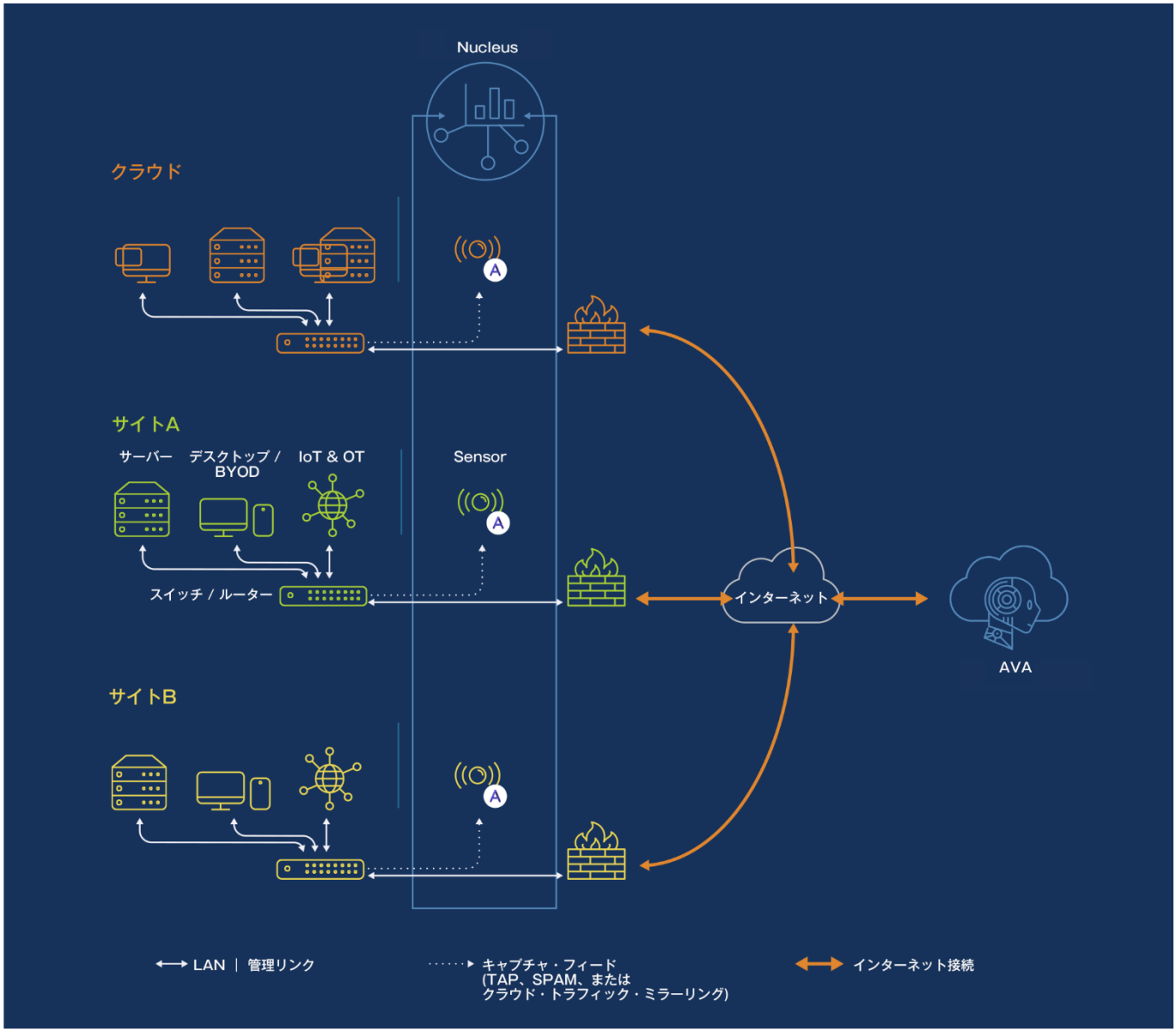
Arista NDR は、お客様の要件とネットワーク・アーキテクチャによって、以下の 2 つのモードのどちらかで展開できます。

オールインワン

AVA Sensor と AVA Nucleus を 1 つのアプライアンスに展開します。この展開方法は、Arista NDR の 1 つのインスタンスを展開するお客様や、展開したインスタンスの隔離されたビューを維持したいお客様に最適です。

分割

このモードでは、AVA Sensor と AVA Nucleus を個別に展開します。AVA Sensor は、Arista スイッチ、物理または仮想のアプライアンス、Amazon Web Services（AWS）、Google Cloud Platform（GCP）など、さまざまなフォーム・ファクターで展開できます。AVA Nucleus は、オンプレミスのハードウェアとして提供され、より高いパフォーマンスが要求される場合はクラスタ・モードで構成できます。また、Arista が提供する SaaS サービスとして利用することもできます。中央コンソールで提供される統合アナリスト・ポータルは、複数の Nucleus 展開にまたがるロールベース・アクセス制御を完備しています。



Awake Security Platform のハードウェア仕様

モデル番号	DCA-NDR-S100	DCA-NDR-S1	DCA-NDR-S5	DCA-NDR-S10	DCA-NDR-NB10	DCA-NDR-A5	DCA-NDR-CC
パフォーマンスと容量							
機能	Sensor のみ	Sensor のみ	Sensor のみ	Sensor のみ	Nucleus のみ	オールインワン	中央コンソール
ネットワーク・パフォーマンス	最大 100 Mbps	最大 1 Gbps	最大 5 Gbps	最大 10 Gbps	最大 10 Gbps[1]	最大 5 Gbps	N/A
メタデータ・ストレージ	N/A	N/A	N/A	N/A	90 日	90 日	N/A
ハードウェア仕様							
ラック・ユニット	1U	1U	2U	2U	2U	2U	2U
CPU コア	8	32	64	64	96	96	96
RAM	64 GB	512 GB	512 GB	512 GB	1 TB	1 TB	1 TB
ディスクストレージ	4x6 TB	4x10 TB	12x 6 TB	12x 18 TB	10x 8 TB	10x 8 TB	10x 8 TB
SSD	-	-	2x 480 GB	2x 480 GB	2x 480 GB	2x 480 GB	2x 480 GB
不揮発性メモリ	1x 480 GB	1x 1 TB	-	-	2x 3.2 TB PCIe NVME	2x 3.2 TB PCIe NVME	2x 3.2 TB PCIe NVME
ネットワーク	2x 1 Gbps オンボード・イーサネット 4x 10 Gbps Intel SFP+ 1x アウトバンド管理インターフェイス	2x 1 Gbps オンボード・イーサネット 4x 10 Gbps Intel SFP+ 1x アウトバンド管理インターフェイス	2x 1 Gbps オンボード・イーサネット 4x 10 Gbps Intel SFP+ポート 1x アウトバンド管理インターフェイス	2x 10 Gbps オンボード・イーサネット 4x 10 Gbps Intel SFP+ポート 1x アウトバンド管理インターフェイス	4x 1 Gbps オンボード・イーサネット 2x 10 Gbps Intel イーサネット 1x アウトバンド管理インターフェイス	4x 1 Gbps オンボード・イーサネット 4x 10 Gbps Intel SFP+ポート数 1x アウトバンド管理インターフェイス	4x 1 Gbps オンボード・イーサネット 2x 10 Gbps Intel イーサネット 1x アウトバンド管理インターフェイス
電源	2x 750W – 冗長化 / ホットスワップ対応	2x 750W – 冗長化 / ホットスワップ対応	2x 1400W – 冗長化 / ホットスワップ対応	2x 1600W – 冗長化 / ホットスワップ対応	2x 1400W – 冗長化 / ホットスワップ対応	2x 1400W – 冗長化 / ホットスワップ対応	2x 1400W – 冗長化 / ホットスワップ対応

モデル番号（スイッチ・センサー）	SS-NDR-G-SWITCH-1M	NDR SS-NDR-G-T1-1M	NDR 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	https://www.arista.com/en/support/product-documentation/supported-features を参照してください。 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。		

モデル番号（仮想センサー）	SS-NDR-SVV.5-1M	SS-NDR-SVV1-1M	SS-NDR-SVV5-1M
パフォーマンスと容量			
機能	Sensor のみ	Sensor のみ	Sensor のみ
ネットワーク・パフォーマンス	最大 500 Mbps	最大 1 Gbps	最大 5 Gbps
システム要件			
サポート対象のハイパーバイザー	VMware ESX/ESXi 6.7+	VMware ESX/ESXi 6.7+	VMware ESX/ESXi 6.7+
サポート対象の vCPU	8	12	36
最小メモリ	128 GB	128 GB	384 GB
最小ディスク・ドライブ	500 GB	500 GB	500 GB
ネットワーク接続	2 x 1 Gbps イーサネット（1 つの管理インターフェイスを含む）	2 x 1 Gbps イーサネット（1 つの管理インターフェイスを含む）	1x 1 Gbps 管理用イーサネット、最大 4 枚の Intel DPDK 対応 NIC

PCAP ストレージ・ディスク・ドライブ	500 GB 追加	500 GB 追加	10 TB 追加 [2]

モデル番号	SS-NDR-SCA1-1M	SS-NDR-SCA5-1M	SS-NDR-SCG1-1M
パフォーマンスと容量			
クラウド	Amazon Web Services	Amazon Web Services	Google Cloud Platform
機能	Sensor のみ	Sensor のみ	Sensor のみ
ネットワーク・パフォーマンス	最大 1 Gbps	最大 5 Gbps	最大 1 Gbps
システム要件			
サポート対象の最小インスタンス・サイズ	r5.4xlarge - 16 vCPU	r5.16xlarge - 64 vCPU	n1-highmem-16 - 16 vCPU
最小ディスク・ドライブ	160 GB	500 GB	160 GB
最小メモリ	128 GB	512 GB	104 GB

モデル番号(SaaS AVA Nucleus)	SS-NDR-NCA2-1M	SS-NDR-NCA5-1M	SS-NDR-NCA10-1M
パフォーマンスと容量			
クラウド	Amazon Web Services(お客様の希望のリージョン)の Arista VPC	Amazon Web Services(お客様の希望のリージョン)の Arista VPC	Amazon Web Services(お客様の希望のリージョン)の Arista VPC
機能	Nucleus のみ	Nucleus のみ	Nucleus のみ
ネットワーク・パフォーマンス	最大 2 Gbps の平均総センサー・スループット	最大 5 Gbps の平均総センサー・スループット	最大 10 Gbps の平均総センサー・スループット
メタデータ・ストレージ [3]	30 日	30 日	30 日

[1] より高スループットとメタデータ保持を提供するためのクラスタ・モードをサポート

[2] ストレージの容量は展開時に決まり、基盤となる VMware ホスト・サーバーの構成と機能によって変わります。

[3] アドオンで追加日数のメタデータ・ストレージを利用できます。

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 2 月 13 日