DARKTRACE

Darktrace / SECURE AI™

プロンプト、エージェント、開発環境、シャドーAI全体にわたるリアルタイムの可視性と制御を提供するAdaptive AIで、安全なAI導入を実現します。

88%

少なくと

も1つの業務機能でAIを利用している組織の割合[1]

66%

現在、

生成AIサービスを利用しているDarktraceのお客様の割合[2]

44%

AIエージェ

ントについて非常に、または極めて懸念しているセキュリティプロフェッショナルの割合[3]

AIの導入が企業の管理体制を上回るペースで進んでいます

AIは急速に企業へ導入されており、そのペースはさらに加速しています。AIの導入とイノベーションが進む一方で、セキュリティ対策は依然として後れを取っています。現在、組織はAIセキュリティの問題に直面しており、ワークフロー、ツール、データ、意思決定の全体にわたってリスクが気付かないうちに積み重なり、多くの場合、その実態をまったく把握できていません。

AIは適応性が高く予測が難しい性質を持つため、効果的なAIセキュリティを実現するには、人間、AIシステム、エージェントにわたる「正常」な状態を深く理解することが不可欠です。これにより、逸脱、不正使用、侵害の兆候を、深刻化する前の極めて初期の段階で検知できるようになります。

AI導入に行動型セキュリティを取り入れる

Adaptive AIを搭載したDarktrace / SECURE AIは、10年以上にわたって培ってきた行動に関する知見を活用し、組織全体におけるプロンプト、エージェント、AIシステムの利用を保護します。

事前定義されたルールやシグネチャに依存するのではなく、組織の運用パターンを学習し、従来のルールベースの制御では検出できない不正利用、設定ミス、ドリフトを明らかにします。

Darktrace Platform Portalを通じて提供されるDarktrace / SECURE AIは、AIとのやり取りを単一のビューに集約し、人間とAIエージェントの両方のアクティビティについて、チームが意図を把握し、リスクを評価し、機密データを保護し、ポリシーを適用できるよう支援します。

ビジネス上のメリット

統合されたAIの可視化
エンタープライズ生成AI、AIエージェント、開発アクティビティ、シャドーAIにわたるAIとのやり取りを、行動インテリジェンスに基づく単一のビューで可視化します。

リアルタイムのリスク検知
事前定義されたルールに依存することなく、プロンプトやエージェントの動作におけるわずかな不正利用、ドリフト、新たなリスクをリアルタイムで検出します。

ポリシーに沿ったガバナンス
独自の組織ポリシーをAIアクティビティにマッピングすることで、ガバナンスをビジネスの優先事項と整合させ、実際のAI利用状況に照らして評価できるようになります。

安心してAIを大規模に導入
大規模なリスク管理に必要な可視性、理解、監視体制を備え、組織全体でAIの活用を拡大します。

企業内のAI向けに設計

エンタープライズ生成AI	AIエージェント
ローコード	ハイコード / Cloud AI
シャドーAI	SaaS
MCP	SASE

1: マッキンゼー「AIの現状2025」
2: Darktrace調査
3: Darktrace「AIサイバーセキュリティの現状 2026」

DarktraceがAIを保護する仕組み

DarktraceのAdaptive AIはすでに、あいまいさを解釈し、わずかな意図を明らかにして、組織全体でアクティビティやイベントが危険な状態に至る前にドリフトを検出します。

同じ行動型アプローチをAIに拡張することは、飛躍ではなく自然な次のステップです。これは、すでに人とインフラストラクチャを保護しているDarktrace Behavioral Defense Platform™を基盤としています。

シャドーAIを見つけ出し、統制

Darktraceは、/ SECURE AIネイティブの可視性と、ネットワーク、クラウド、エンドポイント、SASEのデータソースを組み合わせることで、未承認のローコードエージェントの構築や、ローカルにデプロイされたMCPサーバーなどの隠れたエージェント型インフラストラクチャを含め、未承認または予期しないAIアクティビティがどこで発生しても検出できるよう支援します。その後、環境に適したポリシーと対応手順によって、データ漏えいを抑制し、ユーザーを承認済みの選択肢へと導きます。

生成AIエージェントおよびアシスタントを駆動するプロンプトを監視

Darktrace / SECURE AIは、Microsoft CopilotやChatGPT Enterpriseなどのエンタープライズ AI、Copilot Studioなどのローコード環境、Amazon Bedrockなどのハイコード環境、SalesforceやMicrosoft 365などのSaaSプロバイダーにわたって、プロンプト、セッション、レスポンスをリアルタイムで検査します。行動分析により、新たなリスクの兆候となる可能性があるAIアクティビティのわずかな逸脱を明らかにし、機密データの漏えい、ジェイルブレイクの試行、その他の安全でない、または予期しない動作など、潜在的な問題の検出を支援します。

AIエージェントのアイデンティティをリアルタイムに保護

さまざまなサプライヤーや環境にわたってエージェントのIDを検出し、その権限、ロール、接続関係をマッピングするとともに、SaaS、クラウド、ネットワーク、エンドポイント、OT、メールにわたる動作を監査できます。このリアルタイムの監査ビューにより、AIエージェントがどこにデプロイされ、どのように使用され、どのような権限を持っているかなど、組織のAIエージェントを明確に把握できます。これにより、チームは潜在的なリスクを特定し、大規模な環境でも適切な監視を維持できます。

開発時および運用時のAIリスクを評価

Darktrace / SECURE AIを使用すると、Copilot Studioなどのローコードビルダー、Amazon Bedrockなどのハイコードプラットフォーム、社内ラボにわたって構成されるID、権限、アクセスを可視化できます。また、ポスチャー管理により、エージェントが本番環境に移行する前に、設定ミスや異常なビルドイベントを検出します。/ SECURE AIは、ビルド時に得られた可視性を実行時の動作と結び付けます。

必要な保護を選択してください

Darktrace / SECURE AIは、Darktrace Behavioral Defense Platformの他の製品と同様のCore、Advanced、Completeの導入パスに従い、AIセキュリティのさまざまな成熟度レベルに対応するよう設計されたパッケージで提供されます。

CORE

AIプロンプト分析と統合されたシャドーAI管理を含み、承認済みAIの利用状況とそれに伴うリスクを可視化するとともに、ポリシー整合性マッピングを提供します。

ADVANCED

Coreを拡張し、高度なシャドーAI管理、エージェントのIDとアクション、AIエージェント開発リスク管理を追加することで、AIアクティビティ、エージェントの動作、リスクをより詳細に監視できます。

「「すぐに、これまでずっと不足していた情報、つまり組織内で誰が何を使用し、データをどのように扱っているのかを把握できるようになりました」

■ **IT担当副社長（米国製造部門）**

■ **Darktraceについて**

Darktraceは、組織が日々変化する脅威環境に先手を打てるよう支援する、サイバーセキュリティ向けAIのグローバルリーダーです。2013年に英国ケンブリッジで設立されたDarktraceは、各企業からリアルタイムで学習するAIを活用し、未知の脅威から組織を守るための不可欠なサイバーセキュリティプラットフォームを提供しています。Darktraceのプラットフォームとサービスは、世界中の約10,000社のお客様を保護する2,300人の従業員によって支えられています。詳細については、darktrace.comをご覧ください。

北米：+1 (415) 229 9100　ヨーロッパ：+44 (0) 1223 394 100　アジア太平洋：+65 6804 5010　ラテンアメリカ：+55 11 4949 7696

darktrace.com | info@darktrace.com

© 2026 Darktrace Holdings Limited. All rights reserved.