SOPHOS

SOPHOS AI DEFENSE

シャドー AI を可視化する

自信を持って AI を導入・活用する。

組織では、セキュリティ対策が追いつかないほどの速さで AI の導入が進んでいます。機密データが共有され、AI エージェントが可視化されないまま動作し、セキュリティチームはどの AI ツールが利用されているのか把握できていないことも少なくありません。Sophos Fusion を基盤とする Sophos AI Defense は、環境全体における AI の利用状況を把握し、その実態を理解して制御できるよう支援します。

69%
従業員が禁止されている公共 AI サービスを利用していると疑われる、または証拠がある組織[1]

82%
不明な AI ツールやワークフローを発見した組織の割合[2]

90%
シャドー AI のリスクへの懸念を表明した IT リーダーの割合[3]

13億
2028年までに予測される AI エージェントの数 13億[4]

ソフォスの特長

AI の可視化、制御、保護。

AI が実際に何をしているのかを可視化する。

可視化は、承認された利用状況だけでなく、実際に何が起きているのかを把握することから始まります。

- 従業員、ツール、ワークフロー全体にわたる AI の利用状況を把握する
- 承認済みのツールを確認し、未承認の AI 利用を可視化する
- ブラウザ、エンドポイント、ネットワークの連携ポイント全体で、継続的に可視化する

特に注意すべき AI の動作を特定する。

すべての AI アクティビティがリスクにつながるわけではありません。しかし、コンテキストがなければ、承認された利用と、対応が必要な動作をチームが見分けることはできません。

- アイデンティティ、動作、データのコンテキストを含めて AI の利用状況を評価する
- 許容される AI 利用と、管理されていない、過剰な権限を持つ、またはリスクのあるアクティビティを区別する
- 個々のイベントや影響の小さいイベントに反応するのではなく、実際に脅威につながるリスクに焦点を当てる

AI ポリシーを実際の制御に変える。

AI の利用が拡大すると、静的なポリシーでは対応しきれなくなります。ポリシーは継続的に適用し、実効性を確保する必要があります。

- ポリシーで定義されている AI の利用方法だけでなく、実際の AI 利用全体にガードレールを適用する
- AI の利用とデータ共有をポリシーや規制に合致させるため、主要なインタラクションポイントで管理を強化する
- 承認済みのツールへユーザーを誘導し、シャドー AI を削減する

セキュリティ運用に AI を導入する。

AI によってアタックサーフェスが拡大し、プロンプト、データ、AI エージェントによるアクションに新たなリスクが生じるため、積極的な管理が必要になります。

- AI の不正利用、悪用、侵害を検知と調査のワークフローに組み込む
- AI のアクティビティをより広範なセキュリティテレメトリに統合する
- 通常の脅威への対応に使用しているのと同じプレイブック、ツール、エスカレーションパスを適用する

SOPHOS AI DEFENSE の概要

- 従業員、ツール、ワークフロー全体にわたる AI の利用状況をシャドー AI を含めて把握する
- アイデンティティ、データのエクスポージャ、利用状況のコンテキストに基づいて、リスクのある動作を特定する
- ブラウザ、エンドポイント、ネットワークの連携ポイント全体にガードレールを適用する
- プロンプト、アップロード、AI との連携をリアルタイムで検査することで、機密データが AI ツールと共有されるのを防ぐ
- セキュリティ運用ワークフローに、AI リスク管理を統合する

SOPHOS AI DEFENSE の対象者

- AI の使用状況を可視化し、制御する必要のあるセキュリティリーダー
- AI によるリスクを特定し、対応する責任を負うセキュリティ運用チーム
- AI ツールを安全に導入して展開しようとする組織
- AI リスク管理のために既存のセキュリティ投資を拡大しようとしている企業

実際に脅威につながる AI リスクに焦点を当てる

AI の実際の利用方法に対応する、実践的な AI セキュリティ。

将来の仮定ではなく、今ある AI リスクに対応する。

ほとんどのソリューションは、AI モデルやアプリケーションを保護しています。Sophos AI Defense は、現在実際にリスクを引き起こしている要因に対応します。

- 従業員による管理されていない AI 利用
- 十分に把握できていないツール、AI エージェント、ワークフローの利用状況
- プロンプトや自動化されたワークフローを通じて外部の AI ツールに共有される機密データ

既存のセキュリティ対策を拡張する。

Sophos AI Defense は既存のセキュリティ制御を基盤とし、それらを連携させることで、迅速かつ実践的な成果を実現します。

- 既存の Sophos Workspace Protection、EDR、ファイアウォール、XDR、MDR への投資を拡張する
- 制御ポイントを連携させ、一元的な AI ポリシーフレームワークを構築する
- すぐに価値を提供 — 新たな製品やサービスの導入やリソースの追加は不要

可視化を単なるデータの収集ではなく、成果につなげる。

可視化するだけでは十分ではありません。Sophos AI Defense は、洞察を行動へと変えます。

- AI の利用状況、データ移動、AI エージェントのアクティビティにわたる可視化、コンテキスト、ポリシー適用を 1 つのシステムに統合する
- 同じワークフローでポリシーを適用し、問題の優先順位を付け、対応する
- 単にダッシュボードを追加するのではなく、実際の成果につなげる

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
リーダー、エンドポイント保護

G2 SUMMER 2026
最高評価の XDR と MDR ソリューション

MITRE ATT&CK 評価
100% の検知率

GARTNER PEER INSIGHTS
XDR と MDR 部門で「Customers' Choice」の1社として評価

1 つのシステムで、あらゆる制御ポイントが統合連携し、一体となって防御。

Sophos AI Defense 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/ai-defense →

[1] Gartner、「シャドウAIはより厳格なエンドポイントアプリケーション制御を要求する」、2026年5月25日。 [2] CSA、「企業環境におけるシャドウAIエージェントの問題」、2025年。 [3] Komprise IT調査:AI、データ、そして企業のリスク。 [4] IDC Info Snapshot, sponsored by Microsoft, 1.3 Billion AI Agents by 2028, #US53361825, May 2025.

Gartner Peer Insights のコンテンツは、個々のエンドユーザー自身の経験による主観的な意見が集約されたものであり、Gartner またはその関連会社の見解を表すものではありません。Gartner は、Gartner Peer Insights 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。Gartner は、商品性または特定目的への適合性の保証を含む、その正確性または完全性について、本コンテンツの内容に関する一切の責任を、明示または黙示を問わず負うものではありません。GARTNER は、米国内外における Gartner, Inc. および/またはその関連会社の登録商標およびサービスマークであり、PEER INSIGHTS は Gartner, Inc. および/またはその関連会社の登録商標で、Gartner, Inc. の許可を得て使用されています。All rights reserved.Gartner®, Peer Insights™ Voice of the Customer for Extended Detection and Response、Peer Contributors、2025 年 5 月 23 日Gartner®, Peer Insights™ Voice of the Customer for Managed Detection and Response, Peer Contributors, 31 March 2026.

2026-09-15 SB-JA (MC)

SOPHOS