

Das KI-Zeitalter mit verhaltensbasierter Sicherheit absichern

Preisgekrönte Partnerschaft. Sich ergänzende Technologien.

Microsoft unterstützt Unternehmen dabei, KI zu entwickeln, bereitzustellen und zu skalieren. Darktrace unterstützt Sie dabei, KI sicher zu betreiben.

Wenn KI nicht mehr nur Mitarbeitende unterstützt, sondern über Identitäten, Daten, Anwendungen und Infrastruktur hinweg handelt, müssen Sicherheitsteams mehr verstehen als nur, was zulässig ist. Sie müssen wissen, ob sich Nutzer, KI-Systeme und Agenten erwartungsgemäß verhalten, sobald sie im Unternehmen im Einsatz sind.

Microsoft legt die Identitäts-, Governance-, Datenschutz- und Sicherheitskontrollen fest, die bestimmen, was Benutzer und KI tun dürfen. Darktrace ergänzt den Verhaltenskontext über KI, Mitarbeiter und Infrastruktur hinweg, hilft Teams zu erkennen, wann Aktivitäten nicht mehr dem normalen Geschäftsverhalten oder dem beabsichtigten Zweck entsprechen, und reagiert, bevor Risiken eskalieren.

Wie Darktrace die Microsoft-Sicherheit erweitert



Bestehende Microsoft-Investitionen stärken

Fügen Sie Verhaltenskontext und Autonomous Response hinzu, um die Microsoft-Kontrollen für Identität, Governance, Compliance und native Sicherheit zu ergänzen.



Verstehen Sie Aktivitäten im Geschäftskontext

Gehen Sie über Berechtigungen und Richtlinien hinaus, um zu verstehen, wie sich Nutzer, KI-Agenten, Anwendungen und Infrastruktur tatsächlich verhalten.



Sichere KI bei zunehmender Verbreitung

Erweitern Sie die verhaltensbasierte Sicherheit auf Microsoft 365 Copilot, Microsoft Agent 365 und weitere unternehmensweite KI-Lösungen, während Kunden von E5 zu E7 wechseln.



Über alle Domänen hinweg schneller untersuchen und reagieren

Führen Sie Aktivitäten in den Bereichen KI, E-Mail, Identität, Cloud, Netzwerk, Endpunkt und OT zusammen, damit Angriffe als ein einziger Vorfall und nicht als isolierte Warnmeldungen verstanden werden.

Darktrace + Microsoft für KI, Menschen & Infrastruktur

Microsoft stellt die Plattformen und Sicherheitskontrollen bereit, während Darktrace in Ihrer Microsoft-Umgebung Verhaltenskontext in Echtzeit bereitstellt. Die folgenden Tabellen zeigen, wie Darktrace die Fähigkeiten von Microsoft in den einzelnen Bereichen ergänzt.

/ SECURE AI + Microsoft

Sichern Sie Ihre KI-Einführung von der Nutzung bis zur Runtime ab

Darktrace / SECURE AI erweitert Microsofts KI-, Identitäts- und Governance-Funktionen um Transparenz darüber, wie KI tatsächlich genutzt wird – von Prompts und Nutzern bis hin zu Agenten, Entwicklungsaktivitäten und Schatten-KI.

Microsoft bietet

Darktrace ergänzt

Microsoft 365 Copilot - KI-Erlebnisse für Unternehmen in Microsoft 365.

Überwacht unterstützte Prompts, Sitzungen und Antworten, um die Offenlegung sensibler Daten, Jailbreak-Versuche und unerwartetes KI-Verhalten zu erkennen.

Microsoft Copilot Studio - Tools zum Erstellen, Konfigurieren und Bereitstellen von KI-Agenten.

Verknüpft die Entwicklung und Konfiguration von Agenten mit ihrem Laufzeitverhalten, um Fehlkonfigurationen, anomale Aktivitäten und Abweichungen vom vorgesehenen Zweck aufzudecken.

Microsoft Entra + Agent 365 - Identität, Berechtigungen, Lebenszyklus und Governance für Benutzer und Agenten.

Bietet Einblick in Identitäten, Berechtigungen und Aktionen von Agenten, um übermäßige Zugriffsrechte, unerwartete Verbindungen und riskantes Verhalten zu erkennen.

Microsoft Entra Global Secure Access - Sichere Zugriffskontrollen über Benutzer, Geräte und Web-Aktivitäten hinweg.

Erweitert die Erkennung durch Schatten-KI mithilfe der Aktivitäten des unterstützten Secure-Web-Gateways, um nicht genehmigte KI-Dienste und deren Nutzung aufzudecken.

Microsoft Foundry + Defender for Cloud + Purview - Funktionen für KI-Entwicklung, Sicherheitslage, Governance und Datenschutz.

Identifiziert riskante Entwicklungsaktivitäten, Fehlkonfigurationen und übermäßige Berechtigungen und verknüpft dabei Erkenntnisse aus der Build-Phase mit KI-Aktivitäten zur Laufzeit.

„Darktrace / SECURE AI hat uns einen klareren Einblick in die KI-Aktivitäten im gesamten Unternehmen verschafft, einschließlich der von Mitarbeitenden verwendeten Tools und der Arten von Daten, die in Prompts auftauchen.“¹

■ Matthew Davis

Chief Information Security Officer,
ESL Federal Credit Union

¹: darktrace.com/news/darktrace-extends-behavioral-security-with-general-availability-of-darktrace-secure-ai

Basierend auf adaptiver KI

Adaptive KI ist die proprietäre KI-Technologie von Darktrace, die über mehr als ein Jahrzehnt hinweg weiterentwickelt wurde, um zu lernen, wie jede Organisation arbeitet, und für jede Sicherheitsherausforderung die passende KI-Technik einzusetzen.

Individuelles Verhaltensprofil

Ein sich ständig weiterentwickelndes Bild davon, wie sich Ihr Unternehmen verhält, vernetzt und über KI, Mitarbeiter und Infrastruktur hinweg agiert.

360°-Einblicke

Eine sich ständig weiterentwickelnde, zusammenhängende Übersicht über Erkenntnisse und Bedrohungen in der gesamten digitalen Infrastruktur.

Real-Time AI Analyst

Nutzt Echtzeit-Verhaltensanalysen, um Probleme zu erkennen, zu priorisieren, zu untersuchen und mit maschineller Geschwindigkeit darauf zu reagieren.

/ EMAIL + Microsoft

Kommunikation im Kontext der tatsächlichen Arbeitsweise von Menschen schützen

Darktrace / EMAIL ergänzt die E-Mail-, Kollaborations- und Datenschutzfunktionen von Microsoft, indem es Kommunikation im Kontext der tatsächlichen Arbeitsweise jedes Unternehmens versteht.

Microsoft bietet	Darktrace ergänzt
Defender for Office 365 - Nativer E-Mail- und Kollaborationsschutz.	Verhaltenskontext, der dabei hilft, hochentwickelte und neuartige Angriffe zu identifizieren und zu erkennen, mit einheitlichen Quarantäne-Workflows, die Untersuchung und Behebung optimieren können.
Microsoft Teams - Unternehmenskommunikation und Zusammenarbeit.	Erkennt Social Engineering und verdächtige Aktivitäten in unterstützten Teams-Unterhaltungen.
Microsoft Purview - Datenschutz-, Governance- und Compliance-Kontrollen.	Kombiniert Verhalten, Inhalte und Vertraulichkeitsbezeichnungen, um Datenverlust per E-Mail zu verhindern.
Microsoft Security Copilot - KI-gestützte Sicherheitsuntersuchungen und operative Workflows.	Erkenntnisse aus Darktrace-Untersuchungen und Kontext zur E-Mail-Sicherheit in den Workflows, die Sicherheitsteams bereits nutzen.

/ HYBRID NETWORK + Microsoft

Verstehen Sie Bedrohungen in der Infrastruktur, auf die KI und das Unternehmen angewiesen sind

Darktrace / HYBRID NETWORK erweitert den Microsoft-Sicherheitsschutz auf die gesamte hybride Umgebung und nutzt Verhaltenskontext, um Bedrohungen zu erkennen, während sie sich über Netzwerk, Cloud, Identität, Endpunkt und OT hinweg bewegen.

Microsoft bietet	Darktrace ergänzt
Microsoft Defender for Endpoint - Endpunkterkennung und -schutz.	Verknüpft Endpunktaktivitäten mit dem Netzwerk- und Infrastrukturverhalten, um Bedrohungen aufzudecken, die über einzelne Geräte hinausgehen.
Microsoft Sentinel - Sicherheitsanalysen, Incident-Management und Workflows für Sicherheitsabläufe.	Überführt Darktrace-Vorfälle und Erkenntnisse aus KI-gestützten Untersuchungen in Sentinel-Workflows und hilft Analysten, Bedrohungen zu priorisieren und schneller zu reagieren.
Microsoft Azure - Cloud-Infrastruktur und -Dienste.	Verhaltensbasierte Erkennung und Reaktion über Azure-Workloads und die gesamte hybride Infrastruktur hinweg.
Microsoft 365 + Hybridumgebungen - Produktivität, Identität und Unternehmensdienste.	Domänenübergreifender Kontext über Identität, Netzwerk, Cloud, Endpunkt und OT hinweg, damit Angriffe als ein einziger, sich weiterentwickelnder Vorfall verstanden werden können.

Gemeinsam besser für Sicherheitsteams

Weniger Zeit für das Zusammenführen von Warnmeldungen. Mehr Zeit, um dort zu handeln, wo es darauf ankommt.

Der Real-Time AI Analyst von Darktrace nutzt das Verständnis des Verhaltens der Organisation, um neu auftretende Bedrohungen auf der gesamten Plattform zu erkennen, zu untersuchen und zu priorisieren. In bestehenden Microsoft-Integrationen kann die bestehende Untersuchungsfunktion des Cyber-KI Analyst von Darktrace Workflows in Microsoft Sentinel und Security Copilot anreichern und Darktrace-Kontext in die Tools einbringen, die Analysten bereits nutzen.

„Darktrace und Microsoft bieten einander ergänzende Ansätze, die unserem Sicherheitsteam ein beruhigendes Gefühl geben. Wir wissen: Wenn auf der einen Seite etwas durchs Raster fällt, wird es auf der anderen erkannt.“²

■ **Mark Kane,**
Globaler Leiter für Informationslösungen,
Mainstream Renewable Power

2: darktrace.com/ja/customers/mainstream-renewable-power