ソリューションのカタログ

Sophos Managed Detection and Response サービス

脅威検出と対応の 24時間対応

Sophos MDR は、コンピュータ、サーバー、ネットワーク、クラウド ワークロード、メール アカウントなどを標的とするサイバー攻撃を専門家が検出して対応する 24時間年中無休のフルマネージドサービスです。

ランサムウェアと侵害防止サービス

常時稼働のセキュリティ運用の必要性が不可欠になっています。しかし、最新の運用環境は複雑で、サイバー脅威の速度も速いため、ほとんどの組織が検出と対応を自社で管理することがますます困難になっています。

Sophos MDR を利用することで、ソフォスの専門家チームが高度な人間主導の攻撃を阻止します。ソフォスは、脅威がお客様の業務を中断させたり、機密データを危険にさらす前に、脅威を無力化するための措置を講じます。Sophos MDR は、さまざまなサービスレベルでカスタマイズ可能で、ソフォス独自のテクノロジーを介して、または既存のサイバーセキュリティテクノロジー投資を使用して提供されます。

サイバーセキュリティをサービスとして提供

Sophos MDR は、データが保存されている場所を問わず、完全なセキュリティを提供する XDR (eXtended Detection and Response) 機能により、次のことが可能です。

- セキュリティツールが単独で特定できる以上のサイバー脅威を検出
  ソフォスのツールは、99.98% の脅威を自動的にブロックします。これにより、当社のアナリストは、高度なトレーニングを受けた人間でなければ検出・阻止できない最も巧妙な攻撃者の追跡に専念できます。
- 脅威による業務の中断を阻止するために、お客様に代わってアクションを実行
  本格的なインシデント対応が必要な場合でも、正確な決定を行うサポートが必要な場合でも、ソフォスのアナリストが数分で脅威の検出、調査、対応を行います。
- 脅威の根本原因を特定し、将来のインシデントを防止
  ソフォスは積極的に対策を講じ、お客様の組織のリスクを軽減する推奨事項を提供します。インシデントが減少すれば、IT/セキュリティチーム、従業員、およびお客様にとっての混乱も少なくなります。

すでにご利用中のサイバーセキュリティ製品との互換性

受賞歴のあるソフォス製品ラインアップから必要なテクノロジーを提供、または、当社のアナリストがお客様がご利用中の既存の他社製サイバーセキュリティテクノロジーを活用して、脅威を検出し、対応することができます。

Sophos MDR は、Microsoft、CrowdStrike、Palo Alto Networks、Fortinet、Check Point、Rapid7、Amazon Web Services (AWS)、Google、Okta、Darktrace など、多くのベンダーによるセキュリティテレメトリと互換性があります。テレメトリは、Sophos Adaptive Cybersecurity Ecosystem (ACE) と Sophos X-Ops の脅威インテリジェンスからのインサイトを使用して、自動的に統合、関連付け、優先順位付けをされます。

主な特長

- 24時間年中無休体制の脅威対応の専門家チームにより、ランサムウェアやその他の人間主導型の高度な攻撃を阻止
- 既存のサイバーセキュリティテクノロジーの ROI を最大化
- Sophos MDR が、本格的なインシデント対応を実行し、お客様と連携してセキュリティインシデントを管理、または詳細な脅威の通知とガイダンスを提供
- 24時間年中無休体制の監視と EDR (Endpoint Detection and Response) 機能により、サイバー保険の適用範囲を向上
- 社内の IT スタッフとセキュリティスタッフを作業から解放して、ビジネスの実現に集中

お客様の立場に立った MDR

Sophos MDR では、さまざまなサービスレベルと脅威対応オプションでカスタマイズできます。Sophos MDR 運用チームが本格的なインシデント対応を実行し、お客様と連携してサイバー脅威を管理したり、脅威が検出された場合は社内のセキュリティ運用チームに通知します。チームは、誰が、何を、いつ、どのように攻撃したかを迅速に把握します。ソフォスは、脅威に数分で対応できます。

主な機能

脅威の監視と対応の 24時間対応

脅威がお客様のデータを危険にさらしたり、ダウンタイムを引き起こしたりする前に、脅威を検出して対応します。Sophos MDR は、世界 7か所のセキュリティ オペレーション センター (SOC) に支えられ、24時間体制で対応しています。

ソフォス以外のセキュリティツールと互換性がある

Sophos MDRは、他社製品のエンドポイント、ファイアウォール、ネットワーク、ID、メール、バックアップ/リカバリ、その他のテクノロジーからテレメトリを統合できます。

本格的なインシデント対応

アクティブな脅威を特定すると、Sophos MDR 運用チームは、お客様に代わって、攻撃者をリモートで阻止、封じ込め、完全に排除するための一連の対応策を実行します。Sophos MDR Complete ライセンスを使用すると、追加料金なしで、時間制限なしの本格的なインシデント対応を利用できます。

週次および月次レポート

Sophos Central は、警告、レポート、管理をリアルタイムで行うための単一のダッシュボードです。週次および月次レポートでは、セキュリティ調査、サイバー脅威、お客様のセキュリティ体制に関する洞察を提供します。

Sophos Adaptive Cybersecurity Ecosystem

Sophos ACE は、悪意のあるアクティビティを自動的に防止し、検出、調査、排除をするために人間の手が必要な弱い脅威のシグナルを検索できるようにします。

専門家の主導による脅威ハンティング

高度なトレーニングを受けたアナリストが実行するプロアクティブな脅威ハンティングにより、セキュリティ製品が単独で検出するよりも多くの脅威を発見し、迅速に排除することができます。また、Sophos MDR の運用チームは、サードパーティベンダーのテレメトリを使用して、脅威ハンティングを実行し、展開されたツールセットから検出を回避した攻撃者の行動を特定することもできます。

直接連絡サポート

お客様のチームは、ソフォスのセキュリティ オペレーション センター (SOC) に直接アクセスして、潜在的な脅威やアクティブなインシデントを確認できます。Sophos MDR 運営チームは世界26か国にわたり 24時間年中無休体制でサポートします。

専用のインシデント対応リード

インシデントが特定されるとすぐにお客様の社内チームや外部パートナーと協力し、インシデントが解決されるまでお客様と協力して作業をする、専任のインシデント対応担当者を提供します。

根本原因分析

セキュリティポスチャを改善するためのプロアクティブな推奨事項を提供するとともに、根本原因分析を実行して、インシデントを引き起こした根本的な問題を特定します。セキュリティの弱点に対処するための規範的なガイダンスを提供し、将来的に悪用されないようにします。

ソフォスのアカウントのセキュリティ状態のチェック

Sophos MDR によって管理されているエンドポイントの設定や構成を継続的に確認し、それらが最高の状態で動作していることを確認します。

脅威の封じ込め

Sophos MDR で本格的なインシデント対応を実行しないことを選択した組織の場合、Sophos MDR 運用チームが脅威の封じ込めアクションを実行して、脅威を中断し、拡散を防止することができます。これにより、社内のセキュリティ運用チームの作業負荷が軽減され、修復アクションを迅速に実行できます。

インテリジェンスブリーフィング:「Sophos MDR ThreatCast」

Sophos MDR 運用チームが提供する「Sophos MDR ThreatCast」は、Sophos MDR のお客様のみが利用できる月次ドキュメントです。最新の脅威インテリジェンスとセキュリティのベストプラクティスに関する洞察を提供します。

Breach Protection Warranty

Sophos MDR Complete の年間契約 (1年 ～ 5年) および月次ライセンスに含まれる保証では、最大 100万ドルの対応費用が補償されます。保証レベル、最低契約条件、追加購入要件はありません。

Sophos MDR に含まれる統合

追加料金なしで、以下のソースからのセキュリティデータを統合でき、Sophos MDR 運用チームがそれを監視に利用できるようになります。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。

Ep 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 MDR の価格に含まれる製品

WP 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 MDR の価格に含まれる製品

Mob 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

Fw 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

Em 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

Cld 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

ZT 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

アドオン可能なインテグレーションパック

インテグレーションパックの購入を介して Sophos MDR 運用チームは、以下のサードパーティのソースからのセキュリティデータを無料で使用できるように統合します。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。

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary

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

ソフォスのサービスレベル

	Sophos MDR Essentials	Sophos MDR Complete
24時間年中無休の専門家主導による脅威監視と対応	✓	✓
ソフォス以外のセキュリティ製品と互換性がある	✓	✓
週次および月次レポート	✓	✓
月次のインテリジェンスブリーフィング:「Sophos MDR ThreatCast」	✓	✓
ソフォスのアカウントのセキュリティ状態のチェック	✓	✓
専門家主導の脅威ハンティング	✓	✓
脅威の封じ込め: 攻撃を中断し、拡散を防止 完全な Sophos MDR エージェント (保護、検出、および対応) または Sophos MDR Sensor (検出と対応) を使用	✓	✓
アクティブインシデント時の直接連絡のサポート	✓	✓
本格的なインシデント対応: 脅威を完全に排除 完全な Sophos MDR エージェント (保護、検出、および対応) が必要	IR Retainer アドオン	✓
根本原因解析 (RCA)		✓
専用のインシデント対応リード		✓
Breach Protection Warranty 最大 100万ドルの対応費用を補償		✓

Sophos MDR Guided Onboarding (日本は未提供)

Sophos MDR Guided Onboarding (日本は未提供) は、オプションの追加購入として、リモートでのオンボーディング支援に利用できます。このサービスでは、円滑で効率的な導入のための実践的なサポートを提供し、ベストプラクティスの構成を保証して、MDR サービスへの投資価値を最大化するためのトレーニングを提供します。ソフォスのプロフェッショナルサービス組織の専任担当者が、最初の90日間お客様をサポートし、導入が成功するように支援します。Sophos MDR Guided Onboarding には、次のものが含まれます。

1日目 – 実装

- プロジェクトの開始
- Sophos Central の設定と機能の確認
- 導入プロセスの構築とテスト
- MDR 統合を設定
- Sophos NDR センサーの設定
- 企業全体への導入

30日目 – MDR トレーニング (英語)

- SOC のような考え方と行動を学ぶ
- 感染の痕跡を探す方法を理解
- MDR プラットフォームを管理タスクに使用する方法を理解
- 今後の調査のためのクエリ作成を学ぶ

90日目のセキュリティポスチャの評価

- ベストプラクティスを推奨事項について、現行のポリシーを見直す
- 使用されていない機能のうち、追加の保護を提供できるものについて話し合う
- NIST フレームワークに従ったセキュリティ評価
- レビューからの推奨事項を含む概要レポートを受け取る

Sophos MDR が選ばれる理由

ソフォスは、MDR 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

Gartner Market Guide for MDR (Managed Detection and Response) Services において代表的なベンダーに選出

Gartner peerinsights™

Gartner Peer Insights Customers' Choice for Managed Detection and Response を獲得

Leader

G2 Winter 2024 Grid Reports の MDR ソリューション部門でユーザー評価 1位を獲得

FROST & SULLIVAN

2024年の Frost Radar レポートで Global Managed Detection and Response のリーダーに選出

MITRE ATT&CK

セキュリティサービスプロバイダーの初の MITRE Engenuity ATT&CK Evaluation で卓越した評価を獲得

詳細はこちら

sophos.com/mdr

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

2024-04-02 BREN (NP)

SOPHOS