# Arista NDR と Extrahop Reveal(x)の比較

この比較では、ネットワーク・パフォーマンス監視をセキュリティ利用に適応させたツールと、真の高度なネットワーク脅威検知・対応ソリューションの違いを明らかにします。

ExtraHop と Arista NDR のソリューションの比較では、既存のネットワーク・パフォーマンス監視および診断機能をセキュリティ利用に適応させたツールと、セキュリティに焦点を合わせた高度なネットワーク脅威検知・対応機能の提供を目的として構築されたツールの違いを明らかにします。

## はじめに

世界中の組織が攻撃者によるネットワーク侵入を防ぐことを目的としたソリューションやテクノロジーに投資してきた金額を合計すると、数十億ドルに及びます。それにもかかわらず、執拗な攻撃者は今なお境界の防御をくぐり抜けて、攻撃対象のネットワークにアクセスできています。そのような足がかりがひとたび確立されると、何か月も攻撃者に気付かない可能性があり、データ・アセットの盗難や破損のリスクが高まります。

既知のマルウェアのシグネチャや静的な侵害インジケーター（IoC）に焦点を合わせた従来のポイントインタイム予防ソリューションも引き続き必要ですが、広範囲にネットワーク・セキュリティをカバーするには不十分です。現在では、従来型のセキュリティ・ソリューションを補完するため、疑わしいアクティビティをリアルタイムで検出し、対応するソリューションが不可欠になっています。この市場の最前線に立っているのが、ネットワーク脅威検知・対応（NDR）と呼ばれる新しいテクノロジーです。

アナリスト会社 Gartner は、2019 年 2 月の『Market Guide for Network Detection and Response』で、このテクノロジーについて「エンタープライズ・ネットワーク上の疑わしいアクティビティを検出するため、機械学習、高度な分析、ルールベースの脅威検知を組み合わせて利用するものです。NDR ツールは、生のトラフィックやフロー・レコード（NetFlow など）を継続的に分析し、正常なネットワーク動作を反映したモデルを作成します。異常なトラフィック・パターンを検出すると、NDR ツールはアラートを発行します。NDR ソリューションは、エンタープライズ境界をまたがる垂直型トラフィックの監視に加え、戦略的に配置されているネットワーク・センサーから受信したネットワーク・トラフィックやフロー・レコードを分析して、水平型の通信も監視することができます」と説明しています。[1]

## 適切なソフトウェア・プラットフォームを選択する

Gartner の市場ガイドでは、Arista NDR プラットフォームと ExtraHop の Reveal(x)の 2 つのネットワーク脅威検知・対応ソリューションを取り上げています。市場をリードするポジションと強力な製品群から、NDR プラットフォームを選定している多くの企業の選択肢はこの 2 社に絞られています。

組織に最適な NDR プラットフォームを選択することは、組織が不審な活動を検知し、迅速に対応する能力を与え、より強固なセキュリティ体制を構築することができます。ExtraHop と Arista NDR のソリューションの比較では、既存のネットワーク・パフォーマンス監視および診断機能をセキュリティ利用に適応させたツールと、セキュリティに焦点を合わせた高度なネットワーク脅威検知・対応機能の提供を目的として構築されたツールの違いを明らかにします。このドキュメントでは、処理対象のデータ、そのデータに適用される機械学習やその他のデータ・サイエンス技術、それによって実現されるユースケース、展開と拡張性に関する運用上の考慮事項、この 2 社を支えるセキュリティ専門知識など、企業のお客様にとって最も重要な基準に沿って、両社のプラットフォームを比較します。

## データ

アクティビティ・データはあらゆる NDR プラットフォームにとって血液のようなもので、送信元、送信先、送信者、送信元デバイスなど、ネットワーク上のトラフィックに関する情報を伝えます。現在および過去の（保存されている）データを含め、利用・分析できるデータが詳細であればあるほど、セキュリティが向上します。IP アドレスだけでなく、デバイス、ユーザー、アプリケーション、組織が含まれている方が、コンテキストを踏まえて包括的に理解できるからです。

### データ・ソースの豊富さ

| ARISTA NDR | | EXTRAHOP |
|---|---|---|
| L2〜L7 のネットワーク・データ |  | ワイヤ・データ<br>（独自形式のメタデータ） |

この基準では、プラットフォームが分析するデータの深度を調べます。ExtraHop は全パケットを処理し、保存しますが、脅威検知・分析の実行対象は「ワイヤ・データ」（独自形式のメタデータ）です。一方、Arista NDR は、抽出されたアクティビティ・データと全パケットの情報の両方に対して分析と機械学習を実行します。この手法は、幅広い脅威、特に正当な業務活動に紛れ込んでいる「環境寄生型」の脅威を発見するのに役立ちます。

### ネットワークの可視化

| | | |
|---|---|---|
| デバイス、ユーザー、アプリケーション、<br>外部ネットワーク、組織、ドメイン |  | 限定的<br>ネットワーク・パラメーター |

可視性は、データ・ソースとの相対的な関係で定義され、もしプラットフォームがメタデータしか見ていないのであれば、それは実際にはネットワーク・プロトコル情報（ポート、IP アドレスなど）しか得ていないことになります。Arista NDR プラットフォームはネットワーク全体を調べて、デバイス、ユーザー、アプリケーション、ドメインなどの関係を解決することができます。これにより、エンティティのコンテキストを提供して、垂直型通信と水平型通信の両方で脅威を発見できます。

ExtraHop は、セキュリティ機能を提供しようとするネットワーク・パフォーマンス管理ツールです。このアプローチがもたらす課題の典型的な一例は、得られるエンティティのコンテキストがセキュリティ業務にあまり関連がないということです。さらに、ExtraHop による脅威検知は、ネットワーク・プロトコル・パラメーターにのみ基づく異常の発見に限定されています。Arista NDR は、トラフィックで通信を行うエンティティ、つまり、デバイスやユーザー、外部ネットワーク、組織、ドメインを把握しているので、垂直型通信と水平型通信の両方で脅威を発見できます。ExtraHop と違い、Arista NDR は発見した脅威をまとめて、エンドツーエンドのキャンペーンや、その他の被害を受ける可能性がある対象を識別することもできます。

### 組織のデータ・プライバシー

| | | |
|---|---|---|
| 顧客の環境内にデータを保持。<br>必要に応じて分析機能を<br>プライベート・クラウドに展開可能 |  | 顧客のワイヤ・データを<br>Amazon Web Services（AWS）上の<br>ExtraHop クラウドにアップロード |

多くの場合、組織にはネットワーク・データが組織内の環境から出ないようにするためのデータ・プライバシー・ポリシーやコンプライアンス要件があります。ExtraHop は、Amazon Web Services にホスティングしている独自クラウドに顧客のワイヤ・データをアップロードします。Arista NDR は、すべての顧客データを顧客の環境内に保持し、組織のインフラ外部にアップロードすることはありません。これは、プライベート・クラウド環境や、政府や軍が導入しているエアギャップ環境に分析機能を展開できるのは Arista NDR だけということでもあります。

## データ・サイエンス

もちろん、データの収集は第一歩にすぎません。ネットワーク全体から収集したデータからインサイトや情報を獲得できるようにするのがデータ・サイエンスです。Arista NDR プラットフォームは、さまざまな科学的手法、プロセス、アルゴリズム、システムを利用して、構造化データおよび非構造化データからインサイトを抽出します。Arista NDR では、高度な AI と機械学習による分析が完全に統合されています。ExtraHop は、従来の機械学習ツールをきわめて限定的に提供しています。これは主として教師なし学習で、誤検知が生じたり、説明性に欠ける傾向があります。

### エンティティ相関付けの自動化

| ✓あり | | 限定的 |
|---|---|---|
| プラグアンドプレイ方式、AI ベースの動作に基づくフィンガープリントで、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トラッキング |  | SMB や DNS などのプロトコルの監視によって名前を自動生成、またはユーザーが手動でデバイスに名前を付ける。分析機能は主として IP ベースと考えられる |

この機能は、IP アドレス・レベルではなく、エンティティ・レベルで動作を調べて、さらに詳細にネットワークを可視化するものです。Arista NDR は、アプリケーションを使用しているエンティティやデバイスを自動的に判断し、そのエンティティの移動をトラッキングします。たとえば、あるデバイスが今日はニューヨークのオフィスにあり、明日はダラスのオフィスにある場合、Arista NDR はそのデバイスをトラッキングして、すべてのアクティビティをそのエンティティに関連付けます。ExtraHop の分析機能は、主として IP アドレスベースと考えられます。ExtraHop と Arista NDR はどちらもデバイスのアプリケーションや機能を把握していますが、送信元、送信先、トラフィックについて把握している情報を利用して、脅威となる動作や悪意の検出を実行できるのは Arista NDR だけです。

### 抽出する検出特徴

| ～1200 | | ～4700 |
|---|---|---|
| セキュリティ固有の特徴 |  | ネットワーク・パフォーマンス指標 |

ExtraHop は、ネットワーク・パフォーマンス監視ソリューションから NDR ソリューションに進化したため、セキュリティにほとんど影響を与えない多くの機能を使用しています。誤検知と検知漏れを減少させて最新の脅威を検知することが目標の場合、これは大きな制約になります。一方、Arista NDR は、ポートやプロトコルの情報だけでなく、ネットワーク通信全体への影響に基づいて、セキュリティ固有の特徴を多数抽出します。これにより、誤検知を減少させ、高精度の脅威検知が可能になります。

### セキュリティ・ナレッジ・グラフ

| ✓あり | | ✗なし |
|---|---|---|
| |  | |

ナレッジ・グラフはエンティティの相関付けを拡張したもので、エンティティの位置やエンティティ間の関係、共有している属性、他のエンティティと類似しているエンティティを識別します。たとえば、グラフ内のすべてのデジタル電話をグループ化したり、フランスにあるすべてのデバイスをグループ化したりできます。本質的に、ナレッジ・グラフは Arista NDR が作成し特許を取得した基盤となるデータ・ストアで、ピア・グループと異なる可能性があるエンティティの動作を把握するのに役立ちます。対照的に、いくつかの限定的な手動グループ化機能や、ネットワーク・トランザクションの自動ピア識別機能を除き、ExtraHop は主として各 IP アドレスを単独で扱います。

### 動作分析

| ありArista NDR | 限定的ExtraHop |
|---|---|
| トラフィック分析に加えて送信元と送信先のエンティティを分析 | 異常検出 |

ExtraHop の検知はトラフィックの異常検知に基づいているため、IP アドレスのようなネットワーク情報が一時的で信頼性が低いという固有の課題を抱えています。Arista NDR は、ネットワーク上の全エンティティに対して動作に基づくフィンガープリントを行い、類似分析を実行し、これらすべての情報を利用して脅威を検知します。

### 機械学習

| ありArista NDR | 限定的ExtraHop |
|---|---|
| 教師あり、教師なし、および連合機械学習の組み合わせ | 教師なし機械学習のみを利用したクラウドベース・サービス |

動作についてコンピューター・システムに教える方法は多岐にわたります。ExtraHop は主に教師なし学習を使用して、デバイスの正常な動作を突き止めます。「正常な動作」は新しいソフトウェアの展開などのきわめて正当なビジネス上の理由でしばしば変わるため、このアプローチにはノイズが多いという課題があります。さらに、ベースラインを規定する前にデバイスが既に侵害を受けていると、このアプローチは機能しません。Arista NDR の組み合わされた学習アプローチでは、過去の動作と比較するだけでなく、類似エンティティや、組織の他の部分全体とも比較します。そのため、ExtraHop のようなソリューションではよく見られる誤検知と検知漏れのどちらも排除できます。

### 説明性

| ありArista NDR | 限定的ExtraHop |
|---|---|
| 完全な透明性 | |

説明性は、何かを悪意があると認識した理由について十分なコンテキストを提供する仕組みに関連しています。ExtraHop が提供する検出モデルにはコンテキストと説明性がきわめて乏しく、なぜ検出されたのか、何をすべきなのかを判断しなければならないという課題がセキュリティ・アナリストに突き付けられます。また、セキュリティ・アナリストは、この製品を使用して検出モデルを微調整することもできません。異常検出/教師なし学習アプローチでは、異常は悪意あるものとして扱われるためです。Arista NDR では、すべての顧客が独自の検出モデルを作成することも、Arista NDR 独自のモデルを調査して修正することもできます。

### 立ち上げまでの時間

| 数時間Arista NDR | 4 週間以上のトレーニング期間ExtraHop |
|---|---|

ExtraHop と違い、Arista NDR は時間的なベースライン設定を行う代わりに、関わっているエンティティ、類似エンティティの動作、エンタープライズ環境全体で一般的な動作についての理解に基づく動作分析を実行します。このアプローチでは、新しいソフトウェアが展開されたり、その他の組織改変が発生した場合など、正当な動作が変わった際、煩わしいシステムの再トレーニングを常に行う必要もありません（ExtraHop では必要です）。

## ユースケース

組織はネットワーク脅威検知・対応プラットフォームをどのように活用できるでしょうか。ソリューションでサポートできるユースケースが増え、セキュリティ業務に特化したユースケースになればなるほど、価値が高まり、ROI をより短期間で実現できるようになります。

### ユーザー・エクスペリエンスとワークフロー

| セキュリティに特化 | | セキュリティに特化していない |
|---|---|---|

ExtraHop は、ネットワーク・パフォーマンス監視ツールをセキュリティ・ソリューションとして再利用しようとしています。ExtraHop Reveal(x) 製品がサポートするユーザー・エクスペリエンスとワークフローは、このことに起因する課題をはっきりと示しています。ネットワーク指標を重視し、セキュリティ・パラメーターを軽視する傾向があるのです。Arista NDR は、セキュリティ・ワークフローを重視するように構築されたもので、200 以上のセキュリティ・チームから情報を得ているというメリットがあります。

### 既知の攻撃者 TTP（Tactics, Techniques, and Procedures）の検出

| ✓あり<br>正当な業務活動に紛れ込んでいる<br>非マルウェアやその他の脅威を検知 | | ✗なし |
|---|---|---|

これまで、大部分の脅威検知は侵害インジケーター（IoC）を利用して行われてきました。最近では攻撃者が賢くなり、このインジケーターを絶えず変更するので、攻撃者の TTP を探すことが脅威を検知する効果的な方法となっています。ExtraHop は、主に異常検出と「通常と異なる変化」に焦点を合わせているので、「正常」または正当な権限を悪用する非マルウェア脅威の検知に苦戦しています。また、ExtraHop は、セキュリティ・チームが既知の攻撃者 TTP に対してカスタム検出モデルを作成する仕組みを提供していません。必ずしもすべての異常に悪意があるわけではなく、すべての悪意あるアクティビティが異常とは限らないので、この手法は効果を低下させます。Arista NDR の充実したクエリ言語は、非常に複雑な攻撃者 TTP でも体系化できるボキャブラリーを提供し、システムが自動的かつ継続的に攻撃者 TTP を探せるようにします。この検出モデルは Arista NDR が提供しますが、顧客が作成したり、カスタマイズしたりすることも可能です。

### 回顧的検出

| ✓あり | | 限定的<br>IP アドレスなどのネットワーク IoC |
|---|---|---|

新たな攻撃者 TTP が出現するたび、組織はその TTP が過去に自社環境内で観測されたことがあるかどうかを知りたいと考えます。ExtraHop は既知の IoC の遡及的検出を提供していますが、攻撃者 TTP に対して実行することはできません。Arista NDR は必要に応じて時間をさかのぼり、関連する動作を自動的に突き止めることができます。

### 暗号化トラフィックの可視化

| ✓あり<br>特許取得済みのアプローチ | | 限定的<br>すべてのサーバーやクライアント上でエージェントを使用して SSL/TLS トラフィックを復号化 |
|---|---|---|

暗号化されるネットワーク・トラフィックはますます多くなり、ポリシーやプライバシー上の理由から、復号化を避けようとする顧客が増えています。さらに、攻撃者の側でも、ネットワーク脅威検知を回避する手段として暗号化トラフィックを使用することが増えています。Arista NDR の革新的アプローチは、顧客と関係者のプライバシーを常に守り、アプリケーション（ブラウザ、Microsoft Office アプリ、PowerShell など）

やトラフィックの性質（インタラクティブ・シェル、Web ブラウジング、ビデオ会議、テレフォニーなど）を識別するために暗号化データ分析を利用する一方で、エージェントの展開を不要にします（ExtraHop ではプライバシーを守るためにエージェントの展開が必要です）。

### キャンペーン分析の自動化

| ✓あり | | 限定的 |
|---|---|---|
| 自動インシデント・トリアージでエンティティ、キルチェーン・アクティビティ、時間を相関付け |  | |

現在、ほとんどの攻撃には複数のデバイスと多数のアクションが関わっています。最終目的を達成するため、攻撃者は通常、エンドポイントからサーバーなど、ネットワーク内を移動します。多くのセキュリティ・ソリューションでは、セキュリティ・アナリスト自身が手動でこのような点と点を結ぶ必要があります。Arista NDR ではエンティティ中心の時系列状態を参照できるので、「状況」機能で時間やプロトコルから点と点を統合し、相関付け、結ぶことができます。この機能により、アラート疲れが減り、セキュリティ・チームが情報をアクションに活かせるようになります。対照的に、ExtraHop は検出したものをキルチェーンの段階別に分類しますが、それをまだ個別のアラートとして扱っているので、手動でトリアージを行い、点と点を結び付け、より大きな攻撃キャンペーンにまとめることはセキュリティ・アナリスト任せになっています。

### クエリ言語と脅威検出

| ✓あり | | 限定的 |
|---|---|---|
| インシデント、セキュリティ・ナレッジ・グラフ、アクティビティ、生のパケット・データについて問い合わせることができる拡張可能なプログラミング言語 |  | ネットワーク・パケット・フィルタのドロップダウン・リスト |

ExtraHop が既存のネットワーク・パフォーマンス監視機能を活用していることは、Tx と Rx の統計、ネットワーク・タイプ、ポート、プロトコルなど従来のネットワーキング・パラメーターに焦点を合わせた検索機能から明らかです。このような生のプリミティブ型データ単独では、脅威検出などのセキュリティ・ユースケースに使い勝手が良くありません。単一の検索で時間やプロトコルから動作の複雑な組み合わせを識別し、それによってエンドツーエンドの攻撃者 TTP を識別できる強力なプログラミング言語という強みを持っているのは、Arista NDR だけです。すべてのクエリと脅威検出は、保存して今後の自動検出に利用することができます。

### 完全なデジタル・フォレンジック

| ✓あり | | ✓あり |
|---|---|---|
| 継続的パケット・キャプチャ |  | 継続的パケット・キャプチャ |

ExtraHop と Arista NDR のどちらも、継続的パケット・キャプチャを提供しています。ただし、パケット・キャプチャおよびストレージは ExtraHop では独立した機能で、この製品の脅威検知機能やセキュリティ機能と結び付いていないので、アナリストのワークフローは分割されます。さらに、ExtraHop は得られた「ワイヤ・データ」を Amazon Web Services（AWS）にアップロードしますが、Arista NDR はキャプチャしたすべてのデータを顧客のインフラ内に保持します。

## 展開と拡張性

ネットワーク脅威検知・対応プラットフォームは、ネットワークのあらゆる部分に到達して不可欠な情報を収集する必要があります。また、今日の多くのセキュリティ製品と同様に、単独で動作すべきではありません。

### 展開に関する考慮事項

| ✓あり | | 限定的 |
|---|---|---|
| 生み出されたアーティファクトを利用して、必要なセンサーの数を最小限に抑える |  | 広範囲にカバーするために複数のネットワーク・センサーと構成が必要 |

Arista NDR は、生み出されたアーティファクトを処理する能力に優れています。この重要なイノベーションは、多くの通信によって副次的に生み出されるネットワーク・アーティファクトを利用します。その結果、Arista NDR は必要なネットワーク・センサーの数を最小限に抑えることができます。たとえば、データ・センターから発行された Kerberos チケットを観測し、詳細に解析すると、その通信を直接監視することなく、リモート・ネットワークのデバイス間のラテラル・ムーブメントのエビデンスを提供できます。

さらに、Arista 固有の機能として、既存の Arista ネットワーク・スイッチを使用してデータの監視やプリプロセシングを行い、Arista NDR Nucleus に転送して分析することができます。これらの重要なイノベーションにより、ExtraHop と比べて、必要な専用ネットワーク・センサーやネットワーク・タップなどの数が大幅に減少します。

### サポートされている展開

| センサー<br>物理、仮想、クラウド<br>分析<br>物理、クラウド |  | センサー<br>物理、仮想、クラウド<br>分析<br>クラウド |
|---|---|---|

Arista NDR と ExtraHop がサポートする展開フォーム・ファクタは似ていますが、大きな違いが 1 つあります。オンプレミス環境またはプライベート・クラウド環境に分析機能を展開できるのは、Arista NDR だけです。このため、規制が厳しいユースケースや、政府機関および防衛機関など、さまざまな顧客ユースケースに対応できます。

## 企業のバックグラウンド

### 専門知識とセキュリティの DNA

| ✓高度 | | 限定的 |
|---|---|---|
| |  | |

特定分野の詳細な知識や専門知識に代わるものはありません。ExtraHop チームのセキュリティ分野に関する専門知識は、きわめて限定的です。チームの大部分は、ネットワーク・パフォーマンス管理を専門にしています。Arista NDR のプラットフォームは、Symantec や McAfee から FireEye や Cylance まで幅広い企業のセキュリティ分野に熟練した専門家が構築したものです。また、Arista NDR の社員の 50%以上が修士号または博士号を持っています。

## まとめ

今日、市場には非常に多くの NDR プラットフォームがありますが、Arista NDR は Enterprise Management Associates（EMA）の最新のネットワーク・セキュリティ分析レポートで「バリュー・リーダー」に選出されています。ExtraHop や他のソリューション・ベンダーと比較して、Arista NDR は機能とコストのバランスが最も優れていると評価されました。何よりも重要な点は、EMA のベンダー分析には、Arista NDR のセキュリティ・プラットフォームに高い価値を見出している実際の顧客からのインタビューやインサイトが含まれていることです。

Arista NDR プラットフォームが提供するネットワーク脅威検知・対応機能で、組織は従来のセキュリティ・ソリューションでは見逃していた脅威を検知・検出することができます。ExtraHop Reveal(x)を含む、多くの他のネットワーク脅威検知・対応プラットフォームと異なり、Arista NDR は顧客データを顧客インフラ外にアップロードすることなく脅威を検知できる点も重要です。Arista NDR のアプローチは誤検知と検知漏れを最小化するので、効果的なリスク管理を実現しつつ、既にパンク寸前のセキュリティ・チームの作業負荷を減少させることができます。

## 出典

1. Gartner, Inc.、『Market Guide for Network Detection and Response』（2019 年 2 月）

**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



2023 年 9 月 6 日