ソリューションのカタログ

Sophos Extended Detection and Response

包括的な EDR と XDR でアクティブアドバーサリー (活動中の攻撃者や脅威) を防御

攻撃をすぐに阻止することが重要です。Sophos XDR は、IT 環境全体にわたり、疑わしいアクティビティの検出、調査、対応を行う脅威インテリジェンスを兼ね備えた強力なツールを提供します。

最強の保護を構築

人材が集中している IT チームは、より多くの脅威を事前に阻止できるため、調査して解決するインシデントが少なくなります。ソフォスは、XDR (Extended Detection and Response) と業界最強のエンドポイント保護機能を組み合わせ、手作業による調査が必要になる前に脅威をブロックし、作業を軽減します。

EDR (Endpoint Detection and Response) を搭載

Sophos XDR には、90日分のエンドポイントやサーバーデータへのアクセス、デバイスへの安全なリモートアクセスなど強力でカスタマイズ可能な検索機能を備えた包括的な EDR ツールが含まれています。問題の調査、ソフトウェアのインストール/アンインストール、プロセスの終了などを行います。

エンドポイントを超えた可視性を拡張

情報量が多いほど、迅速な対応が可能になります。ソフォス製品とソフォス以外の製品の両方からのイベントは、取り込み、フィルタリング、相関付け、優先順位付けされます。これにより、すべての主要な攻撃対象領域にわたる可視性が拡張され、アクティブな攻撃者を迅速に検出して阻止できます。

拡張性の高い Sophos XDR 対応ソリューション

ソフォスのテクノロジーは XDR プラットフォームでシームレスに連携して、最高のセキュリティ成果を提供します。ネイティブソリューションの統合には、Sophos Endpoint、Sophos Workload Protection、Sophos Mobile、Sophos Firewall、Sophos NDR、Sophos ZTNA、Sophos Email、Sophos Cloud などがあります。

既存のツールやテクノロジーとの互換性

ソフォス以外のさまざまなセキュリティツールからのテレメトリを活用して、セキュリティ運用を迅速化させながら、既存のテクノロジー投資からより多くの ROI を得ることができます。統合には、アイデンティティ、ネットワーク、ファイアウォール、メール、クラウド、生産性ツール、エンドポイントセキュリティ テクノロジーが含まれています。

主な特長

- すべての主要な攻撃対象領域にわたり疑わしいアクティビティを可視化
- 幅広い統合ソフォスソリューションを備えた統合 XDR プラットフォーム
- ソフォス製品以外の広範なテクノロジーを統合して、既存のツールと投資を活用
- AI による優先順位付けされた検出と最適化されたワークフローにより、脅威を迅速に調査して対応
- 業界をリードするエンドポイント保護と EDR を搭載

脅威の検出、調査、対応を加速化

Sophos XDR は、セキュリティアナリストや IT 管理者の効率性を最大化するように設計されたツールと機能を搭載しています。AI が導く調査により、インシデントの範囲と原因をすばやく把握し、対応までの時間を最小限に抑えることができます。

すべての主要な攻撃対象領域で AI が優先順位を付けて検出

すぐに対応する必要がある疑わしいアクティビティを簡単に特定できます。Sophos XDR は、リスクに基づいて検出に自動的に優先順位を付け、完全なコンテキストを提供します。

MITRE ATT&CK フレームワークマッピング

検出とケースは自動的に MITRE ATT&CK 戦術にマッピングされるため、防御のギャップを簡単に特定し、改善の優先順位を付けることができます。

脅威を迅速に調査してハンティング

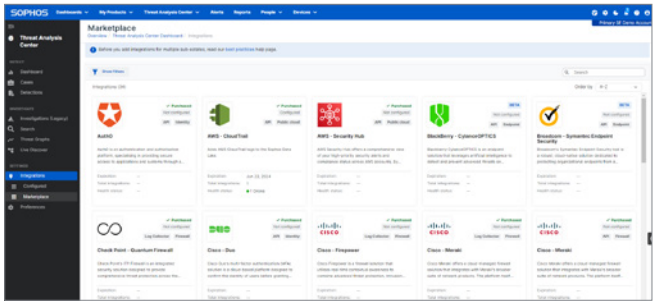
事前定義されたクエリテンプレートなどの強力な検索ツールを使用でき、SQL に精通してなくても、必要なデータを迅速に見つけることができます。

自動化された迅速な対応

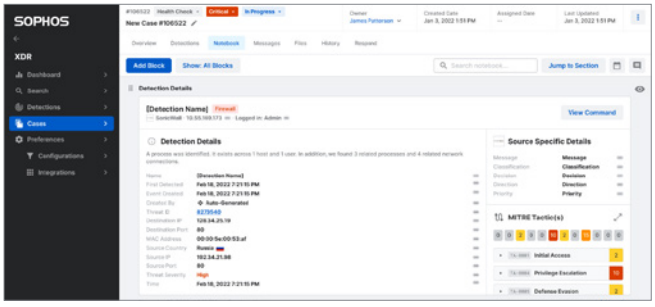
プロセスの終了、ランサムウェアのロールバック、ネットワークの分離などの自動化されたアクションにより、脅威を迅速に封じ込め、貴重な時間を節約できます。

コラボレーションケース管理

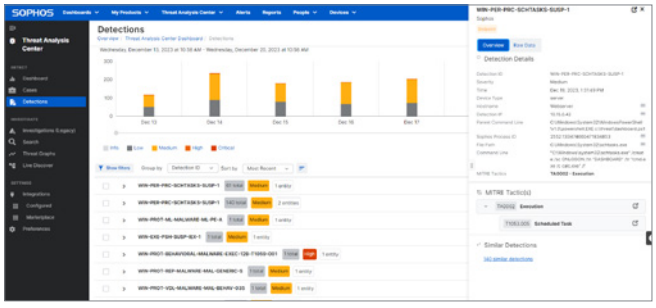
他のチームと一緒にコラボレーションのための包括的なケース管理ツールを使用したケースの自動作成を行うことで、迅速な調査が可能になります。



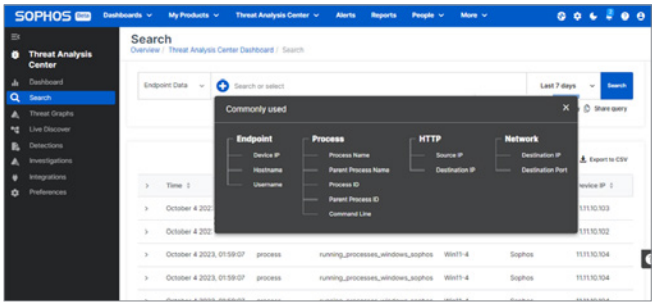
ソフォスとサードパーティソリューションとの互換性



強力なケース管理ツールとコラボレーションツール



すべての主要な攻撃対象領域で AI が優先順位を付けて検出



シンプルで強力な検索 – SQL の専門知識は不要

Sophos XDR に統合

次のソースからのセキュリティデータは、追加料金なしで Sophos XDR プラットフォームに統合できます。テレメトリソースは、環境全体の可視性の拡大、新しい脅威検出の生成、既存の脅威検出の忠実度の向上、脅威ハンティングの実施、追加の対応機能の有効化のために使用されます。

Sophos Endpoint

高度な脅威をブロックし、エンドポイント全体で悪意のある動作を検出

Sophos XDR の価格に含まれる製品

Workload Protection

Windows および Linux のサーバーとコンテナに対する高度な保護と脅威の検出

Sophos XDR の価格に含まれる製品

Sophos Mobile

最新のモバイル脅威から iOS および Android デバイスとデータを保護

製品は別売り。追加料金なしで統合できます

Sophos Firewall

送受信するネットワークトラフィックを監視およびフィルタリングして、高度な脅威が被害を及ぼす前に阻止

製品は別売り。追加料金なしで統合できます

Sophos Email

標的型のなりすまし攻撃やフィッシング攻撃を阻止する高度な AI を活用したマルウェアから受信トレイを保護

製品は別売り。追加料金なしで統合できます

Sophos Cloud

AWS、Azure、GCP など、クラウド侵害の防止および重要なクラウドサービス全体の可視化

製品は別売り。追加料金なしで統合できます

Sophos ZTNA

リモートアクセス VPN を最小権限アクセスに置き換えて、ユーザーをネットワークアプリケーションに安全に接続

製品は別売り。追加料金なしで統合できます

サードパーティ製エンドポイント保護

次の製品と互換性があります。

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- BlackBerry (Cylance)
- Broadcom (Symantec)

+ ソフォスの「XDR Sensor」エージェントを使用した他のソリューションとの互換性

Microsoft セキュリティツール

- Defender for Endpoint
- Defender for Cloud
- Defender for Cloud Apps
- Defender for Identity
- Microsoft Entra ID
- Azure Sentinel
- Office 365 セキュリティ/コンプライアンスセンター

90日間のデータ保持

Sophos Data Lake 内のソフォス製品およびサードパーティ (非ソフォス) ソリューションからのデータを保持

オプションのアドオンで 1年間に延長可能

Microsoft Audit Log

Office 365 管理アクティビティ API 経由で取り込まれたユーザー、管理者、システム、ポリシーのアクションとイベントに関する情報を提供

Google Workspace

Google Workspace Alert Center API からセキュリティテレメトリを取り込む

アドオン可能な統合

統合パックを購入することで、次のソースからのセキュリティデータを Sophos XDR プラットフォームに統合できます。テレメトリソースは、環境全体の可視性の拡大、新しい脅威検出の生成、既存の脅威検出の忠実度の向上、脅威ハンティングの実施、追加の対応機能の有効化のために使用されます。

Sophos NDR

ネットワーク内のアクティビティを継続的に監視し、他の方法では見つからないデバイス間で発生している疑わしいアクションを検出

SPAN ポートミラーリングを介した、あらゆるネットワークと互換性があります

ファイアウォール

次の製品と互換性があります。

- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- Palo Alto Networks
- SonicWall
- WatchGuard

ネットワーク

次の製品と互換性があります。

- Darktrace
- Secutec
- Thinkst Canary
- Skyhigh Security

アイデンティティ

次の製品と互換性があります。

- Auth0
- Duo
- ManageEngine
- Okta

Microsoft の統合が追加料金なしで含まれています

メール

次の製品と互換性があります。

- Proofpoint
- Mimecast

Microsoft 365 と Google Workspace の統合が追加料金なしで含まれています

パブリッククラウド

次の製品と互換性があります。

- AWS Security Hub
- AWS CloudTrail
- Orca Security

別売りの Sophos Cloud 製品を使用して、追加の AWS、Azure、GCP データを統合

バックアップとリカバリ

次の製品と互換性があります。

- Veeam

1年間のデータ保持

Sophos Data Lake 内のソフォス製品およびサードパーティ (非ソフォス) ソリューションからのデータを保持

世界最高レベルのエンドポイント保護を構築

セキュリティ侵害を未然に阻止することで、調査に重点を置きます。ほとんどの他社 XDR 製品では、保護製品によってブロックされるはずだったインシデント調査に、アナリストは貴重な時間を浪費することを余儀なくされています。ソフォスは、XDR と業界最強のエンドポイント保護機能を組み合わせ、手作業による調査が必要になる前に脅威をブロックし、作業を軽減します。

Sophos XDR サブスクリプションには Sophos Intercept X Endpoint が含まれており、高度なランサムウェア対策とエクスプロイト対策、AI を活用したマルウェア対策、保護レベルを動的に適応させる適応型の防御機能を提供します。

詳細については、sophos.com/endpoint を参照してください

フルマネージドサービスとして検出と対応を実現

Sophos XDR を使用して脅威を自ら検出して調査するか、24時間年中無休体制の包括的なマネージドサービスを使用して従業員の負担を減らすかを選択できます。Sophos MDR (Managed Detection and Response) により、ソフォスの脅威ハンターのエキスパートとアナリストのチームが、本格的なインシデント対応機能を含むセキュリティ オペレーション センターを即座に提供します。

詳細については、sophos.com/mdr を参照してください

Sophos XDR サブスクリプションに含まれているもの

	Sophos XDR
AI 優先検出とガイドによる調査	✓
ケース管理、コラボレーション、対応アクション	✓
ハンティングや調査のためのシンプルで強力な検索ツール	✓
Sophos Endpoint および Workload Protection ソリューション (Intercept X Advanced)	✓
EDR (Endpoint Detection and Response) ツール	✓
クラウドデータの保持期間	90日間 (1年間に延長可能)
EDR 用の豊富なエンドポイントおよびサーバーのオンデバイスデータ	✓
ソフォスソリューションとの統合: Sophos Endpoint、Sophos Workload Protection、Sophos Mobile、Sophos Firewall、Sophos ZTNA、Sophos Email、Sophos Cloud	✓
Sophos Network Detection and Response (NDR)	オプションのアドオン
ソフォス製品以外のエンドポイント保護ソリューションとの統合	✓
Microsoft ソリューションとの統合	✓
Google Workspace 生産性ソリューションとの統合	✓
ソフォス製品以外のファイアウォール、ネットワーク、メール、クラウド、アイデンティティ、バックアップ、リカバリソリューションとの統合	オプションのアドオン

Sophos XDR が選ばれる理由

ソフォスは、XDR のリーダーとして確立されており、業界でもその評価を裏付けています。

Gartner

ソフォスは、14回連続で、2023年 Gartner® Magic Quadrant™ for Endpoint Protection Platforms において、リーダーの1社と評価を獲得

Gartner Peer Insights Customers' Choice 2023

ソフォスは、EPP、MDR、ファイアウォール、モバイル脅威防御全体でお客様の選択肢として認められた唯一のベンダー

G2 Leader

G2 Winter 2024 Report で、ソフォスがエンドポイントプロテクション、EDR、XDR、ファイアウォール、MDR 分野のリーダーに選出

OMDIA

ソフォスは、2023年に Omdia Universe の包括的な XDR 分野で業界トップに選ばれた唯一のリーダー

MITRE ATT&CK

ソフォスは、2023 MITRE Engenuity ATT&CK 評価で優れた結果を獲得

SE Labs

ソフォスは独立したテストで業界をリードする保護結果を一貫して達成

無償評価版

無償評価版の登録 (30日間)
sophos.com/xdr

ソフォス株式会社営業部
Email: partnersales@sophos.co.jp

SOPHOS

2024-02-01 DS-JA (NP)