

Protegiendo la era de la IA con seguridad conductual

Colaboración galardonada. Tecnologías complementarias.

Microsoft ayuda a las organizaciones a crear, implementar y escalar la IA. Darktrace le ayuda a operar la IA de forma segura.

A medida que la IA pasa de ayudar a los empleados a actuar en identidades, datos, aplicaciones e infraestructura, los equipos de seguridad necesitan saber algo más que lo que está permitido. Necesitan saber si los usuarios, los sistemas de IA y los agentes se comportan como se espera una vez que operan dentro de la empresa.

Microsoft establece los controles de identidad, gobernanza, protección de datos y seguridad que definen qué tienen permitido hacer los usuarios y la IA. Darktrace aporta contexto de comportamiento en la IA, las personas y la infraestructura, lo que ayuda a los equipos a identificar cuándo la actividad deja de ajustarse al comportamiento empresarial habitual o a la finalidad prevista, y responde antes de que el riesgo se agrave.

Cómo amplía Darktrace la seguridad de Microsoft



Refuerza las inversiones existentes en Microsoft

Añade contexto conductual y respuesta autónoma para complementar la identidad, la gobernanza, el cumplimiento normativo y los controles de seguridad nativos de Microsoft.



Comprende la actividad con el contexto empresarial

Va más allá de los permisos y las políticas para comprender cómo se comportan realmente los usuarios, los agentes de IA, las aplicaciones y la infraestructura.



Protege la IA a medida que aumenta su adopción

Amplíe la seguridad basada en el comportamiento a Microsoft 365 Copilot, Microsoft Agent 365 y una gama más amplia de IA empresarial a medida que los clientes pasan de E5 a E7.



Investiga y responde más rápido en todos los dominios

Reúne la actividad entre IA, correo electrónico, identidad, nube, red, endpoint y OT, para que los ataques se entiendan como un solo incidente, no como alertas aisladas.

Darktrace + Microsoft: protegiendo la IA, las personas y la infraestructura

Microsoft proporciona las plataformas y los controles de seguridad, mientras que Darktrace aporta contexto conductual en tiempo real en todo su entorno de Microsoft. Las tablas siguientes muestran cómo Darktrace complementa las capacidades de Microsoft en cada ámbito.

/ SECURE AI + Microsoft

Proteja la adopción de la IA desde el uso hasta la ejecución

Darktrace / SECURE AI amplía las capacidades de IA, identidad y gobierno de Microsoft al ofrecer visibilidad sobre cómo se utiliza realmente la IA, desde los prompts y los usuarios hasta los agentes, la actividad de desarrollo y la IA en la sombra.

Microsoft proporciona	Darktrace añade
Microsoft 365 Copilot - experiencias de IA empresarial en Microsoft 365.	Supervisa los prompts, las sesiones y las respuestas compatibles para identificar la exposición de datos confidenciales, los intentos de jailbreak y los comportamientos inesperados de la IA.
Microsoft Copilot Studio - Herramientas para crear, configurar e implementar agentes de IA.	Relaciona el desarrollo y la configuración de los agentes con su comportamiento en tiempo de ejecución para revelar configuraciones incorrectas, actividad anómala y desviaciones de su propósito previsto.
Microsoft Entra + Agent 365 - Identidad, permisos, ciclo de vida y gobernanza para usuarios y agentes.	Ofrece visibilidad sobre las identidades, los permisos y las acciones de los agentes para identificar accesos excesivos, conexiones inesperadas y comportamientos de riesgo.
Microsoft Entra Global Secure Access - Controles de acceso seguro para usuarios, dispositivos y actividad web.	Amplía la detección de la IA en la sombra mediante la actividad compatible del gateway web seguro para descubrir servicios y usos de IA no autorizados.
Microsoft Foundry + Defender for Cloud + Purview - capacidades de desarrollo de IA, postura de seguridad, gobernanza y protección de datos.	Identifica actividades de desarrollo de riesgo, configuraciones incorrectas y excesos de permisos, y conecta la información obtenida durante la fase de creación con la actividad de IA en tiempo de ejecución.

“Darktrace / SECURE AI nos ha proporcionado una visión más clara de la actividad de IA en toda la organización, incluidas las herramientas que utilizan los empleados y los tipos de datos que aparecen en los prompts.”¹

■ Matthew Davis

Director de Seguridad de la Información,
ESL Federal Credit Union

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

Impulsado por IA adaptativa

Adaptive AI adaptativa es la tecnología de IA propietaria de Darktrace, perfeccionada durante más de una década para aprender cómo opera cada organización y aplicar la técnica de IA adecuada a cada desafío de seguridad.

Perfil de comportamiento único

Una representación en evolución de cómo se comporta, se conecta y opera su organización en la IA, las personas y la infraestructura.

360° Insights

Una visión correlacionada y en continua evolución de la información y las amenazas en todo el entorno digital.

Real-Time AI Analyst

Utiliza la comprensión del comportamiento en tiempo real para detectar, realizar el triage, investigar y responder a la velocidad de las máquinas.

/ EMAIL + Microsoft

Proteja la comunicación en el contexto de cómo trabajan realmente las personas

Darktrace / EMAIL complementa las capacidades de Microsoft en materia de correo electrónico, colaboración y protección de datos al comprender la comunicación en el contexto del funcionamiento real de cada empresa.

Microsoft proporciona	Darktrace añade
Defender for Office 365 - protección nativa de correo electrónico y colaboración.	Contexto conductual para ayudar a identificar y detectar ataques sofisticados y novedosos, con flujos de trabajo unificados de cuarentena que pueden agilizar la investigación y la remediación.
Microsoft Teams - comunicación y colaboración empresarial.	Detecta la ingeniería social y la actividad sospechosa en las conversaciones de Teams compatibles.
Microsoft Purview - Controles de protección de datos, gobernanza y cumplimiento normativo.	Combina el comportamiento, el contenido y las etiquetas de sensibilidad para evitar la pérdida de datos por correo electrónico.
Microsoft Security Copilot - investigación de seguridad asistida por IA y flujos de trabajo operativos.	Resultados de las investigaciones de Darktrace y contexto de seguridad del correo electrónico en los flujos de trabajo que ya utilizan los equipos de seguridad.

/ HYBRID NETWORK + Microsoft

Comprenda las amenazas en toda la infraestructura de la que dependen la IA y su empresa

Darktrace / HYBRID NETWORK extiende la seguridad de Microsoft al entorno híbrido más amplio y utiliza el contexto de comportamiento para identificar amenazas a medida que se desplazan por la red, la nube, la identidad, el endpoint y la OT (tecnología operacional).

Microsoft proporciona	Darktrace añade
Microsoft Defender for Endpoint - detección y protección de endpoints.	Conecta la actividad de los endpoints con el comportamiento de la red y la infraestructura para descubrir amenazas que van más allá de los dispositivos individuales.
Microsoft Sentinel - Análisis de seguridad, gestión de incidentes y flujos de trabajo de operaciones de seguridad.	Integra los incidentes de Darktrace y los hallazgos de investigaciones basadas en IA en los flujos de trabajo de Sentinel, lo que ayuda a los analistas a priorizar las amenazas y acelerar la respuesta.
Microsoft Azure - Infraestructura y servicios en la nube.	Detección y respuesta basadas en el comportamiento en las cargas de trabajo de Azure y en el entorno híbrido más amplio.
Microsoft 365 + entornos híbridos - productividad, identidad y servicios empresariales.	Contexto multidominio en identidad, red, nube, endpoint y OT (tecnología operacional), para que los ataques puedan entenderse como un único incidente en evolución.

Mejor juntos para los equipos de seguridad

Menos tiempo reuniendo alertas. Más tiempo para actuar sobre lo que importa.

Real-Time AI Analyst de Darktrace utiliza la comprensión del comportamiento de la organización para detectar, investigar y priorizar las amenazas emergentes en toda la plataforma. En integraciones establecidas de Microsoft, la capacidad de investigación existente del Analista de Cyber AI de Darktrace puede enriquecer los flujos de trabajo de Microsoft Sentinel y Security Copilot, incorporando el contexto de Darktrace a las herramientas que ya utilizan los analistas.

“Darktrace y Microsoft ofrecen enfoques complementarios que aportan tranquilidad a nuestro equipo de seguridad. Sabemos que, si algo se escapa por un lado, el otro lo detectará”.²

■ Mark Kane,
Responsable Global de Soluciones de Información,
Mainstream Renewable Power

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