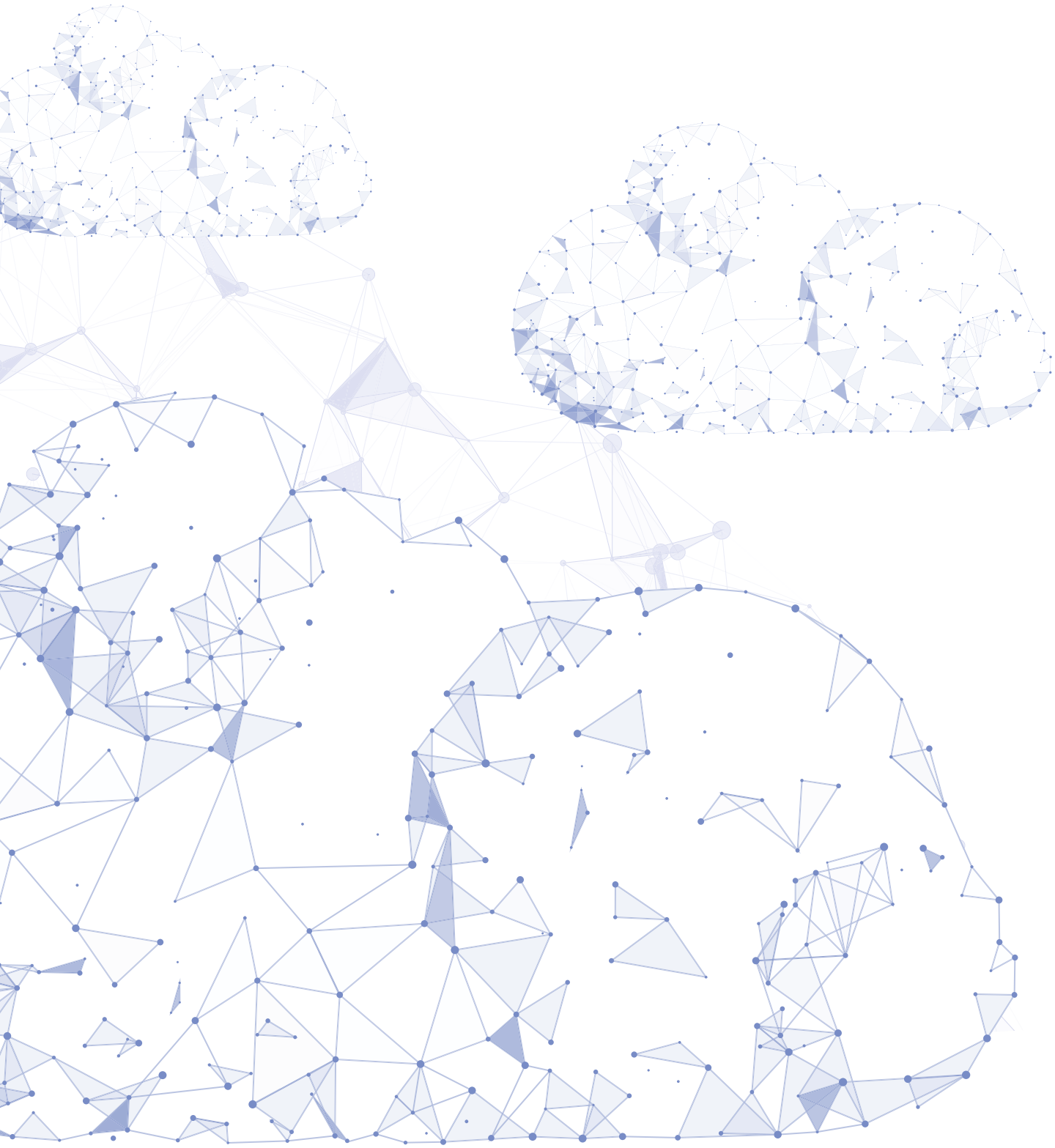
DARKTRACE



Ciber IA de Darktrace

Un sistema inmune para la seguridad en la Nube

> A medida que las organizaciones aumentan sus capacidades digitales en los entornos híbridos, multinube y de IoT, se enfrentan a más áreas que proteger y controlar. Esto también significa que existen más oportunidades para que los delincuentes dañen la fiabilidad operacional, cometan nuevos tipos de delitos y afecten directamente al funcionamiento de un negocio.
>
> **– Forrester**

Introducción

Contenido

Desde pequeñas empresas que buscan reducir los costes hasta centros de innovación corporativos que lanzan proyectos de transformación digital, el viaje a gran escala a la Nube ha reestructurado radicalmente el negocio digital y la estrategia tradicional del perímetro de la red. Al reducirse dicho perímetro, la infraestructura híbrida y multinube se ha convertido en parte de los elementos de un estado digital cada vez más diverso, lo que permite que las organizaciones impulsen los límites máximos de la innovación al mismo tiempo que amplían la superficie de ataque a un ritmo alarmante.

Esta tendencia representa, obviamente, el arma de doble filo de la era digital, y los desafíos de seguridad que deben afrontar los líderes empresariales en su viaje a la Nube son difíciles de estimar. La propia 'Nube' abarca una gran variedad de sistemas y servicios, y un solo equipo de seguridad a menudo puede ser responsable de asegurar las cargas de trabajo de la Nube en AWS y Azure, las comunicaciones por correo electrónico en Office 365, los datos de clientes en Salesforce, los archivos compartidos a través de Dropbox y los servidores virtualizados en centros de datos locales tradicionales.

Este complejo entramado de plataformas basadas en la Nube a menudo impulsa la eficiencia, la flexibilidad y la innovación en perjuicio de una estrategia de seguridad coherente y manejable. La Nube, en todas sus diversas formas, es un territorio con el que no están familiarizados los equipos de seguridad tradicionales, y las antiguas herramientas y prácticas a menudo son demasiado lentas, aisladas o ni siquiera son aplicables para defender los entornos híbridos y multinube contra los ataques avanzados.

Y aunque muchas soluciones de seguridad nativas de la Nube a menudo pueden ayudar con el cumplimiento y el análisis basado en registros, rara vez son lo suficientemente potentes y unificadas como para proporcionar una suficiente cobertura – tanto porque continúan promoviendo un enfoque de 'salida de humos' para la seguridad; como porque confían en reglas, firmas o suposiciones previas y, por lo tanto, no detectan nuevas amenazas ni discretos ataques internos antes de que tengan tiempo de convertirse en una crisis.

Y lo que es peor, la falta de visibilidad y de control a la que se enfrentan los equipos de seguridad en esta área –junto con la nueva y desconocida mentalidad requerida por la agilidad y la velocidad de la Nube– también la convierte en un atractivo objetivo para los ciberdelincuentes, quienes siempre intentan sacar el máximo provecho evitando ser detectados. La seguridad en la Nube no está donde debería, y los ciberdelincuentes lo saben mejor que nadie.

Pero en muchos sentidos, las organizaciones actualmente necesitan algo más que simplemente seguridad en la Nube: necesitan seguridad en toda la empresa y una plataforma unificada que pueda funcionar a la velocidad de los negocios digitales, adaptarse a futuras amenazas y correlacionar las discretas pistas de un ataque avanzado a medida que aumente su presencia en una red.

La Plataforma de Ciber IA

Limitaciones del enfoque aislado para la seguridad en la Nube

Los proveedores de servicios en la Nube y los proveedores externos ofrecen una variedad de soluciones de seguridad 'nativas de la Nube' que ayudan a los clientes a defender su parte del modelo de responsabilidad compartida. Sin embargo, estas soluciones puntuales –ya sean nativas o de terceros– generalmente no están lo suficientemente preparadas para detectar y responder a las amenazas avanzadas en la Nube.

Controles nativos: Necesarios, pero no suficientes

Los controles de seguridad nativos a menudo están diseñados exclusivamente para un único proveedor de la Nube, por lo que cubren solamente una parte de una gran empresa híbrida y multinube. Esto limita enormemente el alcance de la detección y añade más complejidad a una pila de seguridad ya de por sí compleja.

Generalmente, los controles nativos pueden ayudar con el cumplimiento, la recopilación de registros y la creación de políticas estáticas; pero no están diseñados para detectar y responder a amenazas avanzadas en varios silos y servicios en la Nube.

Controles de terceros: Útiles, pero no suficientes

Los controles de terceros, como los CASB y los CWPP, también resultan útiles, pero no son suficientes. Los CASB, por ejemplo, pueden ayudar con la detección, la creación de políticas detalladas y el cumplimiento; pero a menudo no detectan las ciberamenazas que ocupan el extremo más avanzado del espectro –desde ataques a credenciales y ransomware, hasta ataques internos de empleados descontentos y espionaje corporativo.

Aunque los controles de terceros normalmente proporcionan visibilidad cruzada en la Nube, no tienen ningún conocimiento acerca de la red física de una organización. Esta es una limitación importante, ya que la correlación del conocimiento de toda la Nube y la red corporativa a menudo es la única forma de que un sistema de seguridad pueda detectar la presencia de una amenaza emergente.

Un sistema inmune para la Nube y más allá

Con la inteligencia artificial, la Plataforma de Ciber IA de Darktrace llena estos vacíos críticos con un enfoque único de toda la empresa que detecta y responde a las amenazas basadas en la Nube que otras herramientas pasan por alto.

Al igual que el sistema inmune humano, la tecnología desarrolla un sentido innato de su 'forma de ser', aprendiendo el 'patrón de vida' normal de cada usuario, dispositivo y contenedor en entornos híbridos y multinube. Al analizar constantemente el comportamiento de todos y de todo en el negocio, la inteligencia artificial de autoaprendizaje de Darktrace puede correlacionar de forma única las señales discretas y sutiles de un ataque avanzado, sin definir previamente lo que es 'fiable' o 'malicioso'.

Aunque las soluciones puntuales preprogramadas realmente pueden complementar este enfoque, Darktrace es la única tecnología probada que detiene todas las distintas ciberamenazas en la Nube, desde ataques externos e internos maliciosos, hasta errores de configuración críticos que pueden exponer al negocio a futuros ataques –tanto si se producen por campañas de phishing de objetivo definido focalizadas, como por robos de cuentas corporativas, por filtración externa de datos 'pequeña y lenta' o por movimiento lateral en la Nube.

Protección unificada y personalizada

Con una comprensión de toda la empresa del estado digital, Darktrace correlaciona toda la actividad local con el tráfico en entornos híbridos y multinube en tiempo real. Esto le permite comprender que un comportamiento corriente detectado de forma aislada en la Nube puede verse más ampliamente como una actividad maliciosa.

Por ejemplo, podríamos ver que un usuario ha iniciado sesión en AWS en la Nube. Esto no es malicioso de por sí, pero Darktrace también sabe que es posible que la cuenta de Office365 del mismo usuario haya sido atacada previamente, ya que se detectó una ubicación de inicio de sesión muy inusual. Darktrace entiende que la conexión a AWS es, de hecho, muy sospechosa.

> Los líderes de seguridad cada vez piensan más en mejorar su eficiencia cambiando los productos puntuales por plataformas de seguridad más amplias.
>
> **– Gartner**

Correlación de conocimientos a nivel de contenedor

A pesar de la creciente implementación de contenedores por parte de los desarrolladores, la seguridad a menudo se ha quedado atrás. La naturaleza virtualizada de los contenedores dificulta la monitorización del tráfico dentro del servidor. Mientras que los sistemas basados en reglas rastrean los datos únicamente en los servidores, Darktrace es capaz de proporcionar visibilidad en los entornos de contenedores dentro de servidores individuales.

Y lo que es fundamental, Darktrace amplía esta visibilidad de los contenedores y la conecta con la actividad en toda la infraestructura digital (entornos de la Nube, de IoT, de correo electrónico, industriales y el resto de entornos). Por lo tanto, una anomalía en el tráfico de red de un contenedor podría vincularse a una base de datos en la Nube que, a su vez, podría correlacionarse con la cuenta de correo electrónico de una empresa.

Consulte la página 14 para ver los escenarios de implementación

AI Analyst: Investigación de amenazas automatizadas

Cyber AI Analyst da un paso más allá en la investigación automática de amenazas detectadas por el Enterprise Immune System y la creación de un panel de situación dinámico, así como de informes generados por inteligencia artificial que comunican el alcance total de un incidente de seguridad.

AI correlacionar el tráfico en la Nube en tiempo real con el resto de la red, el AI Analyst puede dirigir cientos de investigaciones simultáneamente, uniendo una gran cantidad de alertas e indicadores y desarrollando una excelente comprensión de los incidentes a velocidad de máquina. A continuación, comunica sus resultados y recomendaciones en forma de Incidentes de AI Analyst, los cuales se amplían con conocimientos de contexto y seguridad que pueden ser revisados y procesados por ejecutivos y usuarios finales por igual.

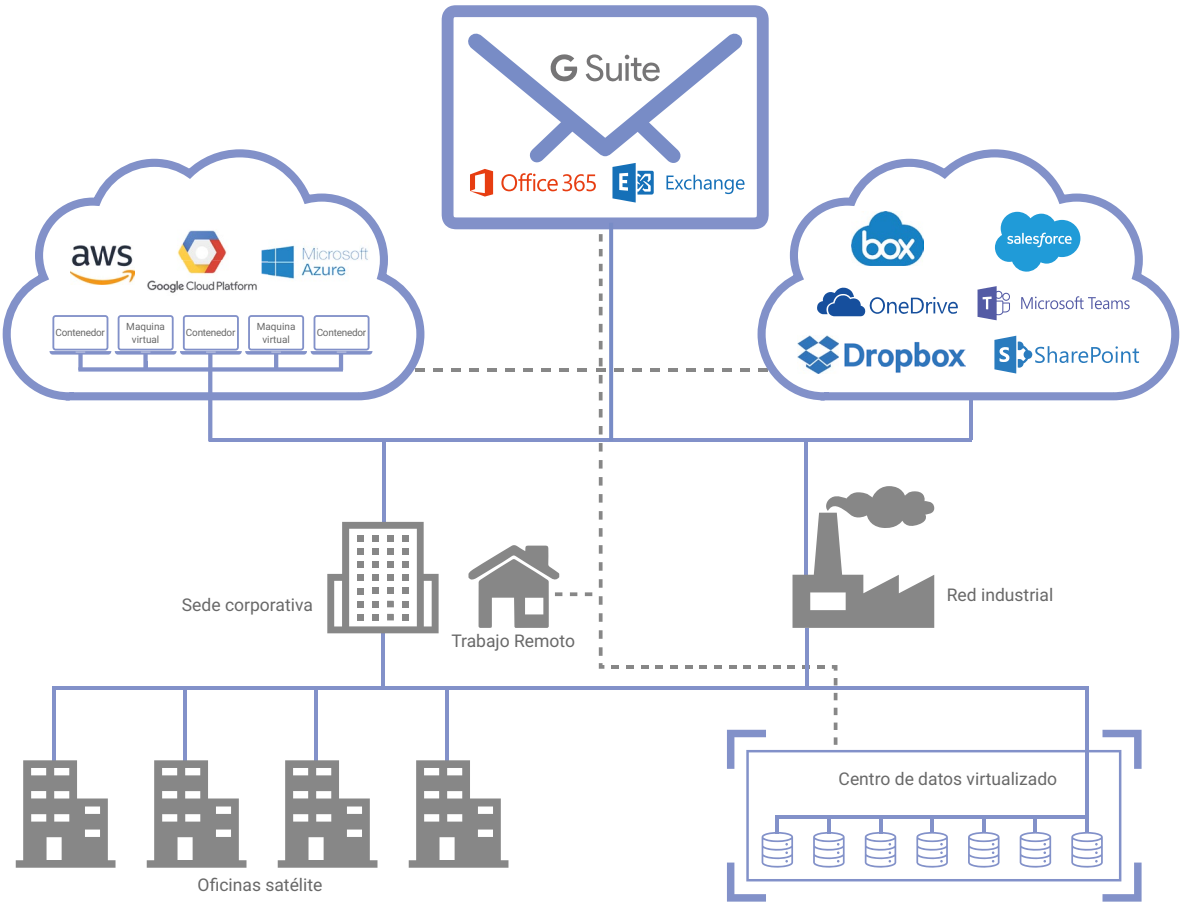


Figura 1: La cobertura unificada de Darktrace de todo el estado digital

Ataque a credenciales

El 29% de las vulneraciones de datos implican el uso de credenciales robadas

Fuente: Verizon 2019

Los ciberdelincuentes avanzados pueden robar credenciales de cuentas corporativas de varias formas, desde ataques de ingeniería social hasta malware 'inteligente' que rastrea el tráfico y los activos efímeros de la Nube en busca de contraseñas. Y con los datos robados fácilmente disponibles para comprar y vender en la Internet oscura, la frecuencia y la gravedad del robo de credenciales aumenta año tras año.

Los casos de robo de cuentas abarcan solo la primera fase de una ciberamenaza. La fase final de un ataque basado en credenciales es el uso real de las contraseñas robadas para autenticar aplicaciones y robar datos. Una vez que un atacante dispone de las credenciales para operar como un usuario válido, poco se puede hacer para distinguir a un intruso del empleado legítimo al que están suplantando.

Al correlacionar datos en entornos híbridos y multinube, Darktrace aprende el 'patrón de vida' de cada usuario a partir de cientos de medidas, lo que le permite detectar inmediatamente las desviaciones del comportamiento que son indicativas de un robo de cuenta. Incluso en los casos de un ataque preexistente; al aprender el 'patrón de vida' del grupo de mismo nivel de dicho usuario, así como de todo el negocio; la inteligencia artificial de Darktrace marcará retrospectivamente cualquier comportamiento inusual.

Figura 2: La inteligencia artificial de Darktrace detectó una actividad inusual relacionada con una cuenta de la Nube robada

Ataque de SharePoint

Después de robar credenciales u obtener, de otra forma, acceso al servicio de transferencia de archivos basado en la Nube de una organización; los ciberdelincuentes a menudo ejecutarán scripts para identificar archivos que contengan palabras claves como 'contraseña'. Darktrace descubrió uno de estos incidentes en un banco europeo, en el que los atacantes lograron encontrar un archivo de Office 365 SharePoint que guardaba contraseñas sin cifrar. Tras haber eludido los controles nativos de Microsoft, es normal que los atacantes hubieran pensado que ya tenían el camino despejado.

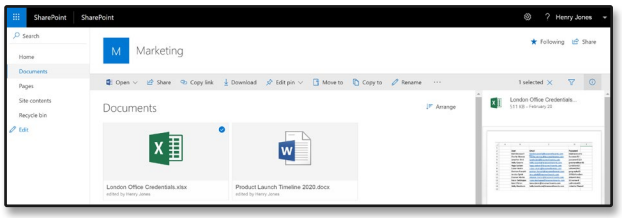


Figura 3: Los archivos confidenciales a los que accedieron en SharePoint

Sin embargo, la inteligencia artificial de Darktrace marcó esta actividad como anómala para el usuario corporativo, su grupo de mismo nivel y toda la organización; detectando el acceso inusual a dichos archivos confidenciales, entre otros indicadores. En última instancia, la comprensión evolutiva y con matices de la inteligencia artificial acerca de lo que era 'normal' en toda la organización resultó fundamental, ya que el acceso sospechoso a los archivos podría haber sido perfectamente fiable en otras circunstancias.

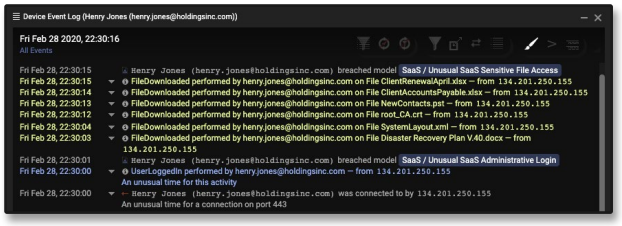
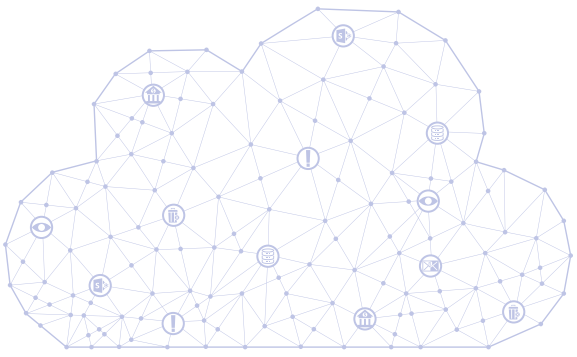


Figura 4: Darktrace mostró las descargas de los archivos confidenciales

Es posible que estos atacantes hubieran aprovechado las contraseñas de texto no cifrado para aumentar sus privilegios e infiltrarse aún más en la organización. Sin embargo, al aprender los 'patrones de vida' únicos de cada usuario y dispositivo de la organización, la inteligencia artificial de Darktrace fue capaz de alertar al equipo de seguridad acerca del incidente antes de que pudiera convertirse en una crisis.



Intento de inicio de sesión de SaaS desde Ecuador

En una organización internacional, Darktrace detuvo un ataque a una cuenta de Office 365 que había eludido los controles nativos de Azure Active Directory. Aunque la organización tenía oficinas en todos los rincones del mundo, la inteligencia artificial de Darktrace identificó un inicio de sesión desde una dirección IP que era históricamente inusual para ese usuario y su grupo de mismo nivel e inmediatamente alertó al equipo de seguridad. A continuación, Darktrace alertó sobre el hecho de que una nueva regla de procesamiento de correo electrónico, que eliminaba los correos electrónicos entrantes, se había configurado en la cuenta. Esto indicaba una clara señal de que se estaba produciendo un ataque y el equipo de seguridad pudo bloquear la cuenta antes de que el atacante pudiera provocar daños.

Cuando el equipo de seguridad investigó más a fondo el incidente, se percataron de que el usuario había recibido un correo electrónico de phishing solo unas horas antes de que Darktrace detectara la amenaza. Aunque la empresa también había implementado la Protección contra amenazas avanzada (ATP, Advanced Threat Protection) de Microsoft para Office 365, las defensas estáticas como ATP solo pueden detectar ataques de phishing al correlacionar enlaces de correos electrónicos con direcciones maliciosas conocidas, y el enlace de phishing no aparecía en la lista. Esto demostró las claras limitaciones de un enfoque basado en firmas en esta área, y la organización pronto implementó la tecnología de Respuesta Autónoma de Darktrace, Antigena, para una mayor protección en Office 365, dada su capacidad de detectar correos electrónicos de phishing igualmente amenazantes sin depender de listas negras.

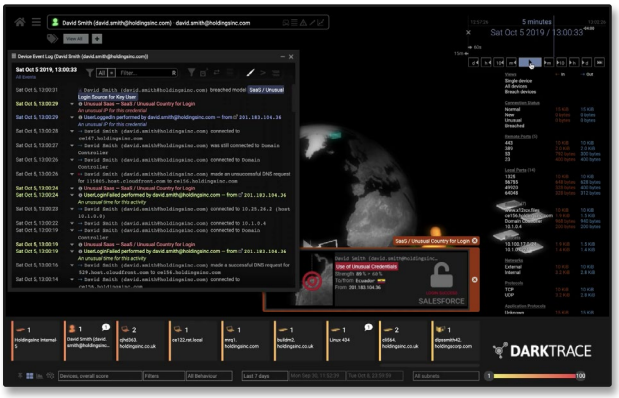


Figura 5: La inteligencia artificial de Darktrace detectó la ubicación inusual del inicio de sesión de SaaS

Inicio de sesión inusual en un banco de Panamá

Se utilizó una cuenta de Office 365 en un ataque por fuerza bruta contra un conocido banco de Panamá, con inicios de sesión que procedían de un país que no coincidía con los 'patrones de vida' normales de las operaciones de la compañía.

Darktrace identificó 885 inicios de sesión durante un periodo de 7 días. Aunque la mayoría de las autenticaciones procedían de direcciones IP de Panamá, el 15% de las autenticaciones procedían de una dirección IP que era 100% extraña y estaba ubicada en la India. Un análisis más exhaustivo reveló que este punto de conexión externo estaba incluido en varias listas negras de correo no deseado y recientemente se había asociado con un comportamiento abusivo en Internet –posiblemente por piratería o detección en Internet no autorizada.

Figura 6: La interfaz de usuario que muestra las ubicaciones de inicio de sesión

Entonces, Darktrace fue testigo de lo que parecía ser un abuso de la función de restablecimiento de la contraseña, ya que se observó que el usuario de la India había cambiado los privilegios de la cuenta de una manera muy inusual. Lo que marcó la actividad como especialmente sospechosa fue el hecho de que después del restablecimiento de la contraseña, se observaron intentos de inicio de sesión fallidos desde una IP normalmente asociada con la organización, lo que sugirió que el usuario legítimo había sido bloqueado.

03/12 20:45:39	Saas::Admin	Regular	UpdateUser
03/12 20:45:39	Saas::Admin	Regular	ChangeUserLicense
03/12 20:26:43	Saas::Login	Regular	UserLoggedIn
03/12 20:26:43	Saas::FailedLogin	Regular	UserLoginFailed
03/12 20:26:36	Saas::FailedLogin	Regular	UserLoginFailed
03/12 18:31:31	Saas::Login	Regular	UserLoggedIn
03/12 17:57:46	Saas::Admin	Regular	ChangeUserLicense
03/12 17:57:46	Saas::Admin	Regular	UpdateUser
03/12 17:06:57	Saas::Admin	Regular	UpdateUser

Figura 7: La actividad asociada con la cuenta de SaaS, destacando las credenciales modificadas

Ataque por fuerza bruta automatizado

Darktrace detectó varios eventos de inicio de sesión fallidos en una cuenta de SaaS todos los días durante una semana. Cada serie de intentos de inicio de sesión se realizó exactamente a las 18:04 h durante seis días. La coincidencia tanto de la hora del día como del número de intentos de inicio de sesión era indicativa de un ataque por fuerza bruta automatizado, que estaba programado para interrumpirse después de un cierto número de intentos fallidos para evitar bloqueos.

Darktrace consideró que este patrón de intentos fallidos era muy anómalo y alertó al equipo de seguridad. Si no fuera por Darktrace, que correlacionó varios indicadores leves y detectó las señales discretas de que se estaba produciendo una amenaza, este ataque automatizado podría haber continuado durante semanas o meses, lo que permitiría hacer averiguaciones informadas sobre las contraseñas de los usuarios basándose en la información que ya había recopilado.

Figura 8: Un gráfico que muestra los intentos repetidos de inicio de sesión

Robo de cuenta de Office 365

Después de hacer clic en un enlace malicioso de un correo electrónico focalizado, una empleada introdujo sus credenciales en una página de inicio de sesión de suplantación de identidad que guardó sus pulsaciones de teclas. Ya teniendo sus credenciales, los atacantes volvieron a Office 365 y los usaron para iniciar sesión de forma remota. Darktrace detectó las ubicaciones inusuales: Bulgaria e Indonesia.

Al aprender los patrones de dónde trabajaban los usuarios, y de cuándo y cómo accedían a los servicios en la Nube, la inteligencia artificial de Darktrace identificó, y podría haber evitado, dichas solicitudes de inicio de sesión inusuales. En este caso, las funcionalidades de seguridad nativas no identificaron ni evitaron estos inicios de sesión maliciosos.

Una vez dentro de la cuenta de Office 365 de la empleada, los atacantes se propagaron a más víctimas, continuando el ciclo. En este caso, Darktrace fue testigo de otro cambio de comportamiento, al ver que se enviaban 99 correos electrónicos con el asunto 'aviso de pago' a numerosas empresas de destino. Aunque dicho comportamiento podría ser normal para algunos empleados, no correspondía al patrón de vida de ese usuario en concreto.

Darktrace también observó que se había creado una nueva regla de reenvío de la bandeja de entrada –a menudo creada por atacantes para propagar spam u ocultar sus actividades.

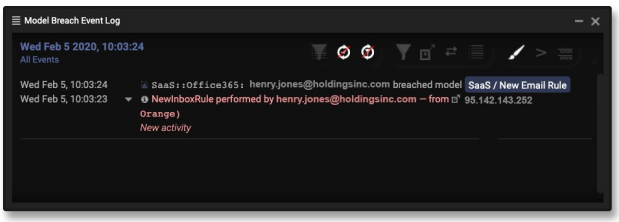


Figura 9: Darktrace detectó la regla de procesamiento de la bandeja de entrada

Al eliminar automáticamente los correos electrónicos después de ser enviados, el rastro de pruebas se destruye en el sistema de correo electrónico. Sin embargo, al monitorizar de manera independiente los correos electrónicos y las actividades de la cuenta de SaaS, Darktrace fue capaz de ver la imagen completa de las actividades del atacante. La capacidad de la plataforma de aprender identidades y comportamientos de toda la empresa le permitió detectar la actividad sospechosa.

Figura 10: Las ubicaciones de inicio de sesión inusuales

Ataques internos maliciosos

> La inteligencia artificial de Darktrace se adapta mientras se está trabajando, iluminando nuestra red y nuestra infraestructura en la Nube en tiempo real y permitiéndonos defendernos en la Nube con confianza

CISO, Aptean

Las amenazas internas en la Nube son a menudo una ciberamenaza para las organizaciones más grave que las de los atacantes externos, por una razón evidente: ya están dentro. Un empleado con malas intenciones está en una posición única para eludir las herramientas tradicionales gracias a su acceso privilegiado y a su profundo conocimiento de la red.

Los servicios en la Nube han ampliado significativamente el alcance de las amenazas internas, con la gran cantidad de aplicaciones que presentan una amplia variedad de vectores para la filtración externa de datos, y la visibilidad limitada en este ámbito que permite que la filtración externa de datos pase desapercibida.

Por naturaleza, las herramientas de seguridad antiguas están ciegas ante la actividad maliciosa que ya está ocurriendo dentro de la organización. La seguridad en la Nube ahora precisa de un enfoque más completo que analice el tráfico en todo el estado digital y que construya constantemente un 'patrón de vida' evolutivo de la organización.

Tanto si se trata de un vendedor que abandona y se lleva con él información del cliente, o de un administrador informático descontento que manipula discretamente datos de vital importancia; la inteligencia artificial se puede utilizar para detectar cualquier actividad anómala e inusual que indique una ciberamenaza.

Figura 11: Darktrace Antigena bloqueó el intento de un ataque interno malicioso de filtrar externamente datos confidenciales

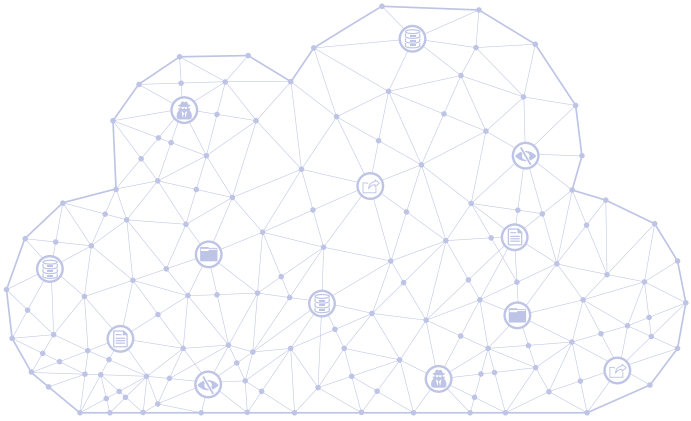
Empleado informático descontento

Darktrace fue testigo de un caso de amenaza interna después de que un empleado fuera despedido de su puesto como administrador del sistema informático. La organización se había visto obligada a realizar varios despidos en la oficina esa misma semana, pero había tenido el descuido de no recuperar el portátil del empleado ni de eliminar su cuenta corporativa. El antiguo administrador informático inició sesión en su cuenta de SaaS y descargó rápidamente numerosos archivos confidenciales –incluyendo los datos de contacto y los números de tarjetas de crédito– de la base de datos del cliente.

Figura 12: Threat Visualizer mostrando un gran pico del número de conexiones

Después, intentó transferir en secreto dichos archivos a un servidor doméstico a través de uno de los servicios comunes de transferencia de datos de la empresa. Antes de hacerlo, creó una nueva 'cuenta oscura' para crear una puerta trasera, asegurándose de que aún pudiera tener un punto de apoyo en la empresa cuando llegara el momento en el que el equipo informático eliminara su cuenta corporativa.

El administrador informático sabía que este servicio en concreto no solo estaba sujeto a las políticas corporativas, sino que también estaba basado en la Nube, y supuso que el equipo de seguridad tendría una visibilidad limitada en esta área. Sin embargo, Darktrace analiza dinámicamente los inicios de sesión y los eventos de acceso a archivos en los servicios corporativos en la Nube, correlacionándolos con los 'patrones de vida' aprendidos de cada usuario de la organización según las nuevas pruebas. Como sistema de autoaprendizaje unificado, la Plataforma de Ciber IA de Darktrace detectó inmediatamente las descargas de archivos inusualmente grandes, la creación de la nueva cuenta y la filtración externa; y su tecnología de Respuesta Autónoma, Antigena, contraatacó bloqueando el intento de carga.



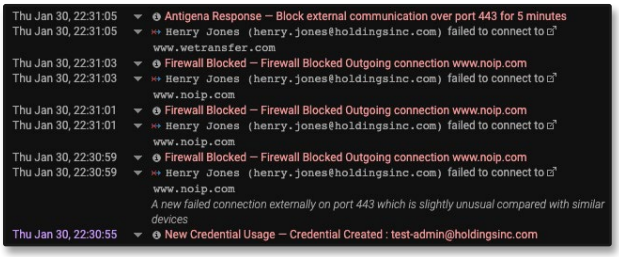


Figura 13: Darktrace Antigena activando una respuesta autónoma focalizada

Una investigación posterior reveló que el empleado primero intentó enviar estos archivos a un servidor personal en casa. Cuando esto falló, intentó continuamente filtrar externamente los datos a varias fuentes distintas. Sin embargo, gracias a que Antigena puede adaptarse dinámicamente a las amenazas a medida que se desarrollan y aumentar su respuesta de la misma forma, fue capaz de interrumpir quirúrgicamente estos intentos en todo momento.

Cuando todo lo demás falló, el empleado intentó transferir todos los archivos a un servidor interno que solía utilizar en la empresa –intentando enviar los archivos desde allí– pero Darktrace intervino y también neutralizó dicha conexión.

Figura 14: Antigena bloqueó el intento del empleado de transferir archivos a través de la Nube

Aunque esta discreta actividad eludió fácilmente los controles nativos del proveedor de la Nube, la inteligencia artificial de Darktrace detectó el comportamiento amenazante en cuestión de segundos. Al aprender continuamente lo que es 'normal' para cada usuario y dispositivo, el sistema pudo correlacionar de manera inteligente conexiones y descargas muy sospechosas desde el dispositivo del administrador informático, a pesar de que el servicio en la Nube lo utilizaban normalmente otros empleados para fines legítimos.

La Plataforma de inteligencia artificial de Darktrace alertó inmediatamente al equipo de seguridad y les proporcionó una información detallada y precisa acerca de la naturaleza del ataque, avisándoles de que revocaran sus credenciales y recuperaran y protegieran rápidamente los datos.

Error de configuración

> Casi todos los ataques realizados con éxito en los servicios en la Nube son el resultado de un error de configuración del cliente.
>
> **– Neil MacDonald, Gartner**

Configurar los controles de seguridad en entornos híbridos y multinube es, a menudo, un proceso complejo; ya que las soluciones nativas y de terceros en esta área son diversas, incompatibles e insuficientes. La falta de familiaridad con la Nube muchas veces da lugar a errores de configuración críticos que exponen al negocio a los ataques. Los desarrolladores actuales ahora tienen la capacidad de iniciar una instancia en la Nube en cuestión de minutos, a menudo sin tener que consultar al equipo de seguridad de su empresa. Como consecuencia, la mayoría de las organizaciones no tienen visibilidad de sus propios entornos en la Nube, y los plazos ajustados pueden provocar grandes vulnerabilidades que pasan desapercibidas durante meses.

Las posibles ramificaciones de un error de configuración se hicieron visibles con la vulneración de datos de Capital One, que afectó a más de 100 millones de personas al explotar una vulnerabilidad en la Nube. Esta importante institución financiera con una posición de seguridad avanzada en la Nube solo fue consciente después de recibir un consejo de una persona externa que se había topado con los datos robados –tres meses después de que se produjera la vulneración.

La inteligencia artificial ahora se utiliza para comprender los 'patrones de vida' normales de cada usuario, dispositivo y contenedor; reconociendo los discretos patrones de comportamiento asociados a un error de configuración. Al utilizar tecnología de autoaprendizaje como la Plataforma de Ciber IA de Darktrace, las organizaciones pueden obtener el conocimiento necesario de entornos complejos en la Nube para detectar vulnerabilidades latentes en sus fases iniciales –antes de que se conviertan en una crisis.

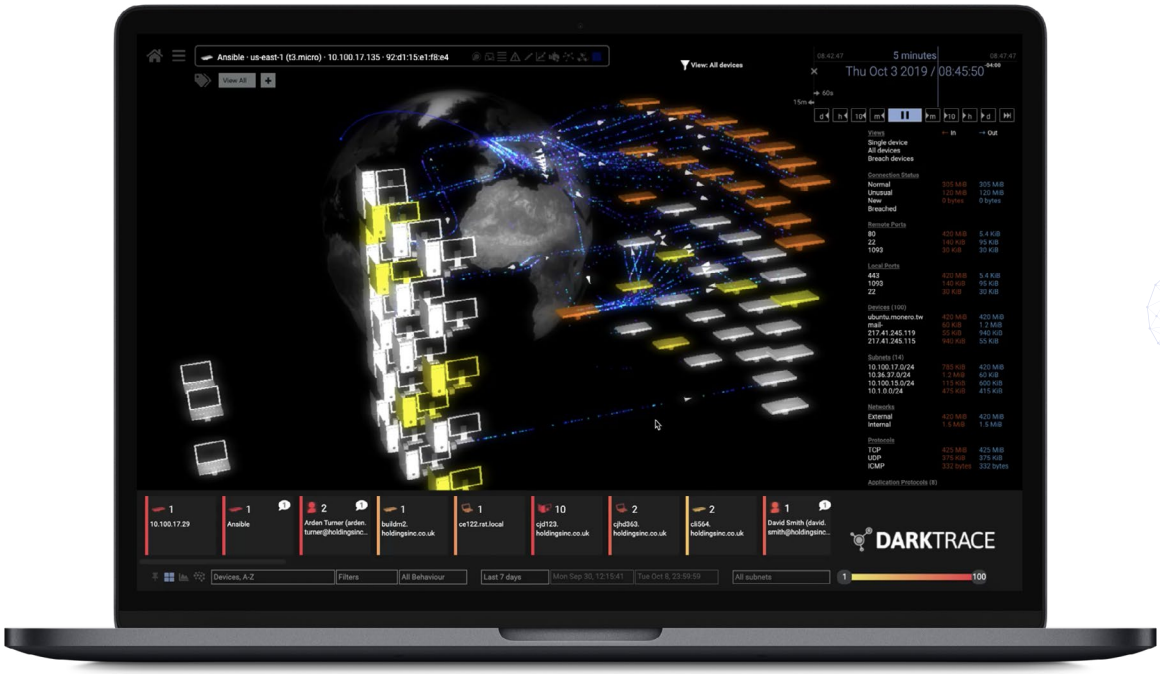


Figura 15: Un error de configuración de DevOps que provoca la rápida propagación del criptomalware

Ataque de Shodan en una vulnerabilidad de la Nube

Una organización de servicios financieros alojaba varios servidores críticos en máquinas virtuales en la Nube, algunos de los cuales estaban destinados a ser públicos, pero otros no. Cuando configuraron sus controles nativos en la Nube, dejaron por error un importante servidor expuesto en Internet, cuando estaba destinado a estar aislado tras un firewall. Esto podría haber ocurrido por varias razones, posiblemente debido a una migración rápida y caótica, o posiblemente por la falta de familiarización con los controles nativos proporcionados por su CSP.

Mientras que el equipo de seguridad desconocía por completo el error de configuración, el servidor expuesto al final fue descubierto y atacado por ciberdelincuentes que escaneaban Internet a través de Shodan. En cuestión de segundos, la inteligencia artificial de Darktrace detectó que el dispositivo estaba recibiendo un número inusual de intentos de conexión entrantes de una gran variedad de fuentes externas extrañas y alertó al equipo de seguridad sobre la amenaza.

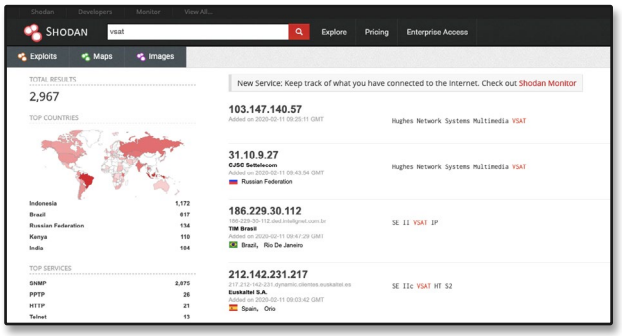


Figura 16: El sitio web de Shodan se utilizó para escanear la vulnerabilidad

DCP sin cifrar en AWS

Un gobierno municipal de los Estados Unidos en el proceso de externalizar bases de datos a AWS no preguntó adecuadamente los protocolos que el servidor utilizaba para descargar la información. Como resultado, todas las direcciones, números de teléfono y números de registro de vehículos de sus ciudadanos se estaban cargando en una base de datos externa a través de conexiones sin cifrar.

Estos datos altamente confidenciales estaban destinados a un acceso limitado por parte de los empleados autorizados del gobierno municipal, pero la supervisión de seguridad había puesto los datos a disposición de cualquier atacante capaz de escanear el perímetro de la red y de recopilar los paquetes llenos de datos que se fuera encontrando.

Inicialmente, la organización desconocía el error de configuración, el cual pasó inadvertido por toda su pila de seguridad. Sin embargo, cuando Darktrace detectó una conexión inusual a una IP externa extraña desde un dispositivo de escritorio de la compañía, verificó que dicha comunicación estaba revelando datos públicos confidenciales, a los que un atacante podía acceder para reunir el material para futuros ataques de phishing de objetivo definido o, incluso, para una suplantación de identidad. La visibilidad completa en tiempo real que proporciona Darktrace reveló este peligroso punto ciego y permitió que el equipo de seguridad corrigiera el error de configuración.

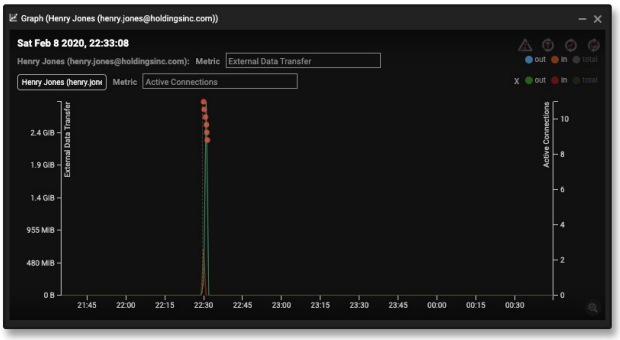
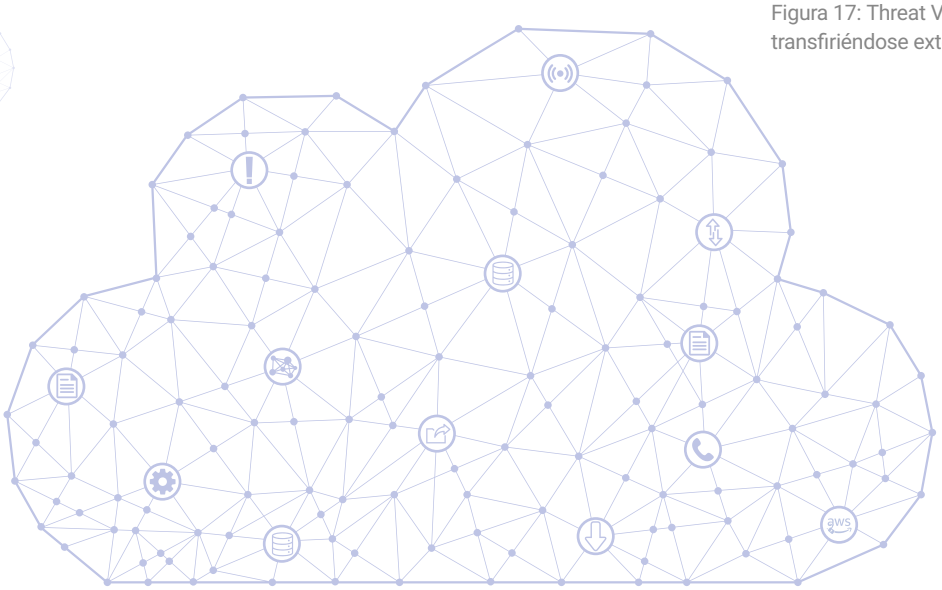


Figura 17: Threat Visualizer mostrando más de 2 GB de datos transfiriéndose externamente



Malware de criptominería instalado involuntariamente

Darktrace detectó un error de un ingeniero junior de DevOps en una organización multinacional que tenía cargas de trabajo en AWS y Azure, y aprovechó los sistemas de contenedores como Docker y Kubernetes. El ingeniero descargó accidentalmente una actualización que incluía un criptominero, el cual provocó una infección en varios sistemas de producción en la Nube.

Tras la infección inicial, el malware comenzó a transmitir a un servidor de comandos y controles externo, el cual fue detectado inmediatamente por Darktrace. Con la conexión externa establecida y las instrucciones de la misión de ataque proporcionadas, la infección del criptomalware pudo propagarse rápidamente por toda la infraestructura en la Nube expansiva de la organización a velocidad de máquina, infectando a 20 servidores en la Nube en menos de 15 segundos.

Gracias a la inteligencia artificial de Darktrace, el entorno en la Nube de la organización no era un punto ciego, con una vista dinámica y unificada de toda su amplia infraestructura híbrida y multinube, lo que permitió que el equipo de seguridad contuviera el ataque en cuestión de minutos, en vez de en horas o días. Y aunque el ataque se movió a velocidad de máquina, Darktrace lo detuvo en una fase lo suficientemente temprana, antes de que los costes empezaran a aumentar.

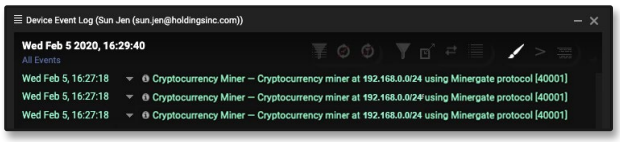


Figura 18: El malware de criptominería detectado en tiempo real

IP expuesta en Azure

Una empresa de fabricación líder en Europa utilizaba un servidor de Microsoft Azure para guardar archivos que contenían información de productos y proyecciones de ventas. Aunque los archivos del servidor y la IP raíz estaban controlados con un nombre de usuario y una contraseña, dichos datos confidenciales se dejaron sin cifrar. Se detectó una actividad anómala cuando un dispositivo descargó un archivo ZIP desde una dirección IP externa extraña que Darktrace consideró muy anómala.

Más tarde, se descubrió que la IP externa era un servidor de Microsoft Azure recién configurado y que el archivo ZIP era accesible para cualquiera que conociera la URL, la cual podría haberse obtenido simplemente interceptando el tráfico de red, tanto interna como externamente. Los atacantes más especializados podrían, incluso, haber atacado por fuerza bruta el parámetro 'clave' del archivo de la URL.

La pérdida o fuga de los archivos confidenciales en cuestión podría haber puesto en peligro toda una línea de productos; pero, al informar de este incidente en cuanto se detectó, Darktrace ayudó a evitar la pérdida de valiosa propiedad intelectual y también ayudó al equipo de seguridad a revisar sus prácticas de almacenamiento de datos en la Nube para proteger mejor la información de sus productos en el futuro.

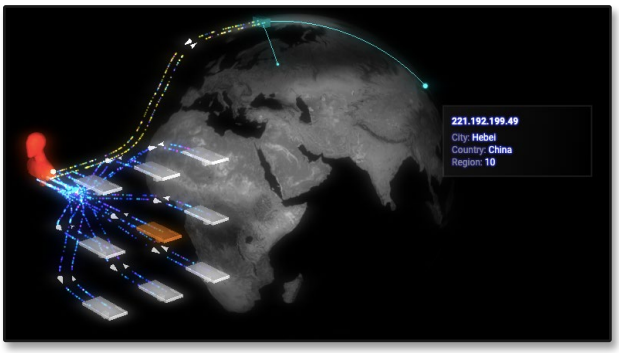
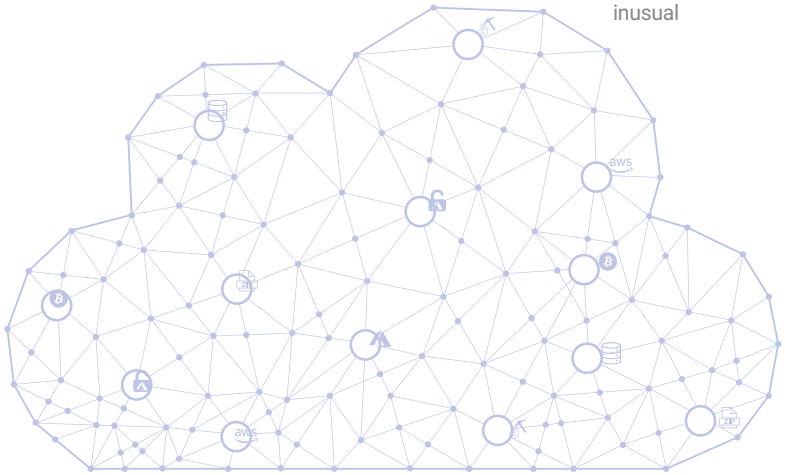


Figura 19: Darktrace monstrando la ubicación de la dirección IP inusual



El ingeniero de DevOps desmesurado

En un grupo asegurador, un ingeniero de DevOps intentaba crear una infraestructura de copia de seguridad paralela en AWS para replicar los sistemas de producción del centro de datos de la organización. La implementación técnica fue perfecta y se crearon los sistemas de copia de seguridad. Sin embargo, el coste de ejecutar el sistema sería de varios millones de dólares al año.

El ingeniero de DevOps no era consciente de los costes asociados al proyecto y mantuvo la gestión en secreto. Se inició la infraestructura en la Nube y los costes comenzaron a aumentar. Pero la inteligencia artificial de Darktrace alertó sobre dicho comportamiento inusual, y el equipo de seguridad pudo realizar acciones preventivas de inmediato.

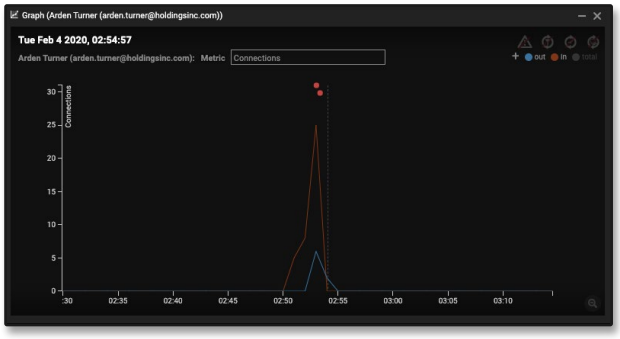


Figura 20: Threat Visualizer mostrando un pico en las conexiones internas y externas

Escenarios de implementación

Nube híbrida (IaaS)

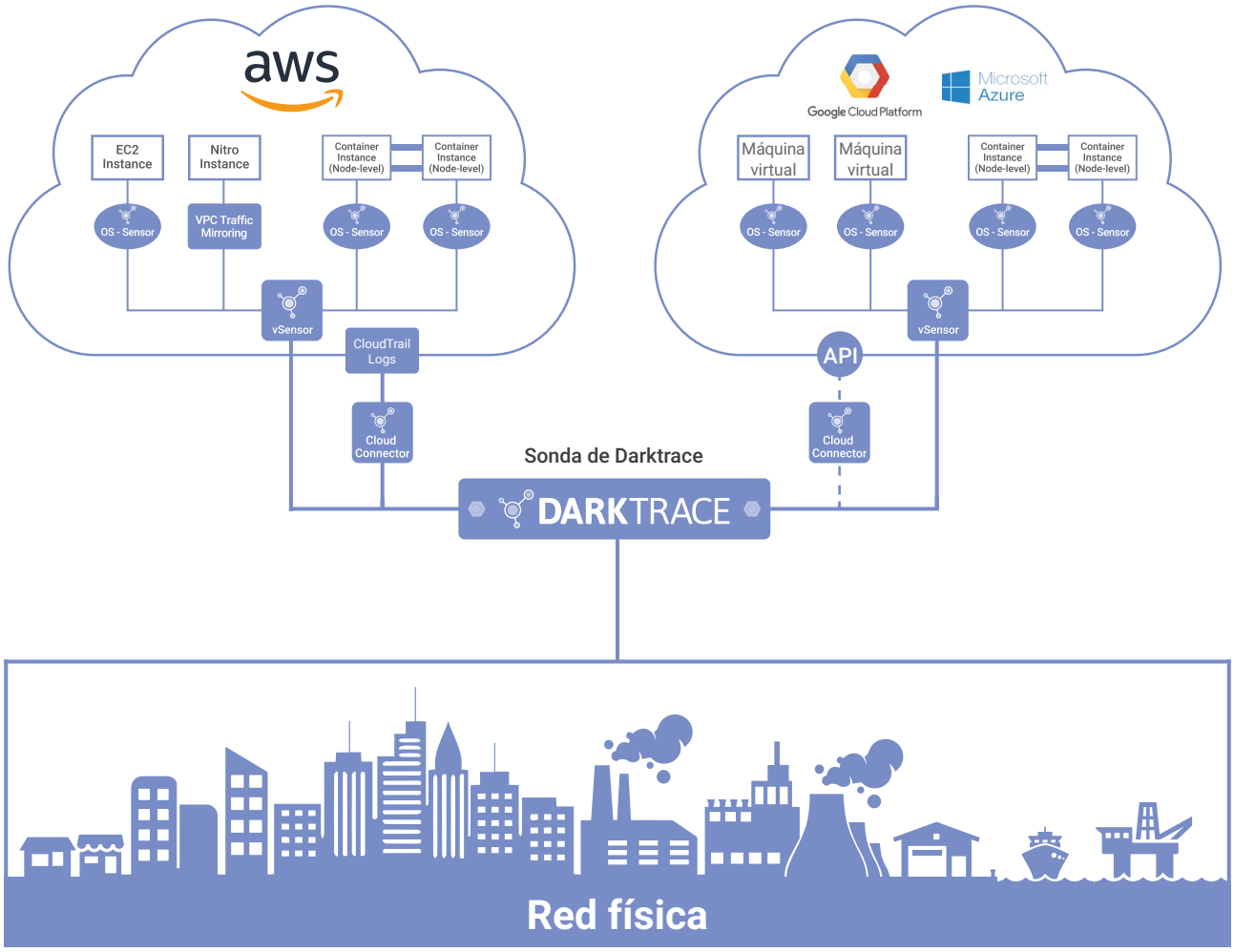
En las organizaciones con una infraestructura de Nube híbrida, Darktrace implementa sondas virtuales o 'vSensors' que capturan el tráfico en tiempo real en la Nube y lo correlacionan con el resto del negocio.

En AWS, los vSensors ingieren el tráfico en tiempo real de las instancias de Nitro a través de VPC Traffic Mirroring. Los metadatos de AWS Nitro se pueden capturar directamente, sin necesidad de una sonda de nivel de servidor adicional. En instancias que no son de Nitro, Darktrace implementa 'OS-Sensors' en cada punto de conexión –cada OS-Sensor envía el tráfico a un vSensor local que, a su vez, envía los metadatos relevantes a una sonda maestra de Darktrace en la Nube o en la red corporativa para su análisis.

En Azure y GCP, entre otros, Darktrace implementa vSensors y OS-Sensors para capturar el tráfico en tiempo real como se ha descrito anteriormente. Darktrace también admite vTAP de Azure, y se está desarrollando una capacidad equivalente para GCP.

Los clientes de AWS y Azure también pueden implementar 'Conectores de Darktrace' para monitorizar la actividad del administrador del sistema a nivel de API, como la actividad de inicio de sesión y las creaciones de recursos.

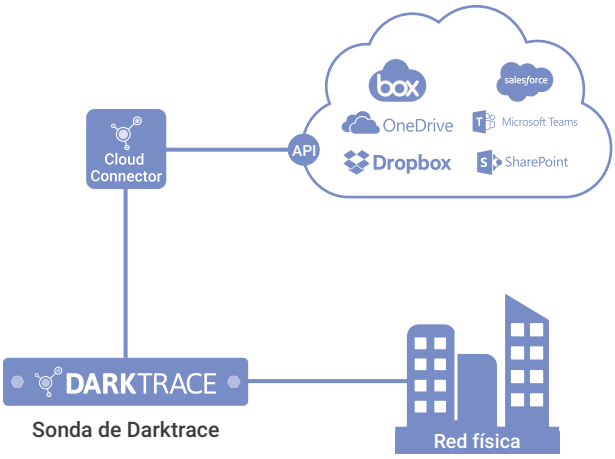
Por último, Darktrace captura el tráfico de contenedores en Docker y Kubernetes a través de un OS-Sensor especializado, que envía de manera similar los datos a un vSensor local y, a su vez, a una sonda maestra de Darktrace para su análisis.



Nube híbrida (SaaS)

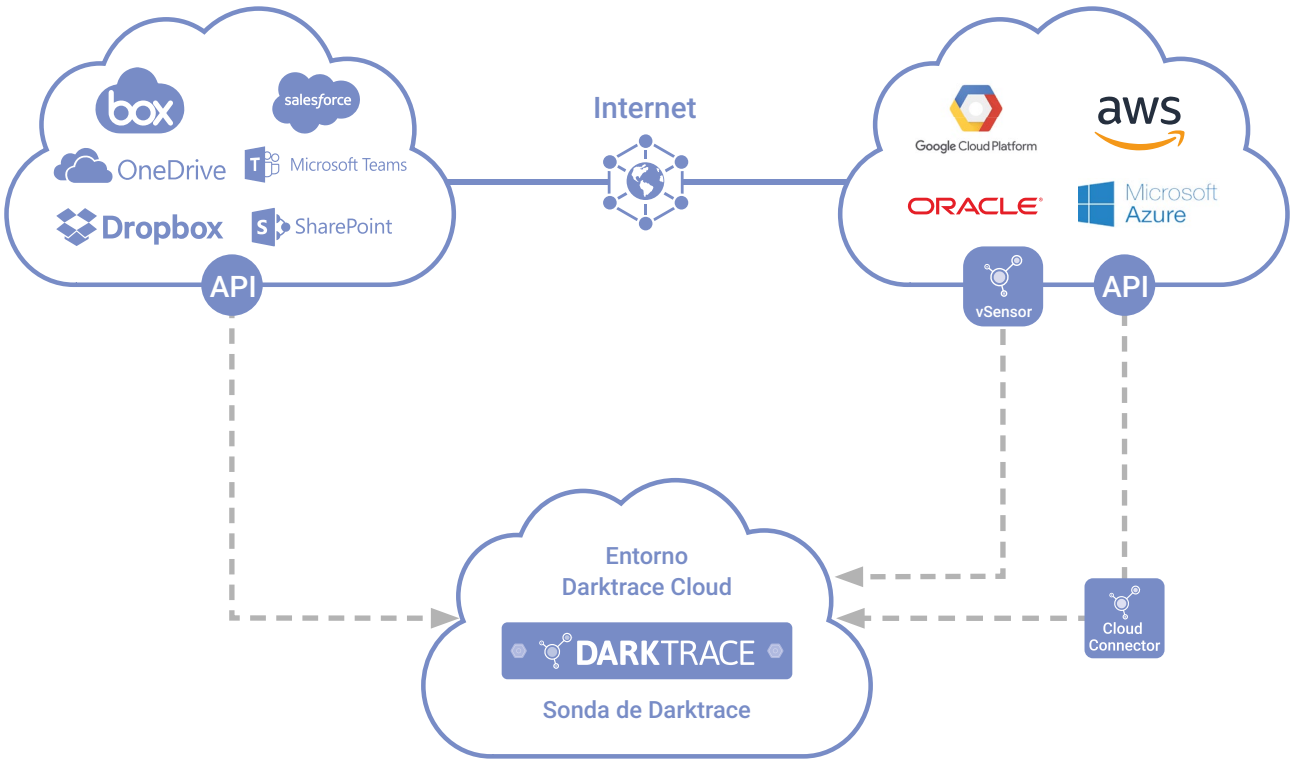
En las implementaciones de SaaS híbridas, los Conectores de Darktrace se instalan de forma remota en la sonda maestra de Darktrace (ya sea física o en la Nube) para preguntar las API de seguridad de las soluciones de SaaS relevantes. Esto incluye Office 365, Salesforce, Dropbox, Box, Egnyte y muchos más.

Una vez implementados los Conectores, Darktrace continuamente analiza y correlaciona los datos de SaaS con el tráfico del resto del negocio en una vista unificada.



Solo en la Nube (IaaS y/o SaaS)

Si un cliente aprovecha la nube pero no dispone de una red local, Darktrace puede proporcionar una implementación solo en la Nube como un servicio dedicado. En las implementaciones solo en la Nube, Darktrace administra una sonda maestra en la Nube que recibe el tráfico de los sensores y conectores de los entornos IaaS y/o SaaS del cliente.



Conclusión

Debido a que las organizaciones confían cada vez más en los servicios en la Nube y las aplicaciones SaaS para optimizar las prácticas de su negocio, la estrategia conocida del perímetro de la red se ha reducido, dejando a su paso un estado digital poroso y en constante cambio que se mueve a la velocidad y la escala del negocio digital.

Aunque los beneficios de la informática en la Nube garantizarán que la migración continúe, los desafíos de seguridad únicos que se presentan en la Nube requerirán tecnologías de autoaprendizaje que puedan moverse a la velocidad y la escala de las implementaciones en la Nube. Además, la creciente aparición de entornos híbridos y multinube requiere una única plataforma de seguridad que pueda correlacionar la actividad en estos diversos sistemas en tiempo real.

El liderazgo mundial de Darktrace en el campo de la inteligencia artificial para la ciberseguridad le convierte en la solución más eficaz y probada para detectar ciberincidentes anómalos y amenazas sin precedentes, dondequiera que se produzcan dentro de la Nube. En lugar de confiar en políticas y reglas predefinidas, la tecnología asume la incertidumbre inherente al complejo entorno digital actual.

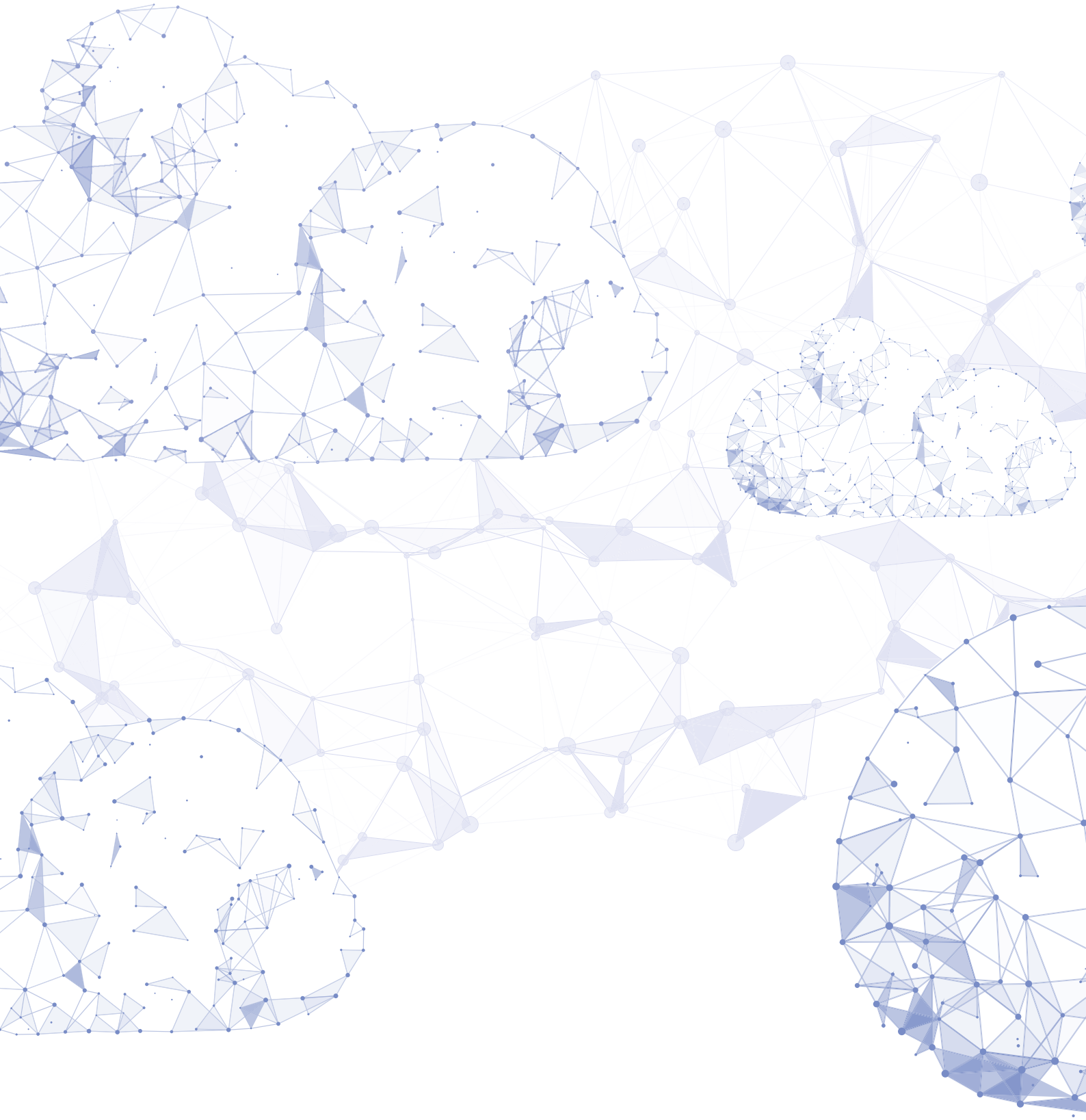
Tanto si se enfrenta a un ataque interno malicioso, a un ataque focalizado de datos confidenciales en contenedores de prueba o a un importante error de configuración que podría ser explotado en el futuro, la Plataforma de Ciber IA de Darktrace ayuda a eliminar los puntos ciegos y a proteger sus datos, dondequiera que se encuentren.

Principales beneficios

- Aprende la 'forma de ser' para detectar las amenazas basadas en la Nube que otras herramientas pasan por alto
- Correlaciona la actividad en los entornos híbridos y multinube
- 100% de visibilidad en tiempo real que deja a los atacantes sin ningún lugar donde puedan esconderse
- Investiga automáticamente los incidentes de seguridad con Cyber AI Analyst

> Darktrace representa una nueva frontera en la ciberdefensa basada en la inteligencia artificial. Nuestro equipo ahora dispone de una cobertura completa en tiempo real de nuestras aplicaciones de SaaS y contenedores en la Nube.

– CIO, City of Las Vegas



Acerca de Darktrace

Darktrace es la compañía de Ciber IA líder en el mundo y la creadora de la tecnología de Respuesta Autónoma. Su inteligencia artificial de autoaprendizaje se basa en el sistema inmune humano y la utilizan más de 3.000 organizaciones para protegerse contra las amenazas en la Nube, el correo electrónico, el IoT, las redes y los sistemas industriales.

La compañía tiene más de 1.000 empleados y sedes centrales en San Francisco y Cambridge (Reino Unido). Cada 3 segundos, la inteligencia artificial de Darktrace defiende contra una ciberamenaza, evitando que cause daños.

Contacte con nosotros

Norteamérica: +1 (415) 229 9100

Europa: +44 (0) 1223 394 100

Asia-Pacífico: +65 6804 5010

Latinoamérica: +55 11 97242 2011

info@darktrace.com | darktrace.com

@darktrace