ソリューションカタログ

Sophos Endpoint

Intercept X テクノロジーを活用

AI を活用した高度なエンドポイントセキュリティソリューション

Sophos Endpoint は Intercept X テクノロジーを活用して最高レベルの保護を提供し、高度な攻撃を食い止めてシステムへの影響を未然に防ぎます。強力な EDR/XDR (Endpoint and eXtended Detection and Response) を使って、組織は疑わしいアクティビティや攻撃の兆候を追跡、調査し、対応できます。

予防重視のセキュリティへのアプローチ

Sophos Endpoint は、1 つのセキュリティテクノロジーに依存することなく、予防を重視しながら包括的なアプローチに基づいて脅威をブロックします。複数のディープラーニング AI モデルが、既知の攻撃や未知の攻撃から組織を保護します。Web、アプリケーション、周辺機器コントロールにより、脅威対象領域を縮小し、一般的な攻撃をブロックします。行動分析、ランサムウェア対策、エクスプロイト対策など、高度なテクノロジーを組み合わせて、脅威を早い段階で阻止して進行を食い止めます。結果として、調査・解決を要するインシデントが少なくなり、少人数の IT スタッフでも対処することが可能となります。

徹底的なランサムウェア対策

Sophos Endpoint は、突出した堅牢性およびゼロタッチのエンドポイント防御を提供し、高度なランサムウェアにも対応します。CryptoGuard テクノロジーによって、悪意のある暗号化をリアルタイムで阻止し、変更されたファイルを自動的に元の状態にロールバックして、ビジネスへの影響を最小限に食い止めます。

適応型の防御機能

アクティブな攻撃者やハンズオンキーボード攻撃に対して適応する業界初の動的な防御です。これにより、攻撃者の操作能力が失われ、攻撃を妨害して封じ込めると同時に、対応するための貴重な時間を確保できます。

セットアップと管理が簡単

Sophos Central は、ソフォスのあらゆる次世代型セキュリティソリューションを統合できる、クラウドベースのパワフルなサイバーセキュリティ管理プラットフォームです。推奨されるテクノロジーと機能はデフォルトで有効になっており、調整することなくすぐに最強の保護を利用できます。

エンドポイントセキュリティの分野で信頼される業界のリーダー企業

Sophos Endpoint は、お客様、アナリスト、そして独立系テスト機関から常に高い評価を得ています。ソフォスは、Gartner® Magic Quadrant™ のエンドポイントプロテクションプラットフォーム部門でリーダーの評価を 15 回獲得しているほか、2025 年冬期の G2 Grid® レポートでは、エンドポイントプロテクションスイート部門で第 1 位を獲得しています。

主な特長

- 複数のディープラーニング AI モデルが、既知の攻撃や未知の攻撃から組織を保護します。
- Web、アプリケーション、および周辺機器の制御により、攻撃対象領域を縮小し、一般的な攻撃経路をブロックします。
- 行動分析、ランサムウェア対策、エクスプロイト対策、その他の高度なテクノロジーにより、脅威が拡大する前に迅速に阻止します。
- 業界トップレベルの保護機能により、ローカルおよびリモートのランサムウェア攻撃からデータを保護します。
- アクティブな攻撃者やハンズオンキーボード攻撃に自動的に対応する、業界初の動的な防御です。
- 強力な EDR ツールおよび XDR ツールにより、不審なアクティビティを探し出し、調査し、対応します。

予防重視のアプローチにより、攻撃対象領域を縮小

攻撃を早期に阻止することは、攻撃チェーンの後半で攻撃を監視して修復することよりもリソースの消費が少なくなります。Sophos Endpoint には、広範な攻撃をブロックする高度な保護テクノロジーが搭載されています。Web、アプリケーション、および周辺機器を制御することで、攻撃対象領域を縮小し、一般的な攻撃経路をブロックします。これにより、攻撃者がお客様の環境に侵入する機会を減らします。

Web プロテクション

悪意のある Web サイトへのアウトバウンドブラウザトラフィックをブロックすることで、配信段階で脅威を阻止し、フィッシングサイトやマルウェアサイトを防ぎます。

Web コントロール

望ましくないコンテンツや不適切なコンテンツへのアクセスをブロックします。Web サイトの閲覧制限を組織全体に適用し、データ損失を防止します。

ダウンロードレピュテーション

SophosLabs のグローバル脅威インテリジェンスを使用して、ダウンロードされたファイルを分析し、感染率、経過時間、ソースに基づいて判定を行い、レピュテーションが低いファイルや不明なファイルをブロックするようにユーザーに促します。

アプリケーションコントロール

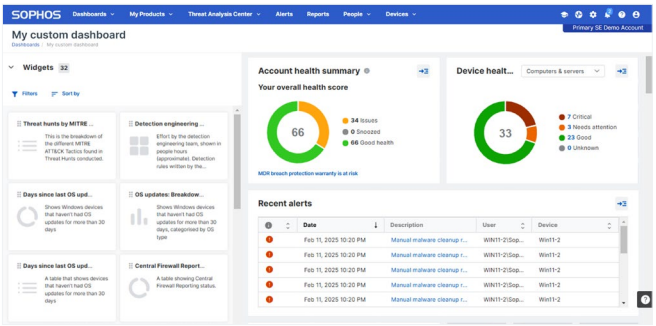
脆弱なアプリケーションや不適切なアプリケーションを事前定義したカテゴリに基づいてブロックするため、ハッシュで個別にアプリケーションをブロックする必要がありません。

周辺機器 (デバイス) コントロール

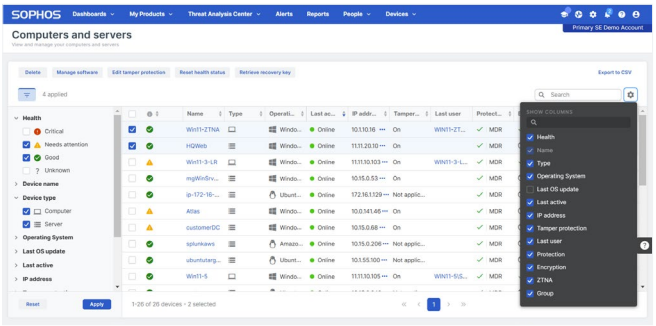
リムーバブルメディア、Bluetooth、モバイルデバイスへのアクセスを監視およびブロックして、特定のハードウェアがネットワークに接続できないようにすることができます。

データ損失防止

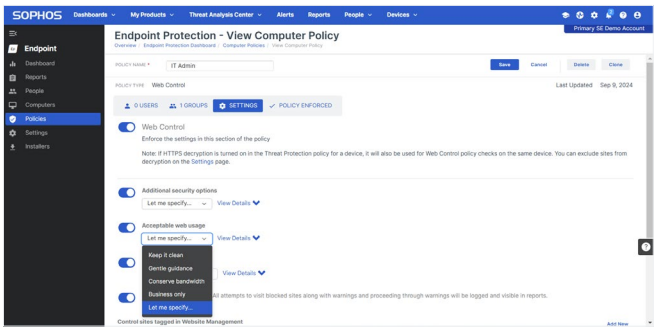
機密データを含むファイルの転送を監視または制限します。たとえば、ユーザーが Web ベースのメールを使用して、機密ファイルを送信できないようにします。



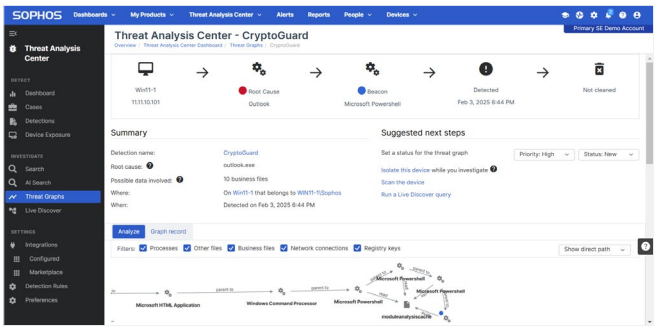
ニーズに合わせてカスタムダッシュボードを作成。



セットアップと管理が容易なエンドポイントセキュリティ。



推奨設定がデフォルトで有効になっている構成可能なポリシー。



脅威を分析し、根本原因を特定。

予防重視のアプローチで脅威を迅速に阻止

脅威をできるだけ早く検出して修復することで、リスクを低減できます。Sophos Endpoint は、脅威が拡大する前にその脅威を迅速に阻止するので、リソースに余裕のない IT チームが調査・解決しなければならないインシデントを削減できます。ソフォスが提供する強力な脅威防御機能は、独立機関によるセキュリティテストで常にトップスコアを獲得しています。

徹底的なランサムウェア対策

「Microsoft デジタル防衛レポート 2024」によると、現在、成功した攻撃の 70% でリモート暗号化が確認されており、その 92% はネットワーク内の管理されていないデバイスで発生しています。Sophos Endpoint は、ローカルおよびリモートのランサムウェアに対する最強のゼロタッチ防御をエンドポイントに提供し、高度な CryptoGuard テクノロジーを活用して、暗号化の試みを (そのソースに関係なく) 検出します。

- 新しいランサムウェアの亜種をブロックします。
- ファイルの変更をリアルタイムで検査し、悪意のある暗号化を検出します。
- リモートのランサムウェアがネットワーク経由でファイルをリモート暗号化するのを防止します。
- Windows シャドウコピーサービスに依存しない独自テクノロジーを使用して、暗号化されたファイルを暗号化されていない元の状態に自動的にロールバックします。
- パフォーマンスへの影響を最小限に抑えながら、すべてのタイプとサイズのファイルを保護します。
- ハードディスクを標的とした高度な攻撃からマスターブートレコード (MBR) を保護します。

AI を活用したディープラーニングによるマルウェア対策

ファイルの属性を分析し、予測推論に基づいて脅威を特定することにより、既知のマルウェアと未知のマルウェアを検出しブロックします。

エクスプロイト対策

メモリのハードニングと 60 以上の悪用防止技術により、プロセスの整合性を保護します。チューニングは不要で、Windows ネイティブの機能や他のセキュリティソリューションを凌駕します。

動作検知

プロセス、ファイル、レジストリのイベントを監視し、悪意のある活動を検出して阻止します。メモリのスキャンと実行中プロセスの検査によって隠れている脅威を検出し、検出回避のために悪意のあるコードを注入する攻撃者を検出します。

Synchronized Security

Sophos Endpoint は、ステータスおよびセキュリティ状態を Sophos Firewall、Sophos ZTNA (Zero Trust Network Access) やその他のソフォス製品と共有し、脅威およびアプリケーションの使用状況を徹底的に可視化して、感染デバイスを自動的に隔離します。

Live Protection

SophosLabs のグローバル脅威インテリジェンスをリアルタイムで検索し、追加のファイルコンテキスト、判定検証、誤検出の抑制、ファイルレピュテーションを実現することで、強力なオンデバイス保護を拡張します。

アプリケーションロックダウン

一般的にこれらのプロセスに関連付けられていないアクションをブロックすることで、ブラウザやアプリケーションの誤用を防止します。

Antimalware Scan Interface (AMSI)

Windows Antimalware Scan Interface (AMSI) は、マルウェアがメモリから直接読み込まれるファイルレス攻撃をブロックします。Sophos Endpoint には、AMSI 検出の回避に対抗する独自の緩和策も搭載されています。

悪意のあるトラフィックの検出

ブラウザ以外のトラフィックを傍受して分析し、悪意のある送信先を検出することで、コマンドアンドコントロール (C2) サーバーと通信するデバイスを検出します。

適応型の防御機能

セキュリティ業界で初めて適応型の防御を組み込んだ Sophos Endpoint は、アクティブアドバーサリやハンズオンキーボード攻撃にリアルタイムで対応し、防御を自動化します。Sophos Endpoint は、通常業務で使用されることがある一般的な操作であっても、攻撃に転用される危険性がある場合はブロックします。攻撃者がレッドフラグを立てたり悪意のあるコードを使用したりせずに、攻撃を進行させ足掛かりを築いている可能性のある場合に、この機能によって動的に対応して阻止します。

適応型攻撃防御 (Adaptive Attack Protection)

ハンズオンキーボード攻撃が検出されると、エンドポイント上での防御強化が動的に有効になるため、攻撃を中断させ、対応により多くの時間を割くことができます。

重大な攻撃に関する警告 (Critical Attack Warning)

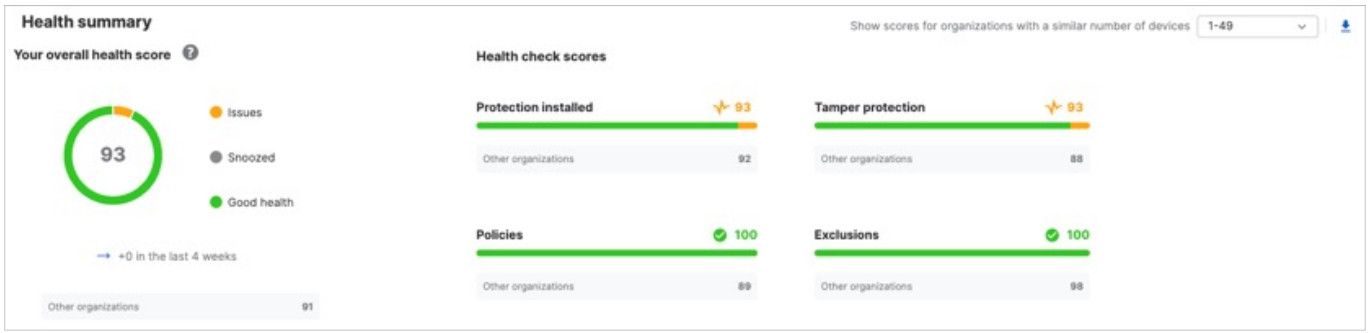
組織全体で検出された脅威に基づいて、複数のエンドポイントで進行中の深刻な攻撃を管理者に通知します。

	動作検知	適応型攻撃防御	重大な攻撃に関する警告
範囲	個々のデバイス	個々のデバイス	環境全体
特長	アクティブアドバーサリによる攻撃の初期段階を阻止する動作検出エンジン	保護の感度 (レベル) を高めて攻撃を防止	即時のインシデント対応が必要な攻撃を警告
トリガー	動作検出ルール	ハッキングツールセットの検出	組織レベルの相関関係やしきい値などの、影響の大きいアクティブアドバーサリの指標
アナロジー	「シールドオン！」	「シールドアップ！」	「レッドアラート！」

Sophos Endpoint における適応型の防御機能

セキュリティポスチャのずれやミスの特定

ポリシーや除外項目などの設定に不備があると、セキュリティ対策が甘くなる恐れがあります。アカウントの状態のチェックによって、セキュリティ対策の偏りやリスクの高い設定ミスを特定し、ワンクリックで問題を修正できるようにします。



アカウントの状態のチェック

追加の保護レイヤー (アドオン)

Sophos ZTNA

究極の VPN の代替機能でユーザーをアプリケーションに安全に接続します。Sophos ZTNA は、次世代型エンドポイントプロテクションと緊密に統合された唯一の Zero Trust Network Access ソリューションです。

デバイスの暗号化

デバイスの紛失や盗難は日常的に発生していることから、フルディスク暗号化は不可欠です。Sophos Endpoint にはデバイス暗号化機能が統合されており、BitLocker (Windows) または FileVault (macOS) を効果的に管理できます。

脅威の検出、調査、対応を加速化

Sophos Endpoint は、ほとんどの脅威を事前に自動ブロックするため、調査を必要とするイベント数を削減できます。不審な活動や、アナリストによる分析が必要な脅威に対しては、すべての主要な攻撃経路において迅速に検出、調査、対応するための強力なソリューションを提供します。

Sophos XDR

Sophos XDR (Extended Detection and Response) は、セキュリティ環境全体にわたって不審な活動や多段階攻撃を検出、調査して、対応できます。ソフォスの強力な生成 AI 搭載ツールは、あらゆるスキルレベルのユーザー向けにセキュリティアナリストが設計したもので、IT ジェネラリストからトップクラスの SOC アナリストまで、あらゆるユーザーが脅威を迅速に調査し、攻撃を無効化することができます。

Sophos XDR は、エンドポイント、ファイアウォール、ネットワーク、電子メール、アイデンティティ、生産性、クラウド、およびバックアップのソリューションの幅広いエコシステムとターンキー統合が可能であるため、既存のセキュリティツールの ROI (投資対効果) が向上します。

詳しくは Sophos.com/XDR をご覧ください。

Sophos MDR

Sophos MDR (Managed Detection and Response) は、脅威の検出と対応を管理するリソースを持たない企業向けに、経験豊富なセキュリティアナリスト、脅威ハンター、インシデント対応担当者で構成される精鋭チームが 24 時間 365 日体制で提供するサービスです。Sophos MDR は、ソフォスのセキュリティテクノロジーとサードパーティのセキュリティテクノロジーの両方から提供されるテレメトリを活用し、極めて巧妙な脅威も検出して無効化します。

Sophos MDR は、組織のニーズに合わせて複数のサービスレベルと対応モードを用意しているほか、既存のツールやテクノロジーとの互換性も備えています。

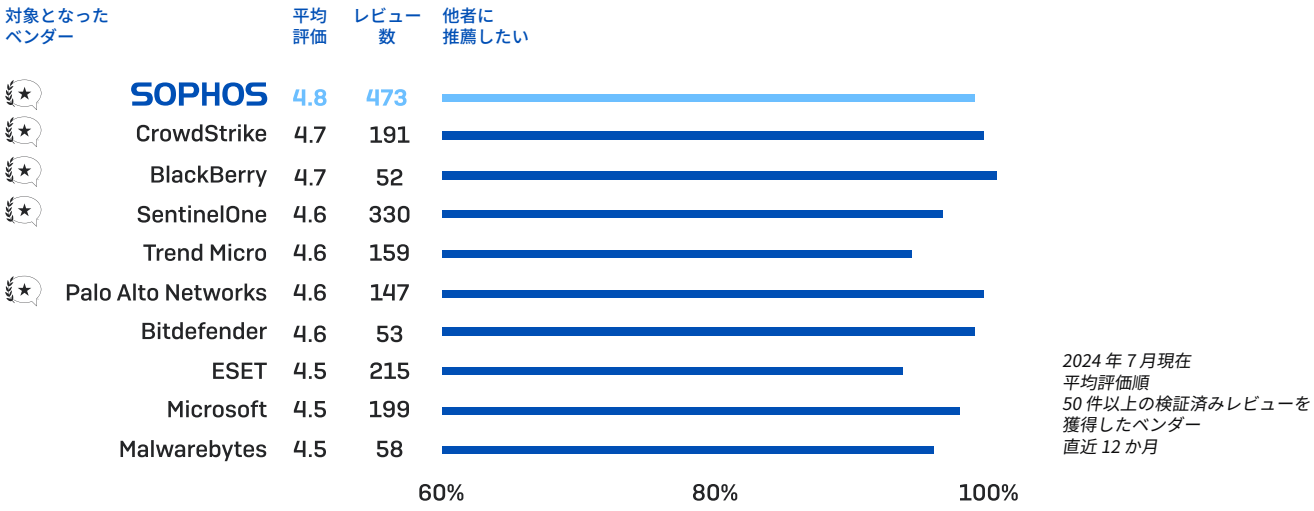
詳しくは Sophos.com/MDR をご覧ください。

	Sophos Endpoint	Sophos XDR	Sophos MDR
次世代型脅威対策 AI を活用したディープラーニングによるマルウェア対策、Web プロテクション	✓	✓	✓
悪意のある活動のブロック ランサムウェア対策、エクスプロイト対策、適応型防御	✓	✓	✓
脅威に晒されるリスクを軽減 DLP、Web、周辺機器、アプリケーションのコントロール機能	✓	✓	✓
検出と対応 強力な脅威調査・対応ツール		✓	✓
主要な攻撃対象領域の可視化 ソフォスとサードパーティのテクノロジー統合		✓	✓
Managed Detection and Response 24 時間 365 日体制の専門家による脅威監視とインシデント対応			✓

レビュー数、評価ともにトップのエンドポイントプロテクションソリューション

Gartner の「2024 年 Voice of the Customer (お客様の声)」レポートのエンドポイントプロテクションプラットフォーム部門において、ソフォスは全ベンダーの中で最も多くのレビューを獲得し、5.0 満点中 4.8 の評価を受けました。また、ソフォスは 2024 年のレポートに記載されている 11 種の業界すべてで、Customers' Choice に選ばれました。

エンドポイントプロテクションプラットフォーム



Sophos Endpoint が選ばれる理由

ソフォスは、エンドポイントセキュリティのリーディングカンパニーとして、業界で高く評価されています。

Gartner

ソフォスは、15 回連続で、2024 年 Gartner® Magic Quadran ™ for Endpoint Protection Platforms において、リーダーの 1 社との評価を獲得

SE Labs

ソフォスは、独立機関によるエンドポイントセキュリティテストにおいて、常に業界をリードする保護結果を達成

G2 Leader

2025 年冬期の G2 Grid® レポートでは、エンドポイントプロテクションスイート、EDR、XDR、ファイアウォールソフトウェア、MDR の各部門において、ソフォスがリーダーの評価を獲得

IDC

ソフォスは、2024 IDC MarketScape for Worldwide Modern Endpoint Security for Small and Midsize Businesses (中小企業を対象とした世界中の最新型エンドポイントセキュリティ製品の評価) でリーダーの評価を獲得

無償評価版

無償評価版の登録 (30 日間)　sophos.com/ja-jp/endpoint

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

2025-03-04 SB-JP (NP)