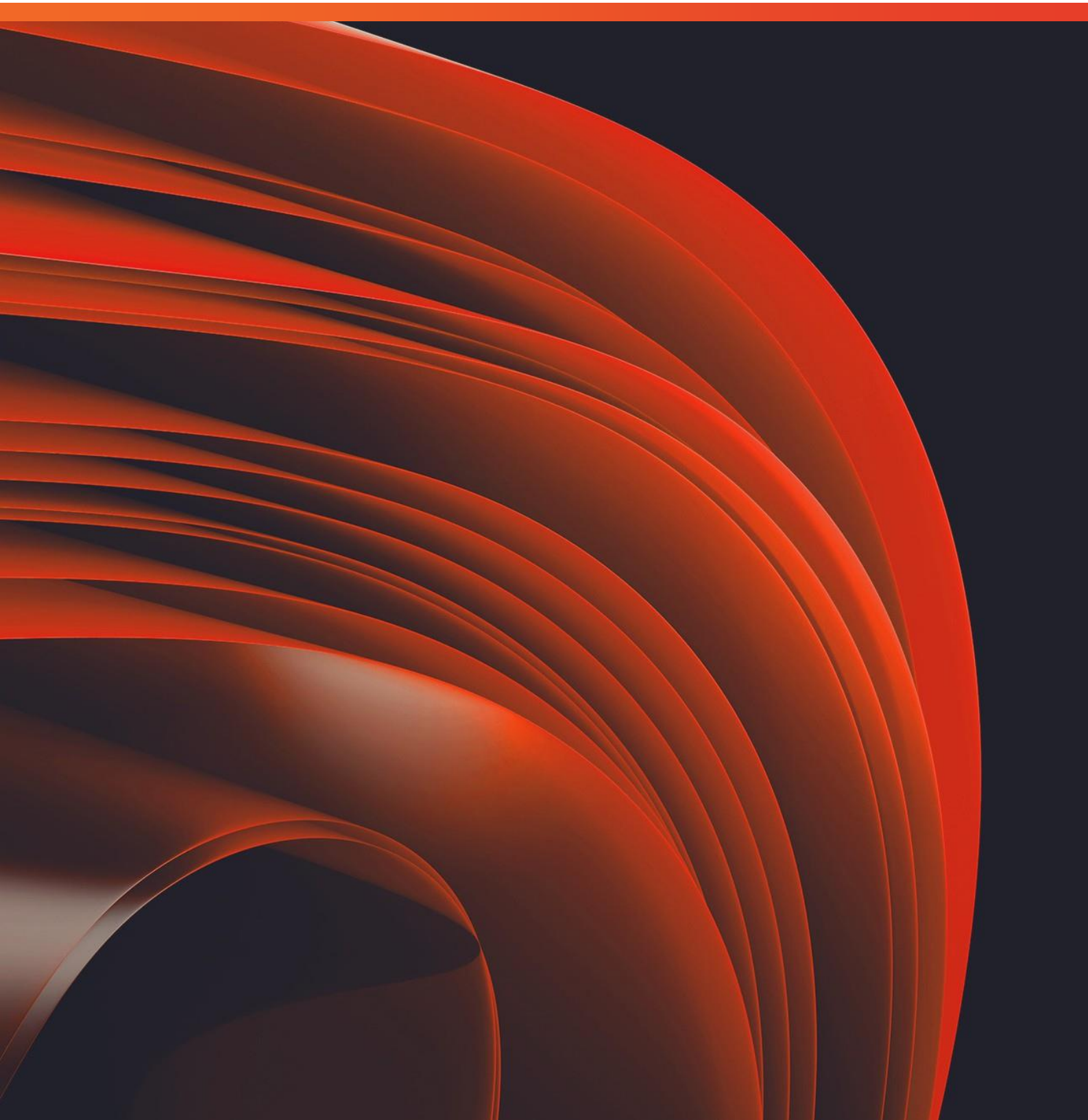
RESUMEN

Darktrace en profundidad



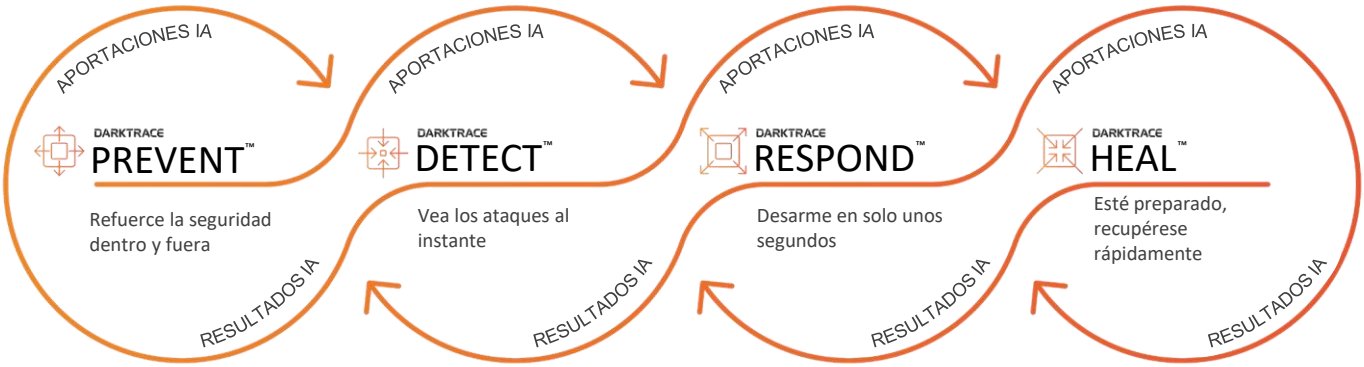
ÍNDICE

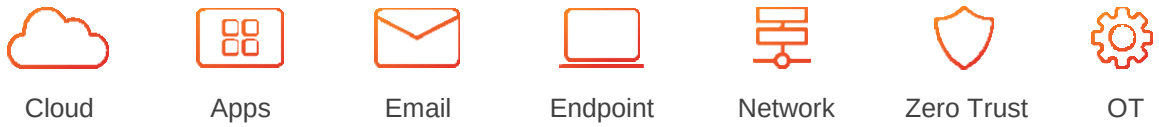
Resumen	**3**
DETECT	**5**
RESPOND	**6**
Email	**7**
Cloud	**9**
OT	**1**
Apps	**1**
Endpoint	**12**
Zero Trust	**13**
PREVENT	**14**
HEAL	**15**
	1
	7

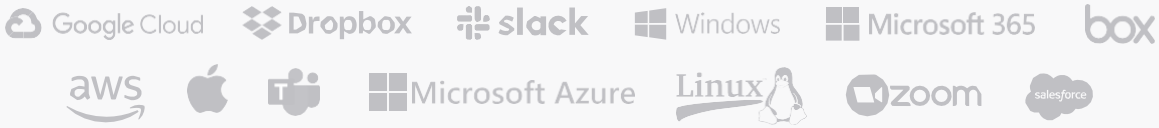
Resumen

Alrededor de 8.900 organizaciones confían en Darktrace para reducir el riesgo y minimizar la ciberinterrupción.

El conjunto de productos de Darktrace está dirigido por una inteligencia artificial que aprende cada detalle de su entorno único, creando una comprensión evolutiva de vuestros "patrones de vida" para detectar incluso las discretas desviaciones que indican una vulnerabilidad o amenaza. En cada interacción de todo su ecosistema digital, Darktrace pregunta: ¿Es esto normal?, basándose en puntos de datos sin procesar y características de datos mejoradas por la inteligencia artificial. Comprender vuestros patrones de vida es la clave para identificar e interrumpir todas las distintas ciberamenazas, desde ataques nuevos hasta amenazas internas. La IA de Autoaprendizaje está detrás de cada componente del Cyber AI Loop™, reforzando las soluciones de seguridad completas, personalizadas, siempre activas y en constante evolución basándose en modelos matemáticos únicos para cada organización individual, sin importar su tamaño o complejidad. No hay dos organizaciones iguales, y sus soluciones de seguridad tampoco deberían serlo.







La tecnología de Darktrace funciona en organizaciones de todos los tamaños y se puede llevar a cualquier entorno, protegiendo los servicios en la Nube y del correo electrónico, los endpoints, las tecnologías zero trust y las redes de IT/OT. En lugar de observar cada una de estas áreas de forma aislada, el análisis y la visibilidad multiplataforma de Darktrace le proporcionan el contexto que necesita para comprender la imagen completa de un ciberataque.

Productos de Darktrace

Darktrace Cyber AI Analyst™
Llevar al humano al bucle

Cyber AI Analyst de Darktrace está en el centro del bucle de Ciber IA, conectando los puntos entre eventos individuales para crear una imagen de todo el incidente de seguridad, antes de informar de ello a los equipos humanos.

Aplicación móvil de Darktrace
Neutralice las amenazas sobre la marcha

La aplicación móvil de Darktrace refuerza los equipos de seguridad para investigar y responder a las amenazas mientras están en curso.

Diseñada para una máxima flexibilidad, la aplicación móvil acelera la reducción de las amenazas al proporcionar notificaciones automáticas acerca de los ataques en curso, al mismo tiempo que permite a las organizaciones clasificar los incidentes y neutralizar las amenazas sin importar el momento o la situación.

> AI Analyst de Darktrace reduce aproximadamente 20 veces el tiempo que necesita un analista de SOC para ponerse al día; para nosotros, como equipo pequeño, esto supone una ventaja enorme y esencial.
>
> CIO
> / Aviación

Darktrace PREVENT™
Refuerce las defensas dentro y fuera

Darktrace PREVENT refuerza los equipos de seguridad para reducir el ciberriesgo priorizando las vulnerabilidades y fortaleciendo las defensas de forma proactiva.

Darktrace DETECT™
Vea los ataques al instante

Dirigida por una comprensión personalizada y en constante evolución acerca de vuestros patrones de vida, Darktrace DETECT ofrece una visibilidad instantánea de las amenazas, incluso de aquellas que utilizan nuevas técnicas o nuevas cepas de malware.

Darktrace RESPOND™
Desarme en solo unos segundos

Darktrace RESPOND utiliza su comprensión acerca de su organización única para realizar acciones precisas y dirigidas, interrumpiendo los ciberataques sin afectar a las operaciones normales del negocio.

Darktrace HEAL™
Esté preparado, recupérese rápidamente

La familia de productos HEAL permite a las organizaciones recuperarse en el caso de un ciberataque devolviendo los sistemas a un estado operativo fiable.

DARKTRACE DETECT™

Reduzca el tiempo de clasificación

Cyber AI Analyst conecta amenazas individuales para investigar ataques a gran velocidad y escala. Crea informes de incidentes acerca de eventos críticos y el contexto que los rodea, sustituyendo el análisis que normalmente correspondería a un humano. Al centrarse en las amenazas de mayor prioridad, su equipo de seguridad puede ahorrarse un valioso tiempo y dirigir su experiencia al trabajo de alto valor que mejor hacen los humanos.

IA de Autoaprendizaje, entrenada en los datos de su negocio

Mientras otras soluciones de ciberseguridad están entrenadas para identificar amenazas basándose en datos y técnicas de ataques antiguos, Darktrace DETECT adopta un enfoque totalmente diferente al tratar de comprender en profundidad su organización y su estado 'normal'. Crea una comprensión personalizada de su entorno digital, analizando continuamente sus usuarios, activos, dispositivos y las complejas relaciones entre ellos.

A través del aprendizaje de la dinámica diaria de su organización, Darktrace DETECT puede identificar las discretas desviaciones de la actividad normal que indican amenazas emergentes y nunca antes vistas: aprende lo que es normal para identificar lo que es anormal.

> Los algoritmos de la inteligencia artificial de Darktrace se centran en una cosa: su organización.

CIO
/ Asistencia sanitaria

Instalación rápida, efectivo en cuestión de días

Tanto si se implementa en un área protegida específica como en toda su organización, Darktrace DETECT es rápido y fácil de instalar: se instala en cuestión de minutos y aprende el patrón de vida normal de su empresa en una semana. Gracias a que DETECT aprende 'sobre la marcha', continúa adaptándose a su organización a medida que crece y cambia, ofreciendo protección a largo plazo contra las amenazas nuevas en un panorama de amenazas en evolución.

> AI Analyst es sofisticado y la información que nos proporciona es clara y procesable, incluso mis empleados más novatos e inexpertos pueden utilizarlo y aprender de él desde el primer día.

CISO
/ Dirección de IT

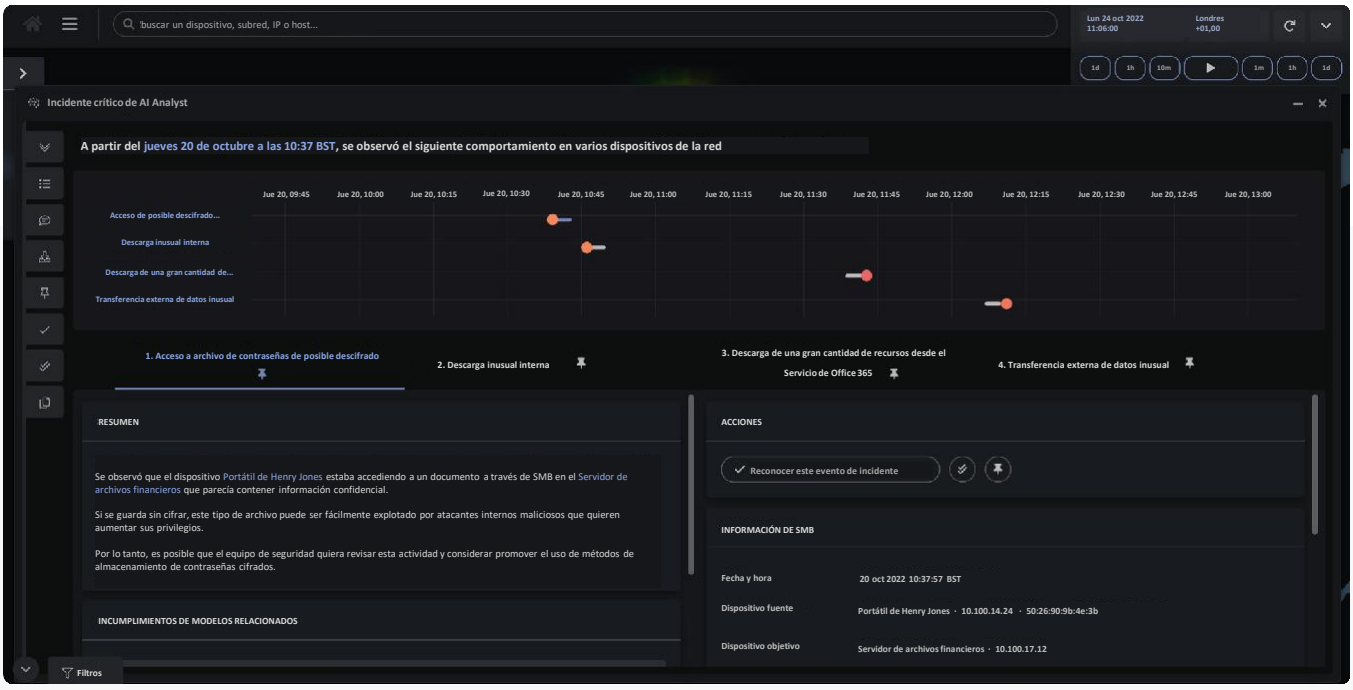


Figura 1: Cyber AI Analyst mostrando un informe de incidentes

DARKTRACE RESPOND™

Respuesta Autónoma para reforzar su 'Normalidad'

Mientras que otras soluciones de respuesta automática normalmente se entrenan en datos de ataques antiguos y, a menudo, se limitan a una respuesta binaria, Darktrace RESPOND adopta un enfoque totalmente diferente.

Utiliza la tecnología de inteligencia artificial para crear una comprensión dinámica de lo que es 'normal' para su organización. Al hacerlo, forma una comprensión personalizada y multidimensional de cada usuario, dispositivo y todas las complejas relaciones entre ellos en cualquier entorno.

Al aprender las operaciones diarias normales de toda su organización, Darktrace descubre patrones discretos, nunca vistos anteriormente, y amenazas emergentes que de otra forma pasarían desapercibidas.

Entonces puede realizar acciones proporcionadas; por ejemplo, bloquear un enlace o reescribir un archivo adjunto en lugar de retener un correo electrónico o bloquear una conexión específica a través de un puerto en lugar de poner en cuarentena un dispositivo. Esto permite que las operaciones del negocio puedan continuar sin problemas al mismo tiempo que se mantienen seguras.

Gracias a que la inteligencia artificial aprende 'sobre la marcha' para mejorar continuamente su comprensión acerca de lo que es 'normal', incluso cuando su negocio crece y realiza cambios, Darktrace RESPOND se adapta a las nuevas tecnologías, empleados y sistemas añadidos.

Cree confianza en la toma de decisiones autónoma

Darktrace RESPOND es personalizable: los usuarios pueden ajustar los parámetros para determinar cómo y cuándo debe actuar.

Es posible que quieran que la inteligencia artificial actúe solamente a ciertas horas del día, en ciertos dispositivos o en respuesta a ciertos eventos. La inteligencia artificial toma millones de microdecisiones en segundo plano, animando a los equipos humanos a centrarse en tomar decisiones estratégicas que se alineen con las necesidades del negocio. A medida que la inteligencia artificial desarrolla su comprensión acerca del entorno, la mayoría de las organizaciones optan por un modo totalmente autónomo fuera del horario laboral y mantienen una autonomía parcial durante las horas de trabajo con el modo de confirmación humana.

> Tardé un poco de tiempo en ganarme la confianza de nuestro equipo con la Respuesta Autónoma, pero ojalá lo hubiera hecho antes, porque es realmente buena.
>
> Pudimos cancelar algunas otras tecnologías y ahorrarnos algunos costes gracias a ello.
>
> Associate Executive Director
> / Legal

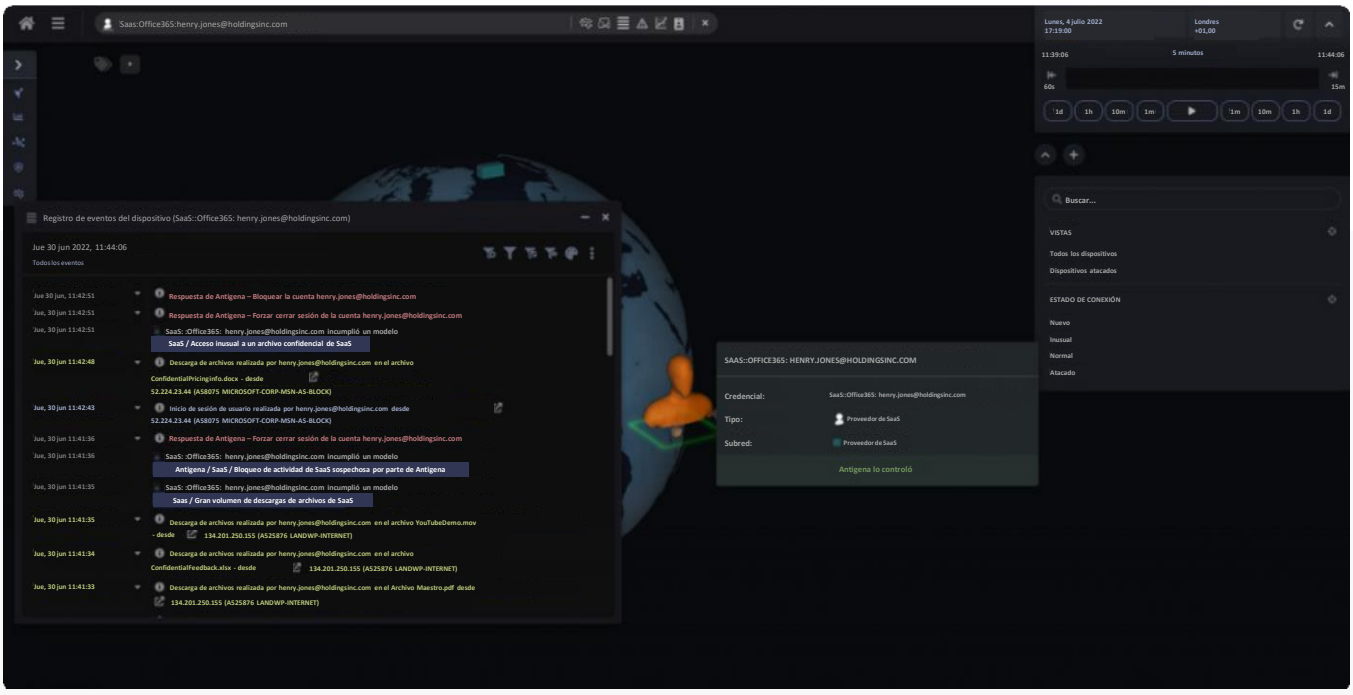


Figura 2: Darktrace RESPOND actuando en una ciberamenaza

DARKTRACE Email

Las amenazas de correo electrónico han evolucionado. Es hora de que evolucione también la seguridad de su correo electrónico.

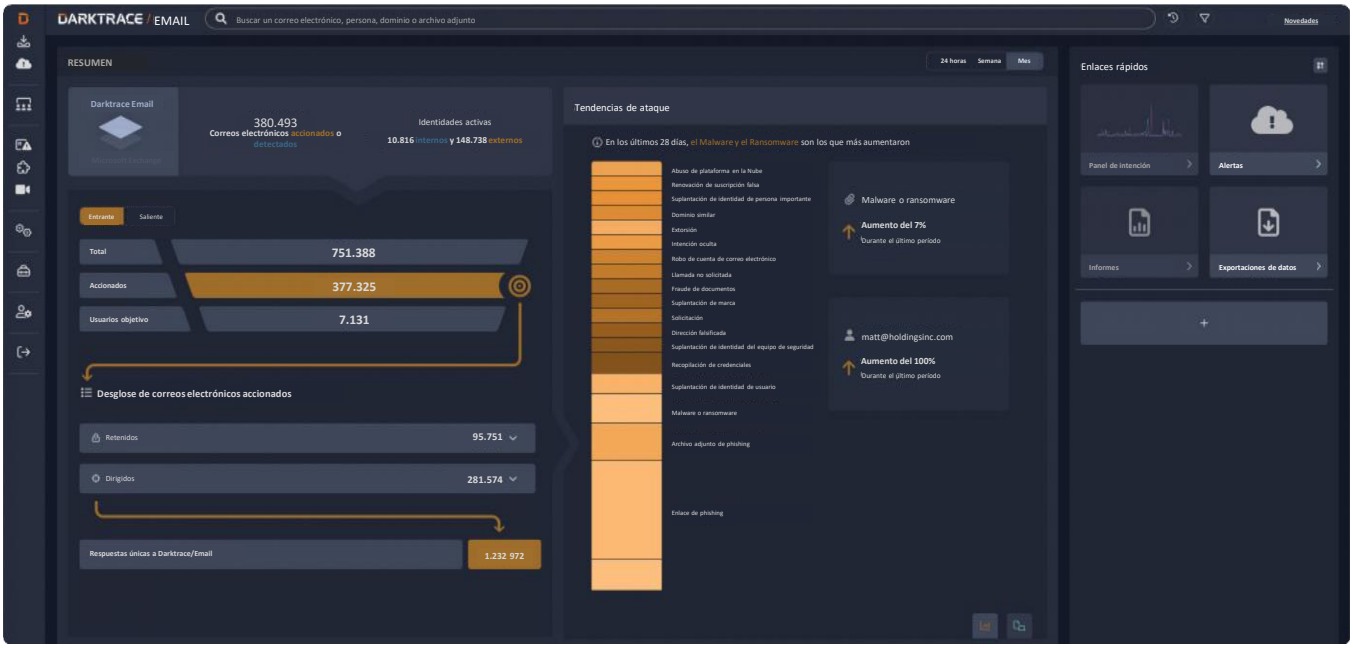
A medida que las campañas de phishing son cada vez más dirigidas y los ataques nuevos son más comunes, la seguridad tradicional del correo electrónico que analiza los ataques antiguos cada vez es más inadecuada.

Se necesita un nuevo enfoque para la seguridad del correo electrónico.

Una comprensión evolutiva de su organización

Darktrace/Email aprende lo que es 'normal' para cada usuario de correo electrónico, incluyendo sus relaciones, tono y sentimiento, patrones de intercambio de contenido y enlaces, y otras miles de señales, en todo el correo electrónico y más allá.

En lugar de entrenarse en ataques antiguos, la IA de Darktrace desarrolla una comprensión evolutiva del humano que hay detrás de las comunicaciones por correo electrónico, lo que significa que puede detectar desviaciones de la actividad normal que indican una amenaza de correo electrónico, incluso aunque sea muy dirigida o nunca se haya visto antes.



Neutraliza todas las amenazas de correo electrónico, incluyendo:

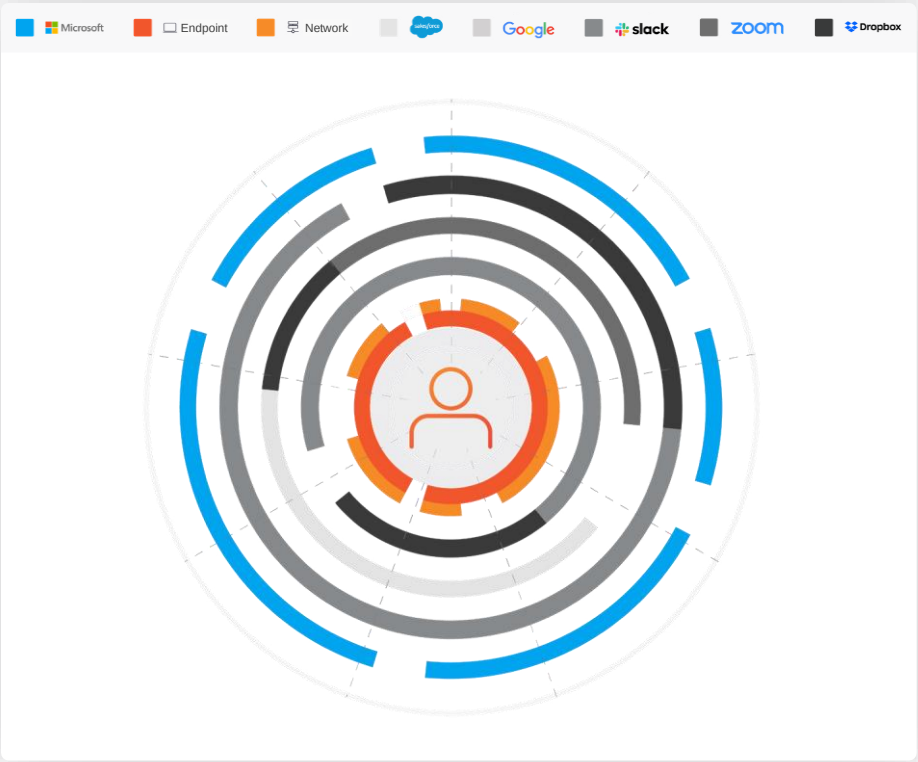
- Phishing
- Robo de cuenta
- BEC
- Suplantación de identidad
- Ataque a cadena de suministro
- Extorsión
- Malware / Ransomware
- Y más

Una respuesta dirigida

Su comprensión del negocio permite a Darktrace/Email entender la naturaleza de una amenaza, lo que permite realizar acciones dirigidas y adecuadas en todos los tipos de ataques. Mientras que otras herramientas se basan en mecanismos binarios de toma de decisiones que "bloquean" o "permiten", Darktrace RESPOND puede realizar la acción menos agresiva necesaria para neutralizar solamente el componente de riesgo del correo electrónico. El resultado para las organizaciones es una interrupción mínima de las operaciones normales, sin tener que comprometer el riesgo.

Las posibles acciones incluyen:

- ✓ Mover a correo no deseado
- ✓ Bloquear un archivo adjunto
- ✓ Reescribir un enlace sospechoso
- ✓ Eliminar la suplantación de identidad del remitente
- ✓ Denegar acceso a un enlace
- ✓ Eliminar un archivo adjunto
- ✓ Retener todo el mensaje



Protección contra robo de cuentas

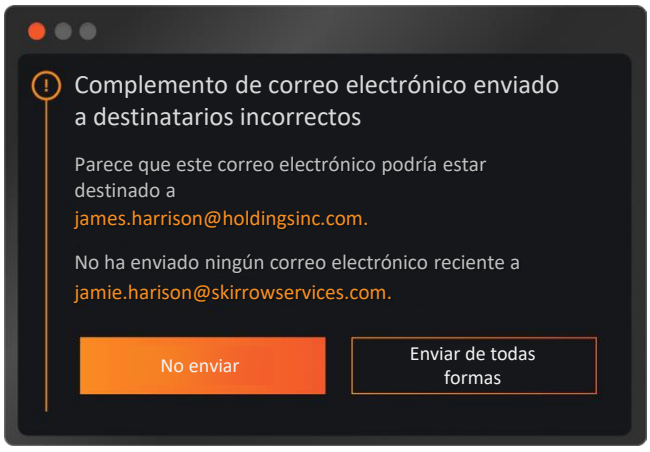
Darktrace comprende el comportamiento 'normal' del usuario, no solo en la bandeja de entrada sino también de la actividad basada en la cuenta, para protegeros contra el robo de cuentas. Los usuarios no se definen únicamente por su actividad del correo electrónico: para tener un contexto completo, es crucial comprender su actividad en Microsoft 365, Salesforce, Dropbox e incluso en su dispositivo en la red.

Con esta vista de 360 grados del usuario, se pueden ver y solucionar los discretos indicadores de un ataque a una cuenta, dondequiera que aparezcan.

Toda la actividad relevante relacionada con un ataque se presenta entonces en un único panel de cristal, con Darktrace respondiendo de forma autónoma para bloquear a los atacantes cuando es necesario.

Evite la pérdida accidental de datos debido a correos electrónicos enviados a destinatarios incorrectos

Gracias a que Darktrace sabe lo que es normal y lo que se espera de cada usuario, puede evitar contratiempos en el correo electrónico, en los que un empleado envía información confidencial al destinatario equivocado.



Bucle de retroalimentación de empleado-IA

Los empleados tienen la opción de ver el análisis completo de Darktrace de un correo electrónico antes de tomar una decisión informada de "marcarlo como seguro" o "informar a seguridad", lo que agiliza los flujos de trabajo del equipo de seguridad y, al mismo tiempo, enseña a los empleados.

Estas acciones se retroalimentan en la IA que, como resultado, mejora gradualmente su toma de decisiones. Darktrace/Email también mejora la productividad de los empleados al aprender sus hábitos de lectura y eliminar el spam y el correo no deseado.

DARKTRACE Cloud

Proteja su Nube en tiempo real

Los líderes empresariales continúan adoptando la Nube para mejorar la eficiencia y la flexibilidad. Si bien la Nube permite entornos escalables, de alta disponibilidad y de rápido movimiento para las empresas, a los ciberdelincuentes se les presentan nuevas vías de explotación.

Los equipos de seguridad tienen dificultades para obtener visibilidad en tiempo real, seguir el ritmo de las amenazas en evolución y manejar la complejidad que ofrece la Nube. Darktrace/Cloud Security utiliza IA de Autoaprendizaje para proporcionar una ciberresiliencia completa para entornos multinube.

Seguridad completa en la Nube

Darktrace/Cloud va más allá de las ofertas tradicionales de CNAPP y combina los aspectos más críticos de la seguridad de la Nube en una **única solución de IA:**

Conocimiento de la arquitectura

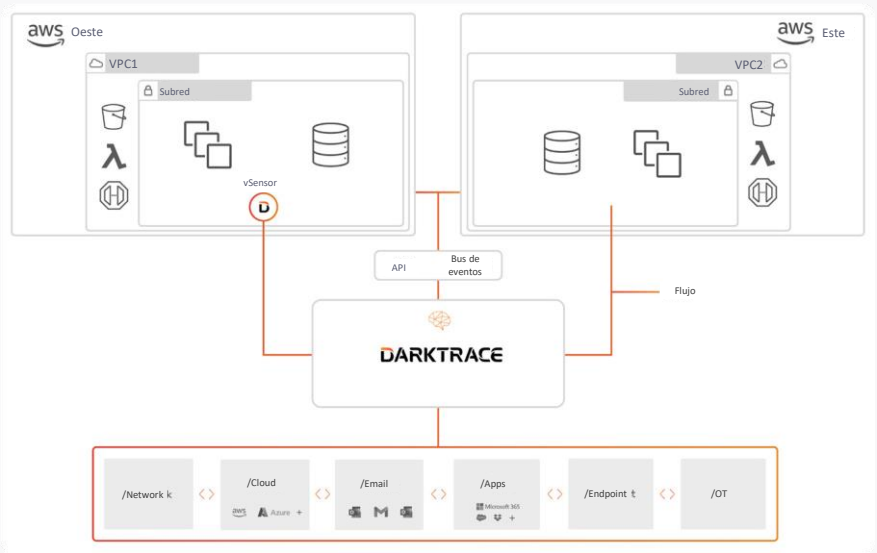
Ofrece a los usuarios una comprensión de su huella en la Nube, incluyendo la visibilidad en tiempo real de los activos, arquitecturas, usuarios y permisos de la Nube. Combina enumeración de activos, arquitecturas modeladas y análisis de registros de flujo. Los conocimientos sobre costes ofrecen una mejor comprensión de la asignación de recursos, lo que ayuda a los equipos a contextualizar los recursos.

Detección y respuesta nativa de la Nube

La IA entiende lo que es 'normal' para su negocio y detiene las ciberamenazas con una respuesta autónoma. La respuesta casi en tiempo real va más allá de simples alertas por correo electrónico o abrir un ticket, e incluye acciones nativas de la Nube como separar instancias EC2 y aplicar grupos de seguridad para contener activos en riesgo.

Cumplimiento y protección en la Nube

Identifique problemas de cumplimiento y posibles errores de configuración, con modelado de rutas de ataque y pasos de solución priorizados. Attack Surface Management (ASM, 'gestión de superficie de ataque') de Darktrace añade una visión externa crítica de su organización, destacando las vulnerabilidades que más afectan a su organización específica y mostrando la TI en la sombra.



Instalación rápida y sencilla con minuciosidad allá donde lo necesite

- ✓ Se despliega desde la Nube en cuestión de minutos
- ✓ Datos extraídos de agentes de servidor ligeros basados en host o de una combinación de duplicación de tráfico y registros de API.
- ✓ Admite entornos híbridos y sin servidor
- ✓ Disponible en el marketplace de AWS

La visibilidad completa de la arquitectura a través de un despliegue sin agentes puede mostrar áreas en las que desee desplegar agentes de Darktrace para un análisis más profundo.

- ✓ Obtenga una comprensión inmediata de su huella en la Nube, incluyendo la visibilidad en tiempo real de los activos y arquitecturas de la Nube, así como de los usuarios y los permisos.
- ✓ Identifique los errores de configuración, las vulnerabilidades y los problemas de cumplimiento y priorice sus acciones basándose en el riesgo real en la Nube.
- ✓ Identifique vías críticas de ataque con Attack Surface Management y modelado de rutas de ataque.
- ✓ Los conocimientos sobre costes le ofrecen una mejor comprensión de la asignación de recursos, lo que ayuda a los equipos a contextualizar los recursos.

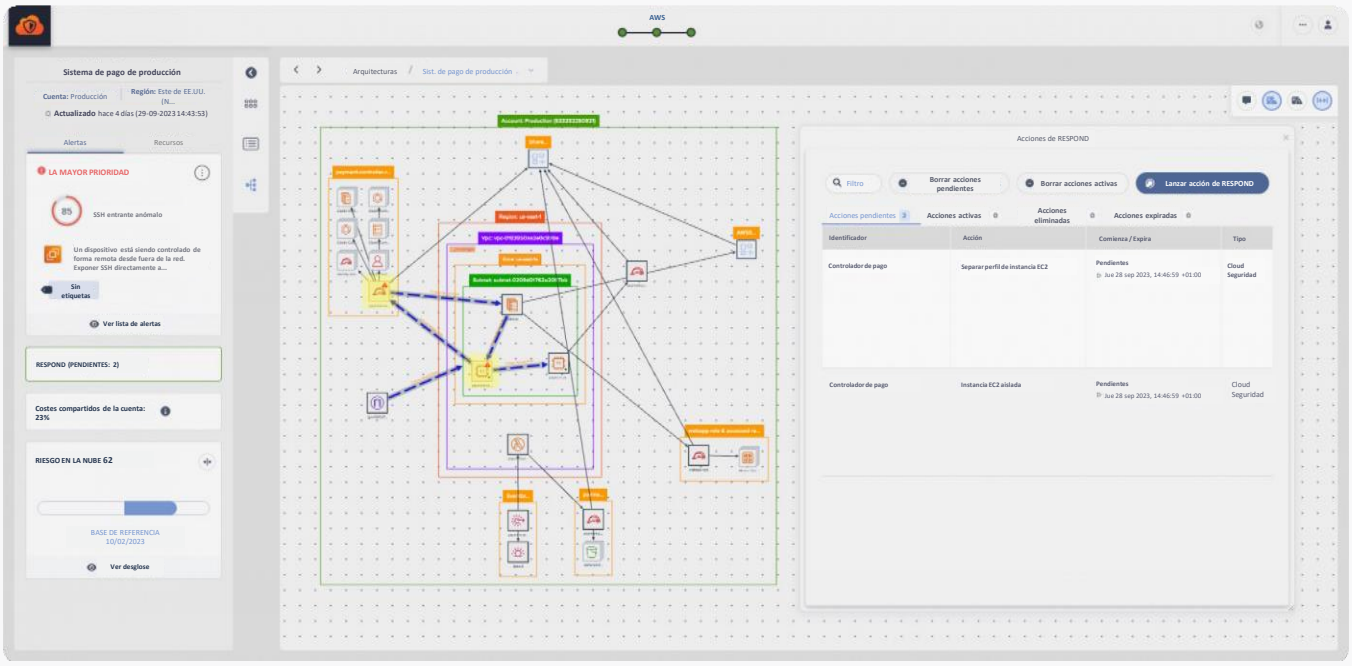


Figura 3: Darktrace modela las arquitecturas en la Nube y destaca los riesgos relevantes

Aprende continuamente lo que es 'normal' en toda su red

La base de Darktrace/Cloud es la tecnología de IA de Autoaprendizaje que aprende de sus datos empresariales únicos para identificar riesgos y amenazas en tiempo real. En lugar de aprender de los datos de ataques de miles de organizaciones, Darktrace utiliza una comprensión dinámica de su huella única en la Nube, en la capa de administración, red y arquitectura.

El 86% de las empresas reportan un aumento en el volumen y/o alcance de sus iniciativas en la Nube desde 2020

Accenture

Esta monitorización profunda del comportamiento en la Nube permite la detección en tiempo real de amenazas en todas las cargas de trabajo y entornos en contenedores como Kubernetes. Cuando se detecte una ciberamenaza, Darktrace iniciará una respuesta inteligente, dirigida y autónoma utilizando controles nativos de la plataforma (grupos de seguridad y restricciones de políticas/roles) e interactuando con la red subyacente.

> Para nuestro pequeño equipo de seguridad, la visión unificada que Darktrace nos ofrece de nuestra infraestructura multinube e híbrida ha cambiado las reglas del juego.

Senior Information Security Engineer
/ Banco Comercial

DARKTRACE OT

Un enfoque de autoaprendizaje para las nuevas amenazas

En lugar de basarse en indicadores de ataques (IoC) predefinidos y retroalimentación de amenazas externas, Darktrace analiza los datos nativos de un ecosistema ICS a través de capas de aprendizaje automático para detectar cualquier comportamiento inusual, sin importar si la fuente es humana o una máquina. Este enfoque de autoaprendizaje permite a Darktrace detectar ataques conocidos y desconocidos en la misma capacidad; incluyendo, entre otros: vulnerabilidades de seguridad de día cero, ataques a cadenas de suministro, amenazas internas, ransomware y dispositivos infectados antes del despliegue.

Visibilidad completa

Al ser independiente de protocolos y tecnologías, Darktrace no necesita acceder a protocolos específicos para realizar su detección de amenazas, lo que permite a la IA identificar la actividad anormal sin importar dónde ocurra en el ecosistema digital. Al mismo tiempo, Darktrace puede leer más de 50 protocolos industriales diversos; incluyendo Modbus, IEX-61950, CIP y BACnet. Esto permite a la tecnología proporcionar visibilidad en una amplia variedad de entornos industriales personalizados, sin importar si emplean dispositivos con décadas de antigüedad o las últimas tecnologías de IIoT e ICSaaS.

Mostrando la convergencia de IT/OT

Con la capacidad de proporcionar una vista unificada de todos los entornos de IT y OT, Darktrace está en una posición única para destacar cualquier punto de convergencia de IT/OT.

En un estudio anónimo de su base de clientes, Darktrace detectó más de 6.500 casos sospechosos de uso de protocolos de ICS en 1.000 entornos empresariales. El protocolo de ICS que más se detectó en esta revisión fue BACNet, observado en aproximadamente el 75% de los casos.

Mostrar estos puntos de convergencia es un paso fundamental para evitar que los ataques pasen de infecciones virtuales a interrupciones de procesos físicos.

Vista unificada

Darktrace/OT proporciona una visión unificada de todos los sistemas de IT y OT. En el panorama de amenazas actual, donde muchos ataques están dirigidos a la infraestructura de OT después de pasar por entornos de IT, esta vista unificada se ha convertido en una herramienta invaluable para detectar y neutralizar las amenazas antes de que se produzca el daño.

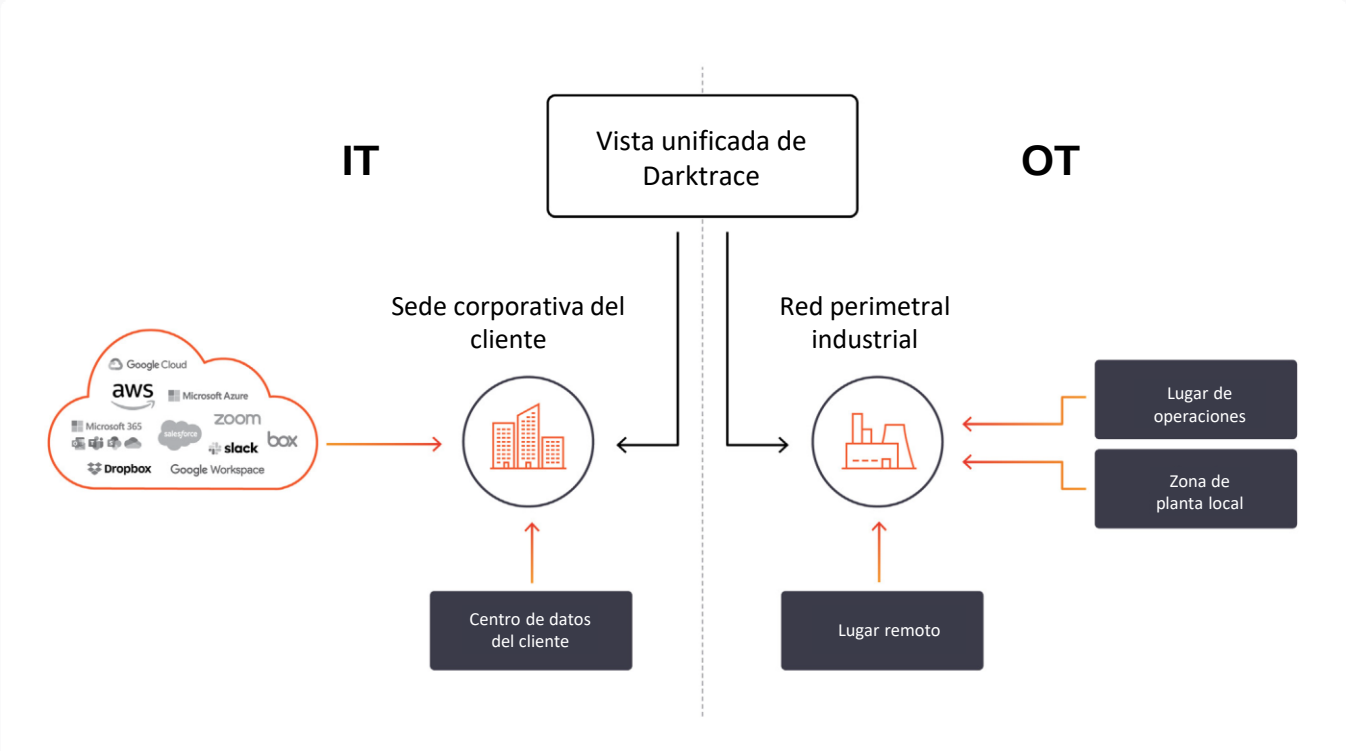


Figura 4: Darktrace ofrece una visibilidad completa de todo el OT, IT e IIoT

DARKTRACE

Apps

Proteja su SaaS con la Respuesta Autónoma

Nunca ha habido tantos datos críticos en aplicaciones en la Nube, lo que significa que los equipos de seguridad deben encargarse de defender un complejo entramado de servicios con controles de seguridad nativos que generalmente se basan en datos de ataques anteriores y son incompatibles con todas las plataformas. Los líderes de seguridad están abandonando las herramientas que se centran en el ataque, se basan en la información de amenazas y se limitan a una sola área del estado digital.

Darktrace/Apps comprende el negocio digital, muestra las discretas desviaciones que indican una ciberamenaza y, después, actúa con una respuesta autónoma y específica.

Proteja su SaaS con la Respuesta Autónoma

zoom Dropbox box Google slack salesforce Microsoft 365

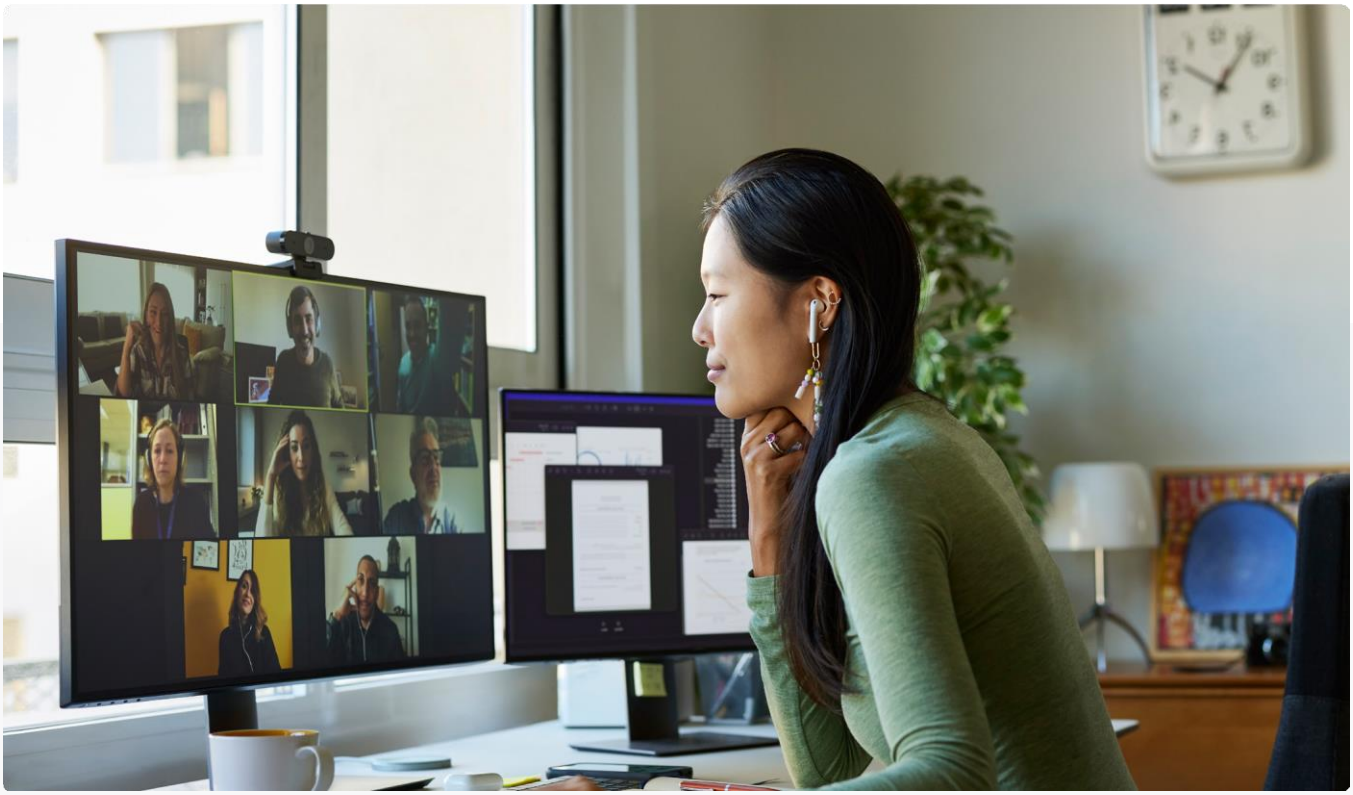
Uso de la inteligencia artificial con contexto

Los ciberataques modernos atraviesan múltiples campos de operación.

Los datos de las aplicaciones en la Nube a menudo son solo una pieza del rompecabezas, por eso la IA de Darktrace proporciona un contexto obtenido a partir de todo su ecosistema digital, aprende el "patrón de vida" normal de cada usuario para identificar las posibles amenazas, basándose en millones de puntos de datos, incluyendo el comportamiento de inicio de sesión, la actividad de administración, las transferencias de archivos y mucho más. Darktrace/Apps aprende su negocio único, así como todos los usuarios de aplicaciones en la Nube y las aplicaciones que utilizan, para detectar comportamientos que no pertenecen a ellos.

> Añadimos Darktrace a nuestra pila de ciberseguridad y ya ha dado sus frutos: nos notifica en cuestión de minutos cuando se vulnera una cuenta de Microsoft 365.

Director of IT
/ Agencia de Empleo



DARKTRACE

Endpoint

Protección para cada dispositivo

Debido a que los empleados se alejan de los lugares de trabajo corporativos tradicionales, las VPN no siempre son suficientes para mantener la red y los dispositivos seguros. Darktrace/Endpoint monitoriza todas las actividades en los dispositivos endpoint y realiza acciones contra cualquier ataque emergente.

Protección contra las amenazas conocidas y nuevas

Darktrace/Endpoint no se basa en información de amenazas, suposiciones previas ni algoritmos basados en reglas. La IA de Autoaprendizaje de Darktrace comprende los patrones normales de los usuarios de endpoints y detecta la actividad inusual que podría representar una amenaza, incluso amenazas que su organización nunca había visto antes.

Respuesta Autónoma frente a ataques de endpoint

Las actividades de los endpoints se investigan y analizan comparándolas con toda la empresa digital para obtener un mejor contexto y conocimiento de la situación. Los resultados se retroalimentan en el sistema de forma autónoma para determinar al instante la respuesta adecuada a las amenazas y realizar acciones quirúrgicas cuando sea necesario.

Microsoft

Darktrace/Endpoint se integra rápida y fácilmente con soluciones de antivirus y EDR como Microsoft Defender for Endpoint.

Mientras que Defender se enfrenta a malware y amenazas externas conocidas, la IA de Autoaprendizaje de Darktrace ofrece la comprensión necesaria para detectar y responder a ataques internos maliciosos y detener las amenazas.

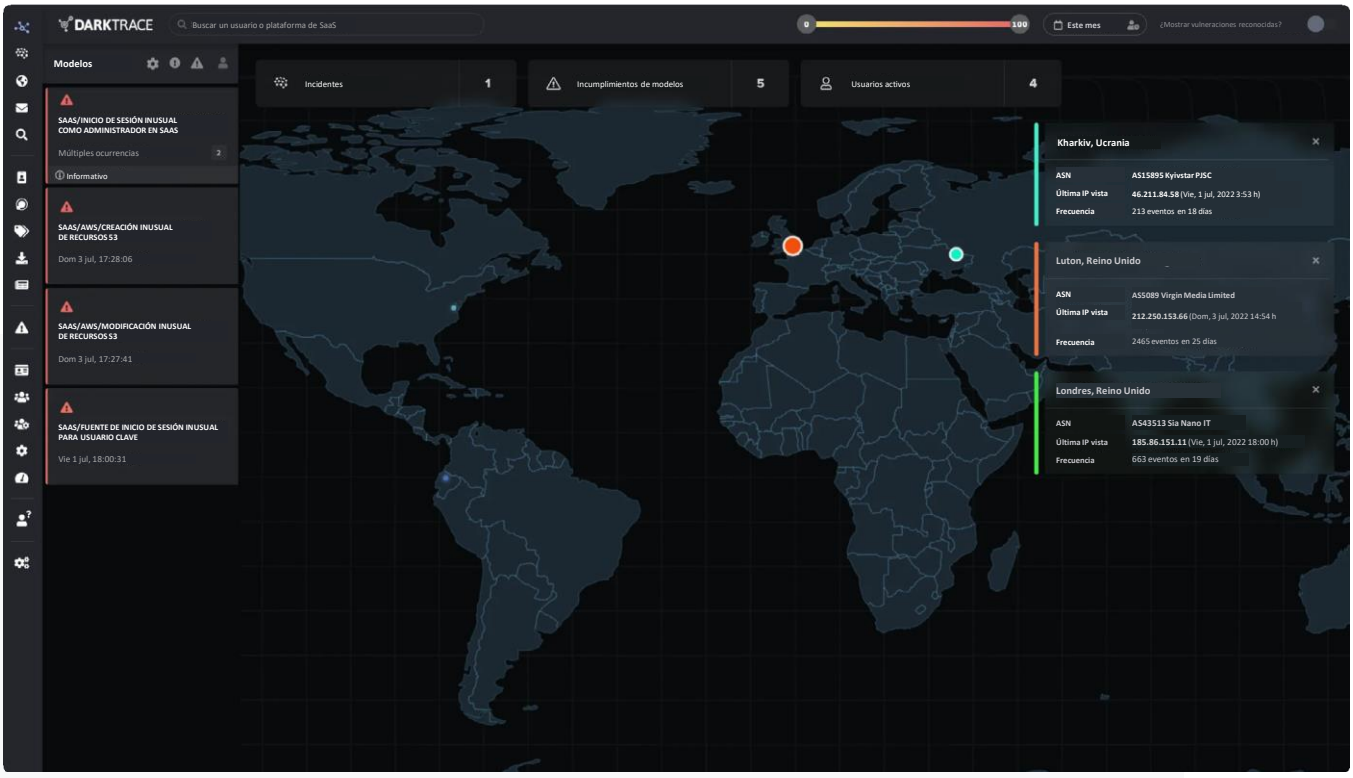


Figura 5: La IA de Autoaprendizaje de Darktrace analiza cada conexión del endpoint

DARKTRACE

Zero Trust

IA que se adapta a su negocio único

Sus políticas de confianza cero son tan sólidas como su conocimiento del ecosistema digital en constante cambio de la organización.

Darktrace/Zero Trust aplica un aprendizaje continuo que forma patrones normales y anormales de toda la red corporativa, el correo electrónico, la Nube y las plataformas de colaboración, así como de los endpoints remotos.

Acción dirigida contra amenazas

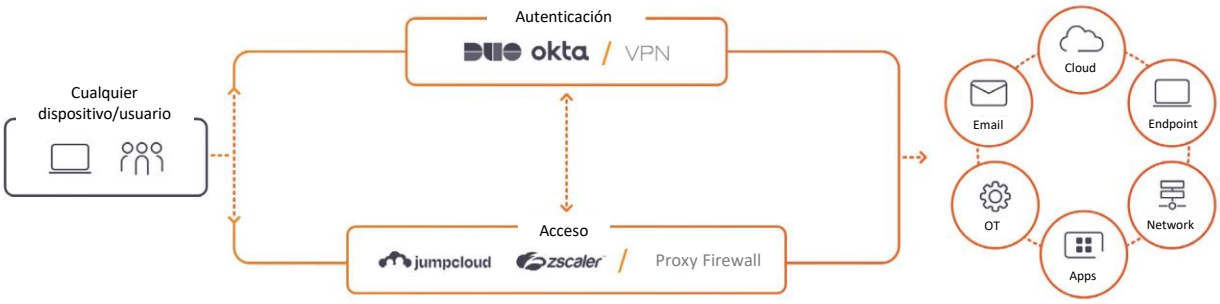
Cuando se produce una actividad maliciosa a pesar de forzar reglas y políticas de confianza cero, Darktrace puede alertar y activar al instante una respuesta proporcionada para contener el ataque.

Cuando se despliega con tecnología de confianza cero, el alcance de la actividad visible para Darktrace se amplía y sus tecnologías de inteligencia artificial también pueden analizar, contextualizar y actuar en ese ámbito. Al detectar un comportamiento inusual que indica una clara ciberamenaza, la Respuesta Autónoma de Darktrace puede realizar directamente las acciones adecuadas a través de la API correspondiente, que van desde acciones tan quirúrgicas como bloquear conexiones entre dos endpoints hasta la finalización completa de toda la actividad específica de un dispositivo.

Se integra con herramientas existentes

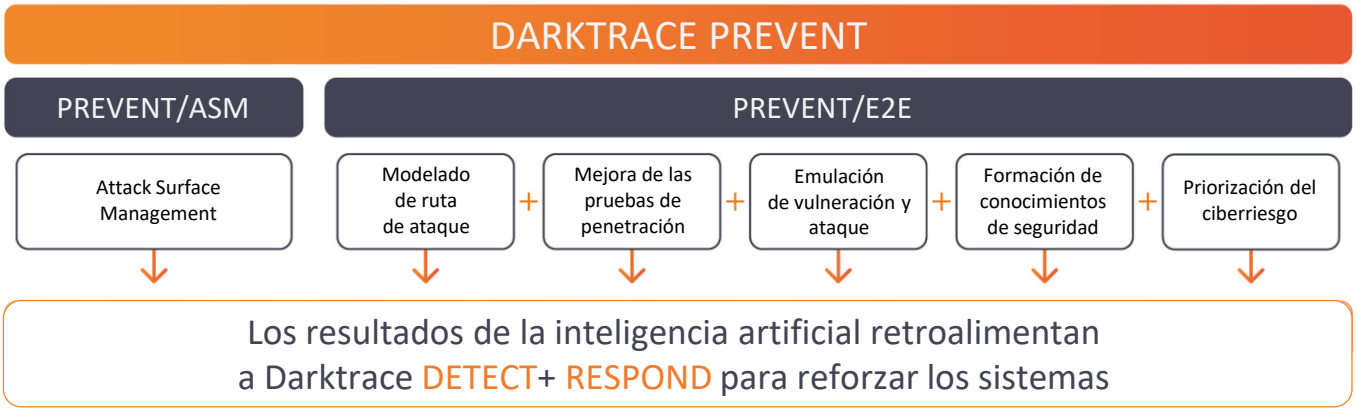
DUO okta IBM Jira
jumpcloud HUNTERS
zscaler LogRhythm
FORTINET Microsoft
paloalto NETWORKS RAPID7

Asegurando su viaje hacia la confianza cero



Con la protección Darktrace/Zero Trust

DARKTRACE PREVENT™



La importancia de fortalecer sus defensas

Los atacantes actuales usan más automatización, dirigiendo sus ataques a cadenas de suministro y TI en la sombra, y utilizando nuevas técnicas en sus campañas de ataque. Las operaciones y los enfoques de seguridad necesitan evolucionar para gestionar los ciberriesgos y evitar las interrupciones. También es una cuestión de eficiencia: muchas organizaciones están ampliando el uso de pruebas manuales de expertos poco frecuentes para tratar de identificar vulnerabilidades que requieren aún más esfuerzo manual de los equipos de TI para revisar los sistemas. Aunque existen productos puntuales que tratan de abordar diferentes aspectos del problema, la mayoría de ellos son aislados y trabajan en un solo momento determinado. Y en el caso de las pruebas de penetración, la mayoría de ellas se convierten en ejercicios de verificación de casillas para que las empresas mantengan el cumplimiento, pero no permiten una acción efectiva. Los equipos de seguridad pueden tener que trabajar con una enorme cantidad de información de vulnerabilidad, gran parte de la cual es irrelevante para los riesgos de seguridad que preocupan a los ejecutivos.

Introducción de Darktrace PREVENT

Darktrace PREVENT es un conjunto interconectado de productos de inteligencia artificial que proporciona una ciberseguridad proactiva para ayudar a las organizaciones a anticiparse a los futuros ciberataques. Esta familia de productos fortalece al CISO y al personal de seguridad para que se conviertan en un *Red Team* dirigido por inteligencia artificial; simulando ataques, identificando activos críticos y probando vías de vulnerabilidad para reforzar después las defensas con el fin de evitar que los atacantes lleguen a los datos y sistemas vitales.

Darktrace PREVENT / Attack Surface Management™

Darktrace PREVENT/ASM les ofrece una visibilidad incomparable de las partes de su organización que están expuestas al mundo exterior, permitiendo a su equipo de seguridad identificar los riesgos de forma proactiva antes de que se produzca un ataque.

La solución supervisa continuamente la superficie de ataque externa, evaluando todos sus activos en busca de riesgos, vulnerabilidades de alto impacto y amenazas externas. Las empresas utilizan PREVENT/ASM para mostrar la TI en la sombra, los riesgos en la cadena de suministro, los posibles dominios de phishing, las vulnerabilidades, los errores de configuración y los riesgos derivados de fusiones y adquisiciones.

PREVENT/ASM también comunica sus hallazgos a Darktrace DETECT + RESPOND que, a su vez, aumenta la sensibilidad en torno a los cuellos de botella críticos.

Darktrace PREVENT / End-to-End™

Darktrace PREVENT/E2E evalúa los riesgos estratégicos a los que se enfrenta su organización, dándoles la posibilidad de prepararse para los ataques antes de que se produzcan. Identifica y prioriza las vías y los objetivos de alto valor para proteger los activos y sistemas internos vitales.

Modelado de ruta de ataque

Crea las rutas de ataque más relevantes y de mayor impacto a través de su organización en tiempo real

Mejora de las pruebas de penetración

Prueba todas las posibles vías de ataque durante las 24 horas del día

Emulación de vulneración y ataque

Despliega “ataques” inofensivos que emulan malware, phishing, suplantación de identidad y otras amenazas comunes.

Formación de conocimientos y seguridad

Identifica a los usuarios que están expuestos o son vulnerables al phishing, lo que permite a los equipos de TI adaptar la formación según los datos del mundo real.

Priorización del ciberriesgo

Actualiza continuamente sus hallazgos para mostrarles en qué áreas deberían centrarse para reducir lo máximo posible el riesgo.

Figura 6: PREVENT identifica y prioriza las vías y los objetivos de alto valor para los activos y sistemas internos

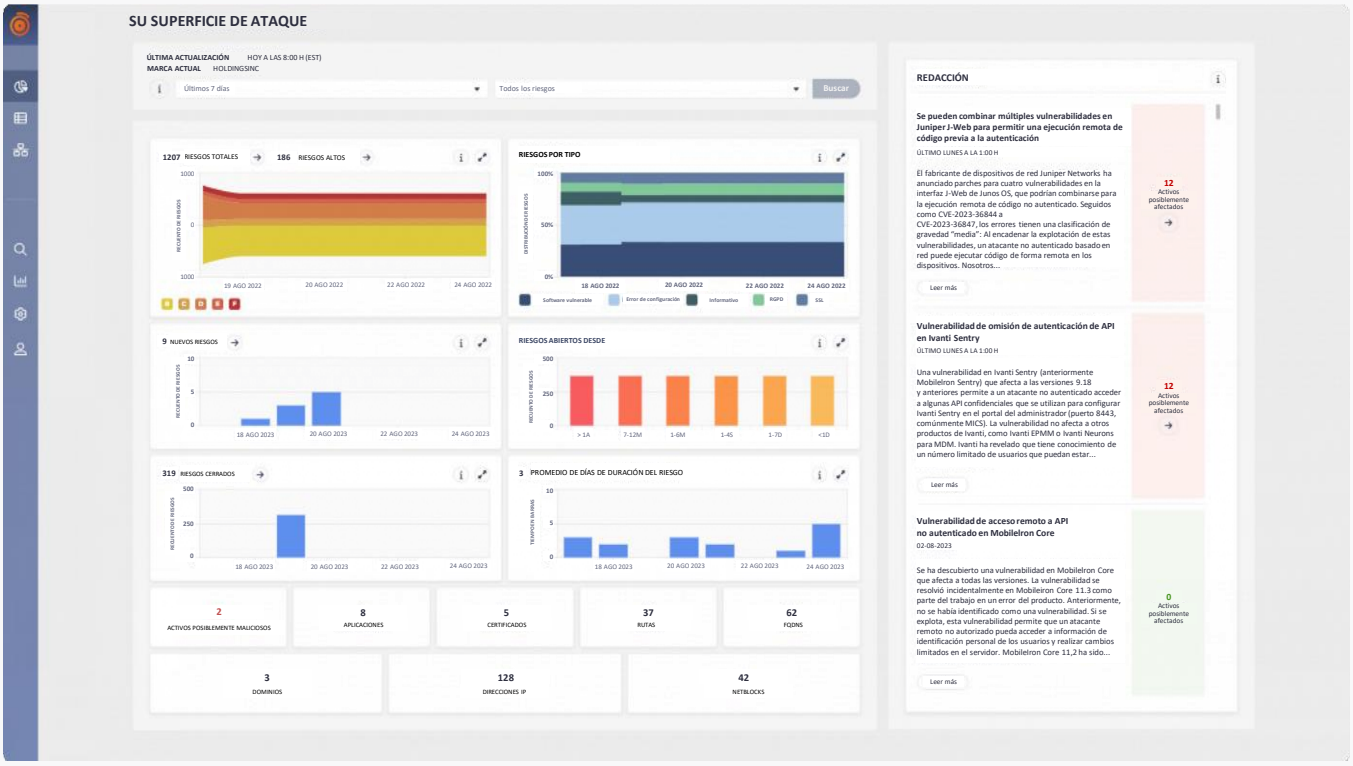


Figura 7: PREVENT ofrece una evaluación continua de su superficie de ataque, incluyendo las vulnerabilidades críticas recientes.

> Al introducir PREVENT en nuestro ecosistema, nos permite identificar activos que anteriormente pensábamos que las unidades de negocio habían retirado. PREVENT me permite volver a casa al final del día sabiendo que mi red, mis usuarios, la identidad de mis usuarios y mi ecosistema están en buenas manos.

President of IT and Cyber Security
/ Servicios de instalaciones

DARKTRACE HEAL™

Organizaciones en constante cambio, amenazas en constante evolución

En un panorama de amenazas en constante cambio, los equipos de seguridad enfrentan limitaciones a la hora de prepararse y responder a incidentes de ciberseguridad emergentes debido a limitaciones de recursos humanos, deficiencias en los procesos y soluciones técnicas inadecuadas que no cumplen con los requisitos del mundo real.

Es importante que los CISO sean conscientes tanto de la preparación de su tecnología (incluyendo la configuración adecuada para un uso eficaz) como de la capacidad de su equipo de seguridad para manejar la recuperación de un ciberataque. A medida que las organizaciones evolucionan continuamente, los libros de tácticas permanecen estáticos y sin cambios, lo que provoca un desajuste entre los ataques y los planes de respuesta.

Aumento del 135% en ataques de 'nueva ingeniería social' en 2023 en medio de una disponibilidad generalizada de ChatGPT[1]

[1]Basándose en el cambio promedio en los ataques de correo electrónico entre enero y febrero de 2023 detectados en implementaciones de Darktrace/Email con control de signos inusuales

Darktrace HEAL™ utiliza IA para comprender los datos de su negocio, garantizar la preparación para recuperarse de un ciberataque activo y restaurar rápidamente el negocio a un estado operativo.

Características destacadas

Análisis de preparación

Prepárese para cualquier cosa

Utiliza el conocimiento existente de Darktrace acerca de su organización (los dispositivos y las comunicaciones recopilados de Darktrace DETECT) para establecer: ¿cómo está preparado para un ciberataque?

Con una evaluación continua, las organizaciones pueden obtener una comprensión clara de su ciberresiliencia y cómo mejorar su posición de riesgo de manera más efectiva.

Simulaciones de incidentes y simulacros de preparación

Practique como si fuera real para estar preparado cuando ocurra

Garantice la preparación para responder a incidentes mediante simulaciones de amenazas que ejecutan incidentes del mundo real adaptados a su organización. Al ejecutar y rastrear incidentes simulados, los equipos pueden identificar puntos débiles y deficiencias en sus planes de respuesta.

Motor de toma de decisiones para la recuperación

Vuelva a conseguir que todo funcione

Cuando ocurren incidentes, adapta las respuestas automáticamente a los detalles precisos del incidente, en lugar de obligar a que un libro de tácticas universal funcione para todos. Automatiza gran parte del proceso de recuperación y, cuando es necesario, presenta recomendaciones a los equipos humanos basándose en desarrollos en tiempo real: promulga, delega y rastrea acciones para solucionar y recuperar activos.

Canal seguro de colaboración y comunicaciones

Tenga a las personas adecuadas en su puesto

Centraliza y coordina los equipos integrando Darktrace HEAL con el canal de comunicaciones de sus equipos, lo que permite a los usuarios reunir rápidamente a todas las personas que deban intervenir para dar respuesta al incidente mientras transfieren fácilmente información esencial.

Informe de incidentes del bucle completo

Ahorre tiempo con la generación automática de informes

Las acciones, decisiones y notas de HEAL completadas y planificadas también se registran y combinan automáticamente en un PDF exportable con el análisis de incidentes y la información de contención para obtener un informe detallado sobre el incidente.

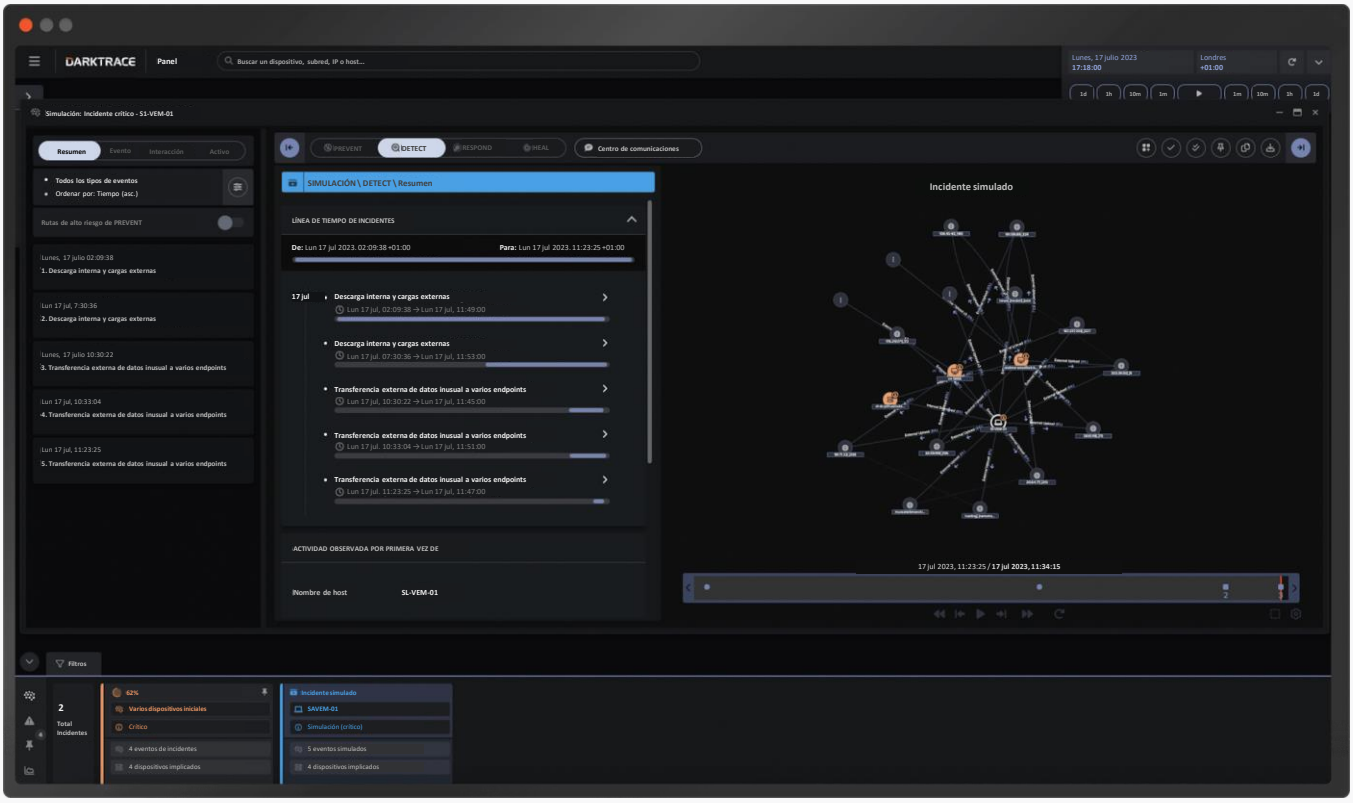


Figura 8: Los incidentes simulados ayudan a los equipos a probar sus planes de respuesta en caso de un ataque real

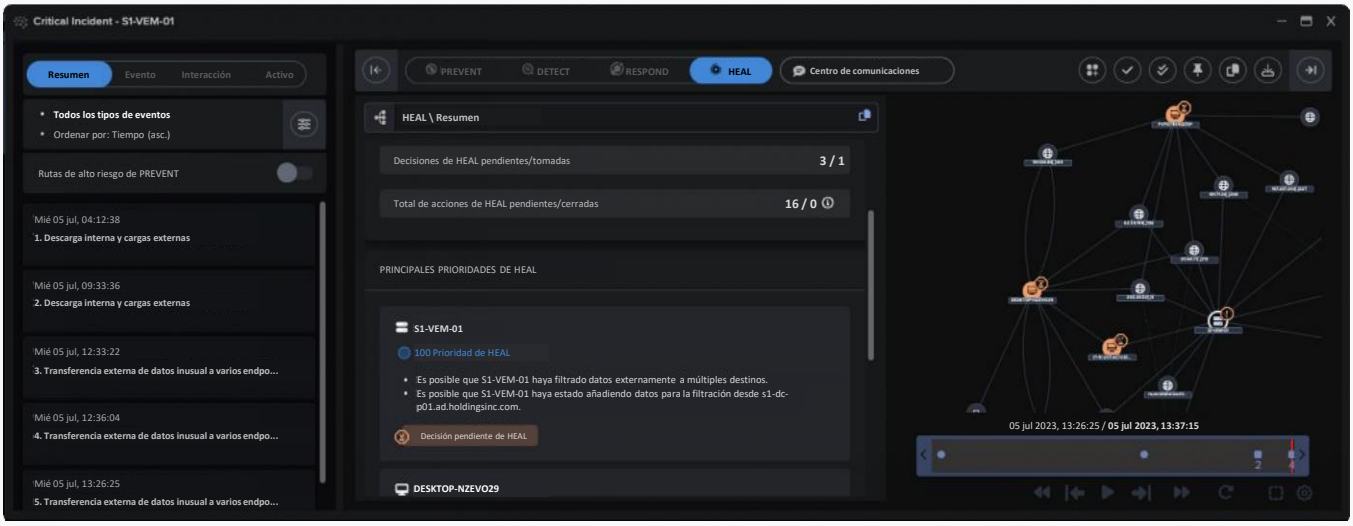


Figura 9: Darktrace HEAL permite a los defensores priorizar las acciones de respuesta para recuperarse rápidamente de un ataque emergente

> La IA nos ayuda a comprender el evento y vuelve a poner en línea nuestros sistemas, lo que reduce las interrupciones en las operaciones de nuestro negocio.

CISO
/ Gobierno municipal

Acerca de Darktrace

Darktrace (DARK.L), líder global en inteligencia artificial para la ciberseguridad, ofrece soluciones completas dirigidas por inteligencia artificial para cumplir su misión de liberar al mundo de la ciberinterrupción. Su tecnología aprende y actualiza continuamente su conocimiento acerca de la 'forma de ser única' de su organización y aplica ese conocimiento para lograr un estado óptimo de ciberseguridad. Las innovaciones revolucionarias de nuestros centros de I+D han dado lugar a la presentación de más de 145 solicitudes de patente. Darktrace cuenta con más de 2.200 empleados en todo el mundo y protege a unas 8.900 organizaciones globalmente contra las ciberamenazas avanzadas.

Escanear para obtener MÁS INFORMACIÓN

DARKTRACE
Evolving threats call for evolved thinking™

Norteamérica: +1 (415) 229 9100
Europa: +44 (0) 1223 394 100
Asia-Pacífico: +65 6804 5010
Latinoamérica: +55 11 4949 7696

info@darktrace.com

darktrace.com