SOPHOS XDR と次世代型 SIEM

エージェント型 AI 時代に対応するセキュリティ運用とコンプライアンス

AI を利用する攻撃から組織を守り、運用の複雑さを増やさずコンプライアンス対応を簡素化します。

AI がアタックサーフェスを拡大し、攻撃を加速させる中、断片化したセキュリティツールでは十分に対応することが困難になっています。次世代型 SIEM を搭載した Sophos XDR は、保護、検知、調査、対応を統合するとともに、統合された AI ネイティブのサイバーセキュリティ防御システムを通じて、コンプライアンス要件への対応を支援します。

55%
正規の認証情報を使用や脆弱性を悪用するランサムウェア攻撃の割合[1]

76%
アラートによってサイバーセキュリティ担当者が燃え尽き症候群に陥った組織の割合[2]

80%
ワークフローがサイロ化されているためにコンプライアンス対応が冗長になっていると述べた CISO の割合[3]

13億
2028 年までに予測される AI エージェントの数 (アタックサーフェスの拡大)。[4]

ソフォスの特長

AI 搭載のアーキテクチャが、よりスマートで迅速な対応を可能に。

すべてのアナリストが大規模な環境でも効率的に業務を遂行できように支援。

AI ツールと自動化により、習熟までのハードルを下げ、負荷を軽減し、検知、調査、対応をより効率化します。これにより、アナリストはより多くの業務を、より迅速かつ自信を持って遂行できます。

- AI アシスタントが調査と脅威ハンティングを迅速化
- ケースを中心としたワークフローが、関連するアクティビティを自動的にグループ化し、優先順位付けするとともに、コンテキストを付与
- 自動化プレイブックを標準搭載し、対応アクションを迅速化し、手動のタスクを排除

相乗効果を生むインテリジェンス。

Sophos XDR は、あらゆる脅威から学習し、グローバル規模の実環境インテリジェンスを活用することで、検知と対応能力を強化します。

- ソフォスが保護している 625,000 社以上の組織から得られたインテリジェンスを AI モデルと検知ロジックに供給
- 年間 380,000 件以上の MDR 調査から得られた洞察
- 学習内容をリアルタイムで自動的に適用

検知、調査、対応、データ保持。

重複作業を排除します。次世代型 SIEM を搭載した Sophos XDR は、最新のセキュリティ運用と長期的なコンプライアンス対応を、設計段階から統合された単一基盤で実現します。

- 保護、検知、調査、対応、監査のワークフローをすべて 1 つのシステム内で実現
- セキュリティ向けとコンプライアンス向けのテレメトリを最大 10 年間保持
- データ量ではなく、ユーザーとサーバー数によってライセンスが付与されるため、コストを予測しやすい

すでにお持ちの製品やソフォス製品と連携可能。

ベンダーに依存しない設計となっており、すでに使用しているツールから、セキュリティシグナルからコンプライアンス向けのテレメトリまですべてを取り込みます。

- 豊富な AI 支援連携により、セキュリティおよびコンプライアンス関連のさまざまなデータソースからテレメトリを取り込み
- 双方向の統合により、既存のツールから直接対応アクションを実行可能
- Sophos Endpoint と Sophos Email Monitoring System (EMS) が標準で含まれ、優れた保護機能を提供

概要

- セキュリティ運用 (脅威対策、検知、調査、対応) とコンプライアンスの取り組みを 1 つの包括的なシステムに統合
- AI ツールとアシスタントによる、調査や対応の迅速化
- エンドポイント、アイデンティティ、メール、クラウド、ネットワーク、生産性ツールにわたる多段階攻撃を特定
- 標準搭載の SOAR プレイブックを使用して脅威対応を自動化
- Sophos X-Ops に組み込まれているアドバーサリーインテリジェンスで脅威を未然にブロック

対象者

- アラートノイズと手動調査に疲弊しているセキュリティチーム
- AI を利用する脅威に対するセキュリティ運用の近代化を検討している組織
- 脅威への対応とコンプライアンスワークフローの統合を検討している企業
- 従来の SIEM のような複雑な運用やコストをかけずに監査要件を満たす必要があるコンプライアンスチーム
- スケーラブルで高付加価値な SecOps ソリューションを提供する MSPとリセラー

SOPHOS MDR へのアップグレード

自社で SOC を構築せずに、世界最高クラスの SOC を利用可能。

24 時間 365 日体制の フルマネージドの脅威対応。

Sophos XDR および次世代型 SIEM は、Sophos MDR にシームレスにアップグレードでき、専門家主導の調査と対応が可能になります。

AI のスピードと、 人の判断の組み合わせ。

Sophos MDR は、世界最大規模のエージェント型 SOC です。AI が数秒で脅威を調査して解決する一方で、アナリストがその結果に責任を持ちます。

グローバルスケールの 専門知識。

アナリスト、脅威ハンター、調査担当者、対応担当者、AI エンジニアなど、ソフォスのグローバルなセキュリティエキスパートがお客様の社内チームを拡張します。

業界での高い評価

業界のアナリストや影響力のある組織から評価されています。

GARTNER 2026

エンドポイント保護で
17 回リーダーに位置付けられる

G2 SUMMER 2026

XDR ソリューションで
ナンバー 1 の評価

MITRE ATT&CK 評価

100% の検知
カバレッジ

GARTNER PEER INSIGHTS

XDR 部門で「Customers' Choice」に選出

1 つのシステムが、あらゆる制御ポイントを一体的に保護。

次世代型 SIEM を搭載した Sophos XDR は、世界で最も包括的なサイバー防御システムである Sophos Fusion の一部です。防御側が対応できる速度を上回る AI 活用型の脅威から、組織を保護します。**Sophos.com/XDR →**

[1] ソフォス、ランサムウェアの現状レポート 2026 年版。 [2] ソフォス、サイバーセキュリティの燃え尽き症候群への対処 2025 年版。 [3] The CISO Society、継続的統制モニタリングの現状レポート 2025 年版。 [4] IDC Info Snapshot、2025 年。

2026-07-27 SB-JA (AT)

SOPHOS