

Sophos Endpoint



セキュリティ侵害、ランサムウェア、データ流出を防止

Sophos Intercept X は、高度な攻撃に対して比類のない保護を提供します。幅広い高度なテクノロジーのパッケージを採用して、システムに影響を与える前に広範な脅威を阻止します。強力な EDR および XDR ツールにより、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。

予防第一のアプローチ

Intercept X は、1つのセキュリティ技術に依存することなく、エンドポイント保護への包括的なアプローチを採用しています。Web、アプリケーション、周辺機器をコントロールにより、攻撃対象領域を縮小し、一般的な攻撃をブロックします。脅威が拡大する前に、AI、行動分析、ランサムウェア対策、エクスプロイト対策、その他の最先端テクノロジーが脅威を阻止します。つまり、人手による調査や対処が必要なインシデントを減らし、リソースが限られている IT チームの負担を減らすことができます。

適応型の防御機能

これらの動的な防御機能は、業界初の取り組みです。攻撃のコンテキストに応じて自動保護機能を提供します。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、すべてのソフォス製品を管理するためのクラウドベースの管理プラットフォームです。ソフォスが推奨する保護テクノロジー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設定を利用できます。細かい制御設定も可能です。アカウントの状態チェックは、セキュリティ対策のずれとリスクの高い設定ミス特定し、管理者がワンクリックで問題を修正できるようにします。

Synchronized Security

Intercept X は、Sophos Firewall、Sophos ZTNA、およびその他の製品とステータスおよびセキュリティ状態の情報を共有して、脅威とアプリケーションの使用状況をさらに可視化します。Synchronized Security は、クリーンアップの実行中に侵害されたデバイスを自動的に隔離し、脅威が無力化されるとネットワークアクセスを自動的に復旧します。これらが管理者の介入なしで実現できます。

主な特長

- ▶ ディープラーニング AI を活用して未知の脅威を阻止
- ▶ ランサムウェアをブロックし、影響を受けたファイルを安全な状態にロールバック
- ▶ 攻撃チェーン全体で使用されるエクスプロイト手法と悪意のあるアクティビティを防止
- ▶ 変化する攻撃者の行動に合わせて自動的に防御を適応
- ▶ アプリ、デバイス、Web コントロールで、攻撃対象領域を削減
- ▶ ワンクリックの修正で、セキュリティ対策のずれとリスクの高い設定ミス特定
- ▶ EDR/XDR を使用して、ソフォスの脅威ハンティングと IT 運用セキュリティ予防策を実行
- ▶ フルマネージドサービスとして提供される24時間年中無休のセキュリティを提供
- ▶ リモートの作業環境でも、導入、設定、保守が簡単

ランサムウェアのブロック

Intercept X には、新しい亜種や未知のランサムウェアを阻止する高度なランサムウェア対策テクノロジーである CryptoGuard が含まれています。CryptoGuard は、ファイルの内容を検査して、ネットワーク上で実行されている暗号化とランサムウェアを検出します。ランサムウェアによって暗号化されたファイルは、サイズやファイルの種類に関係なく、自動的に安全な状態にロールバックされ、ビジネスの生産性への影響を最小限に抑えます。

XDR (Extended Detection and Response)

強力な EDR/XDR 機能により、Sophos や他社製品のセキュリティコントロール全体で疑わしいアクティビティを検出、調査、対応できます。Sophos Data Lake を介した脅威ハント、またはデバイスへのピボットにより、リアルタイムデータと最大 90 日間の履歴データを取得できます。SOC 専任チームと IT 管理者向けに設計された脅威の検出、調査、対応のための Sophos X-Ops 脅威インテリジェンスを強化して、組織の環境の全体像を把握します。

ライセンス概要

機能	Intercept X Advanced	Intercept X Advanced with XDR	Intercept X Advanced with MDR Complete
次世代型脅威対策 ウェブ保護、ディープラーニングマルウェア対策	✓	✓	✓
悪意のあるアクティビティのブロックと適応型の防御機能 ランサムウェア対策、エクスプロイト対策テクノロジー、適応型攻撃防御	✓	✓	✓
脅威への危険性を軽減 Web コントロール、周辺機器コントロール、アプリケーションコントロール、DLP、アカウントの状態チェック	✓	✓	✓
検出と対応 (EDR/XDR) 疑わしいアクティビティの検出、脅威ハンティング、調査ツール、対応アクション		✓	✓
MDR (Managed Detection & Response) 脅威ハンティング、検出、インシデント対応のための 24 時間年中無休のフルマネージドサービス			✓

エクスプロイトを防止

エクスプロイト対策テクノロジーは、攻撃者によるデバイスの侵害、認証情報の盗取、マルウェアの配布に使用される技術を阻止します。Sophos は、すべてのアプリケーションに対して、新しいオンデバイスエクスプロイト対策アプローチを大規模に導入しています。Intercept X は、Microsoft Windows で利用できる基本的な保護機能を基盤としてすでに構築されており、事前に構成および調整された 60 以上の独自のエクスプロイト対策が追加されています。Intercept X は、攻撃チェーン全体で使用される手法を阻止することで、ファイルレス攻撃やゼロデイ攻撃から保護します。

MDR (Managed Detection and Response)

Sophos MDR は、Sophos および他社製のセキュリティ制御と統合されたフルマネージドの脅威ハンティング、検出、インシデント対応サービスです。最も高度で複雑な脅威を検出して無力化するために 24 時間年中無休の専任セキュリティチームを提供します。

無償評価版

無償評価版の登録 (30 日間)
sophos.com/intercept-x

ソフォス株式会社営業部
Email: sales@sophos.co.jp