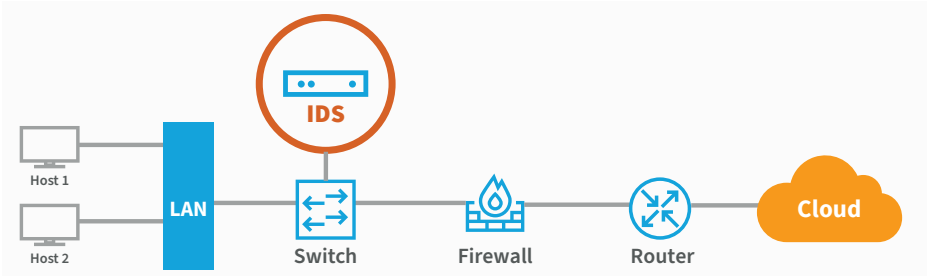
VECTRA
SECURITY THAT THINKS.®

競合分析概要

# 次世代IPSは従来の問題を解決するのか？

**Cisco Firepower（旧Sourcefire）、Trend Micro Deep Discovery、McAfee Network Threat Behavior Analysisなどの侵入検知システム（IDS: Intrusion Detection System）は、全てシグネチャーベースの検知や保護機能を前提とした、従来型のテクノロジーと位置付けることができます。**

**これらのソリューションは、Vectra®が提供するネットワークの検知および対応プラットフォームに対する真の競合製品にはなり得ませんが、最近では、Vectra製品と同等の位置付けで、自社製品のマーケティング活動を開始しています。Vectraはこれら従来のIPSテクノロジーに比べて、以下の差別化要素を持っています。**




## 振る舞い検知機能の欠如

シグネチャーベースの検知機能と単純なヒューリスティックでは、限定された既知の攻撃パターンしか検知することができません。現在のほとんどの攻撃は、仮にそれが場当たり的なものでも、攻撃者の目的達成に向け最大の効果が得られるよう、少なくとも最小限の修正が加えられています。これはVectraの「Spotlight Report on Ransomware（ランサムウェアに関するスポットライトレポート）」でも指摘した通りです。

手当たり次第にばらまき、あとは運任せといった攻撃は、もう過去のものとなっています。攻撃者は、攻撃の成功確率を高めるため、既に標的型攻撃に切り替えています。IDSに依存してネットワークを保護するという形態は、例えば、2000年代当初からKasperskyの無償版のアンチウィルスを使っているユーザーが、2020年になって感染したことに驚いているようなものです。

**97%**

**Vectraプラットフォームは、MITREのATT&CKフレームワークの97%以上をサポートしています。**

## レガシーなセキュリティモデルに対応する設計

多くの企業がゼロトラストモデルに移行するに従い、外部とオンプレミスの境界線を防御することに終始した時代遅れのシステムは、撤廃されていく運命にあります。これにより、IDSを使って確認できる対象は、ファイアウォールを通過するトラフィックのみに限定されることになります。

このため、一旦攻撃者が内部ネットワークへ侵入してしまえば、その後はIDSがどんなに高機能であっても、ラテラルムーブメント（横方向への自由な移動）が可能となります。IDSが示す唯一の顕著な違いは、ファイアウォールを通過するパケットに対してヒューリスティック機能を実行することにより、ファイアウォールのパフォーマンスに著しい低下が見られるという点です。

さらに現代の企業は、クラウド環境でオンプレミスのネットワークと同等の量のトラフィックを発生させています。IDSはネットワークに入ってくるトラフィックに焦点を当てているため、侵害されたクラウドサービスのアカウントを使って侵入する攻撃者については、まったく把握できません。

Vectraプラットフォームは、マルチクラウド環境を含め、ネットワーク上の全ての箇所に導入できるため、セキュリティアナリストはその所在に関わりなく、企業のアセット全体を完全に把握することができます。

さらにVectraプラットフォームでは、特権アクセス分析（PAA: Privileged Access Analytics）によって、ゼロトラストへの取り組みを強化することができます。PAAによって、ネットワーク上でのアカウントの使用方法を推測し、侵害を受けた認証情報を使ってさらに攻撃をしかけようとする、内部の不正行為者を検知することができます。

## 膨大なアノマリーアラートに備える

アノマリーベースの検知システムであるIDSでは、最もリスクの高い攻撃を特定することができないだけではなく、大量に発生するアラートによって、セキュリティチームを疲弊させる結果となります。

このようなアラートについては、手作業で個別にトリアージを行う必要があるため、セキュリティオペレーションの負荷が増加します。このため、既にオーバーワークになっているセキュリティチームに、さらなる無用な負担をかけることになります。

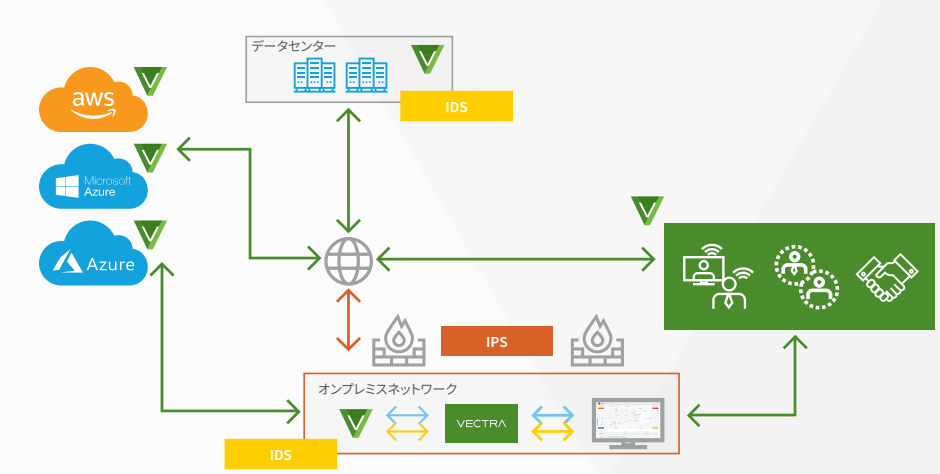
その一方で、Vectraのアルゴリズムは、攻撃者の視点で一連の流れを捉えるため、単純なシグネチャーやヒューリスティックによる検知よりも、遙かに優れた検知精度となっています。実際にVectraプラットフォームは、MITREのATT&CKフレームワークの97%以上をサポートしています。このような包括的な検知機能は、お客様が実施するPOCの過程ですぐに明らかになります。

さらにVectraの場合には、セキュリティオペレーションにおける負荷を1/38へと削減することができます。Vectraでは、アラートを自動的にトリアージしてインシデントに落とし込み、高いリスクを持つホストデバイスに対して優先順位付けを行います。さらにネットワークトラフィックからセキュリティ強化メタデータを抽出し、調査やフォレンジックのために提供します。

## ベストな結果が得られないベンダーロックイン

IDSは、通常、広範なプラットフォームの一部として位置付けられており、単独では不完全なものとなります。そして、ファイアウォールやURLフィルタリング、アプリケーションの可視化ツール、高度な攻撃検知機能など、さらに多くの投資が必要になります。また、一貫したエクスペリエンスを得るためには、全ての製品を同一ベンダーから購入する必要があります。

一方、Vectraプラットフォームの場合には、API経由で企業のセキュリティスタックと容易に連携することができます。Vectraのテクノロジーパートナーのエコシステムは、エンドポイントセキュリティ(EDR)、次世代ファイアウォール、SIEM、セキュリティオーケストレーション(SOAR)、ネットワークアクセスコントロール(NAC)など、いずれも各分野のリーディング企業によって形成されています。Vectraの連携機能によって、最高クラスのセキュリティ戦略に対応し、既存の投資を保護しながら継続的に付加価値を提供していくことができます。




## 次世代IDSとVectraプラットフォーム

Vectraプラットフォームは、次世代型のIDSと比較して様々な優位性を持っています:

- 教師あり、および教師なしの機械学習アルゴリズムをベースに、**現実世界の攻撃を検知**します。
- ファイアウォールから流入するデータだけでなく、企業のネットワークからクラウドに至るまで全てを**完全に可視化**することができます。
- **セキュリティオペレーションのワークロード**を最大で1/38へ**削減**することができます。Vectraでは、検知した攻撃者をトリアージして、インシデントを優先順位付けすることで、迅速な原因特定が可能となります。
- お客様所有のセキュリティソリューションと連携しながら、**プラットフォームの能力を最大限に発揮**できます。

お問い合わせ:info-japan@vectra.ai　vectra.ai/jp