SOPHOS

Sophos MDR で Microsoft Defender の強化

世界で最も信頼されている MDR サービス プロバイダーによる 24 時間年中無休の人間主導の脅威の検出と対応により Microsoft Defender を強化することで、サイバー リスクを軽減し、セキュリティ投資の効率と効果を高め、保険の適用可能性を向上させましょう。

ソフォス ホワイトペーパー2023年 7月

はじめに

エンドポイントセキュリティは、重要な保護レイヤーですが、、あらゆる脅威を阻止できるわけではありません。今日の洗練された敵対者は、セキュリティ技術によるブロックを回避するために、未修正の脆弱性を悪用したり、、盗まれた認証情報を利用したり、正規の IT ツールを悪用するなど、ステルス戦術、技術、手順 (TTP) をますます利用するようになってきています。

高度なランサムウェア攻撃を阻止するには、Microsoft Defender を 24 時間 365 日体制の人間主導の脅威検出と対応で、補完することが重要です。しかし、マイクロソフトのセキュリティ テクノロジーによって生成される膨大な量のアラートと、脅威環境の複雑さのために、セキュリティ運用はほとんどの企業にとってリソースを浪費する困難な作業となっています。

その結果、企業や組織は Microsoft Defender を強化するために、世界で最も信頼され、最も高く評価されている管理型検出と対応 (MDR) プロバイダーであるソフォスを頼ることが増えています。ソフォスのアナリストは、マイクロソフトのセキュリティ アラートを 24 時間 365 日監視し、優先順位を付けて対応し、確認された脅威を阻止するために直ちに措置を講じます。また、ソフォスのアナリストはソフォス独自の検出、脅威インテリジェンス、人間主導の脅威ハンティングを使用して、Microsoft Defender では検出されないような脅威も検出して阻止します。

Sophos MDR は、既存の IT 投資とセキュリティ投資、および社内リソースと連携して、お客様の所在地に関わらず対応できるように設計されています。社内セキュリティチームを付加的な専門知識を補完したり、24時間対応のサイバーディフェンスを拡張したり、脅威検出と対応を完全に外部に委託したりする場合でも、Sophos MDR は優れたサイバーセキュリティの成果を達成するのに役立ちます。

Sophos MDR で Microsoft Defender の強化

✓ サイバーリスクの低減

- Microsoft Defender を回避する人間主導の脅威など、高度なランサムウェア攻撃や侵害を阻止

✓ セキュリティ投資の効果と効率を高める

- 戦略的プログラムを提供するため、IT リソースを有効活用する
- 重大なインシデントに復旧コストが発生する可能性を軽減する
- 今までの投資から、今まで以上の利益を得る

✓ 保険の適用可能性を向上させる

- サイバーリスクの軽減を認識し、報酬を与える、改善された保険オファーへのアクセスを得ることができます。

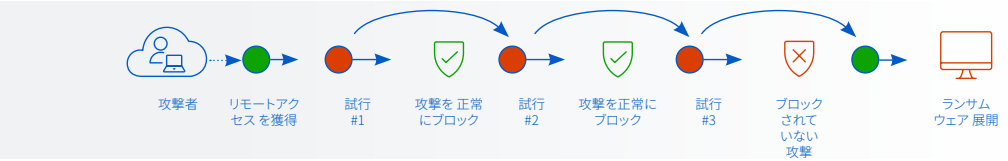
敵は侵入するのではなく、ログインするのだ。

実際、Microsoft Defender を含むテクノロジー ソリューションだけではすべてのサイバー攻撃を防ぐことはできません。アクティブアドバーサリ(アクティブな脅威行為者)は、セキュリティ技術や防御側による行動に応じて、リアルタイムに実際にキーボード操作による対応として、その場の状況に応じて、戦術、技術、手法 (TTP) を適応させ、検出を回避する手段として行動する脅威行為者です。

アクティブな脅威行為者による攻撃により、壊滅的なランサムウェアやデータ侵害のインシデントにつながることも多く、防止することも最も困難な攻撃の 1 つです。また、この攻撃は広く蔓延しており、中小企業の 23% が昨年中にアクティブな脅威行為者による攻撃を経験したと報告しています。こういった攻撃による壊滅的な被害の可能性を反映して、IT/サイバーセキュリティのリーダーの 30% は、アクティブな脅威行為者が 2023 年の最大のサイバー脅威の 1 つであると考えています[1]。

セキュリティ技術でブロックするだけでは、アクティブな脅威行為者の阻止には十分ではありません。これらの特殊技術を身に付けた執拗な攻撃者は、目的を達成するために次のような複数の革新的なアプローチを展開します。

- 認証情報の盗難、パッチが適用されていない脆弱性、セキュリティツールの設定ミスなど、セキュリティの弱点を悪用して敵が組織に侵入し、ネットワーク内に入ると、次に横方向に移動
- PowerShell、PsExec、RDP など、防御側が検出のトリガーを回避するために使用する正規の IT ツールを悪用する
- セキュリティ制御に対応してリアルタイムで攻撃を修正し、目標を達成する方法が見つかるまで、新しい技術に枢軸を置き続ける。



アクティブな脅威行為者による攻撃戦略の例

匿名化されたユーザーをエミュレートし、組織の防御の弱点を利用することで、悪意のある攻撃者は、自動検出技術が正規ユーザーと攻撃者を区別するのに四苦八苦している間に自動検出技術によるトリガーを回避できてしまいます。

防御側の課題をさらに複雑にしているのは、こんにちの潤沢な資金を持つ敵対者もまた、ビジネス モデルの革新と進化を続けている、という事実です。ランサムウェア・アズ・ア・サービスやフィッシング・アズ・ア・サービスなどのサイバー犯罪モデルが近年、急速に成長しているため、脅威アクター候補が参入する際の壁が低くなり、そのため大規模な攻撃の実行が容易になり、攻撃の質も向上させています。

脅威におけるこうした進展の結果、ランサムウェアによるデータ暗号化率は現在史上最高となっており、サイバー犯罪者は攻撃の 4 分の 3 (76%) 以上でデータの暗号化に成功しています[2]。

ランサムウェアの実態

- 2017年の 1年間にランサムウェア攻撃を受けた企業の割合は 66%
- ランサムウェア攻撃の 76% はデータ暗号化につながる
- データが暗号化された攻撃の 30% ではデータも盗まれていた
- 攻撃の根本原因 1 位: 脆弱性の悪用 (36%)
- 攻撃の根本原因 2 位: 認証情報の漏洩 (29%)

1 サイバーセキュリティの現状 2023年版：脅威行為者の事業への影響、ソフォス
2 ランサムウェアの現状 2023,年版、ソフォス

24 時間 365 日体制の脅威の検出と対応: 現代のサイバーセキュリティに欠くことができないもの

テクノロジーと人間の専門家を結集すれば、人間主導の高度な攻撃を阻止できます。敵対者が行動を起こす都度、シグナルが生成されます。人間の専門知識と、高度な AI を搭載した機械学習モデルおよび拡張された検出および対応 (XDR) ツールを組み合わせることで、セキュリティ アナリストはセキュリティおよび IT テクノロジーからのシグナルを活用し、最も高度な人間主導の攻撃でさえ、検出、調査、無力化し、ランサムウェアとデータ漏えいを防ぐことができます。

24 時間 365 日体制の脅威の検出と対応は、現在あらゆるサイバーセキュリティ スタックに必要不可欠なものとなっていますが、ほとんどの組織はそれを効果的に実現できずにおり、攻撃の危険にさらされています。こういった点にうまく対応する上で、最も一般的な 2 つの障壁は、専門知識の欠如と能力不足です。

問題 1: 専門知識の欠如

脅威の検出、調査、そして対応は、高度に専門化されたアクティビティであり、攻撃手法と調査戦略に関する深い知識に加え、防御側が使用するツールを使いこなすことが必要です。この複雑な (かつ高価な) スキルの組み合わせを社内に確保している組織はほとんどなく、93% が重要なセキュリティ運用タスクの実行が困難であると感じていると認めています。

- 71% は、ノイズからシグナルを識別するのが難しいと感じている (つまり、どのシグナル/アラートを調査すればよいのかを理解するのが難しい) と回答
- 71% は、シグナルが悪意あるものなのか無害なものであるかを識別するために十分なデータを取得することが難しいと回答
- 75% は、インシデントの根本原因 (敵対者がどのように組織に侵入したか) を特定するのが難しいと回答

防御側がサイバーセキュリティ ツールから受け取るデータを見れば、この課題の甚大さが明らかです。この表には、Microsoft Defender イベントと、イベント カテゴリのリストが含まれています。ただしこの表にはすべてが含まれているわけではありません。

アラートの理解は、脅威の検出と対応プロセスの一部にすぎません。防御側は、脅威を完全に理解し、最適な行動方針を特定できるように、状況に応じた洞察と脅威インテリジェンスを適用する必要があります。

イベントのタイトル	イベントの種類
疑わしい URL がクリックされた	初期アクセス
3CXDesktopApp.exe プロセスに関連する、悪意のあるファイルまたはネットワーク接続	マルウェア
新規にユーザーアカウントが作成された	常駐
TS_BL_Suspicious イベントログのクリアまたは Wevtutil を使用した構成	防御回避
権限昇格を処理する	権限昇格
Microsoft Defender マルウェア対策をオフにされた	防御回避
脅威アクター Storm-0867 に関連するファイルまたはネットワーク接続が検出された	資格情報へのアクセス
TS_BL_Script エンジンがインターネットに接続中	コマンド&コントロール
人間が操作する、潜在的に悪意のある活動	疑わしい活動
TS_BL_Malicious オフィス バイナリ経由のペイロードのダウンロード	実行
新たな脅威アクティビティ グループ DEV-0867 が検出された	資格情報へのアクセス
新たな脅威アクティビティ グループ Citrine Sleet が検出された	マルウェア

Microsoft Defender からのケース作成検出の例(本来英語ですが理解を深めるために意図的に翻訳しています)

問題 2: 能力不足

脅威の検出、調査、対応は時間のかかる作業です。この点を例証すると、アラートの検出、調査、対応にかかる時間の中央値は、従業員数 100 ～ 3,000 人の組織では 9 時間ですが、従業員数が 3,001 ～ 5,000 人の組織では 15 時間に上昇します。

セキュリティ アラートの処理には、膨大な IT 時間が費やされますが、作業には緊急性があるため、IT チームはより戦略的な課題への集中ができなくなる可能性があります。さらに、敵対者は昼夜を問わず攻撃を実行するため、効果を最大なものとするには、脅威の検出と対応を 24 時間 365 日実行する必要があります。ほとんどではないにしても、多くの組織は、必要なリソースの確保に苦労しています。

ソリューション: 管理型検出と対応 (MDR) による防御の補完

IT/サイバーセキュリティ リーダーの 52% が、組織が自力で対処するにはサイバー脅威が高度すぎると話しており、社内の機能を補完および拡張するために、ソフォスなどの管理型検出と対応 (MDR) の専門プロバイダーに頼ることが増えています。

MDR の定義

管理型検出と対応 (MDR) は、技術的解決策だけでは防ぐことができないサイバー攻撃の検出と対応を専門とする専門家が提供する、完全管理型の 24 時間年中無休のサービスです。

拡張検出および対応 (XDR) は、複数のソースからのセキュリティ データを統合して、隔離ポイント ソリューションではできない方法で、脅威の検出、調査、対応を自動化および高速化するプラットフォームです。

Sophos MDR アナリストは、Sophos XDR プラットフォームを活用して、お客様に代わって脅威を捕まえ、調査、無力化します。Sophos MDR アナリストは、ファイアウォール、電子メール、クラウド、モバイル セキュリティ ソリューションなどの IT スタック全体からのシグナルを活用して、脅威の検出と対応にかかる時間を短縮します。

Sophos MDR で Microsoft Defender の強化

Sophos MDR は、Microsoft Defender 環境に、実証済みの 24 時間 365 日体制の脅威の検出と対応を提供します。ソフォスのアナリストは、マイクロソフトのセキュリティ アラートを 24 時間 365 日監視し、優先順位を付けて対応し、確認された脅威を阻止するために直ちに措置を講じます。また、ソフォスのアナリストはソフォス独自の検出、脅威インテリジェンス、人間主導の脅威ハンティングを使用して、Microsoft Defender では検出されないような脅威も検出して阻止します。

より多くの情報を得ることで、より迅速に行動することができます。Sophos MDR は、E3 および E5 ライセンスに含まれる追加の マイクロソフト セキュリティ イベント ソースと、サードパーティのファイアウォール、クラウド、電子メール、ID、およびネットワーク検出と対応 (NDR) への投資からのシグナルを利用して、脅威の検出と対応にかかる時間を短縮します。

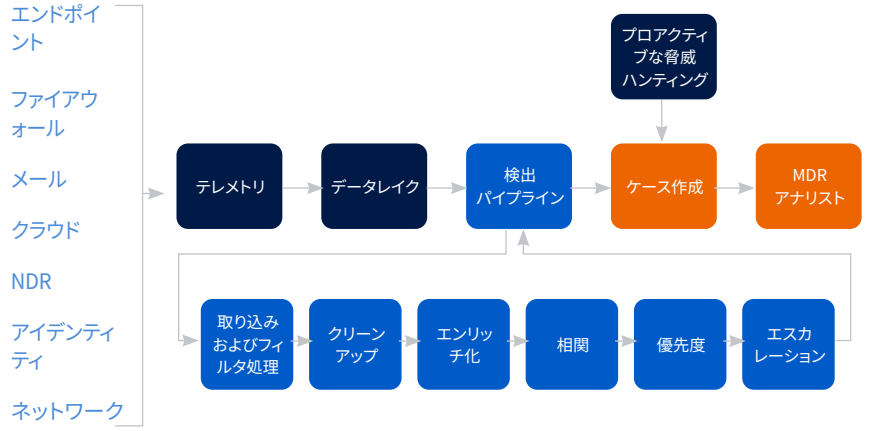
Microsoft Defender ユーザーは、ソフォスのセキュリティ運用専門家に 24 時間 365 日電話ですぐにアクセスできるほか、Sophos Central プラットフォームにおける脅威アクティビティに関する詳細なレポートを利用できます。

Sophos MDR for Microsoft Defender は、Microsoft Security Event Sourcesと互換性がある

- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- MS O365 セキュリティおよびコンプライアンス センター
- Microsoft Azure Sentinel
- Office 365 管理アクティビティ (統合監査ログ)

Sophos MDR のセキュリティイベントフロー

ソフォスの特許取得セキュリティイベントフローは、Sophos MDR サービスの主要な要素です。Microsoft Defender を含む、セキュリティ環境全体からのテレメトリは、ソフォスのデータレイクに取り込まれ、その後検出パイプラインを経由して処理されます。このパイプラインは、マイクロソフト やサードパーティの大量のアラートを、効率的に調査し対応できるように、使いやすく、優先度の付いた洞察に変換します。



Sophos MDR のセキュリティイベントフロー

取り込みおよびフィルタ処理 – テレメトリを取り込み、不要なノイズをろ過する

クリーンアップ – データを正規化されたスキーマに変換し、MITRE ATT&CK®にマップする

エンリッチ化 – 付加的なサードパーティの脅威インテリジェンスと業務コンテキスト情報を追加する

相関 – エンティティに基づいたクラスタアラート、MITRE ATT&CK のカテゴリ化、および時間

優先度 – 優先順位をつけるため、アラートやクラスタにスコアを付けてランク付けする

エスカレーション – クラスタを調査対象のケースにエスカレーションするためにロジックを適用する

24時間365日体制で、7 つのグローバルセキュリティ運用センター（SOC）から対応

脅威は、北米 (インディアナ、ユタ、ハワイ)、欧州 (イギリス/アイルランド、ドイツ)、アジア太平洋 (インド、オーストラリア) にまたがる 7 つのグローバルセキュリティ運用センター (SOC) に所属する、脅威検出および脅威対応のグローバルチームによって調査・修復されます。Sophos MDR には、マルウェア、自動化、AI、修復の専門家を含む、500人以上の専門家が脅威環境全体をカバーしており、これほど広範かつ奥深い専門知識を社内に配置するのはほとんど不可能です。

世界をリードする検出時間と対応時間

人間、技術、および脅威に関する専門知識。これらのユニークな組み合わせにより、Sophos MDR は世界をリードするインシデント対応時間わずか 38 分を実現しています。そのため、優れたサイバーセキュリティの成果をもたらします。

- 検出にかかる時間の中央値 (MTTD)　1分
- 調査にかかる時間の中央値 (MTTI)　25分
- 対応にかかる時間の中央値 (MTTR)　12分

Sophos MDR の利用者

IT リソースが限られている中小企業から、社内に SOC グループを持つ大企業に至るまで、あらゆるセクターの何千もの組織が Sophos MDR サービスを使用しています。最も人気がある Sophos MDR 対応モデルは次の 3 つです。

- 顧客に代わって Sophos MDR で脅威への対応を完全管理
- 社内チームと連携し、Sophos MDR で脅威への対応を共同管理
- Sophos MDR で、社内チームをサポートおよび補完し、注意が必要なインシデントを警告し、脅威に関する洞察と修復ガイダンスを提供

脅威ケース: Microsoft Defender を活用しコマンド アンド コントロールを検出

業界
プロフェッショナルサービス

本社
米国

従業員数
750 名

サービス階層
Sophos MDR for Microsoft Defender

SOPHOS MDR 統合テレメトリ ソース

- ✓ エンドポイント
- X アイデンティティ
- ✓ ファイアウォール
- X クラウド
- X メール製品サポート終了日
- ✓ ネットワーク製品サポート終了日

コマンド & コントロールとは?

コマンド & コントロール (C&C または C2 とも呼ばれる) は、攻撃者が標的のネットワーク内の制御下にあるシステムと通信し、コマンドを送信するために使用する攻撃手段で構成されます。

標的の環境と攻撃者のインフラストラクチャの間と、コマンド & コントロールのチャネルは、フィッシング メール、ソーシャル エンジニアリング、マルウェア、ブラウザ プラグインにある穴など、さまざまな方法で確立できます。脅威行為者は、検出されたり疑いをかけられることを避けるために、一般に利用可能なリソースを使用し、予想されるネットワーク トラフィックを模倣することがよくあります。

検出

Microsoft Defender は、悪意のある IP アドレスに対する通信にアラートを生成します。

マイクロソフト セキュリティ アラートは、自動的に Sophos XDR データレイク内のイベントと相関し、お客様のファイアウォールにより攻撃がブロックされたかどうか、および複数のエンドポイントに影響が及んでいるかを判断します。

調査

Sophos MDR のアナリストは、Microsoft Defender アラートに関連付けられている悪意のある接続がブロックされ、差し迫った脅威が阻止されたことを確認します。

この攻撃のファミリー、感染の痕跡 (IOC)、攻撃者が使用した既知の IP とドメインを特定するため、SophosLabs Intelix が使用されます。

オリジナルの マイクロソフト アラートは、この脅威インテリジェンスでエンリッチ化されるため、根本原因分析に使用できます。

対応

危険にさらされたデバイスは隔離され、攻撃は阻止されます。

Sophos MDR は、電子メール フィッシングによって初期アクセスが達成されたことを確認します。フィッシング メールの構成を特定する調査が実行され、他のユーザー アカウントが危険にさらされていないことを確認します。

ソフォスは、今後フィッシング攻撃が成功する可能性を低減するための奨励事項を提供します。

サービスを利用するメリット

社内のセキュリティ運用チームを補完・サポートしたい場合でも、自社の SOC を立ち上げる手間をかけずに 24 時間 365 日体制の専門家主導の検知と対応を利用したい場合でも、Sophos MDR がそのお手伝いをします。Sophos MDR を使用して Microsoft Defender を強化している組織は、サイバーリスクの削減、セキュリティ投資の効率と効果の向上、保険の適用可能性の改善などの優れた成果を享受できます。

Microsoft + Sophos MDR で高度な脅威を阻止する

専門家チームによる 24 時間 365 日体制の監視および対応
Sophos MDR アナリストは、Microsoft Defender のアラートを 24 時間 365 日監視し、優先順位を付けて対応し、確認された脅威を阻止するために直ちに措置を講じます。

Microsoft Defender を回避する脅威を検出し、阻止
ソフォス独自の検出、脅威インテリジェンス、人間主導の脅威ハンティングにより、追加の防御層が追加されます。

可視性を強化し、Microsoft Defender アラートの状況を把握
E3 または E5 ライセンスに含まれる、追加の マイクロソフト セキュリティ イベント ソースを統合します。

セキュリティ オペレーションの専門家に直ちにアクセス
Sophos MDR のアナリストは、24 時間 365 日体制で電話対応しており、脅威アクティビティに関する詳細なレポートも Sophos Central からご利用いただけます。

サイバーリスクの削減

Sophos MDR で Microsoft Defender を強化することの主な利点の 1 つは、ランサムウェアやその他の高度なサイバー脅威に対する保護が強化されることです。

ソフォスのアナリストは、広範かつ奥深い経験をもっているだけではなく、テレメトリおよび脅威ハンティングツールの使用も堪能にこなします。これらは社内での再現がほとんど不可能です。これにより、潜在的なインシデントの調査につながる重要な信号の特定から、悪意のあるアクティビティの無力化に至るまで、プロセスのあらゆる段階で迅速かつ正確に対応できるようになります。

Sophos MDR は他のプロバイダーのどこよりも多くの組織を保護しているため、比類ない「コミュニティ免疫」が提供できるのです。ひとつの顧客を防御する際の情報は、似たようなプロファイルを持つ他のすべての顧客に自動的に適用されます。これにより、そのコミュニティにおいて同様の攻撃を予防的に防ぐことが可能となります。

★★★★★

「ペンテスターは、脆弱性が見つからなかったことに感動していました。その時に、ソフォスのサービスは絶対に信頼できると確信しました。」
オーストラリア、サザンクイーンズランド大学

★★★★★

「Sophos MDR のおかげで、脅威への対応時間が大幅に短縮されました。」
インド、Tata BlueScope Steel 社

★★★★★

「リアルタイムで脅威の通知を受信します。」
イタリア、Bardiani Valvole 社

セキュリティ投資の効率と効果を高める

Sophos MDR は、お客様のスタッフやセキュリティツールの効率と効果を向上させることができます。

脅威の検出と対応には、膨大な IT リソースを消費します。Sophos MDR はこの負担を引き受け、戦略的なプログラムの実行に貴重な IT リソースを解放します。同時に、ソフォスのセキュリティ運用の専門家による 24 時間 365 日対応の電話対応と、Sophos Central プラットフォームを通じた脅威アクティビティの詳細な報告により、社内チームはアラートに対してより迅速かつ正確に対応できるようになります。

Sophos MDR は、既存の マイクロソフト およびサードパーティのセキュリティツールからテレメトリ情報を活用し、脅威の検出と対応にかかる時間を短縮化することで、防御力を向上させ、それと同時に既存の投資による収益を増加させます。

さらに、ランサムウェア攻撃を修復するための平均請求額は現在 185 万ドルとなっており、ランサムウェア被害者の 84% が、攻撃によりビジネスや収益を失ったと回答しているため[2]、Sophos MDR などのサービスに投資することでサイバーセキュリティ全体の TCO が削減されます。

★★★★★

「ソフォスを導入して以来、運用時間を大幅に短縮することができたため、学生の満足度を高める取り組みに注力できるようになりました。」

英国、ロンドン・サウスバンク大学

★★★★★

「Sophos MDR は脅威を迅速に修正または削除し、注意を喚起することができるたえ、価値の高い作業に集中することができます。」

オーストラリア、Tomago Aluminium 社

保険性を向上させる

Sophos MDR を使用すると、組織は、24 時間 365 日体制の検出と対応、サイバーインシデント対応計画、ログ記録と監視、その他を含む、保険性や優れた保険提供の鍵となるサイバー制御の多くを実現できます。

Sophos MDR 利用者は、サイバーリスクが軽減されたため、これを認識して報酬を与える保険だけでなく、よりよい保険の利用ができるようになったと報告しています。

★★★★★

「当社で下した、XDR および MDR でソフォスと提携するという決定は、サイバーセキュリティ保険料の削減を達成する上で大きな要因でした。この業界に踏み込むと、保険料は 2 倍になると言われていたんです。これは真の価値を示す素晴らしい勝利です... 実際、CFO から私たちのチームが上げた成果に感謝するメモを受け取りました。MDR に負うところは大きいです。」

Bob Pellerin、CISO、The Fresh Market、米国

2 ランサムウェアの現状 2023,年版、ソフォス

世界で最も信頼されている MDR サービス

ソフォスは世界第一位の MDR プロバイダーであり、他のベンダーよりもはるかに多い組織を、ランサムウェア、侵害、およびその他のテクノロジーだけでは阻止できない脅威から保護しています。

Sophos MDR は、世界中のあらゆる業界の何千もの組織を保護しているため、それぞれの分野が直面している脅威について、比類のない深みと広範な専門知識が構築できています。ソフォスは、この広範なテレメトリを活用して「コミュニティ免疫」を生成し、ある組織の防御から学んだことを同様のプロファイルを持つ他のすべての顧客に適用することで、皆様の防御を強化します。

もちろん、最も重要なことは、ソフォスがお客様に提供するサイバーセキュリティの成果です。ソフォスは、2023 年 6 月 14 日現在、Gartner® Peer Insights™ で最高評価かつ最もレビューされた MDR ソリューションで、300 件のレビューで 4.8/5 の評価を受けています。また、顧客の 97% がソフォスを推薦しています。

また、ソフォスは、G2 Grid® レポートにおいては管理型検出と対応 (MDR) におけるリーダーとして指名されているだけではなく、G2 全体、中堅企業、および大企業といった各セグメントにおいても MDR のリーダーとされています。

最高の信頼性

17,000 社を超える組織が Sophos MDR を使用 (2023 年第 2 四半期)

もっとも高い評価

個々のカスタマー評価で 4.8/5 の評価を受ける

もっとも多いレビュー数

過去 12 か月間に Gartner Peer Insights で 300 件のレビューを受ける

Sophos MDR の詳細と、Sophos MDR がどのように Microsoft Defender ユーザーのサイバー リスクを軽減し、セキュリティ投資の効率と効果を高め、保険性を向上させる方法に関する詳細は、www.sophos.com/mdr　をご覧ください

Sophos Endpoint Protection を知る

Sophos Intercept X Endpoint Protection は、お使いの方のために働き、そして機能します。その際は、攻撃への対応で防御を適応させます。

Sophos Intercept X Endpoint Protection は、強力かつ多層の防御機能を備えており、ランサムウェアや高度な脅威に対して攻撃チェーンのすべての段階で優れた保護を提供します。行動ベースのランサムウェアのロールバックや、60 種類のエクスプロイト防止もデフォルトで有効化されており、微調整は必要ありません。

ソフォスの革新的な Adaptive Attack Protection は、人間主導の攻撃に動的に対応し、自動的に付加的な防御策を展開して敵を撃退し、脅威行為者に対応するための時間を確保します。

Microsoft Defender を実行しているソフォスの MDR サービスを利用ユーザーは、いつでも Sophos Endpoint Protection に切り替えることができます。これにより、完全な柔軟性を持ちながら、将来に向けたセキュリティ導入が図れます。

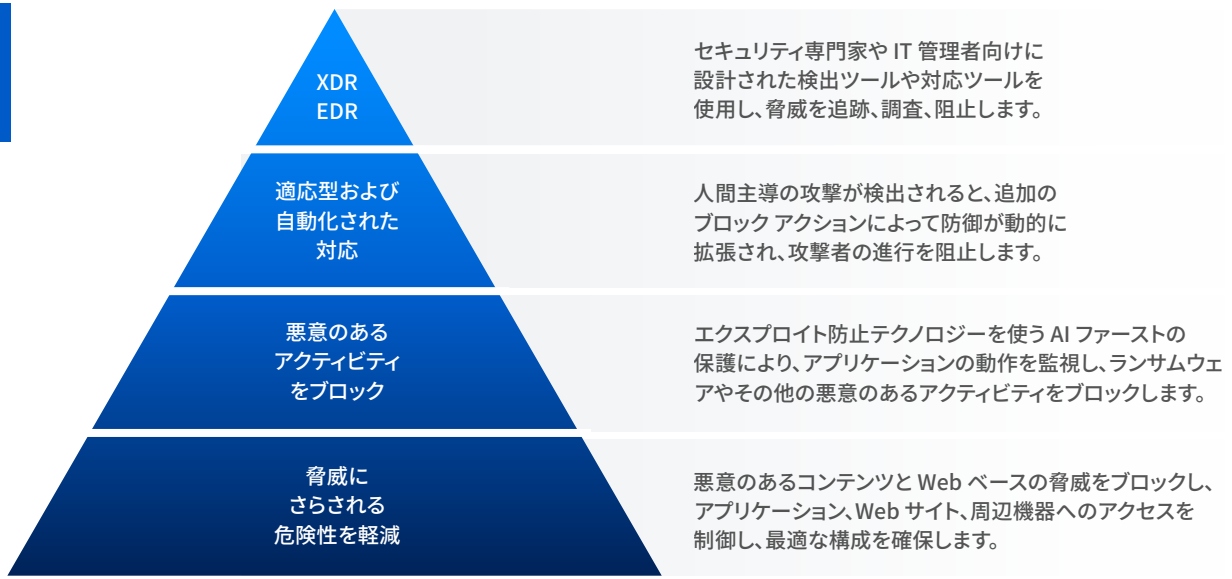
✓ Gartner のリーダー賞を連続 13 回受賞
2008 年以来、ソフォスは Gartner Magic Quadrant for EPP のすべてのレポートでリーダーと指名されています

✓ Gartner Peer Insights で最高評価を獲得
個々のカスタマー評価で 4.8/5 の評価を受けています

✓ G2 のリーダーとして、エンタープライズ、ミッドマーケット、SMB (中小企業) の全セグメントで認定
カスタマーレビューに則ったものです

✓ SE Labs による「100% Protection Score (保護スコア 100%)」
エンタープライズおよび小規模事業向けセキュリティにおいて、AAA の評価です

ソフォス製品の詳細と、無償評価版の試用のアクティベーションについては、www.sophos.com/endpoint をご覧ください。



Gartner® “Magic Quadrant™ f or Endpoint Protection Platforms” By Peter Firstbrook, Chris Silva, 31 December 2022
GARTNER, MAGIC QUADRANT または Gartner Peer Insights は、Gartner Inc. または関連会社の米国およびその他の国における登録商標およびサービ スマークであり、同社の許可に基づいて使用しています。All rights reserved.
GARTNER は、Gartner リサーチの発行物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。また、最高のレーティング又はその他の評価を得たベンダーのみを選択するように助言するものではありません。Gartner リサーチの発行物は、Gartner リサーチの見解を表したものであり、事実を表現したものではありません。GARTNER は、明示または黙示を問わず、本リサーチの商品性や特定目的への適合性を含め、一切の保証を行うものではありません。
Gartner Peer Insights のコンテンツは、独自の経験に基づいた個々のエンドユーザーの意見で構成されており、事実を示すものではありません。また、Gartner やその関連会社の見解を表すものでもありません。Gartner は、本コンテンツに記載されているベンダー、製品、サービスを保証するものではなく、本コンテンツに関して、商品性や特定目的への適合性を含む正確性または完全性について、明示的または黙示的に保証するものでもありません。

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。

2023-06-27 (WP-NP)

SOPHOS