proofpoint.

ソリューション概要

生成AIのデータセキュリティ

生成AIの安全使用を確保する

主なメリット

- 生成AIツールの許可されていない使用を可視化
- エンタープライズ生成AIツールやLLMを使用した開発による機密データ漏えいを防止
- クラウドやエンドポイントにおける生成AI適正利用規定を定める
- リスクのあるAI使用に関する動的な規定で内部脅威を監視
- 生成AIツールの利用規定に関するトレーニングを従業員に提供

このソリューションは、人に起因する4つの主要リスクを低減する、プルーフポイントのHuman-Centric Security統合型プラットフォームの一機能です。

生成AI（GenAI）は、生産性の向上、イノベーションの推進、データインサイトの活用といった面で、非常に大きな可能性を秘めています。しかし、生成AIを導入すれば課題も生じます。特にデータセキュリティ、プライバシー、コンプライアンスにおいては注意が必要です。パブリック生成AIツールを使用すれば機密データや知的財産が流出してしまうリスクがあり、ガバナンスが不十分な場合、Microsoft 365 Copilotなどのエンタープライズ ツールによる許可されていないデータアクセスや、機密の出力データが正しく分類されないなどといった事態を招く可能性があります。カスタムLLMを顧客データでトレーニングすれば個人を特定できる情報（PII）が開示されるおそれがあり、GDPR（EU一般データ保護規則）、HIPAA（米国 医療保険の相互運用性と説明責任に関する法律）、CCPA（カリフォルニア州消費者プライバシー法）などの規制に対するコンプライアンス上のリスクになります。強力なガバナンスがなければ、組織は、セキュリティ侵害や、規制違反による罰金のリスクに直面する可能性があります。

プルーフポイントでは、可視性、制御、教育を統合した、「人」を中心とした包括的なアプローチにより、生成AIツールやモデルの許可された範囲内での使用を確保します。

Proofpoint DLP (Data Loss Prevention) ソリューションは、エンドポイントでの生成AIの使用を監視し、ユーザーによる操作に関する知見を提供し、承認されていないツールを特定します。プルーフポイントでは、情報漏えいを防止するために、機密データが生成AIプロンプトに入力されるのをブロックまたは編集するポリシーを適用します。Proofpoint DSPM (Data Security Posture Management) は、機密データを許可されていないアクセスから保護することで、生成AIツールやLLMによるデータ漏えいを防ぎます。また、ZenGuideは、カスタマイズされたセキュリティ意識向上トレーニングを提供し、安全な生成AIプラクティスについて従業員を教育します。これにより、責任ある使用の文化の定着を促進します。

プルーフポイントは、これらの戦略を統合することで、進化する生成AIの状況において組織の機密データを保護します。

生成AIツールの許可されていない使用を可視化する

プルーフポイントのソリューションにより、組織は、誰が生成AIツールを使用しているかや、機密データがこれらのツールやカスタムLLMに入力されているかを理解することができます。プルーフポイントが提供する、AI使用に関するデータセキュリティ レポートでは、パブリック生成AIツールに送信された機密データの種類、最もアクティブなユーザー、アクティビティ別の上位サイトなどを確認できます（図1）。

クラウドAPIから、OpenAIなど、サードパーティ AIアプリの許可を特定し、アラートを受け取ることができます。AWS BedrockやAzure OpenAIにおいて、機密データを使用しているAIデプロイを検知することもできます。

主なメリット

- エンタープライズ生成AIツールやLLMを使用した開発による機密データ漏えいを防止

生成AIツールやLLMによる機密データ漏えいを防止

Proofpoint DSPMは、AIワークフローにおいて機密データの検知と分類を行い、侵害を招くような流出を防ぎます。さらに、暗号化やアクセス制御といった、保護ポリシーを適用するために使用される、MIP (Microsoft Information Protection) ラベルを適用することで、Microsoft Copilotがアクセスするデータも保護します。

機密データが基本的なモデルやカスタムモデル、RAG (Retrieval-Augmented Generation) ワークフローに取り込まれると、これを検知することで、AWS BedrockやAzure OpenAIなどのプラットフォームでのカスタムLLMやAIアプリケーションを保護します。

プルーフポイントは、LLMセキュリティに専用APIを提供し、LLMに取り込まれる、LLMから取り出されるデータの機密性をリアルタイムで分析します。これらのAPIは、データ使用状況について完全なガバナンスを提供し、可視化します。顧客のワークフローにシームレスに統合できるため、効果的なデプロイが可能です。

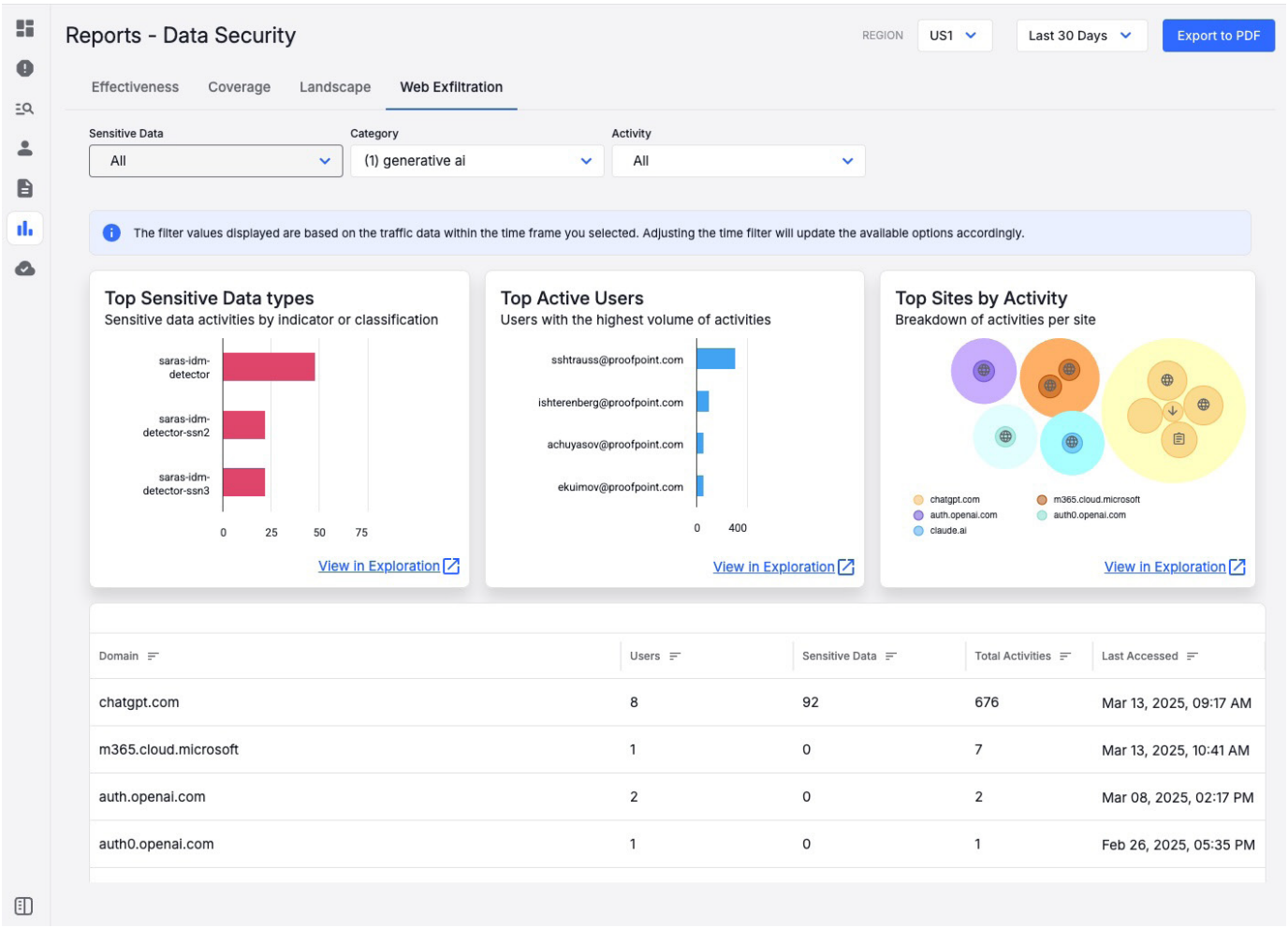

図1：生成AIによるデータ抜き出しのリスクを示したレポート

主なメリット

- クラウドやエンドポイントにおける生成AI適正利用規定を定める
- リスクのあるAI使用に関する動的な規定で内部脅威を監視
- 生成AIツールの利用規定に関するトレーニングを従業員に提供

生成AIの使用に関連した情報漏えいと内部脅威を阻止

エンドポイントでは、Web分類を使用して、生成AIサイトを閲覧しているユーザーを監視できます。ユーザーが許可されていないAIアプリをインストールしようとすれば、アラートで通知されます。プルーフポイントの動的なポリシーにより、リスクのある行動に応じてユーザーのエンドポイント監視を強化することができます。例えば、ユーザーが機密コンテンツを、許可されていない生成AIサイトに送信した前後において、メタデータとスクリーンショットを保存することができます。これにより、ユーザーによる生成AIツール操作の調査にかかる時間を短縮させることができます。

Proofpoint DLPにより、ユーザー、グループ、部門ごとに、600以上の生成AIツールについてエンドポイントDLPポリシーを適用でき、生成AIプラットフォームへのWebアップロードをブロックしたり、プロンプトに入力される機密データを編集したりできます。プルーフポイントのソリューションは、生成AIの利用規定を確認するようユーザーに促したり、防止ポリシーを適用する代わりに業務上の正当な理由を尋ねたりすることもできるため、ユーザーの生産性が損なわれる心配はありません。

クラウドAPI経由で、Microsoft 365 Copilotに過剰に共有されているファイルを可視化し、ユーザーがCopilotを悪用して機密情報が含まれるファイルの場所を突き止めようとすればセキュリティチームにアラートで通知されます。

例えば、プルーフポイントのソリューションは、リスクのある内部関係者がCopilotを使用して機密データが含まれる多くのファイルにアクセスすれば、これを検知します。また、クラウド アプリケーション内のAI生成コンテンツの分類、ラベル付け、保護を行います。承認されていないサードパーティAIアプリの許可を無効化またはブロックすることもできます。

生成AIツールの利用規定に関する教育を従業員に提供する

プルーフポイントは、組織における生成AIの安全な使い方をユーザーに指導します。ZenGuideは、動画、ポスター、インタラクティブなモジュールやニュースレターを用いて、データの安全な取り扱いに関するトレーニングをユーザーに提供します。ZenGuideにより、高リスクのユーザーに関する知見を活用し、開発者などの的を絞ったグループや、最もリスクの高いユーザーに、カスタマイズされた、リスクベースの学習を自動的に提供します。

トレーニング アクティビティは、アセスメント、カスタマイズされたナッジ、コーチング エクスペリエンスを通じて安全な行動を促進します。アクティビティには、ナレッジアセスメント、トレーニング割り当て、通知、ポリシー確認などがあり、これらすべてはセキュリティ意識を高め、生成AIツールの許可された範囲内での安全な使用を推進するために設計されています。

セキュアな生成 AI でビジネスを推進する

プルーフポイントは、最新のデータセキュリティ課題に対し、「人」を中心としたソリューションを提供します。生成 AI ツールや LLM モデルによるデータの漏えいや損失のリスクに関する知見を提供します。

プルーフポイントにより、教育、高レベルの監視、適切なデータ制御と共に、ユーザーが生成 AI のツールやモデルにアクセスできるようにする戦略を採用できるため、ユーザーの生産性とデータセキュリティのバランスを簡単に取ることができます。

proofpoint.

Proofpoint, Inc. は、サイバーセキュリティのグローバル リーディング カンパニーです。組織の最大の資産でもあり、同時に最大のリスクともなりえる「人」を守ることに焦点をあてています。プルーフポイントは、クラウドベースの統合ソリューションによって、世界中の企業が標的型攻撃などのサイバー攻撃からデータを守り、そしてそれぞれのユーザーがサイバー攻撃に対してさらに強力な対処能力を持てるよう支援しています。また、Fortune 100 の 85% の企業などさまざまな規模の企業が、プルーフポイントのソリューションを利用しており、メールやクラウド、ソーシャルメディア、Web 関連のセキュリティのリスクおよびコンプライアンスのリスクを低減するよう支援しています。詳細は www.proofpoint.com/jp にてご確認ください。

プルーフポイントとつながる：LinkedIn

プルーフポイント プラットフォームをご覧ください →

0207-017-08-01 03/25