

AI活用を妨げず、 リスクを低減 ESET AI Security

課題

AIツールや自律型AIエージェントは、急速に日常の業務プロセスへ組み込まれつつあります。これらが業務フローに統合され、外部コンテンツと連携することで、新たな脅威の侵入経路が組織内に生まれています。

リスクそのものは必ずしも新しいものではありません。しかし、その現れ方は変化しています。AIが生成する出力、AIによる自動実行、そしてユーザーとの相互作用を通じて、セキュリティチームやコンプライアンス担当者にとって見えにくい「AIの死角」が生まれています。

ソリューション

ESET AI Security

ESET AI Securityは、組織内で利用されるAIを安全に活用するために設計された専用のセキュリティレイヤーです。

AIツール、AIエージェント、ユーザーがデータ、システム、外部コンテンツと接する実際のリスクポイントに焦点を当て、AI利用に伴う脅威から保護します。

仕組み

不審な活動の早期検知

リスクを示唆する挙動をエスカレーション前に検知し、セキュリティインシデントとなる前に警告します。

AI行動の監視

AIツールやAIエージェントがエンドポイント上でどのように動作しているかを監視し、通常とは異なる挙動を検出します。

AIアクティビティの可視化

AIの挙動に関する洞察を提供し、リスクの理解や調査をより迅速に行えるよう支援します。

インシデント報告と対応

ESET AI Securityは、調査および対応を効率化するため、ESET PROTECT上に自動的にインシデントを作成します。

ESET AI Security の特長

既存のセキュリティ環境に統合

AI SecurityはESETのエンドポイント保護製品へ直接統合されています。新たなツールを追加することなく、現在のセキュリティ対策範囲を拡張できます。

AIが利用される場所をリアルタイムに保護

AIによる活動が発生するあらゆる場所にセキュリティ対策を適用します。エンドポイント、ユーザー操作、自動化プロセス全体を対象に保護を提供します。

安全なAI活用を実現

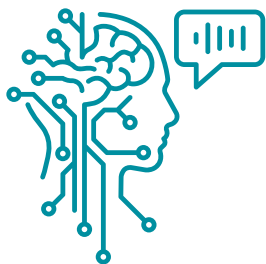
ESETは、生産性やイノベーションを損なうことなくリスクを低減し、組織が安心してAIを導入できる環境を提供します。

ESET AI Security

AIは、個人利用から企業利用まで、あらゆるワークフローやアプリケーションに組み込まれつつある新たな攻撃対象領域です。

こうしたワークフローやアプリケーションを保護するためには、それらに加えてAIサプライチェーン全体を保護できる、AIネイティブなセキュリティアーキテクチャが必要です。

ESET AI Securityの新しいモジュールにより、AIを悪用する最新の脅威から組織を保護します。

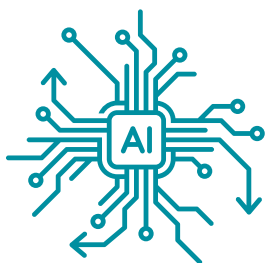


AI Agent Security

AI Agent Securityは、AIエコシステム経由で侵入する脅威に対応するため、エンドポイントセキュリティに専用の保護レイヤーを追加します。

AIサプライチェーン全体を通じて、悪意のあるAIエージェントへのアクセスやダウンロードを防止

AI関連ファイル、コンポーネント、URL、ダウンロードチェーンをスキャンし、多段階攻撃を阻止
新たなセキュリティリスクを生じさせることなく、自律型AIエージェントの導入を支援



AI Behavioral Monitoring

AI Behavioral Monitoringは、自律型AIエージェントの可視性を高める機能です。
AIエージェントの行動や実行内容を監視し、不審な活動を特定します。

不審なAIエージェントの挙動を検知し、潜在的な脅威を阻止

不審なAIエージェントの活動をインシデントとして記録し、調査を支援

DATASHEET

お問い合わせ

イーセツジャパン株式会社
jp-marketing@eset.com

www.eset.com/jp