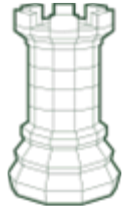
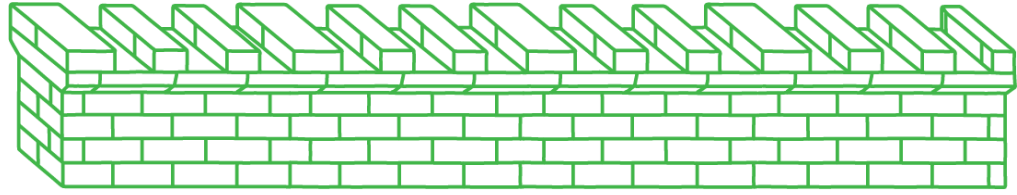


信頼できる AI アプリケーションの 運用と開発

Prediction Guard および SeekrFlow のご紹介

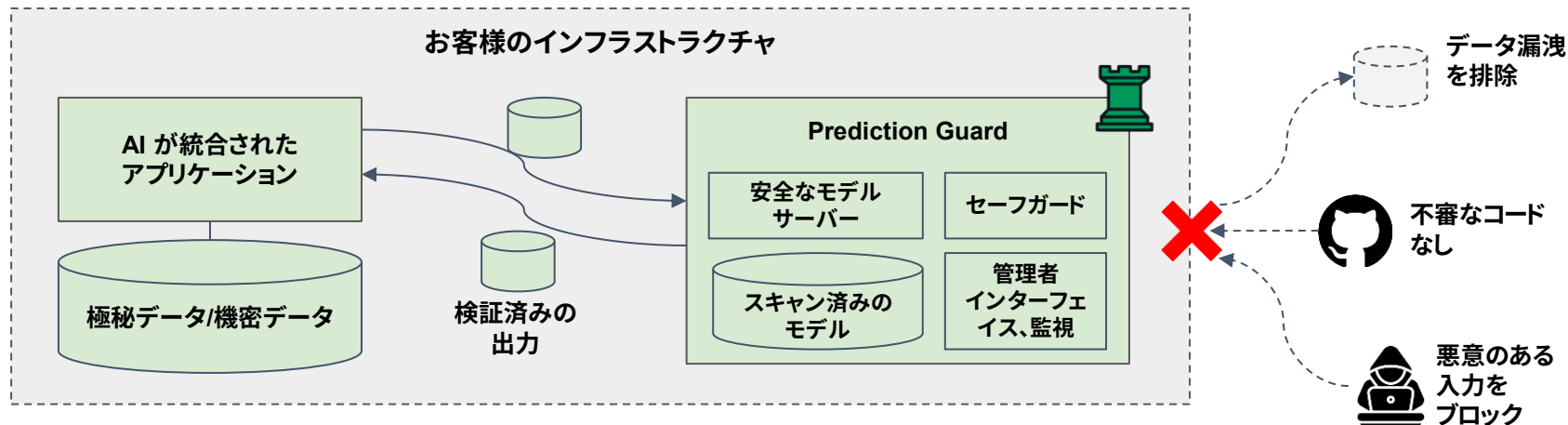
エクセルソフト株式会社

2025年9月12日

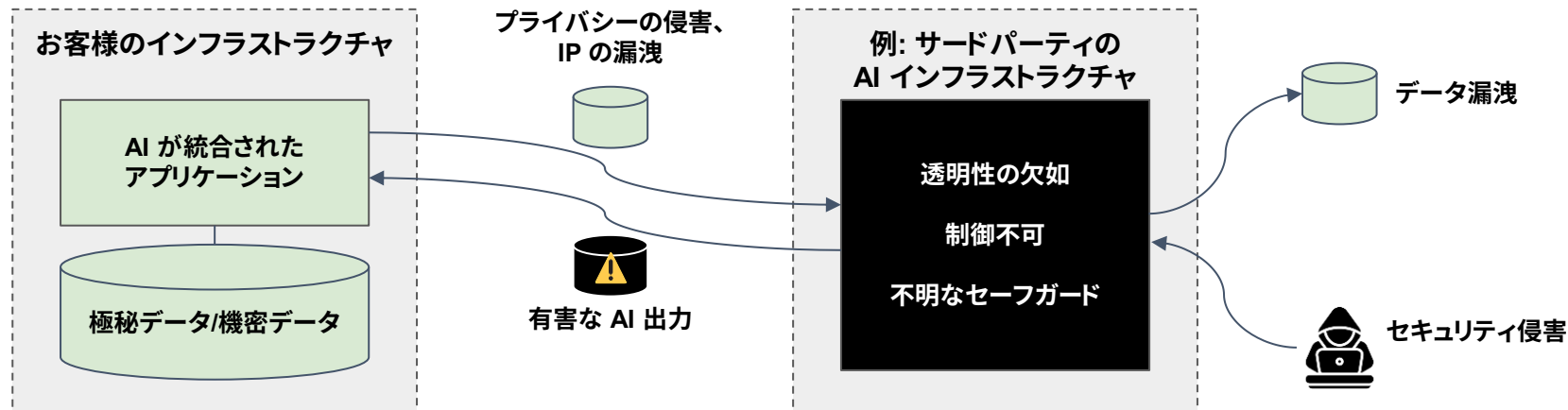


Prediction Guard

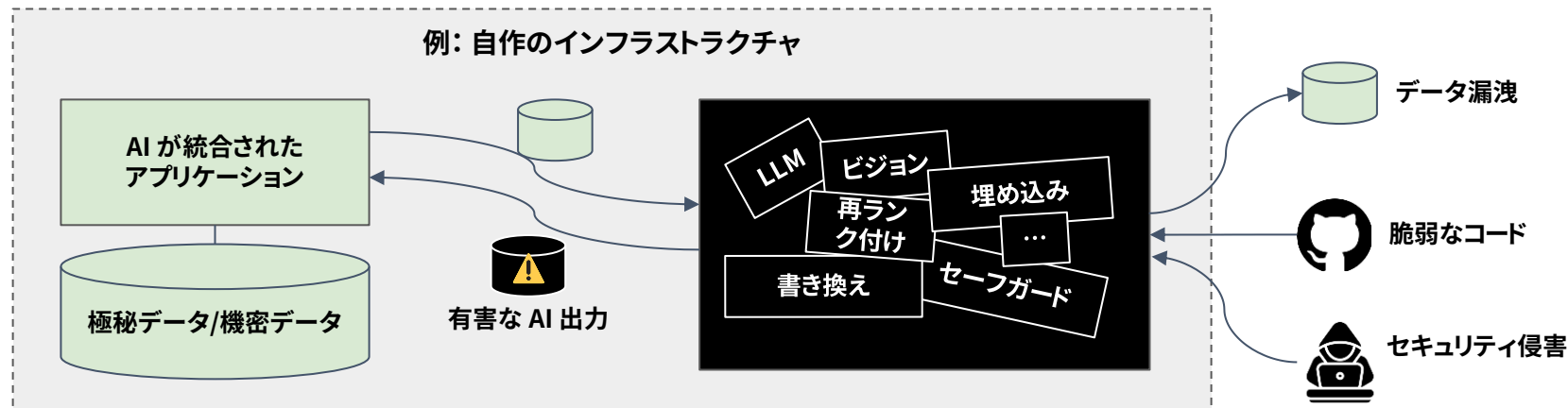
Prediction Guard はセキュリティの ベストプラクティスに準拠した強固な AI システムの実現を支援します



不透明な AI システムは、 潜在的なリスクを含みます



不透明な AI システムは、 潜在的なリスクを含みます



Prediction Guard は 信頼性の高い AI の運用を実現します



「Prediction Guard を使用して AI で信頼性の高い救命ツールを実現」

- CNN の特集記事で、当社のお客様の EMS や軍隊の医療従事者を支援するアプリが取り上げられました。

[ビデオのリンク](#)

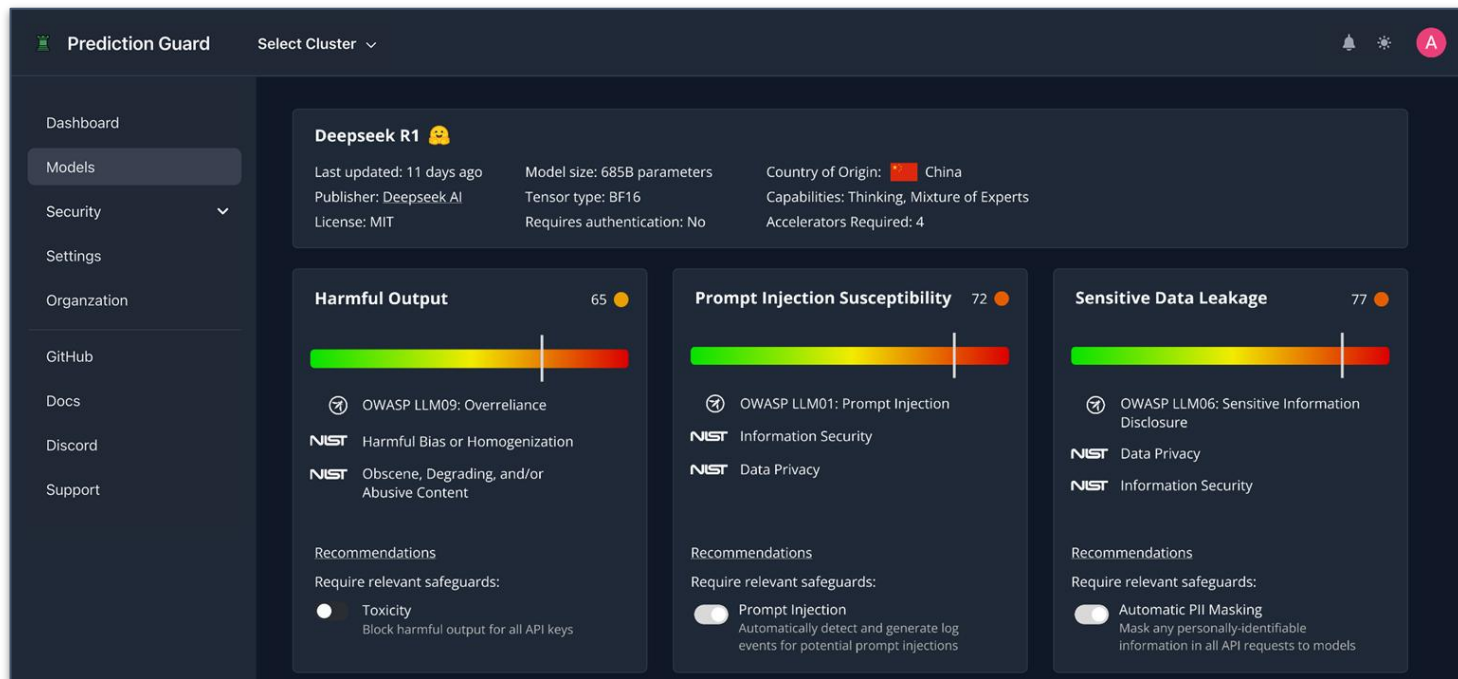
セキュリティ/プライバシー ベストプラクティスに準拠

Prediction Guard は、NIST と OWASP が推奨する
AI セキュリティ/プライバシーのベストプラクティスを実装し、
コンプライアンスとセキュリティの維持を確保します

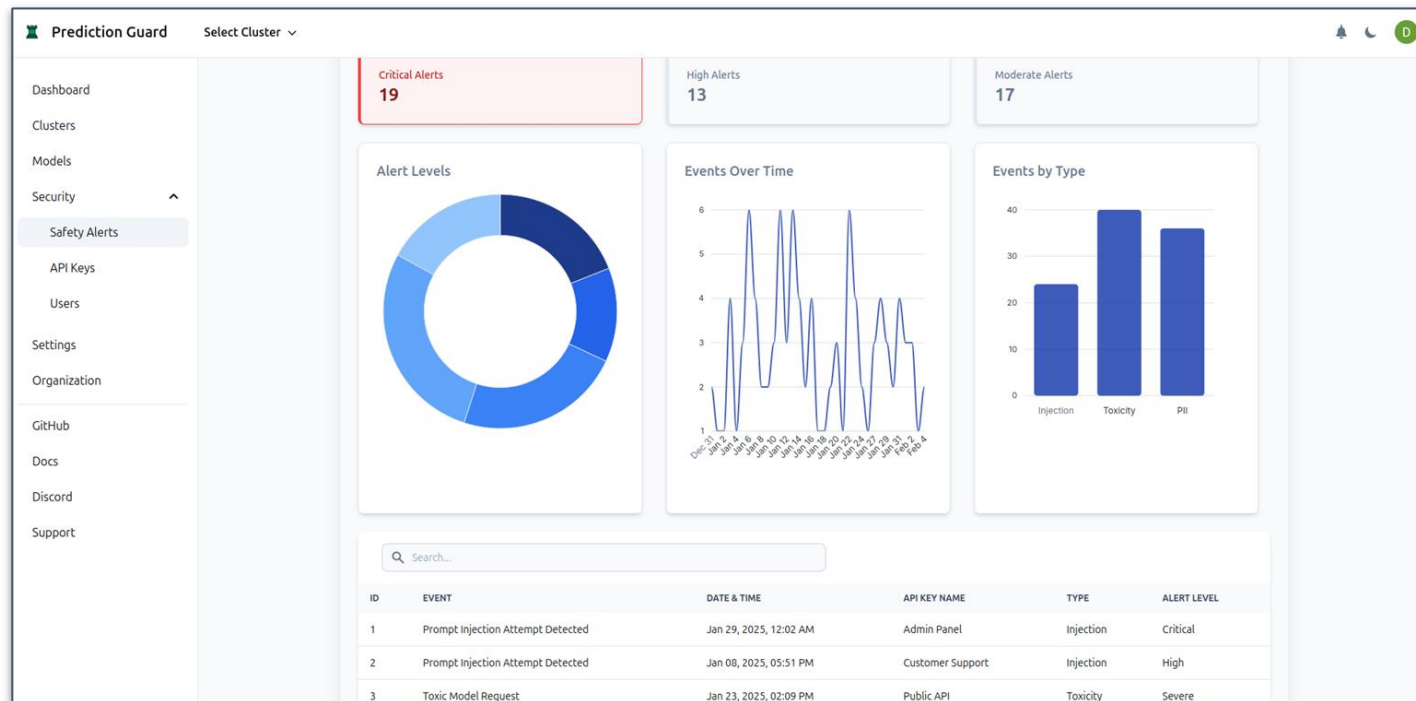


[OWASP TOP 10 for LLM](#)

モデル スキャンによりモデルの感度を判断し適切なセーフガードを推奨



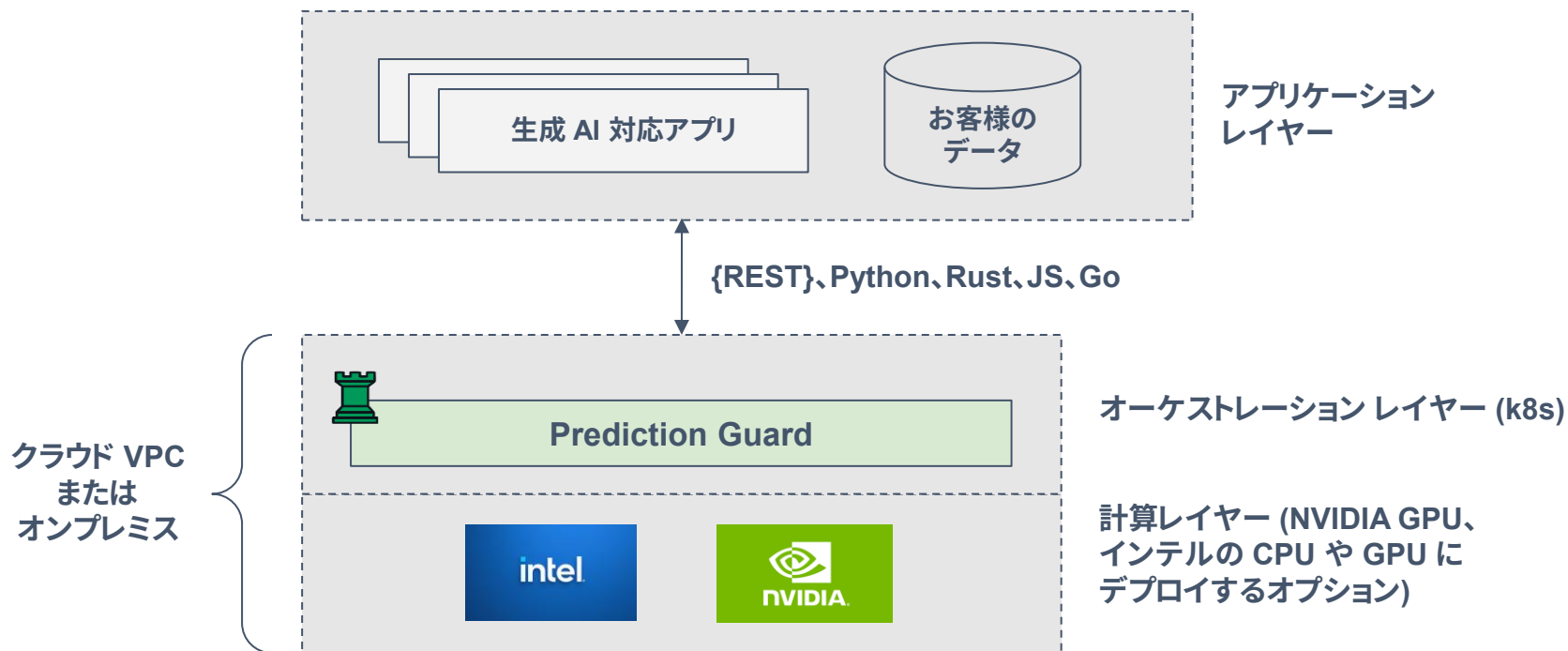
ゼロトラスト監視 管理パネルと構造化されたログを活用



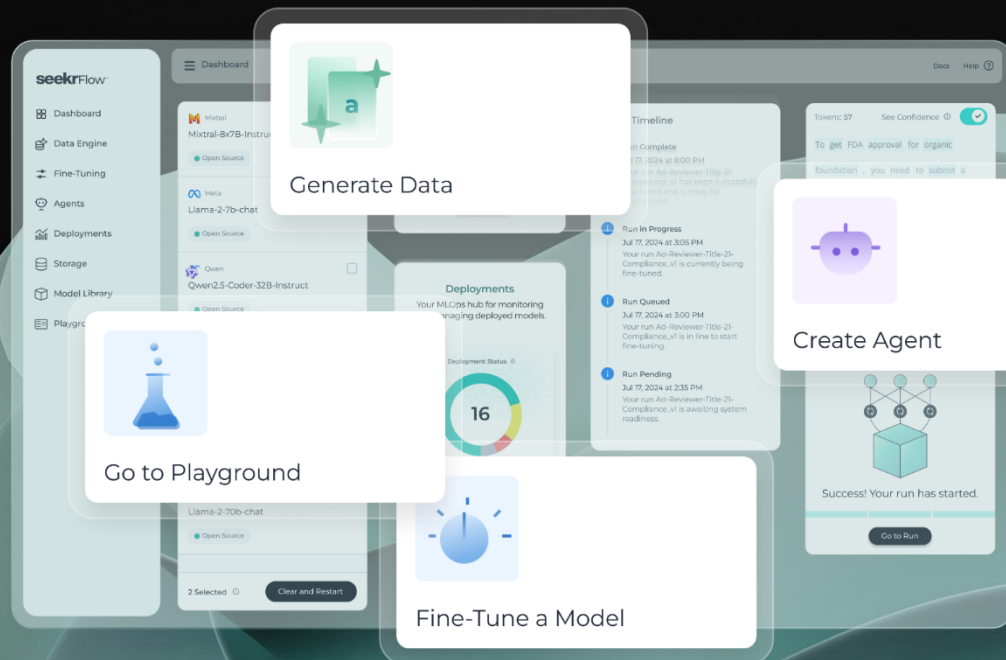
ホスティング オプション 制御と構成を選択可能

- オプション 1: Managed Cloud (管理型クラウド)
 - ✓ Prediction Guard がホストして管理します
迅速かつ簡単に利用を開始できます (通常 1 日以内)
 - ✓ HIPAA 準拠
- オプション 2: Self-hosted (自己ホスティング)
 - ✓ モデルの選択、AI セーフガードの監視、アクセス制御など、完全な制御と構成が可能です
 - ✓ 任意のインフラストラクチャ内にホストします
オンプレミス、ハイブリッド、クラウド VPC
 - ✓ 既存の Kubernetes コントロール プレーンを活用して
Prediction Guard が事前に構成した方法でデプロイできます
 - ✓ SRE (一部) およびエンタープライズ サポートを利用可能です。

自己ホスティングのアーキテクチャー



seekrFlow™



企業や政府機関で AI の採用が進まない制約

1

不正確さ、ハルシネーション (幻覚)、
リスクにつながる、バイアスを含むデータ、
誤情報、著作権で保護されたデータ

2

透明性と反論の余地がない、
不正確で主観的な出力

3

複数のポイント ソリューションの複雑さ、
熟練した AI 技術者への制限された
アクセス

4

データの流れや使用方法を
把握できない、データ主権の欠如

5

効率的でエッジに最適化された
モデル サイズという競合環境における
エッジ デプロイメントのニーズ

seekrFlow™

すべてを備えたソフトウェアインフラストラクチャ



構築、トレーニング、検証、
デプロイ、監視のための
エンドツーエンドのソフトウェア
インフラストラクチャ



事前ビルド済みの
AI エージェントのライブラリ



モデルの出力を検証する
ガードレール、信号検出器、
批評エージェント



信頼できる、説明可能で、
競合可能な AI



任意形式の独自のデータで
モデルをトレーニング



ドメイン固有の知識に基づいて
トレーニングされた
推論エンジン



ハードウェアと
プラットフォームに非依存

Seekr 社のクラウド /
お客様のクラウド



自然言語でクエリ可能な
次世代のフル 3D ビジョン
言語モデル



透明性の高いデータ ポリシー

データが存在するセキュリ
ティが確保された場所に
インストール



一般的なオープンソース
モデル / お客様のモデル

AI-Ready Data

- 構造化されていない一般的なドキュメントから
ファインチューニング用の学習データを生成します
学習データの準備にかかるコストを削減します

seekrFlow

Dashboard

Data Engine

AI-Ready Data

Storage

Development

Fine Tuning

Agents

Deployments

Model Library

Playground

Model Chat

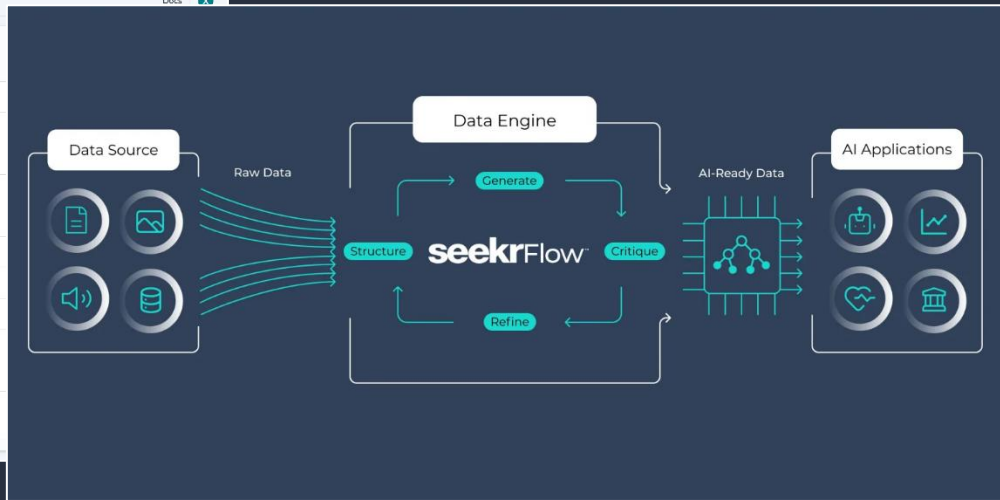
Agent Chat

Help & Support

AI-Ready Data Jobs

Generate training data from your unstructured documents to fine-tune a model.

Job ID	Status
aj-cf0ef8c-8b4b-403c-908b-85c25a252a4	Completed
aj-9f8ee0c-d423-402d-4043-470723d97f7	Completed
aj-a94b47b-2d76-4f8e-860c-670c24a960c	Completed
aj-c75f767-d960-46a3-9c44-d729f0c0933	Completed
aj-c85974e-d84c-4d75-894c-e5a32d7e0ed	Completed
aj-8c8699c5-df61-4a8e-b308-a29f644773f	Completed
aj-fd48697c-a238-4e71-bec3-2aeb6379510	Completed
aj-c3238ab-d38a-4763-b302-92a1bb7f803e	Completed
aj-c0d027a0-c0e6-8050-8043-0e4a9996506	Completed
aj-99fb532-72d8-429e-a278-4c38473cd88	Failed
aj-fc1a1a83f-a268-477c-b4ab-9a7c794da794	In Progress



ケース スタディ: Exiger + Seekr

Exiger は、SeekrFlow™ を米国国防総省向けの AI ソリューションとして選定し、信頼性が高く説明可能な AI 機能を迅速かつコンプライアンスに準拠して調達できるようにしました。

■ 課題

1,600 万のサプライ チェーンにおけるリスク報告の遅延

AI の精度不足による不十分なリスク予測

■ ソリューション

製品の強化: 自動化、マルチエージェント ワークフロー

6 億の事業体の FOCI、運用健全性、財務、風評、
規制リスクについて独自のデータを分析

顧客のデュー デリジェンスのリスクの説明を生成

中国が世界的な影響力を得るために用いた戦術を分析

レアアース鉱物とエネルギー供給リスクを解明

■ 効果

モデルの精度が 3 倍向上し、顧客のリスクを軽減

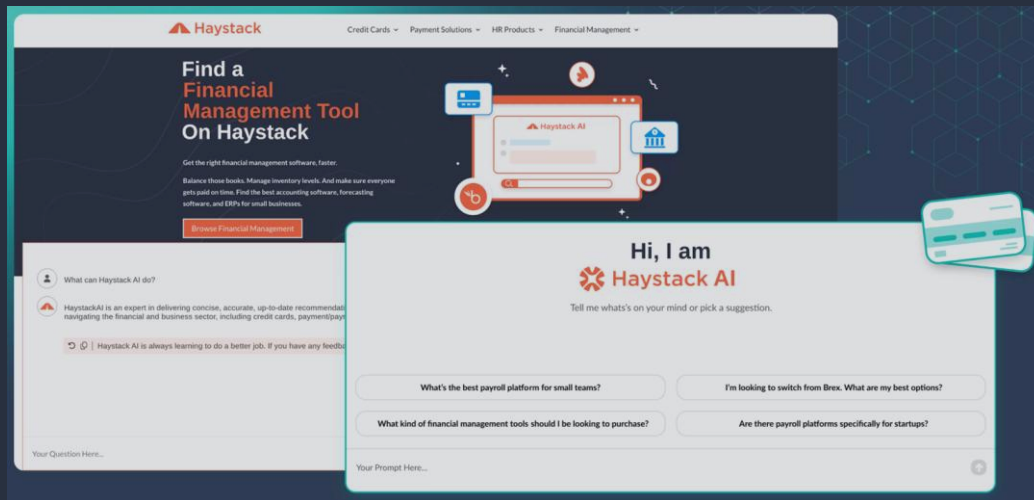
レポート生成時間を 90% 短縮 (5 時間からほぼリアルタイム)

競合他社との差別化を強化

「Seekr の導入以前は、商用基盤モデルに頼って信頼性が高くエラーのないリスクレポートを迅速に生成することは不可能でした。今では、Seekr のエージェント型 AI を活用することにより、自社のデータに基づく実用的な洞察を備えた、非常に正確なリアルタイムのリスクレポートを迅速に生成できるようになりました。」

ケース スタディ: OneValley + SeekrFlow

OneValley は、SeekrFlow™ を利用して、起業家の商品検索を効率化し、パーソナライズされたレコメンデーションを通じて新たな収入源の創出に寄与する、AI を搭載したチャットボットを導入しました



「Seekr のおかげで、信頼性と正確性を確保しながら、AI から真の価値を引き出すパートナーを見つけることができました。」
- OneValley CPO、Alec Wright 氏



ONEVALLEY



- **ユーザーの信頼度の向上:** 60% 以上のユーザーから、Haystack とやり取りしたことで、購入の決定に対する信頼度が高まったという回答が得られました。
- **新たな収入源:** チャットボットは OneValley に新しいアフィリエイトの収益をもたらし、事業の成長に貢献しました。
- **スケーラブルなデプロイメント:** 25,000 人を超える直接メンバーと 175,000 人以上の間接ユーザーからなるグローバル コミュニティのサポートに成功し、ソリューションのスケーラビリティと有効性を実証しました。

透明性があり任意の場所に デプロイメント: 実環境向けに構築

- ✓ トークンレベルの信頼度スコアリング、回答批評、
ヒューマンインザループ
- ✓ モデルとプロンプト チューニングのための比較評価
- ✓ クラウド、オンプレミス、エアギャップ環境でのデプロイメント
- ✓ AWS Marketplace で利用可能。SOC2、RBAC、Helm をサポート

利用事例

- ソリューション ライブラリ
- 利用事例を公開しています



技術者の発掘

AI を活用した能力マッピングとスキル分析により、クリエイティブなプロジェクトに最適な技術者を見つけ出し、マッチングします。



コンテンツの整合性検出

大量のコンテンツから矛盾、誤情報、欠落を検出し、メッセージの正確性と信頼性を維持します。



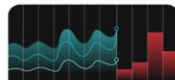
ラベル インテリジェンス コバイロット

ラベルの検証と品質チェックを自動化し、出荷および梱包データの正確性とコンプライアンスを確保します。



インテリジェンス、調査 分析

オープンソースや社内データを集約および分析し、調査チーム向けに、隠れたつながり、リスク、インサイトを発見します。



エビデンススペースの研究 アシスタント

臨床研究、技術論文、規制データを統合し、科学的根拠に基づいた実用的なインサイトを生成します。



コンテンツ モデレーショ ン

説明可能な AI のモデレーションワークフローにより、不適切または有害なコンテンツを分類、フラグ付け、フィルタリングします。



地域を超えた戦略とガバ ナンス

複数の地域にわたる政策、規制、地政学的要因を分析し、ガバナンスとコンプライアンスに関する意思決定を支援します。



フリート入札向けのコバ イロット

フリート調達に関する入札案件を発見および評価し、提案書を自動生成して応答時間を短縮することで、落札率を向上させます。



センサー洞察エージェン ト

複雑な環境におけるセンサーのデータを処理および解釈し、生



要約

自社データに基づいた、インテリジェントな要約アプリケーション



会話型 AI

正確かつ説明可能な会話型 AI でビジネスを強化します。

お問い合わせはこちらまで
<https://www.xlssoft.com/jp/qa>