Sophos Managed Detection and Response

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提供する 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。

すでにお持ちのサイバーセキュリティツールとの互換性

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、サイバー保険の対象範囲を拡大
- 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

SOPHOS

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 6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、Sophos ACE の一部として、サードパーティのエンドポイント、ファイアウォール、ID、メール、その他のセキュリティテクノロジーからのテレメトリを統合することができます。

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。

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。

専用の脅威対応リード

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状態チェック

Sophos XDR 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。

ソフォスのサービスレベル

	Sophos Threat Advisor	Sophos MDR	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状態チェック		✓	✓
専門家の主導による脅威ハンティング		✓	✓
脅威の封じ込め: 攻撃を中断し、拡散を防止 完全な Sophos XDR エージェント (保護、検出、および対応) または Sophos XDR 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 XDR エージェント (保護、検出、および対応) が必要			✓
根本原因解析			✓
専用の脅威対応リード			✓

無償で提供される統合機能

Sophos MDR 運用チームが、以下のソースからのセキュリティデータを無償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 XDR

ネイティブのエンドポイント、サーバー、ファイアウォール、クラウド、メール、モバイル、Microsoft の統合を組み合わせた唯一の XDR プラットフォーム

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

Microsoft Graph Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Identity
- Azure Active Directory
- Microsoft Defender for Cloud Apps
- Microsoft Sentinel
- Azure Information Protection
- Microsoft 365

Sophos Endpoint

高度な脅威をブロックし、正当なユーザーのふりをした攻撃者を含む悪意のある行動を検出

Sophos Network Detection and Response

ネットワーク内のアクティビティを継続的に監視して、他の方法では見えないデバイス間で発生している疑わしい動作を検出

サードパーティ製 Endpoint Protection

以下と互換性があります

- Microsoft
- CrowdStrike
- SentinelOne
- Check Point
- Trend Micro
- BlackBerry (Cylance)
- McAfee
- Malwarebytes

Sophos Cloud

AWS、Azure、Google Cloud Platform 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

Sophos Email

マルウェアから受信トレイを保護し、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

90日間データ保管

Sophos XDR および Sophos Endpoint Protection 製品は、Sophos MDR サービスに含まれています
Sophos MDR サービスに統合する前に、Sophos Firewall、Sophos Cloud、Sophos Email、および Sophos NDR 製品を購入し、導入する必要があります

アドオン統合

統合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。

ファイアウォール

以下と互換性があります

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco
- SonicWall

クラウド

以下と互換性があります

- AWS
- Microsoft Azure
- Orca Security
- Google Cloud

ID

以下と互換性があります

- Okta
- Duo

ネットワークセキュリティ

以下と互換性があります

- Darktrace
- Forcepoint
- McAfee (Web gateway)

メール

以下と互換性があります

- Proofpoint
- Mimecast

1年間 データ保管

Sophos MDR 向けの Onboarding Plus パッケージ

Onboarding Plus サービスは、Sophos MDR のお客様が利用できるリモートガイド付きのオンボーディングサービスです。(英語での対応)ソフォスのプロフェッショナルサービス組織内の専任担当者にアクセスして、オンボーディングとスケジューリング、導入とトレーニングのサポート、およびソフォスのベストプラクティスを最大限に活用するためのセキュリティ状態のチェックを行います。Onboarding Plus には次のものが含まれます。

1日目 - 実装計画と実行:

- プロジェクトのキックオフ
- Sophos Central の設定
- Sophos Central の機能のレビュー
- 導入プロセスの構築とテスト
- 組織全体に Sophos Central を導入

30日目 – XDR トレーニング (英語)

- SOC のような考え方や行動様式を学ぶ
- IOC の追跡
- 今後の調査のためのクエリを作成

90日目 – XDR トレーニング (英語)

- 現在のセキュリティポリシーを見直し、必要に応じて更新
- サイバー保護をさらに強化するために使用できる機能 (ある場合) を判断
- セキュリティ状態のチェックから推奨事項が記載された文書を受け取る

詳細はこちら

sophos.com/mdr

ソフォス株式会社営業部
Email: sales@sophos.co.jp

22-10-17 DS-JP (DD)