DARKTRACE

Darktrace / SECURE AI™

Schützen Sie Ihre KI-Einführung mit adaptiver KI, die Echtzeit-Transparenz und -Kontrolle über Eingabeaufforderungen, Agenten, Entwicklungsumgebungen und Schatten-KI bietet.

88 %

der Unternehmen

nutzen KI in mindestens einem Geschäftsbereich[1]

66 %

der Darktrace-Kunden

nutzen mittlerweile generative KI-Dienste[2]

44 %

der Sicherheitsexperten

sind sehr oder extrem besorgt über KI-Agenten[3]

Einführung von KI überholt Kontrollmöglichkeiten von Unternehmen

KI hat in rasantem Tempo Einzug in Unternehmen gehalten – und diese Dynamik beschleunigt sich weiter. Während Einführung und Innovation voranschreiten, hinkt die Sicherheit noch hinterher. Unternehmen stehen nun vor einem KI-Sicherheitsproblem, da sich Risiken über Arbeitsabläufe, Tools, Daten und Entscheidungen hinweg unbemerkt summieren – oft ganz ohne jegliche Transparenz.

Die adaptive und unvorhersehbare Natur von KI bedeutet, dass wirksame KI-Sicherheit ein tiefes Verständnis dafür erfordert, was bei Menschen, KI-Systemen und Agenten „normal" ist, damit die frühesten Anzeichen von Abweichungen, Missbrauch oder Kompromittierung erkannt werden können, bevor sie eskalieren.

VORTEILE FÜR UNTERNEHMEN

Einheitliche KI-Transparenz
Erhalten Sie Einblick in KI-Interaktionen über generative KI im Unternehmen, Agenten, Entwicklungsaktivitäten und Schatten-KI hinweg – in einer zentralen Ansicht für Verhaltensintelligenz.

Risikoerkennung in Echtzeit
Erkennen Sie subtilen Missbrauch, Abweichungen und entstehende Risiken in Prompts und im Verhalten von Agenten unmittelbar, ohne sich auf vordefinierte Regeln zu verlassen.

Richtlinienkonforme Governance
Gleichen Sie Ihre eigene Unternehmensrichtlinie mit KI-Aktivitäten ab, sodass die Governance an den Geschäftsprioritäten ausgerichtet und anhand der tatsächlichen KI-Nutzung bewertet wird.

Sichere KI-Einführung in großem Maßstab
Erweitern Sie den Einsatz von KI im gesamten Unternehmen – mit der Transparenz, dem Verständnis und der Kontrolle, die für ein Risikomanagement in großem Maßstab erforderlich sind.

1: McKinsey State of AI 2025
2: Darktrace-Forschung
3: Darktrace State of AI Cybersecurity 2026

Verhaltensbasierte Sicherheit für Ihre KI-Einführung

Basierend auf adaptiver KI nutzt Darktrace / SECURE AI mehr als ein Jahrzehnt an Erkenntnissen zum Nutzerverhalten, um die Nutzung von Prompts, Agenten und KI-Systemen in Ihrem gesamten Unternehmen abzusichern.

Anstatt sich auf vordefinierte Regeln oder Signaturen zu stützen, lernt es die Betriebsmuster Ihres Unternehmens kennen und deckt Missbrauch, Fehlkonfigurationen und Abweichungen auf, die herkömmliche, regelbasierte Kontrollmechanismen nicht erkennen können.

Bereitgestellt über das Darktrace Platform Portal, führt Darktrace / SECURE AI KI-Interaktionen in einer zentralen Ansicht zusammen und hilft Teams dabei, Absichten zu verstehen, Risiken zu bewerten, sensible Daten zu schützen und Richtlinien sowohl für menschliche Aktivitäten als auch für Aktivitäten von KI-Agenten durchzusetzen.

ENTWICKELT FÜR UNTERNEHMENS-KI-UMGEBUNGEN

Enterprise-GenAI	KI-Agenten
Low-Code	High-Code / Cloud-KI
Schatten-KI	SaaS
MCP	SASE

Wie Darktrace Ihre KI schützt

Die adaptive KI von Darktrace interpretiert bereits Mehrdeutigkeiten, deckt subtile Absichten auf und erkennt Abweichungen, bevor Aktivitäten oder Ereignisse in Ihrem Unternehmen gefährlich werden.

Die Ausweitung dieses Verhaltensansatzes auf KI ist ein logischer nächster Schritt – kein Sprung ins Ungewisse –, der auf der Darktrace Behavioral Defense Platform™ aufbaut, die bereits Menschen und Infrastruktur schützt.

Schatten-KI entdecken und kontrollieren

Darktrace hilft Ihnen dabei, nicht genehmigte oder unerwartete KI-Aktivitäten aufzudecken, wo immer sie auftreten – einschließlich der unbefugten Erstellung von Low-Code-Agenten und versteckter agentenbasierter Infrastruktur wie lokal bereitgestellter MCP-Server –, indem native und SECURE-KI-Transparenz mit Datenquellen aus Netzwerk, Cloud, Endgeräten und SASE kombiniert wird. Auf die jeweilige Umgebung abgestimmte Richtlinien und Reaktionspfade tragen dann dazu bei, Datenrisiken einzudämmen und Benutzer zu genehmigten Optionen zu leiten.

Überwachen Sie die Prompts, die GenAI-Agenten und -Assistenten steuern

Darktrace / SECURE AI bietet eine Echtzeitüberprüfung von Prompts, Sitzungen und Antworten in unternehmensweiten KI-Lösungen wie Microsoft Copilot und ChatGPT Enterprise, Low-Code-Umgebungen wie Copilot Studio, High-Code-Umgebungen wie Amazon Bedrock sowie bei SaaS-Anbietern wie Salesforce und Microsoft 365. Verhaltensanalysen können subtile Abweichungen in der KI-Aktivität aufdecken, die auf aufkommende Risiken hindeuten könnten, und helfen Unternehmen so, potenzielle Probleme wie die Offenlegung sensibler Daten, Jailbreak-Versuche und anderes unsicheres oder unerwartetes Verhalten zu erkennen.

Identitäten von KI-Agenten in Echtzeit absichern

Sie können Agentenidentitäten über Anbieter und Umgebungen hinweg ermitteln, deren Berechtigungen, Rollen und Verbindungen abbilden und das Verhalten in SaaS, Cloud, Netzwerk, Endgeräten, OT und E-Mail überprüfen. Diese Echtzeit-Auditansicht verschafft Unternehmen ein klares Verständnis ihrer KI-Agenten, einschließlich der Frage, wo sie eingesetzt werden, wie sie genutzt werden und über welche Berechtigungen sie verfügen. Dies hilft Teams dabei, potenzielle Risiken zu identifizieren und die Kontrolle in großem Maßstab aufrechtzuerhalten.

Bewerten Sie KI-Risiken bei der Entwicklung und Bereitstellung

Mit Darktrace / SECURE AI erhalten Sie Einblick in die Identitäten, Berechtigungen und Zugriffsrechte, die über Low-Code-Entwicklungsumgebungen wie Copilot Studio, High-Code-Plattformen wie Amazon Bedrock und interne Labore hinweg zusammengestellt werden. Das Posture-Management weist dabei auf Fehlkonfigurationen und anomale Entwicklungsereignisse hin, bevor ein Agent in die Produktion gelangt. / SECURE AI verknüpft diese Transparenz aus der Entwicklungshase anschließend mit dem Laufzeitverhalten.

Wählen Sie den Schutz, den Sie benötigen

Darktrace / SECURE AI ist in Paketen erhältlich, die darauf ausgelegt sind, verschiedene Reifegrade der KI-Sicherheit zu unterstützen, und folgt dabei demselben Einführungsweg „Core“, „Advanced“ und „Complete“ wie der Rest der Darktrace Behavioral Defense Platform.

CORE

Umfasst eine sofortige KI-Analyse und ein integriertes Schatten-KI-Management, um Transparenz über die genehmigte KI-Nutzung und die damit verbundenen Risiken sowie eine Zuordnung zur Richtlinienkonformität zu bieten.

ADVANCED

Erweitert Core um umfassendes Shadow-AI-Management, Agentenidentitäten und -aktionen sowie das Risikomanagement bei der Entwicklung von KI-Agenten, um eine tiefgreifendere Kontrolle über KI-Aktivitäten, das Verhalten der Agenten und die damit verbundenen Risiken zu ermöglichen.

„Sofort erhielten wir Einblick in die Informationen, die uns die ganze Zeit gefehlt hatten: **Wer nutzt was in unserem Unternehmen und was macht er mit den Daten?“**

■ VP of IT, US-Fertigung

■ **Über Darktrace**

Darktrace ist ein weltweit führender Anbieter von KI-gestützter Cybersicherheit, der Unternehmen dabei hilft, der sich ständig verändernden Bedrohungslandschaft jeden Tag einen Schritt voraus zu sein. Darktrace wurde 2013 in Cambridge, Großbritannien, gegründet und bietet eine unverzichtbare Cybersicherheitsplattform, die Unternehmen vor unbekannten Bedrohungen schützt, indem sie künstliche Intelligenz einsetzt, die in Echtzeit von jedem einzelnen Unternehmen lernt. Die Plattform und die Dienstleistungen von Darktrace werden von 2.300 Mitarbeitern unterstützt, die weltweit fast 10.000 Kunden schützen. Weitere Informationen finden Sie unter darktrace.com.

Nordamerika: +1 (415) 229 9100 | Europa: +44 (0) 1223 394 100 | Asien-Pazifik: +65 6804 5010 | Lateinamerika: +55 11 4949 7696

darktrace.com | info@darktrace.com

© 2026 Darktrace Holdings Limited. Alle Rechte vorbehalten.