DARKTRACE

Darktrace / SECURE AI™

Sécurisez votre adoption de l'IA grâce à une IA adaptative qui offre une visibilité et un contrôle en temps réel sur les prompts, les agents, les environnements de développement et l'IA fantôme.

88%
des organisations
utilisent l'IA dans au moins une fonction de l'entreprise[1]

80%
des clients Darktrace
utilisent désormais des services d'IA générative[2]

44%
des professionnels de la sécurité
sont très ou extrêmement préoccupés par les agents IA[3]

L'adoption de l'IA dépasse les capacités de contrôle des entreprises

L'intelligence artificielle a fait son entrée dans les entreprises à un rythme effréné qui ne cesse de s'accélérer. Alors que l'adoption et l'innovation progressent, la sécurité tente encore de rattraper son retard. Les organisations sont désormais confrontées à un problème de sécurité lié à l'IA, avec des risques qui s'accumulent discrètement au sein des flux de travail, des outils, des données et des décisions, souvent sans la moindre visibilité.

La nature adaptative et imprévisible de l'IA implique qu'une sécurité efficace de l'IA nécessite une compréhension approfondie de ce qui est « normal » pour les humains, les systèmes d'IA, et les agents, afin que les signes précurseurs de dérive, d'utilisation abusive, ou de compromission puissent être détectés avant qu'ils ne s'aggravent.

AVANTAGES POUR L'ENTREPRISE

Visibilité unifiée sur l'IA
Visualisez les interactions de l'IA à l'échelle de l'entreprise — IA générative, agents, activités de développement et IA fantôme — grâce à une vue d'ensemble de l'intelligence comportementale.

Détection des risques en temps réel
Détectez immédiatement les moindres signes d'utilisation abusive, de dérive et de risques émergents dans les prompts et dans le comportement des agents, sans vous appuyer sur des règles prédéfinies.

Gouvernance alignée sur les politiques
Associez votre propre politique organisationnelle à l'activité de l'IA, afin que la gouvernance soit alignée sur les priorités de l'entreprise et évaluée en fonction de l'utilisation réelle de l'IA.

Adopter l'IA en toute confiance et à grande échelle
Déployez l'utilisation de l'IA à l'échelle de l'entreprise en bénéficiant de la visibilité, de la compréhension et du contrôle nécessaires pour gérer les risques à grande échelle.

1 : Rapport McKinsey sur l'état de l'IA en 2025
2 : Darktrace Research
3 : Darktrace : état des lieux de la cybersécurité basée sur l'IA 2026

Intégrer la sécurité comportementale à votre adoption de l'IA

Propulsé par l'IA adaptative, Darktrace / SECURE AI s'appuie sur plus d'une décennie de compréhension des comportements pour sécuriser l'utilisation des prompts, des agents et des systèmes d'IA dans l'ensemble de votre entreprise.

Plutôt que de s'appuyer sur des règles ou des signatures prédéfinies, il apprend les schémas opérationnels de votre organisation et signale les usages abusifs, les mauvaises configurations et les dérives que les contrôles traditionnels fondés sur des règles ne sont pas conçus pour détecter.

Fourni via le Darktrace Platform Portal, Darktrace / SECURE AI rend visibles toutes les interactions de l'IA sur un tableau de bord unique, aidant les équipes à comprendre les intentions, évaluer les risques, protéger les données sensibles et appliquer les politiques tant pour l'activité humaine que pour celle des agents IA.

CONÇU POUR L'IA DANS VOTRE ENTREPRISE

IA générative d'entreprise	Agents IA
Low-Code	High-code / IA Cloud
IA fantôme	SaaS
MCP	SASE

Comment Darktrace sécurise votre IA

L'IA adaptative de Darktrace est déjà capable d'interpréter les ambiguïtés, de mettre au jour les intentions subtiles et de détecter les dérives avant que des activités ou des événements ne deviennent dangereux au sein de votre entreprise.

Étendre cette même approche comportementale à l'IA constitue une suite logique et non un saut dans l'inconnu, en s'appuyant sur la Darktrace Behavioral Defense Platform™ qui protège déjà les collaborateurs et les infrastructures.

Découvrez et contrôlez l'IA fantôme

Darktrace vous aide à détecter toute activité d'IA non autorisée ou inattendue, où qu'elle se produise, y compris la création non autorisée d'agents low-code et les infrastructures d'agents cachées telles que les serveurs MCP déployés localement, en combinant la visibilité native de / SECURE AI avec des sources de données provenant du réseau, du cloud, des points de terminaison et du SASE. Des politiques et des processus de réponse adaptés à l'environnement permettent ensuite d'endiguer l'exposition des données et de guider les utilisateurs vers des solutions approuvées.

Surveiller les prompts qui pilotent les agents et assistants d'IA générative

Darktrace / SECURE AI assure une inspection en temps réel des prompts, des sessions et des réponses au sein des solutions d'IA d'entreprise telles que Microsoft Copilot et ChatGPT Enterprise, des environnements « low-code » comme Copilot Studio, des environnements « high-code » comme Amazon Bedrock, ainsi que des fournisseurs SaaS tels que Salesforce et Microsoft 365. L'analyse comportementale permet de mettre en évidence des écarts subtils dans l'activité de l'IA qui peuvent signaler l'émergence d'un risque, aidant ainsi les organisations à détecter des problèmes potentiels tels que la divulgation de données sensibles, les tentatives de jailbreaking et d'autres comportements dangereux ou inattendus.

Sécurisez les identités des agents IA en temps réel

Vous pouvez identifier les agents au sein des différents fournisseurs et environnements, cartographier leurs autorisations, leurs rôles et leurs connexions, et contrôler leur comportement sur les solutions SaaS, le cloud, le réseau, les points de terminaison, les systèmes OT et la messagerie électronique. Cet aperçu d'audit en temps réel permet aux organisations de bien cerner leurs agents IA, notamment leur lieu de déploiement, leur mode d'utilisation et les autorisations dont ils disposent, ce qui aide les équipes à identifier les risques potentiels et à maintenir une supervision à grande échelle.

Évaluez les risques liés à l'IA lors du développement et du déploiement

Avec Darktrace / SECURE AI, vous bénéficiez d'une visibilité sur les identités, les autorisations et les accès configurés via des outils de développement « low-code » tels que Copilot Studio, des plateformes « high-code » comme Amazon Bedrock et des laboratoires internes, grâce à une gestion de la posture de sécurité qui signale les mauvaises configurations et les événements de développement anormaux avant qu'un agent n'atteigne l'environnement de production. / SECURE AI associe ensuite cette visibilité acquise lors du développement au comportement au moment de l'exécution.

Choisissez la protection dont vous avez besoin

Darktrace / SECURE AI est disponible sous forme de suites conçues pour prendre en charge différents niveaux de maturité en matière de sécurité de l'IA, suivant le même parcours graduel d'adoption, Basique, Avancé et Complet, que le reste de la Darktrace Behavioral Defense Platform.

CORE

Comprend l'analyse des prompts adressés à l'IA et la gestion intégrée de l'IA fantôme afin d'offrir une visibilité sur les usages autorisés de l'IA et les risques associés, ainsi qu'une cartographie de l'alignement des politiques.

AVANCÉ

Élargit les fonctionnalités Core grâce à une gestion approfondie de l'IA fantôme, aux identités et actions des agents, ainsi qu'à la gestion des risques liés au développement des agents IA, pour une supervision plus poussée de l'activité de l'IA, du comportement des agents et des risques.

"Nous avons immédiatement eu accès aux informations qui nous avaient manqué jusqu'alors : **qui utilise quoi au sein de notre organisation** et **comment ces données sont-elles exploitées.**"

- **Vice-président informatique, industrie manufacturière américaine**

À propos de Darktrace

Darktrace est un leader mondial dans le domaine de l'IA appliquée à la cybersécurité, qui permet chaque jour aux entreprises de garder une longueur d'avance face à l'évolution constante des menaces. Fondée en 2013 à Cambridge, au Royaume-Uni, Darktrace propose une plateforme de cybersécurité indispensable pour protéger les entreprises contre les menaces inconnues grâce à une IA qui apprend en temps réel à partir des données propres à chaque entreprise. La plateforme et les services de Darktrace s'appuient sur les 2 300 employés qui assurent la protection de près de 10 000 clients à travers le monde. Pour en savoir plus, rendez-vous sur darktrace.com.

Amérique du Nord: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asie-Pacifique: +65 6804 5010 | Amérique latine: +55 11 4949 7696

darktrace.com | info@darktrace.com

© 2026 Darktrace Holdings Limited. Tous droits réservés.