Sophos Network Detection and Response

Sophos XDR と Sophos MDR への強力な追加機能

Sophos NDR は、管理下のエンドポイントおよびファイアウォールと連携して、エンドポイントやファイアウォールが確認できない疑わしいパターンや悪意のあるパターンがないかどうかネットワークアクティビティを監視します。管理対象外のシステムや IoT デバイスからの異常なトラフィックフロー、不正なアセット、インサイダー脅威、これまで検知されなかったゼロデイ攻撃、ネットワークの深部にある異常なパターンを検出します。

Sophos NDR は、他のセキュリティ製品が見逃していたネットワークアクティビティに対する重要な可視性を提供

攻撃者は検出を回避することに優れていますが、あらゆる攻撃はネットワーク内を移動する必要があります。Sophos NDR は、管理下のエンドポイントおよびファイアウォールでは認識されない、次のような疑わしいネットワークトラフィックパターンを検出します。

- **不明または保護されていないネットワークデバイス** – エンドポイントセンサーで完全に管理できない正規の IoT デバイスまたは OT デバイス、およびネットワーク上の不明なシステム、未特定のシステムを含みます。これらのデバイスは侵害されるか、もしくは攻撃の一部として侵害される可能性があります。Sophos NDR は、攻撃の兆候となる可能性のある疑わしい動作や悪意のある動作がないか、これらのデバイスを特定して監視します。
- **不正なアセット** – すでに侵害されている可能性がある、または攻撃の開始に使用されている可能性があるネットワークに持ち込まれたこのアセットは、Sophos NDR によって容易に特定および監視できます。
- **これまでに検出されなかった新しいコマンド＆コントロール (C2) アクティビティ** – 多くの攻撃や侵害は、悪意のある攻撃者とネットワーク内のリモートプロセスとの間で正当な通信のように見せかけて、リモートでオーケストレーションされています。Sophos NDR を使用すると、新しいゼロデイ C2 アクティビティを検出して、攻撃が始まったばかりのカスタマイズされた標的型攻撃を特定できます。
- **攻撃が疑われる、あるいは悪意のあるネットワークトラフィックフローとパターン** - これらのフローやパターンは、サイバー攻撃を早期に特定するための重要なシグナルとなる場合があります。営業時間外の異常なネットワークアクティビティやリモートアクセス、不審なデータのアップロードや流出、異常なトラフィックパターン、既知のマルウェアによって生成された悪意のあるトラフィックなどが、これらの兆候に含まれます。

NDR は既存のファイアウォールと連携して動作

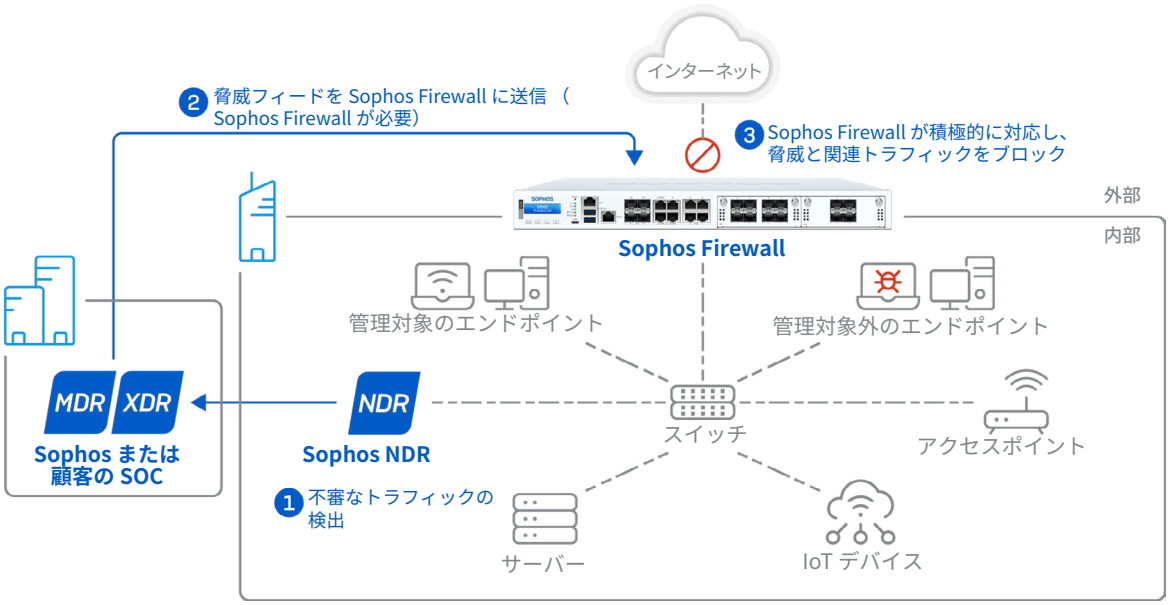
ファイアウォールは、ネットワーク境界を保護し、出入りするものを制御する上で重要な役割を果たします。Sophos NDR は、ファイアウォールソリューションを完全に補完し、それらが連携してお使いのファイアウォールの可視性が欠けているネットワークの奥深くまで確認し、対応します。また、他社のファイアウォールやエンドポイント保護製品では検出できない、内部ネットワークを通過する疑わしいアクティビティや悪意のあるアクティビティを一意に識別するテクノロジーも含まれています。

主な特長

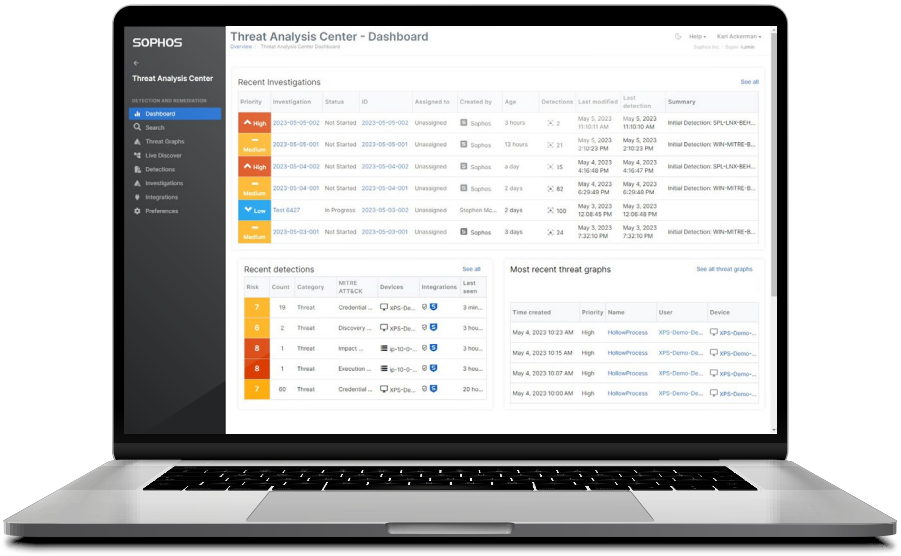
- Sophos XDR と Sophos MDR への完全な追加機能により、ネットワークの奥深くまで検出
- ファイアウォールと連携して、ネットワークアクティビティと脅威を検出
- 不明または非管理対象デバイス、不正なアセット、ゼロデイ C2 サーバーから発生した疑わしいネットワークアクティビティを検出
- PII を侵害することなく、暗号化されたトラフィックフローを検査
- Sophos Central からの導入、設定、管理
- 調査コンソールを活用し、攻撃が疑われるネットワークアクティビティに関する知見を獲得し、異常なパターンを分析・調査

SOPHOS

Sophos NDR はネットワークの奥深くで動作し、攻撃を検出

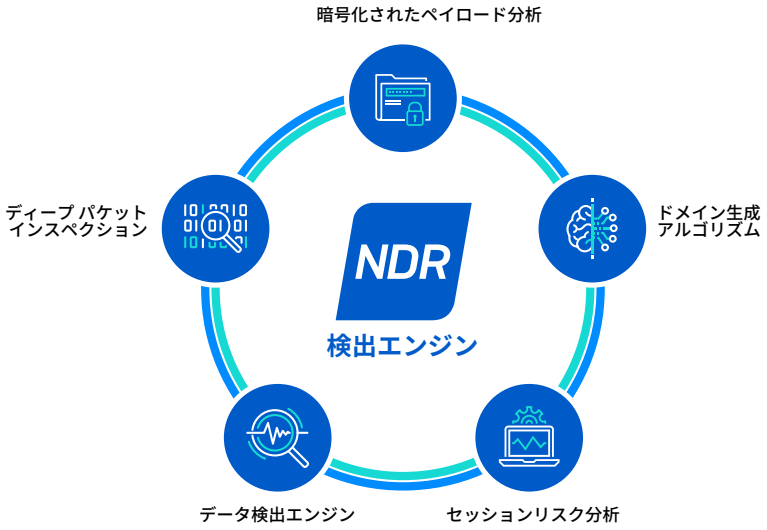


- 5 つのリアルタイムエンジンを使用して、ネットワーク内のトラフィックを監視
- 非管理対象システム、IoT デバイス、および不正なアセットなどのすべてのネットワークアセットの活動を検出し、製造業者、OS、およびこれらのデバイスで発生する不審なトラフィックパターンを特定
- データと警告を Sophos Central の Data Lake と MDR SOC チーム、または XDR チームに提供
- 使いやすい調査コンソールで、ネットワークおよびアプリケーションのアクティビティ、リスクの高いフロー、攻撃が疑われるトラフィックを可視化して、知見を提供
- Sophos Firewall を使用している場合は、脅威を即座にブロックし、ラテラルムーブメントを防ぐ自動脅威対応機能を利用
- VMware や Hyper-V などの一般的なハイパーバイザープラットフォーム上で仮想アプライアンスとして動作
- SPAN ポートミラーリングを介してスイッチに直接接続し、すべてのトラフィックを監視
- PII データを損なうことなく、暗号化されたパケットデータを検査



Sophos NDR の検出エンジン

Sophos NDR には、ネットワーク トラフィック フローを継続的に分析し、AI 機械学習分析を適用して、ネットワークの深部にある疑わしいアクティビティや悪意のあるアクティビティを特定する 5 つの検出エンジンが含まれています。



検出エンジン	説明
暗号化ペイロード分析 (EPA)	セッションサイズ、方向、および到着間隔で検出されたパターンに基づいて、ゼロデイの C2 サーバーとマルウェアファミリーの亜種を検出します。
ドメイン生成アルゴリズム (DGA)	マルウェアが検出を回避するために使用する動的ドメイン生成テクノロジーの存在を特定します。
ディープ パケット インスペクション (DPI)	既知の IOC を使用して暗号化されたトラフィックと暗号化されていないトラフィックの両方を監視し、脅威アクターと TTP を迅速に特定します。
セッションリスク分析 (SRA)	強力なロジックエンジンを搭載し、セッションに応じた様々なリスク要因で警告するルールを活用します。
デバイス検出エンジン (DDE)	ディープラーニング予測モデルを使用した拡張可能なクエリエンジンで、関連性のないネットワークフロー全体のパターンに対して暗号化トラフィックを分析し、ポートスキャンや SSH ブルートフォース攻撃に関するアクティビティを検出します。

Sophos NDR ライセンス

Sophos NDR は Sophos XDR と Sophos MDR を完全に補完するものであり、統合パッケージとして利用できます。Sophos NDR の価格は、組織内のユーザーとサーバーの合計数に基づいて決定されます。仮想アプライアンスソフトウェアはライセンスに含まれており、必要な数の NDR センサーを導入できます。これは、インスタンス単位に課金される競合製品よりも手頃な価格で柔軟性があります。

Sophos NDR 技術仕様

対応プラットフォーム

- VMware ESXi6.7 以上
- Microsoft Hyper-V 6.0.600118016 (Windows Server 2016) 以降
- Amazon AWS c5n.2xlarge
- 認定ハードウェア

ハードウェア	最大スループット	最大接続数 / 秒	CPU 数 :	メモリ
Dell R660 (2 ソケット)	40Gbps	120K	64	128 GB
Dell R660 (1 ソケット)	40Gbps	80K	32	64 GB
Dell R650	20Gbps	40K	24	64 GB
Dell R450	10Gbps	20K	16	32 GB
Dell R350	4Gbps	8K	8	32 GB
Intel Nuc 13th Gen	2.5Gbps	4K	12	32 GB

VM のシステム要件

Sophos NDR VM は、センサーごとに最大 1 Gbps をサポートします。

- トラフィック量が中程度の場合は、デフォルトの VM 設定を使用します。
  - 最大 500 Mbps
  - 最大 70,000 パケット / 秒
  - 最大 1,200 フロー / 秒
- トラフィック量が多い場合は、8 vCPU 用に VM のサイズを変更します。
  - 最大 1 Gbps
  - 最大 300,000 パケット / 秒
  - 最大 4,500 フロー / 秒

その他の参考資料 :

- Sophos Community にある NDR 資料
- Sophos NDR (Network Detection and Response) によるセキュリティオペレーションの強化
- 認定ハードウェアの仕様

詳細はこちら

sophos.com/ndr

ソフォス株式会社営業部
Email: sales@sophos.co.jp

24-12-19 DS-JA (MP)