ホワイトペーパー

EDRだけでは不十分な5つの理由

EDRにNDRがなぜ必要なのか

VECTRA®

EDR (エンドポイント検知とレスポンス) は、企業のサイバーセキュリティにおいて不可欠です

しかし、回避技術の高度化、管理対象外のデバイスの悪用、アイデンティティ (ID) の不正利用など、攻撃者の手法が急速に進化していることで、ホスト中心のセキュリティ対策には限界があることが明らかになってきています。本ホワイトペーパーでは、インシデント対応調査、レッドチーム演習、業界統計、顧客事例に基づき、この限界について詳細に検証します。現代のハイブリッド環境を保護するにあたり、EDRだけでは不十分である理由、そして現代のSOCがNDR (ネットワーク検知とレスポンス) を活用してネットワークレイヤーとアイデンティティレイヤーにわたる可視性を広げなければならない理由を明らかにします。

EDRだけでは不十分な理由とすべてのEDRにNDRが必要な5つの理由

1. EDRエージェントは導入できない場所がある
2. EDRは回避され、迂回され、無効化されてしまう
3. EDRの可視性はネットワークやID経路の攻撃を見逃す
4. NDRはアラートによるストレス、検知漏れ、誤検知を軽減する
5. NDRはSOCの可視性、効率性、有効性を実現する

理由1：

EDRエージェントは導入できない場所がある

エンドポイント保護プラットフォーム (EPP) およびエンドポイント検知とレスポンス (EDR) はエージェントが必要なため、エージェントがインストールされていないデバイスに関しては把握できません。

現代のネットワーク環境では、エージェントが導入できないデバイスが多くあります。例としては、IoTデバイス (スマートプリンター、HVACセンサー、医療機器) 、管理対象外の個人用ノートパソコンやスマートフォン、ネットワーク機器、ルーター、さらにはクラウドワークロードなどが挙げられます。攻撃者はこれを認識しており、導入していないデバイスを意図的に標的にします。感染した管理対象外のデバイスがネットワークスキャンを開始したり、侵害された請負業者のノートパソコンが外部へビーコン信号を送信し始めても、エンドポイントソリューションはそれを検知できない可能性が高いのです。

1 2024年11月に発表されたCISAアラートコードAA24-326A「Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a US Critical Infrastructure Sector Organization (サイバーレジリエンスの強化：米国重要インフラセクター組織に対するCISAレッドチーム評価からの知見)」では、以下の事実が明らかになりました。

> **評価対象組織は、悪意のある活動を防止・検知するための技術的制御が不十分であった。組織はホストベースのEDRソリューションへの依存度が高すぎ、十分なネットワークレイヤー保護を実施していなかった。**

2 Vectra AIのネットワークデータテレメトリによれば、最大

50%

のデバイスにはEDRエージェントがインストールされていない、

あるいはエージェントのインストールが不可能なデバイスが含まれていることが判明しました。

3 2023年から2024年にかけて、IoT/OTデバイスに対するマルウェア攻撃は

↑45%から66%

へ増加。もしくは、攻撃はネットワークルーターを標的にしていました。

Zscaler ThreatLabz 2024 Mobile, IoT and OT Threat Report

4 IoT/OTデバイスの

50%以上

が、既知の脆弱性を持つレガシーなサポートやサポート終了の近いOS、高リスクなレガシープロトコルやサービスに依存しています。

それは、内部の東西ネットワーク接続の

20%以上

を占めています。

Zscaler ThreatLabz 2024 Mobile, IoT and OT Threat Report

5 **NDR**

などのエージェントレス監視がない場合、管理対象外のエンドポイントや新しい形式のデバイスは、攻撃者の移動経路となる監視対象外の経路を形成します。

事例：近鉄百貨店

近鉄百貨店では、ネットワーク内のPOSシステムや業務専用の端末、ハンディターミナルなど、EDRサポートが難しいデバイスを抱えていました。エージェントレス監視のためVectra AIのNDRを導入し、約1か月で実際に疑わしいホストを検知し未然に対応することができました。

エージェントを導入している場合でも、攻撃者はそれを完全に回避する方法を見つけ出しています。次のページで詳しくご紹介します。

理由2：

EDRは回避され、迂回され、無効化されてしまう

エンドポイント防御は攻撃者を遮断することを前提としていますが、意図的に無効化される可能性があります。それによって、ネットワークおよびIDテレメトリによる帯域外検知が不可欠となります。

チーム演習では、バイナリパディングや既知の悪質シグネチャ回避によりEDRが迂回される事例が確認されました。その結果、IDを標的とした攻撃はまったく検知されませんでした。

複数の検証済みEDR回避手法が実際のインシデントで確認されており、これらはアンダーグラウンドのフォーラムで共有されたり、サブスクリプション型ツールとして販売されたりしています。具体的には以下が含まれますが、これに限定されるわけではありません。

Retrosigned Driver Bypass

ランサムウェアを活用した攻撃者は、システム時刻を改ざんして期限切れの証明書で署名された悪意のあるカーネルドライバをロードし、EDRプロセスを停止させます。

Mounted Guest EDR Bypass

攻撃者はハイパーバイザーからVMディスクイメージをマウントし、オフライン状態でEDRファイルを削除した後、保護されていない状態でゲストを再起動します。

Bring Your Own Installer

攻撃者は、改ざん防止制御を回避し、エンドポイントを無防備な状態に保つためにEDRエージェントのアップグレードプロセスを中断します。

EDR Hook Removal Tools

商用で入手可能なEDR回避ツールは、ランサムウェア・アズ・ア・サービスキットで頻繁に使用され、EDRフックを削除しエージェントを無効化することで、秘匿性の高い認証情報の窃取を可能にします。

EDRは意図的に無効化される可能性があるため、ネットワークおよびIDテレメトリによる帯域外検知が不可欠です。NDRは侵害を前提とし、攻撃者が既にネットワーク上で活動しているという認識で動作します。エンドポイント防御にはカバーできない領域があり、NDRはSOCにとって重要な侵害後の安全策を提供します。

事例：

アブドゥル・ラティフ・ジャミール (ALJ)

アブドゥル・ラティフ・ジャミール (ALJ) は、自動車、不動産、金融サービスなどを扱うグローバル複合企業であり、35カ国で事業を展開しています。同社では多様なネットワーク全体にわたる広範な脅威可視性が求められていました。従来のエンドポイント検知ではALJのグローバルITインフラ全体に点在する脅威に対する死角がありました。Vectra AIのエージェントレスNDRは、エンドポイントのテレメトリだけでなく、ネットワーク機器、ID、クラウドコンポーネントへの可視性を拡大しました。これにより、エージェントベース監視では達成できなかった包括的なカバレッジを実現。EDRでは検知できなかった攻撃者の振る舞いを迅速に特定しました。また、誤検知アラートを90%削減し、アナリストが真の脅威に集中できるようになりました。

問題はエンドポイントでの回避だけではありません。攻撃者はネットワークを横断し、EDRでは検知不可能な方法でIDを悪用しています。

理由3:

EDRの可視性はネットワークやID経路の攻撃を見逃す

EDRはエンドポイント上で発生する事象に焦点を当てますが、システム間を横断する活動 (東西方向) 、クラウド環境で発生する活動 (南北方向) 、あるいはアイデンティティレイヤーのみで発生する活動を完全に監視することはできません。

1 Vectra Gap Analysisにより、攻撃者が

既に暗号化されたSSLチャネル内にC2を埋め込む、

古いドメインを使用してURLフィルタリングを回避する、Kerberosの無制限委任などのIDメカニズムを悪用するといった手法でEDRを回避していることが判明しました。

2 CISAのレッドチーム評価では、EDRはデバイスレベルの検知に優れる一方、

> “ハッカーがラテラルムーブや異常なデータ転送を悪用する”

> “ネットワーク全体にわたる攻撃に対しては脆弱であることが明らかになりました。こうした活動は、検知にネットワークレベルの可視性を必要とする場合が多いです。”

3 CISAレッドチームのSILENTSHIELDによるシミュレーションでは、

攻撃者がサーバー間を自由に移動し、

最終的にドメイン侵害を達成する事例が確認されました。

防御側はネットワークログと内部トラフィックを分析することで初めて完全な状況認識を得ることができ、

EDRだけでは不十分であることが明らかになりました

これらの事例が明らかにしているのは、EDRが個々のホストを監視する一方で、内部ネットワーク経路を潜行するラテラルムーブを追跡できないという事実です。この盲点を補うためにも、ホスト間トラフィックを分析するNDRが、横方向の拡散を検知・理解・阻止するために不可欠となります。

事例：

Schaefer Kalk

同社では、ランサムウェアの侵入がEDRを完全に回避したインシデントがありました。それに対して、Vectra AIのネットワーク (NDR) およびアイデンティティ脅威検知とレスポンス (ITDR) の振る舞いベースAIが、不審なネットワーク活動とアイデンティティ活動を検知し、暗号化前に介入を可能にしました。

ラテラルムーブやIDの不正利用を可視化できない場合、セキュリティチームは手探りの対応を余儀なくされます。さらに、ノイズの多い低価値なアラートに埋もれ、真の脅威を見逃すケースが頻発します。

理由4:

NDRはアラートによるストレス、検知漏れ、誤検知を軽減する

セキュリティオペレーションセンター (SOC) はノイズを大量に受け取ります。

アナリストは平均して1日あたり約4,000件のアラートを受け取りますが、現実的に確認できるのはその半分以下であり、無数の潜在的な脅威が未検証のまま残されています。これらのアラートの大部分は誤検知であり、調査によれば対応が必要なものは1%未満です。そのためアナリストは、実際の攻撃に集中する代わりに、無意味なシグナルの選別に何時間も費やすことを余儀なくされています。この低価値なアラートが大量に発生すると、疲労とストレスを助長し、検知ツールへの信頼を損ない、SOC担当者は毎週、重大な脅威を見逃しているのではないかという不安を抱え続けることになります。

1 セキュリティチームは1日平均 **3,832** 件のアラートを受信しています。

しかしアナリストが確認できるのはその38%に留まり、大半は未対応のままです。

Vectra AI 2024 State of Threat Detection and Response Report

2 「アラート管理」にかかる時間はアナリスト1人あたり

1日約 3 時間

労働時間の27%以上が費やされており

SOCチームは自動化可能なタスクに

1日約 9.6 時間を費やしています

Vectra AI 2024 SOC Efficiency Report

3 Vectra MDR/MXDR顧客からの110万件の振る舞いシグナル分析により、確認できた悪意のあるものは

300 件未満 (0.02%) であり、

検知の

99.98%

はノイズとしてフィルタリングされ、アナリストに到達する前に排除されていました。

Vectra AI 2025 Research Brief: Reducing Noise, Elevating Threats: A Data-Driven Look at SOC Efficiency

4 173万件の検知のうち、対応優先度が付けられたのはわずか

0.53% であり、

顧客あたり月平均70件未満規模の

対応不可能なアラートが浮き彫りとなりました。

Vectra AI 2025 Research Brief: Reducing Noise, Elevating Threats: A Data-Driven Look at SOC Efficiency

5 **SOC担当者の 71%** は、毎週受け取る大量のアラートの中に実際の攻撃が埋もれてしまうことを懸念しており、

62% はベンダーが

侵害の責任回避のために無意味なアラートを大量に送り込んでいると考えています。

Vectra AI 2024 State of Threat Detection and Response Report

事例：
Globe Telecom

Globe Telecomでは、インフラ全体に可視性の死角が存在し、EDRツールを回避する脅威を検知する能力に限りがありました。Vectra AIのNDRプラットフォームとマネージド検知サービスを導入した結果、セキュリティチームはネットワーク環境全体 (IDレイヤーやクラウドレイヤーを含む) をリアルタイムで可視化できるようになり、次の成果を達成しました。

アラートノイズを99%削減し、セキュリティアナリストが高精度なアラートのみに集中できるようにしました。また、インシデント対応時間を78%短縮し、検知と封じ込めを大幅に加速。さらにエスカレーション作業負荷を96%削減し、8,000万人の顧客が利用するサービスのカバー率を維持しながら、アナリストの負担を大幅に軽減しました。

ノイズの除去は重要ですが、全体像を把握することも同様に重要です。NDRは、あらゆるSOCが必要とする広範な可視性と深い洞察を提供することで、この課題を解決します。

理由5：

NDRはSOCの可視性、効率性、有効性を実現する

SOC可視性のトライアド

NDRの重要性を理解する有用な方法のひとつが、ガートナーの「SOC Visibility Triad (SOC可視性のトライアド)」という概念です。ガートナーのアナリストは、包括的な脅威可視性を実現するためには、組織が以下の3つの主要な検知技術を連携させて活用すべきであると提言しています。

1

SIEM/ログ管理：

イベントログの分析とシステム横断的なアラートの相関分析。

2

エンドポイント検知とレスポンス (EDR)：

エンドポイント (ワークステーション、サーバー、モバイルデバイス) における悪意のある活動を監視・封じ込めるための技術。

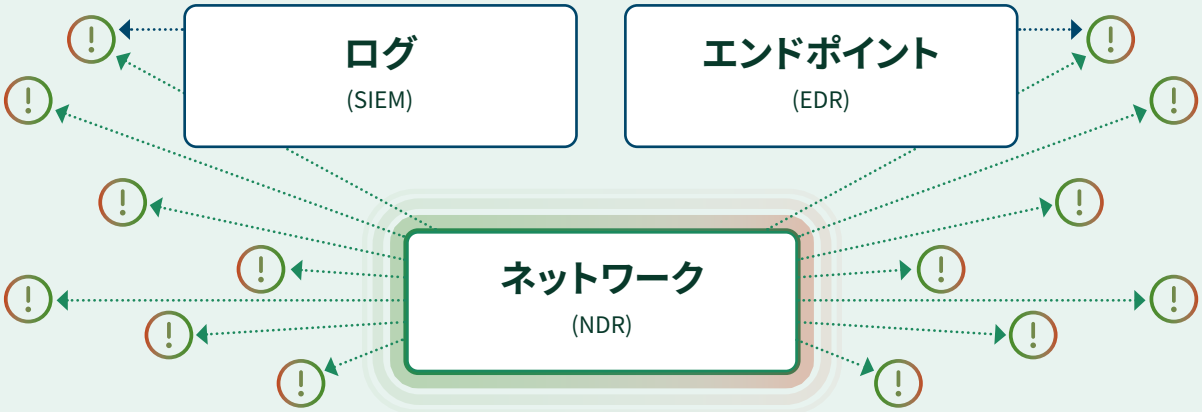
3

ネットワーク検知とレスポンス (NDR)：

ネットワークトラフィックを監視し、デバイス間の通信に現れる脅威を発見する。

この三本柱はそれぞれ環境の異なる側面をカバーしており、これらを組み合わせることでSOCの攻撃検知とレスポンス能力が大幅に向上します。これらのうち1つまたは2つだけを頼りにすると、死角が生じる可能性があります。例えば、EDRではネットワーク上や管理対象外のデバイスで発生している事象を見逃す恐れがあり、一方、ログ分析だけではライブトラフィックを完全に可視化できない場合があります。しかし、3つすべてを導入すれば、その重複部分によって多層防御と脅威の相互検証が実現されます。つまり、組み合わせたシグナルとコンテキストを通じて、誤検知 (偽陰性) と誤警報 (偽陽性) の両方を最小限に抑えることが可能となります。

SOC可視性のトライアド



組織は包括的なセキュリティ対策のため、ログ (SIEM) 、エンドポイント (EDR) 、ネットワーク (NDR) の可視化が必要です。ネットワークに焦点を当てたNDRは、他では検知できないネットワークトラフィックに顕在化する脅威を捕捉します。

特筆すべきは、この三要素の中でNDRがネットワーク活動の真実性を担うコンポーネントである点です。ネットワークパケットは嘘をつきません。デバイスが外部サーバーや別の内部ホストと通信している場合、その活動はネットワークを経由して伝播し、観察可能です。なぜなら、事実上すべての悪意のある操作がネットワークパケットを生成するからです。攻撃者はエンドポイント上のログを消去したり、ディスクへのファイル書き込みを回避したり (アンチウイルスを迂回するため) できるかもしれませんが、パケットを送信せずに侵入を実行することはできません。これらのパケット (またはそのメタデータ) を収集・分析することで、NDRは攻撃者が痕跡を隠蔽しにくくする証拠源を提供します。さらに、攻撃者は組織がネットワークトラフィックを密かに監視していることに気づかない場合が多く、ネットワーク上での検知回避策を講じられないため、NDRはあらゆるセキュリティスタックにおいて強力かつ不可欠な構成要素となります。

NDRの重要性に対する業界の評価は高く、ガートナーが初のNDRのマジック・クアドラントを発表したことは市場の成熟を示しており、他のアナリスト会社 (IDC、GigaOm、Forrester) もその重要性を裏付けています。主要な専門家は、NDRがもはや「あれば便利な機能」ではなく、現代の攻撃に対抗するために不可欠であると指摘しています。セキュリティ組織やマネージドセキュリティサービスプロバイダー (MSSP) は、SOC機能を強化するにあたり、可視性のギャップを埋め、検知されずに潜伏する高度な脅威を捕捉するため、SIEMやEDRの導入と並行してNDRの導入を加速させています。

NICEフレームワーク

2025年5月のガートナー セキュリティ & リスク・マネジメント サミットで発表されたNICEフレームワーク (ネットワーク、アイデンティティ、クラウド、エンドポイント) は、効果的な脅威の検知、調査、対応に必要な重要なテレメトリ領域を統合するモデルです。

4つの柱にわたる可視性と分析を統合することで、SOCチームは独立したシグナルを相関させ、侵害の迅速な確認と誤検知の削減を実現できます。最新のNDRはこのモデルにおいて独自の位置付けにあります。ネットワーク、アイデンティティ、クラウド領域に対する深いネイティブカバレッジを提供すると同時に、エンドポイントツールとシームレスに連携し、全体像を完成させます。この統合アプローチにより、SOCチームは管理対象、非管理対象、オンプレミス、クラウド接続資産を横断して悪意のある活動を検知し、アタックサーフェス全体およびサイバーキルチェーン全体にわたる迅速かつ自動化された対応を調整することが可能となります。

最新のNDRプラットフォームがNICEフレームワークに適合する方法

N

ネットワーク

ネットワークパケットとメタデータを継続的に分析し、暗号化されたトラフィックにおいてもコマンド&コントロール (C2) 通信、ラテラルムーブ、データ流出などの振る舞いを特定します。ネットワーク上の攻撃者の振る舞いを示す高精度なシグナルと豊富なコンテキストを提供します。

I

アイデンティティ

盗まれた認証情報の使用、不審な認証パターン、権限昇格の試みを検知し、活動をアイデンティティコンテキストにマッピングすることで、ゼロトラストポリシーを適用し、アカウントベースの攻撃を早期に阻止します。

C

クラウド

コントロールプレーンイベント、APIコール、ワークロードの挙動、SaaSアプリケーションログを監視し、AWS、Azure、GCP全体におけるリスクの高いアクセス、悪意のある自動化、不正なデータ移動を検知します。

E

エンドポイント

EDR/EPPプラットフォームと連携し、エンドポイントのアラートをネットワーク、アイデンティティ、クラウドの活動と相関分析します。これにより、エージェントが存在しない場合や回避された場合の検知能力が強化され、管理対象外デバイスやIoT/OTデバイス上の脅威を可視化します。さらに、APIやSOAR連携による自動化されたホスト隔離を実現します。

4つのNICEドメインすべてからのテレメトリを統合することで、最新のNDRプラットフォームはSOCチームがより迅速かつ正確に検知、調査、対応することを可能にします。このクロスドメイン相関により、複数の独立した攻撃の兆候 (IoA) を結びつけることで攻撃の確認が可能となり、誤検知を大幅に削減し、平均復旧時間 (MTTR) を短縮します。

NDRはシームレスな統合によりEDRを補完する

EDRはデバイスレベルの脅威を捕捉する上で重要な役割を果たしますが、攻撃者はエンドポイントで止まることはありません。検知も同様に、そこで止まるべきではありません。EDRとNDRを統合することで、セキュリティチームは可視性のギャップを埋め、断片的なアラートを連携した高精度な検知へと変革します。

両者の連携による効果は以下の通りです。

1. **エンドポイントのシグナルをネットワーク、ID、クラウドのテレメトリデータと関連付けます。**NDRはEDRの検知結果にコンテキストを追加し、ホスト上のアラートが以下のいずれかと関連しているかを確認します。
   - 不審な東西方向の移動
   - 権限昇格または異常な認証活動
   - 悪意のあるクラウドAPIの動作またはデータ漏洩
2. **弱い兆候から確実な攻撃を認識する。**単独では、EDRの検知には対応をトリガーするのに十分なコンテキストが不足している場合があります。NDRは信頼度の低いアラートを関連する振る舞いと結びつけ、侵害を確認します。
3. **エンドポイントを超えた対応を拡張します。**NDRが攻撃者の振る舞いを検知した場合 (管理対象外やエージェントレスのデバイスも含む) 、以下の対応が可能です。
   - ホストの隔離をトリガー
   - ユーザーアカウントの無効化
   - ネットワークレベルの証拠でEDRアラートを強化し、迅速なトリアージを実現
4. **アナリストに単一かつ統合されたビューを提供します。**統合された検知機能により、以下の方法で手動作業を削減し、調査時間を短縮し、SOCの効率性を向上させます。
   - ツールの乱立とコンソール切り替えの削減
   - 事前相関データによるより豊富な検知機能の提供
   - より優れたコンテキストに基づく迅速な意思決定の実現

Vectra AIのNDRプラットフォームは、主要なEDRベンダーとシームレスに連携し、これらのワークフローを標準でサポートします。対応ベンダーには、CrowdStrike、SentinelOne、Microsoft Defenderなどが含まれます。

EDRとNDRは一体となり、エンドポイントおよびそれに接続されたすべてのデバイスで発生している事象を可視化する、統合された検知とレスポンスレイヤーを形成します。

EDRとNDRが連携することで、統合された検知とレスポンスレイヤーが形成されます。このレイヤーは、エンドポイント上およびそれに接続されたすべてのデバイスで発生している状況を可視化します。

まとめ：

現代の攻撃に対応するにはNDRが必要である

現実的に、EDRだけでは、今日の複雑なハイブリッド環境を防御し、現代的な攻撃に対するレジリエンスを構築するために必要なカバレッジ、可視性、制御を実現できません。

現代の攻撃者は、管理対象外のデバイスを悪用し、エンドポイント制御を迂回するなど、ホスト中心のツールでは検知不可能な方法でIDを悪用します。ネットワーク検知とレスポンス (NDR) は、ネットワーク、ID、クラウド活動の実際の状況を継続的に監視し、ノイズを低減し、コンテキストを伴った最も重大な脅威のみを可視化することで、死角を解消します。セキュリティリーダーにとって、NDRへの投資は任意の選択肢ではありません。これはEDRを補完する不可欠な要素であり、SOCを「反応的で対応に追われる状態」から「先手を打つ効率的で回復力のある体制」へと変革します。NDRがあることで、組織は重要な脅威を確実に検知し、迅速に対応し、攻撃者の一歩先を行くことが可能となります。

VECTRA

Vectra AIについて

Vectra AIは、現代のネットワークを最新の攻撃から保護するAI主導のサイバーセキュリティを提供しています。高度なサイバー攻撃が既存の制御を回避し、検知を逃れて顧客のデータセンター、キャンパス、リモートワーク、アイデンティティ、クラウド、IoT/OT環境にアクセスした場合、Vectra AI プラットフォームは攻撃のあらゆる動きを監視し、リアルタイムで点と点を結び付けて、侵入を阻止します。また、当社はAIセキュリティに関する35件の特許を取得し、MITRE DEFENDで最も多くのベンダーリファレンスを誇ります。他のツールでは検知できない攻撃を見つけ、阻止するために世界中の組織がVectra AIを活用しています。詳細については、https://ja.vectra.ai/ をご参照ください。

---

ja.vectra.ai/

お問い合わせ:info-japan@vectra.ai