SOPHOS

SOPHOS NDR

AI 時代のネットワーク全体に潜む脅威を可視化し、阻止する。

既知および未知の脅威を検知し、防御するための一つの解決策。

Sophos NDRは、AIと機械学習を活用した行動分析、暗号化トラフィック分析、ネットワーク分析、脅威ハンティングを、ディープ パケット インスペクションおよびIDS/IPS機能と組み合わせたソリューションです。柔軟な導入オプション、アクティブなインライン対応、Sophos Fusionを通じた連携防御により、組織はハイブリッドネットワーク全体の可視性を高め、管理対象外のアセットやエージェントレスのアセットを監視して、脅威をより迅速に阻止し、連携防御を強化できます。

77%
の IT チームが
ハイブリッド環境全体を
完全には把握できていません[1]

3.4時間
攻撃者がアクセス権を
取得してからActive Directoryを
標的にするまでの時間の中央値[2]

3日間
環境内で攻撃者が
検出されるまでの時間の中央値[2]

SOPHOS NDRが提供するもの

ネットワーク防御を強化するための4つの成果。

ネットワーク全体をもっと見通せるように。

管理対象のアセット、管理対象外のアセット、エージェントレスのアセットに関わる通信について、ネットワークレベルでの可視性を確保します。個々の制御機能では検出できない可能性のある不審な振る舞いや攻撃活動を特定します。

- ネットワーク全体における不審な行動を特定するための行動分析
- 管理対象外のアセット、IoT、OT、エージェントレスアセットの可視性
- ラテラルムーブメントと指揮統制の検出

脅威をより迅速に阻止。

検出から対応までの時間を短縮する。IDS/IPSアドオンを搭載したSophos NDRアプライアンスでは、アクティブインラインモードにより、ネットワークパス上の既知の悪意のあるパケットを自動的にブロックできます。

- 既知の悪意のあるパケットをリアルタイムでブロックする
- 受動的な監視から能動的なインラインでの脅威防止へと移行する
- トラフィックパスにディープ パケット インスペクションとIDS/IPSを直接適用する

ニーズに合った方法で導入できます。

仮想アプライアンスとして、または専用の Sophos NDR ハードウェアや互換性のあるサードパーティ製ハードウェア上に導入できます。監視と制御の適用を、アーキテクチャ、要件、リスク許容度に合わせて調整してください。

- 仮想環境への導入数は無制限
- 環境に合わせたハードウェアオプション
- 運用要件に合わせたSPAN/TAPおよびインライン導入モード

Sophos Fusionで業務を簡素化しましょう。

ネットワークのテレメトリ、検出結果、コンテキストを、エンドポイント、ファイアウォール、ID、メール、クラウドに関するインサイトと併せてSophos Fusionに取り込むことで、調査と連携した対応が可能になります。

- Sophos Fusion全体からのインサイトを活用してネットワーク コンテキストを統合
- Sophos MDRおよびXDRの調査をNDRテレメトリで強化する
- Sophos Fusion防御システム全体で検出と対応を調整する

SOPHOS NDRの概要

- AIと機械学習を活用した行動分析により、未知の脅威や検出を回避する脅威を明らかにする
- 実績のあるディープ パケット インスペクションとIDS/IPS機能により、既知の脅威を特定
- 既知の悪質なトラフィックをアクティブにインラインブロック
- 仮想アプライアンス、Sophos 専用ハードウェア、互換性のあるサードパーティ製ハードウェアから選べる導入オプション

SOPHOS NDR の対象

- ネットワークの可視性のギャップを解消しようとしている組織
- 管理されていないアセットやエージェントレスのアセットの可視化を求めるセキュリティチーム
- 多様な分散ネットワーク全体にわたって柔軟なNDRの導入を必要とする組織
- ネットワーク監視、脅威ハンティング、マネージドセキュリティサービスを拡充するMSPおよびMSSP

ネットワーク脅威に対する優位性

振る舞い検知とアクティブな防御の融合。

検出範囲の拡大

攻撃者は、ハイブリッドネットワーク、管理されていないデバイス、およびエージェントレスのアセット全体にわたる可視性のギャップを悪用することができます。Sophos NDRは、行動分析、暗号化トラフィック分析、脅威ハンティング、ディープ パケット インスペクション、IDS/IPSを組み合わせて、既知および未知の脅威を検出します。

ネットワーク経路上の脅威を直接ブロックする

検出だけでは、悪質なトラフィックがすでに宛先に到達してから、セキュリティチームが対応せざるを得なくなる可能性があります。IDS/IPSアドオンを搭載したSophos NDRアプライアンスでは、アクティブインラインモードがトラフィックをリアルタイムで検査し、ネットワーク経路上の既知の悪質なパケットを自動的にブロックします。

Sophos Fusion による連携防御

ネットワークの脅威が単独で存在することはほとんどありません。Sophos NDRは、ネットワークテレメトリ、検出結果、およびコンテキストをSophos Fusionに提供することで、チームが調査を迅速化し、防御システム全体で対応を調整できるよう支援します。

お客様の声

「全体的に、Sophos NDR を使用した経験はかなり良かったです。異常なネットワークの挙動を把握し、従来の監視では通常見逃されるパターンを検知するのに大いに役立ちます。私が本当に評価しているのは、アラートが明確で解釈が容易なため、解析と意思決定が迅速化される点です」[3]

ITセキュリティおよびリスク管理、銀行業界 — Gartner® Peer Insights™

SOPHOS FUSION

1 つのシステムが、あらゆる制御ポイントを連携させ、一体となって防御。

Sophos NDR は、世界で最も包括的なサイバー防御システムである Sophos Fusion の一部です。防御策のスピードを上回る AI の脅威から、組織を守ります。

sophos.com/NDR →

[1] SolarWinds、2026年モニタリングおよび可観測性に関する現状報告

[2] Sophos、アクティブアドバーサリーに関するソフォスのレポート 2026

[3] https://www.gartner.com/reviews/market/network-detection-and-response/vendor/sophos/product/sophos-ndr/review/view/6513218

Gartner Peer Insights のコンテンツは、個々のエンドユーザー自身の経験による主観的な意見が集約されたものであり、Gartner またはその関連会社の見解を表すものではありません。Gartner は、Gartner Peer Insights に掲載された特定のベンダー、製品またはサービスを推奨するものではありません。Gartner は、商品性または特定目的への適合性の保証を含む、その正確性または完全性について、本コンテンツの内容に関する一切の責任を、明示または黙示を問わず負うものではありません。

Gartner® および Peer Insights™ は、Gartner, Inc. および / またはその関連会社の商標です。All rights reserved.

© Copyright 2026.Sophos Ltd.All rights reserved.Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UKSophos は、Sophos Ltd. の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。

2026-10-23 SB-JA (TA)

SOPHOS