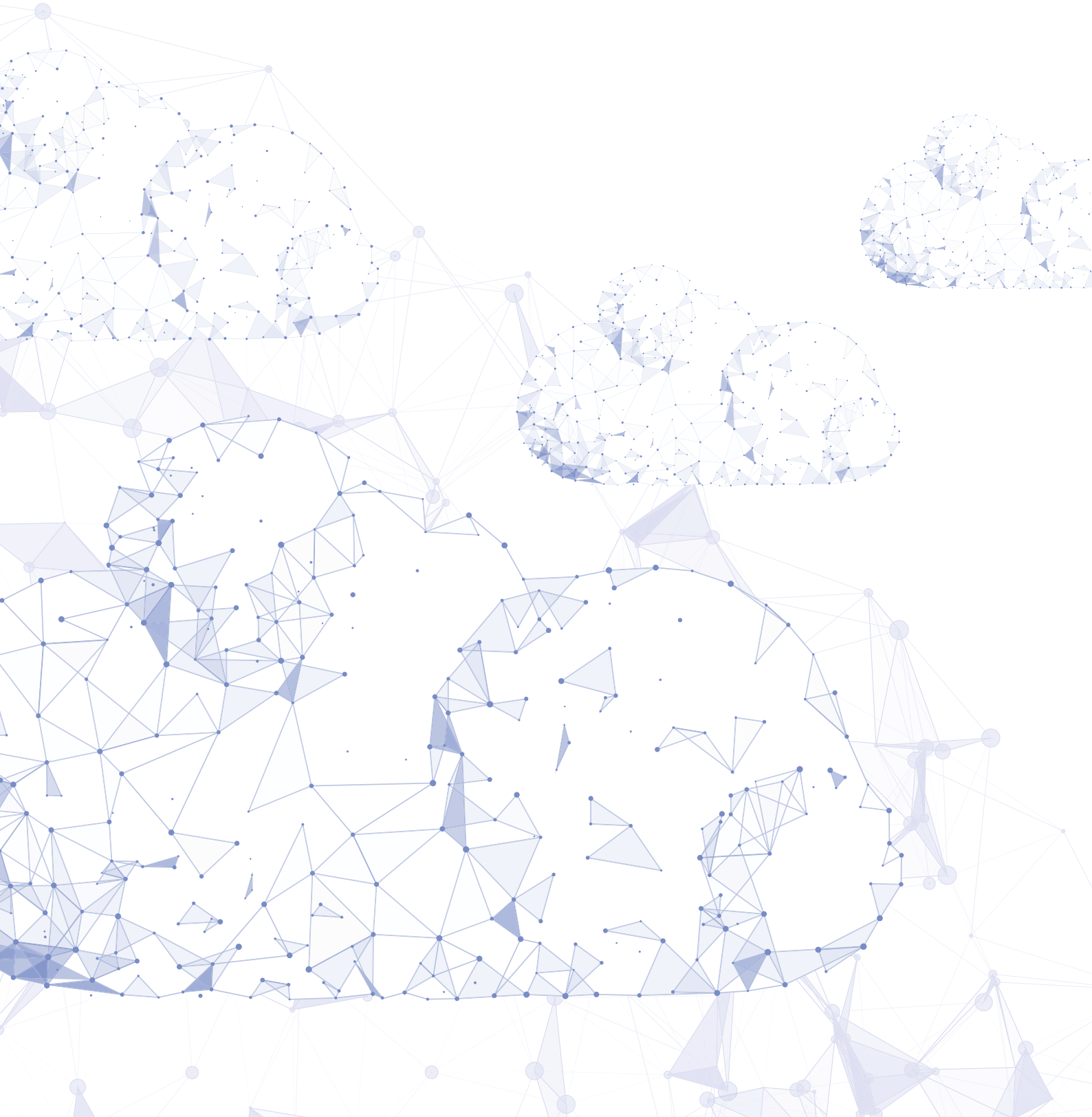
DARKTRACE

Darktrace Cyber AI

Un ‘sistema inmunológico’ para la seguridad de la nube



> A medida que las organizaciones amplían sus capacidades digitales a través de entornos híbridos, multinube y de IoT, se enfrentan a un aumento de las zonas que deben proteger y controlar. Esto también significa que existen más oportunidades para que los delincuentes dañen la confiabilidad operativa, realicen nuevos tipos de delitos y que la gestión de la empresa se vea directamente afectada.
>
> – Forrester

Índice

Introducción

Desde pequeñas empresas que buscan reducir los costos hasta los centros corporativos de innovación a la hora de emprender proyectos de transformación digital, el viaje a gran escala a la nube ha redefinido completamente la infraestructura digital y el paradigma tradicional del perímetro de la red. Debido a la desaparición de este perímetro, la infraestructura híbrida y multinube se ha convertido en una parte del mobiliario de una propiedad digital cada vez más diversa, habilitando a las organizaciones a ampliar los límites superiores de la innovación y, al mismo tiempo, ampliando la superficie de ataque a una velocidad alarmante.

Esta tendencia representa sin duda la espada de doble filo de la era digital, mientras que los retos de seguridad a los que se tienen que enfrentar los líderes empresariales en su viaje hacia la nube son difíciles de exagerar. La 'nube' en sí misma comprende una amplia gama de sistemas y servicios, y a menudo un único equipo de seguridad se responsabiliza de garantizar la seguridad de las cargas de trabajo de la nube en AWS y Azure, las comunicaciones de correo electrónico en Office 365, los datos de los clientes en Salesforce, el intercambio de archivos a través de Dropbox y los servidores virtualizados en centros de datos físicos tradicionales.

Esta amalgama de plataformas basadas en la nube a menudo impulsa la eficacia, flexibilidad e innovación a costa de una estrategia de seguridad coherente y manejable. La nube en todas sus diversas formas es un territorio desconocido para los equipos tradicionales de seguridad, y las herramientas y prácticas anteriores resultan a menudo demasiado lentas, aisladas e incluso no aplicables para defender entornos híbridos y multinube contra ataques avanzados.

Y mientras las soluciones de seguridad nativas de la nube a menudo pueden ayudar al cumplimiento y a los análisis basados en registros, raramente son lo suficientemente robustas y unificadas como para ofrecer una cobertura adecuada, tanto por seguir alentando un enfoque descontextualizado hacia la seguridad, como por basarse en reglas, firmas o presuposiciones, por lo que no detectan amenazas novedosas e intrusos sutiles antes de que puedan llegar a generar una crisis.

Peor aún, la falta de visibilidad y control a la que se enfrentan en esta zona los equipos de seguridad –sumados a la nueva y desconocida mentalidad necesaria debido a la agilidad y velocidad de la nube– también representa un objetivo atractivo para los ciberdelincuentes, quienes siempre buscan generar unas ganancias máximas y evitar su detección. La seguridad de la nube no está donde tiene que estar y los ciberdelincuentes lo saben mejor que nadie.

Sin embargo, en muchos sentidos, las organizaciones modernas necesitan mucho más que la mera seguridad de la nube, necesitan seguridad en toda la empresa y una plataforma unificada que puedan gestionar a la velocidad de la infraestructura digital, que les permita adaptarse a futuras amenazas y que correlacione los rasgos sutiles de un ataque avanzado conforme amplía su presencia dentro de una red.

La plataforma de

Limitaciones del enfoque de silos para la seguridad de la nube

Los proveedores de servicios en la nube y otros proveedores ofrecen una gama de soluciones 'nativas de la nube' que ayudan a los clientes a defender su parte del modelo de responsabilidad compartida. Sin embargo, estas soluciones específicas, ya sean nativas o de terceros, suelen estar deficientemente equipadas para detectar y responder a amenazas avanzadas en la nube.

Controles nativos: necesarios, pero no suficientes

Los controles de seguridad nativos se diseñan a menudo exclusivamente para un único proveedor de la nube y cubren solo una parte de esta vasta organización híbrida y multinube. Esto limita considerablemente el alcance de detección y aumenta la complejidad de una pila de seguridad ya de por sí compleja.

En general, los controles nativos pueden ayudar con el cumplimiento, la recopilación de registros y la creación de políticas estáticas, pero no se han diseñado para la detección de amenazas avanzadas ni para responder en múltiples silos y servicios de la nube.

Controles de terceros: útiles, pero no suficientes

Los controles de terceros tales como los CASB y las CWPP también son útiles, pero no suficientes. Los CASB, por ejemplo, pueden ayudar con el descubrimiento, la creación de políticas granulares y el cumplimiento, pero a menudo no detectan las ciberamenazas que ocupan el extremo más avanzado del espectro, desde credenciales comprometidas y ransomware, hasta intrusos descontentos y espionaje corporativo.

Si bien los controles de terceros suelen proporcionar visibilidad en la nube, no pueden ver en el interior de la red física de una organización. Esto supone una importante limitación, ya que la correlación de información en la nube y la red corporativa constituye a menudo el único modo en que un sistema de seguridad puede señalar la presencia de una amenaza emergente.

Un 'sistema inmunológico' para la nube y más allá

Impulsada por la inteligencia artificial, la plataforma de Darktrace cubre estos vacíos críticos mediante un enfoque único para toda la empresa capaz de detectar y responder a amenazas basadas en la nube que pasan desapercibidas para otras herramientas.

Al igual que el sistema inmunológico humano, la tecnología desarrolla un sentido innato de la 'forma de ser', aprendiendo el 'patrón de vida' normal de cada usuario, dispositivo y contenedor a través de entornos híbridos y multinube. Mediante un análisis continuo del comportamiento de todos y de todo en la empresa, la IA con capacidad de autoaprendizaje de Darktrace puede correlacionar de un modo único las señales débiles y sutiles de un ataque avanzado, sin definir de antemano qué es 'benigno' y qué es 'malicioso'.

Mientras que las soluciones específicas preprogramadas complementan sin duda este enfoque, Darktrace es la única tecnología probada para detener toda la gama de ciberamenazas de la nube, desde intrusos maliciosos y ataques externos, hasta errores críticos de configuración que pueden exponer la empresa a peligros futuros, independientemente de que su origen sean campañas de spear phishing dirigidas, robo de cuentas corporativas, filtración de datos 'low and slow' o movimientos laterales por la nube.

Protección unificada a medida

Gracias a la comprensión de la propiedad digital de toda la empresa, Darktrace correlaciona en tiempo real toda la actividad en las instalaciones con el tráfico en los entornos híbrido y multinube. Esto le permite comprender que un comportamiento apenas perceptible en la nube, si se considera de forma aislada, puede señalar una actividad maliciosa de mayor envergadura.

Por ejemplo, podríamos ver que un usuario ha iniciado sesión en AWS en la nube. Esto no es en sí nada malicioso, pero Darktrace también sabe que el mismo usuario de la cuenta de Office 365 se vio probablemente comprometido momentos antes, ya que se detectó una ubicación de inicio de sesión muy inusual. Darktrace comprende que la conexión a AWS es, de hecho, muy sospechosa.

> Los líderes de seguridad consideran cada vez más mejorar su eficacia eliminando productos específicos en favor de plataformas de seguridad más amplias.
>
> **– Gartner**

Correlación de información a nivel de contenedor

A pesar de la creciente adopción de contenedores por parte de los desarrolladores, la seguridad a menudo ha quedado rezagada. La naturaleza virtualizada de los contenedores dificulta la monitorización del tráfico interno de servidores. Mientras que los sistemas basados en reglas realizan un seguimiento de los datos solo a través de los servidores, Darktrace es capaz de ofrecer visibilidad en los entornos contenerizados dentro de los servidores individuales.

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

Consulte en la página 14 los escenarios de implementación

AI Analyst: investigación de amenazas automatizada

El Cyber AI Analyst da un paso más e investiga automáticamente las amenazas detectadas por el Enterprise Immune System y crea un panel dinámico de la situación, así como informes generados por la IA que detallan todo el alcance de un incidente de seguridad.

Mediante la correlación en tiempo real del tráfico de la nube con el resto de la red, el AI Analyst puede realizar cientos de investigaciones simultáneamente, conectando una constelación de alertas e indicadores, y desarrollando una profunda comprensión de los incidentes a la velocidad de la máquina. A continuación, comunica sus resultados y recomendaciones en forma de Incidentes de AI Analyst, que se complementan con información del contexto y la seguridad que es posible revisar y permite tanto a ejecutivos como a usuarios finales adoptar medidas.

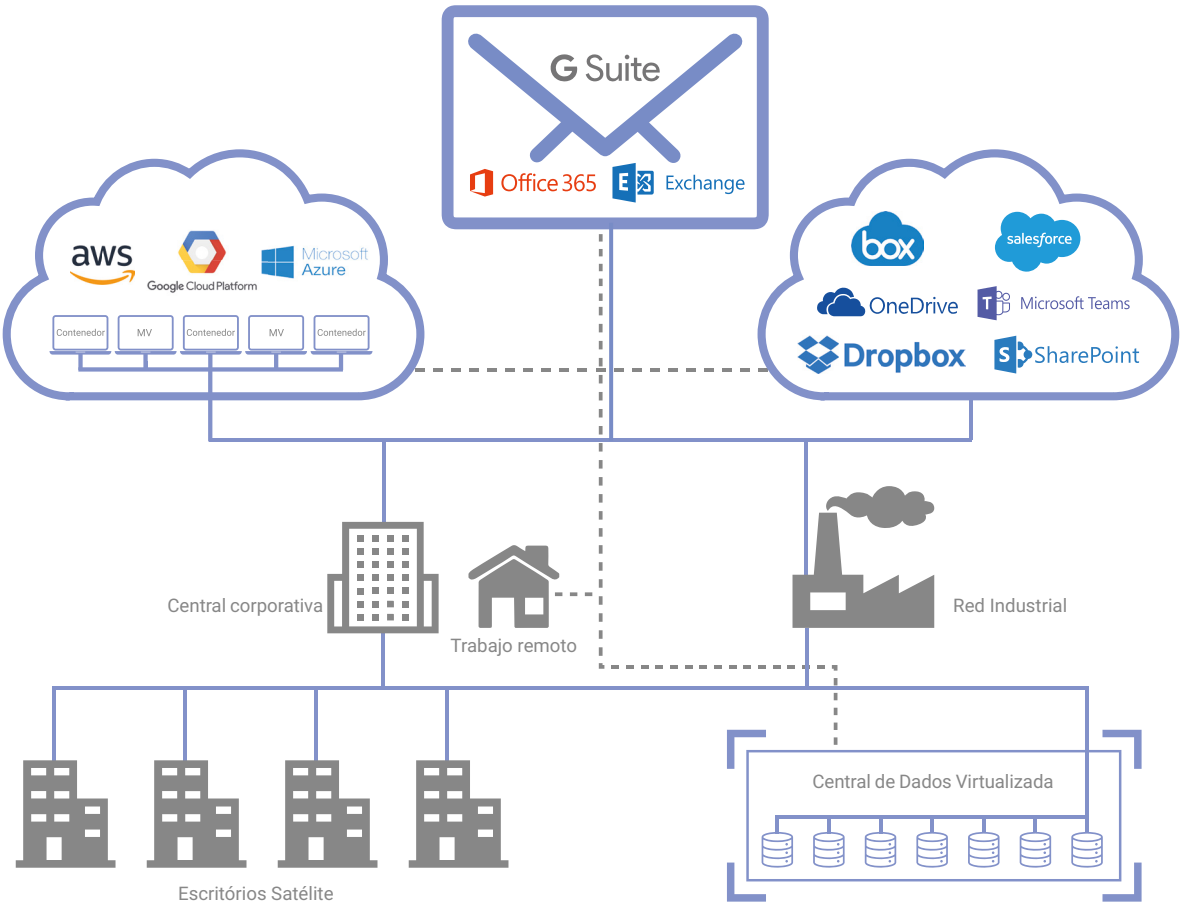


Figura 1: Cobertura unificada de Darktrace de toda la propiedad digital

Credenciales comprometidas

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

Fuente: Verizon 2019

Los ciberdelicuentes avanzados pueden robar las credenciales de cuentas corporativas de distintos modos, desde ataques de ingeniería social hasta malware 'inteligente' que analiza todo el tráfico y activos temporales de la nube buscando contraseñas. Además, en la Dark Web es posible tener acceso fácilmente a datos robados, por lo que la frecuencia y la gravedad del robo de credenciales aumenta año tras año.

Los casos de robo de cuentas representan solo la primera etapa de una ciberamenaza. La meta final de un ataque basado en credenciales es el uso de contraseñas comprometidas para autenticar aplicaciones y robar datos. Cuando el atacante se ha hecho con las credenciales para operar como un usuario válido, se puede hacer muy poco para distinguir al intruso del empleado legítimo al que están suplantando.

Mediante la correlación de datos a través de entornos híbridos y multinube, Darktrace aprende el 'patrón de vida' de cada usuario sobre una base de cientos de métricas y esto le permite detectar inmediatamente desviaciones en el comportamiento indicativas de un robo de cuenta. Incluso en casos de compromiso preexistente, la IA de Darktrace señalará de forma retrospectiva cualquier comportamiento inusual mediante el aprendizaje del 'patrón de vida' del grupo de compañeros de dicho usuario, así como del resto de la empresa.

Figura 2: La IA de Darktrace detecta una actividad inusual relacionada a una cuenta de la nube comprometida

Ataque de SharePoint

Después de obtener credenciales robadas o de acceder de cualquier otro modo al servicio de transferencia de archivos basado en la nube de una organización, los ciberdelincuentes ejecutarán frecuentemente scripts para identificar archivos que contengan palabras clave como, por ejemplo, 'contraseña'. Darktrace descubrió un incidente de este tipo en un banco europeo, en el que los delincuentes lograron encontrar un archivo de SharePoint en Office 365 que almacenaba contraseñas sin cifrar. Tras haber eludido los controles nativos de Microsoft, los delincuentes podrían haber esperado razonablemente estar a salvo.

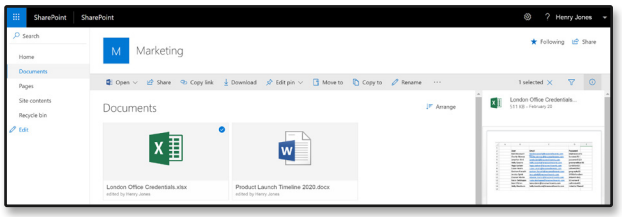


Figura 3: Los archivos confidenciales a los que se accedió en SharePoint

Sin embargo, la IA de Darktrace marcó la actividad como anómala para el usuario corporativo, su grupo de compañeros y el resto de la organización, detectando un acceso inusual a estos archivos confidenciales, entre otros indicadores. En última instancia, la comprensión matizada y en constante evolución que tiene la IA de lo 'normal' en toda la organización demostró ser crítica, dado que el acceso sospechoso al archivo podría haber sido 'benigno' en otras circunstancias.

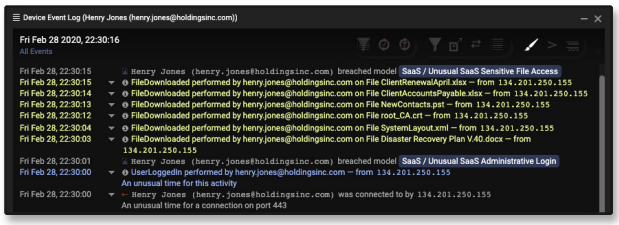


Figura 4: Darktrace detecta descargas de archivos confidenciales

Es muy probable que estos delincuentes hubieran aprovechado las contraseñas sin cifrar para aumentar sus privilegios e infiltrarse más en la organización. Sin embargo, gracias al aprendizaje único del 'patrón de vida' de cada usuario y dispositivo de la organización, la IA de Darktrace fue capaz de alertar al equipo de seguridad sobre este incidente antes de que desembocara en una crisis.

Intento de inicio de sesión de SaaS desde Ecuador

En una organización internacional, Darktrace detectó un problema en una cuenta de Office 365 que eludió los controles nativos de Azure Active Directory. Aunque la organización tenía oficinas en todos los rincones del mundo, la IA de Darktrace identificó un inicio de sesión desde una dirección IP que era históricamente inusual para dicho usuario y su grupo de compañeros, y alertó inmediatamente al equipo de seguridad. Darktrace también alertó del hecho de que se había configurado en la cuenta una nueva regla de procesamiento del correo electrónico que borraba los mensajes de correo electrónico entrantes. Esto era una clara evidencia de que la cuenta estaba comprometida y el equipo de seguridad pudo bloquearla antes de que el delincuente pudiera infringir daños.

Cuando el equipo de seguridad investigó más a fondo el incidente, descubrieron que el usuario había recibido un mensaje de correo electrónico de phishing solo horas antes de que Darktrace detectara la amenaza. A pesar de que la empresa también había implementado la Protección contra amenazas avanzada de Office 365 (ATP) de Microsoft, defensas estáticas como ATP solo pueden detectar ataques de phishing correlacionando enlaces de mensajes de correo electrónico con direcciones maliciosas conocidas y el enlace de phishing no aparecía en la lista. Esto evidenció las claras limitaciones de un enfoque basado en firmas en este área, por lo que organización no tardó en implementar la tecnología de respuesta autónoma de Darktrace, Antigena, en Office 365 como defensa adicional, dada su capacidad para detectar mensajes de correo electrónico de phishing similares sin depender de listas negras.

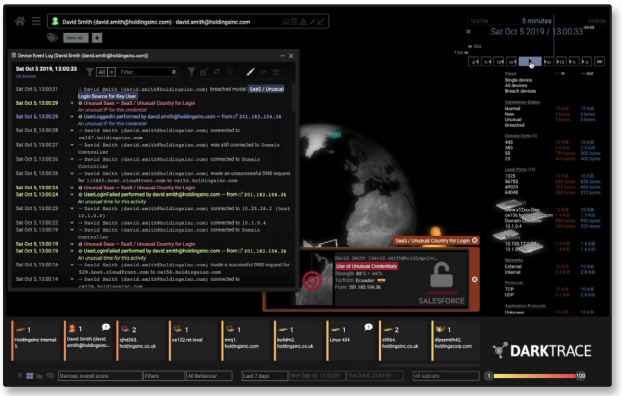


Figura 5: La IA de Darktrace detecta una ubicación de inicio de sesión de SaaS inusual

Inicio de sesión inusual en un banco panameño

En un ataque de fuerza bruta contra un conocido banco de Panamá, se utilizó una cuenta de Office 365 con inicios de sesión que se originaban en un país que se apartaba de los 'patrones de vida' normales de las operaciones de la empresa.

Darktrace identificó 885 inicios de sesión en un periodo de 7 días. Mientras que la mayoría de las autenticaciones tenían su origen en direcciones IP de Panamá, el 15% de las autenticaciones se originaban en una dirección IP que era 100% extraña y se encontraba en la India. Un análisis más detallado reveló que este punto de conexión externo estaba incluido en varias listas negras de spam y que recientemente se había asociado con un comportamiento abusivo en línea –posiblemente escaneados no autorizados de Internet o piratería.

Figura 6: La interfaz de usuario mostrando las ubicaciones de inicio de sesión

Darktrace también detectó lo que parecía ser un abuso de la función de restablecimiento de contraseña, ya que se observó que el usuario de la India cambiaba los privilegios de la cuenta de una manera muy inusual. Lo que señaló esta actividad como especialmente sospechosa fue que, tras el restablecimiento de la contraseña, se observaron inicios de sesión fallidos desde una IP asociada normalmente con la organización, lo que sugería que el usuario legítimo estaba 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 de fuerza bruta automatizado

Darktrace detectó varios eventos fallidos de inicio de sesión en una cuenta de SaaS todos los días durante toda una semana. Cada lote de intentos de inicio de sesión se realizó exactamente a las 18:04 durante seis días. La coherencia tanto en la hora del día, como en el número de intentos de inicio de sesión indicaba un ataque de fuerza bruta automatizado programado para dejar de hacerse después de un número determinado de intentos fallidos con el fin de evitar bloqueos.

Darktrace consideró muy anómalo este patrón de intentos fallidos y alertó al equipo de seguridad. Si Darktrace no hubiera correlacionado los múltiples indicadores débiles y no hubiera concretado las señales sutiles de una amenaza emergente, este ataque automatizado podría haber continuado durante semanas o meses, realizando conjeturas sistemáticas de la contraseña del usuario sobre la base de otra información que ya había reunido.

Figura 8: La actividad asociada con la cuenta de SaaS destacando las credenciales modificadas

Robo de cuenta de Office 365

Después de hacer clic en un enlace malicioso contenido dentro de un mensaje de correo electrónico dirigido, una empleada introdujo sus credenciales en una página de inicio de sesión falsificada que registró sus pulsaciones de teclas. Tras hacerse con sus credenciales, los delincuentes volvieron a Office 365 y las usaron para iniciar sesión de forma remota. Darktrace detectó ubicaciones inusuales como Bulgaria e Indonesia.

Mediante el aprendizaje de los patrones de los lugares desde los que trabajaban los usuarios, así como del momento y el modo en que accedían a los servicio de la nube, la IA de Darktrace identificó, y podría haber impedido, estas peticiones inusuales de inicio de sesión. En este caso, las funciones de seguridad nativas no identificaron ni impidieron estos inicios de sesión maliciosos.

Una vez dentro de la cuenta de Office 365 de la empleada, los delincuentes se propagaron a más víctimas, continuando el ciclo. Aquí, Darktrace detectó otro cambio de comportamiento –se trataba de 99 mensajes de correo electrónico enviados a un gran número de empresas con el texto 'Aviso de pago' en la línea de asunto. A pesar de que este comportamiento podría ser normal para algunos empleados, quedaba fuera del patrón de vida de dicha usuaria específica.

Darktrace también advirtió la creación de una nueva regla de reenvío para la bandeja de entrada, algo que a menudo crean los delincuentes para difundir spam u ocultar sus actividades.

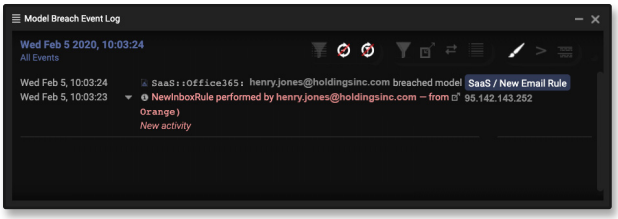


Figura 9: Darktrace detecta la regla de procesamiento de la bandeja de entrada

La eliminación automática de los mensajes de correo electrónico tras su envío destruye el rastro de pruebas dentro del sistema de correo electrónico. Sin embargo, la monitorización independiente, tanto de los mensajes de correo electrónico como de las actividades de la cuenta de SaaS, permitió a Darktrace obtener una imagen completa de las actividades del delincuente. La capacidad de la plataforma para aprender identidades y comportamientos en toda la empresa le permitió detectar esta actividad sospechosa.

Figura 10: Las ubicaciones de inicio de sesión inusuales

Intrusos maliciosos

> La IA de Darktrace se adapta mientras trabaja, arrojando luz sobre la infraestructura de nuestra red y la nube en tiempo real, y nos permite defender la nube con confianza
>
> **CISO, Aptean**

Las amenazas internas en la nube a menudo representan una mayor ciberamenaza para las organizaciones que los atacantes externos por un razón obvia: ya están dentro. Un empleado con intenciones maliciosas se encuentra en una posición privilegiada para eludir las herramientas tradicionales, dado su acceso privilegiado y el profundo conocimiento de la red.

Los servicios de la nube han ampliado enormemente el alcance de las amenazas internas debido al gran número de aplicaciones que ofrecen una amplia gama de vectores para la filtración de datos, mientras que la visibilidad limitada de este área permite filtrar datos de manera desapercibida.

Debido a su naturaleza, las herramientas de seguridad heredadas son incapaces de detectar la actividad maliciosa que se produce dentro de la organización. La seguridad de la nube requiere ahora un enfoque más amplio que incluya el análisis del tráfico en toda la propiedad digital y establezca de un 'patrón de vida' cambiante para la organización.

Ya se trate de un vendedor que ha desertado llevándose consigo información de clientes o un administrador de TI descontento que manipula sutilmente datos cruciales, la inteligencia artificial puede utilizarse para detectar cualquier actividad inusual y anómala indicativa de una ciberamenaza.

Figura 11: Darktrace Antigena bloquea a un intruso malicioso que intenta filtrar datos confidenciales

Empleado de TI descontento

Darktrace fue testigo de un caso de amenaza interna después del despido de un empleado que trabajaba como administrador del sistema de TI. Aquella semana, la organización se vio obligada a hacer una serie de despidos en la oficina, pero se olvidó de retener las computadoras portátiles de los empleados y de eliminar sus cuentas corporativas. El ex-administrador de TI inició sesión en su cuenta de SaaS y descargó rápidamente numerosos archivos confidenciales de la base de datos de clientes, incluida información personal y números de tarjetas de crédito.

Figura 12: El Threat Visualizer mostrando un gran aumento en el número de conexiones

A continuación, intentó trasferir secretamente estos archivos a un servidor principal a través de uno de los servicios de transferencia de datos de la empresa. Antes de hacerlo, creó una nueva 'cuenta anónima' para crear una puerta trasera, asegurándose así de que podía mantener un brecha abierta en la empresa cuando el equipo de TI finalmente cerrara sus cuentas corporativas.

El administrador de TI sabía que este servicio en particular no solo estaba sancionado por las políticas corporativas, sino que además estaba basado en la nube, y asumió que el equipo de seguridad tendría una visibilidad limitada de este área. Sin embargo, Darktrace analizó dinámicamente los eventos de inicio de sesión y acceso a archivos en los servicios de la nube corporativa, y los correlacionó con los 'patrones de vida' aprendidos para cada usuario de la organización a la luz de nuevas pruebas. Como sistema unificado con capacidad de autoaprendizaje, la plataforma de ciber IA de Darktrace detectó inmediatamente las descargas de archivos inusualmente grandes, la creación de la cuenta nueva y la filtración de datos. A continuación, se activó su tecnología de respuesta autónoma, Antigena, para bloquear el intento de descarga.

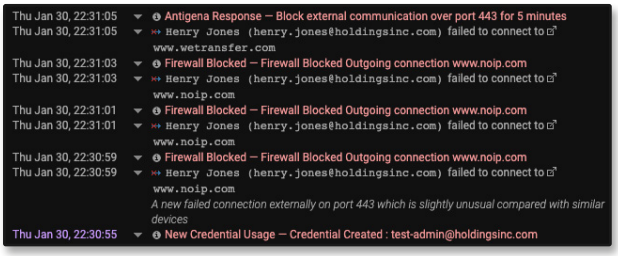


Figura 13: Darktrace Antigena pone en marcha una respuesta autónoma dirigida

Investigaciones posteriores revelaron que el empleado trató de enviar estos archivos a un servidor personal ubicado en su hogar. Cuando fracasó en su intento, continuó tratando de filtrar los datos a otras fuentes. Sin embargo, gracias a que Antigena puede adaptarse dinámicamente a las amenazas a medida que se despliegan y, al mismo tiempo, escalar su respuesta, fue capaz de interrumpir quirúrgicamente estos intentos cada vez que se producían.

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 neutralizo también esa conexión.

Figura 14: Antigena bloquea el intento del empleado de transferir los archivos a través de la nube.

A pesar de que esta actividad sutil eludió fácilmente los controles nativos del proveedor de la nube, la IA de Darktrace detectó el comportamiento amenazador en cuestión de segundos. Mediante el aprendizaje continuo de lo 'normal' para cada usuario y dispositivo, el sistema fue capaz de correlacionar de manera inteligente conexiones y descargas muy sospechosas desde el dispositivo del administrador de TI, incluso cuando el servicio de la nube se utilizaba regularmente por otros empleados con fines legítimos.

La plataforma de ciber IA de Darktrace alertó inmediatamente al equipo de seguridad, proporcionando información detallada y precisa sobre la naturaleza de la amenaza y motivando al equipo a revocar sus credenciales y a recuperar y asegurar rápidamente los datos.

Errores de configuración

> si todos los ataques exitosos a los servicios de la nube son resultado de un error de configuración del cliente.
>
> **– Neil MacDonald, Gartner**

La configuración de los controles de seguridad en entornos híbridos y multinube es a menudo un proceso complejo, ya que las soluciones nativas y de terceros en este área son diversas, incompatibles e insuficientes. El desconocimiento de la nube con frecuencia da lugar a errores de configuración críticos que dejan la empresa expuesta a ataques. Ahora, los programadores modernos pueden poner en marcha una instancia en la nube en cuestión de minutos, a menudo sin tener que consultarlo con el equipo de seguridad de la empresa. Como consecuencia, la mayoría de las organizaciones carecen de visibilidad sobre sus propios entornos de nube, por lo que unas entregas precipitadas pueden dar lugar a unas vulnerabilidades enormes que pasan desapercibidas durante meses.

Las posibles ramificaciones de un error de configuración se pusieron de manifiesto con la violación de datos que sufrió Capital One, que afectó a más 100 millones de personas aprovechando una vulnerabilidad en la nube. Esta importante institución financiera, con un enfoque maduro hacia la seguridad de la nube, solo detectó este evento cuando una persona ajena a la empresa se lo comunicó después de haberse tropezado con los datos robados –tres meses después de que ocurriera dicha violación.

La inteligencia artificial se utiliza ahora para comprender los 'patrones de vida' normales de cada usuario, dispositivo y contenedor, reconociendo los patrones sutiles de comportamiento asociados con un error de configuración. El uso de tecnología con capacidad de autoaprendizaje, como la plataforma de ciber IA de Darktrace, permite a las empresas adquirir los conocimientos necesarios sobre los complejos entornos de nube para detectar vulnerabilidades latentes en sus etapas iniciales, antes de que generen una crisis.

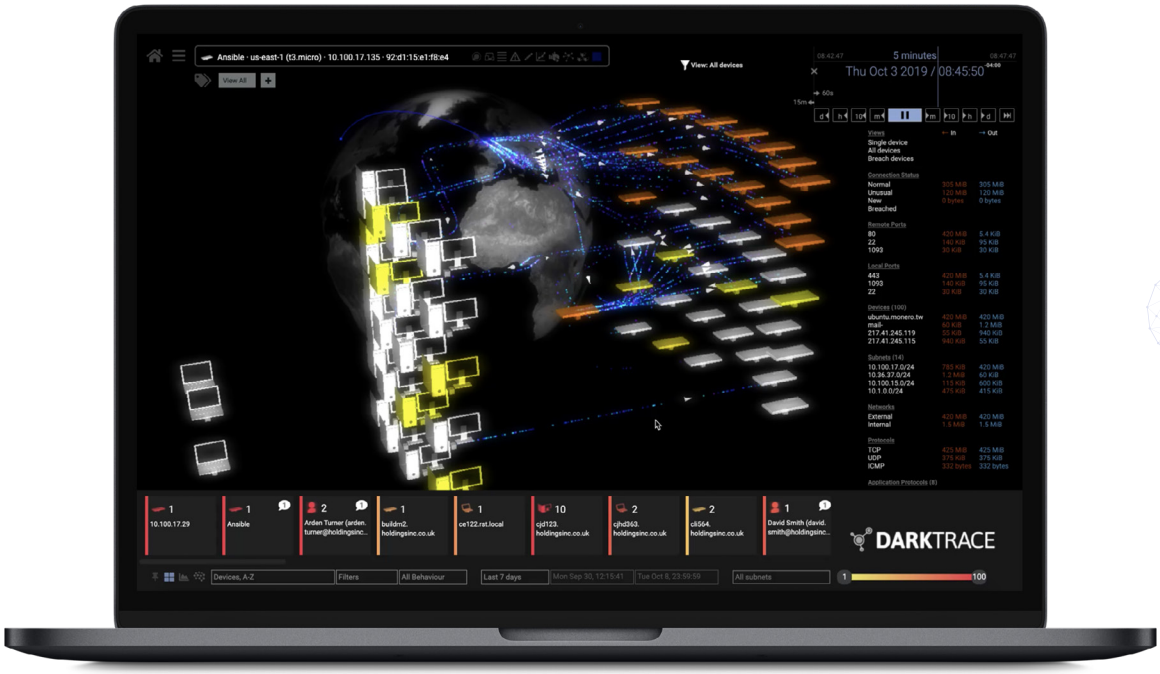


Figura 15: Un error de configuración de DevOps provoca la rápida propagación de crypto-malware

Ataque desde Shodan contra la vulnerabilidad de la nube

Una organización de servicios financieros alojaba distintos servidores críticos en máquinas virtuales en la nube, algunas de las cuales estaban orientadas al público mientras que otras no lo estaban. Al configurar sus controles nativos de la nube, dejaron por error un importante servidor expuesto a Internet, cuando se suponía que debía estar aislado por un firewall. Esto podría haber sucedido por multitud de razones, posiblemente debido a una migración rápida y caótica o bien, porque no estaban familiarizados con los controles nativos proporcionado por su CSP.

Aunque el equipo de seguridad ni siquiera se había dado cuenta del error de configuración, al final fue descubierto y se convirtió en blanco de ataque de unos ciberdelincuentes que escaneaban Internet a través de Shodan. En cuestión de segundos, la IA de Darktrace detectó que el dispositivo estaba recibiendo una cantidad inusual de intentos de conexión desde una amplia gama de fuentes externas extrañas y alertó al equipo de seguridad sobre esta amenaza.

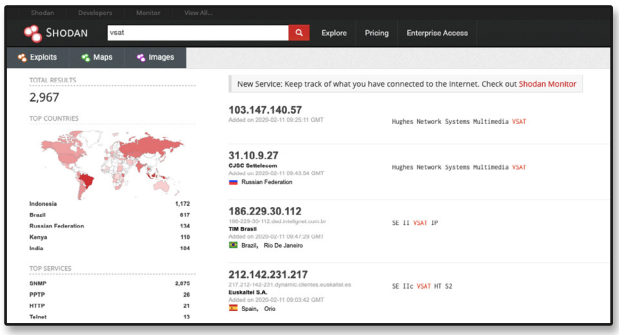


Figura 16: La página web Shodan se utilizó para escanear vulnerabilidades

Información personalmente identificable (PII) en AWS sin cifrar

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

Se había previsto que esta información altamente confidencial solo estuviera accesible de forma limitada para empleados municipales seleccionados, pero un descuido de la seguridad había puesto los datos a disposición de cualquier delincuente capaz de escanear el perímetro de la red y recoger los paquetes de datos que se encontrara por el camino.

Inicialmente, la organización no se había dado cuenta de este error de configuración, que pasó desapercibido para toda la pila de seguridad. Sin embargo, cuando Darktrace detectó una conexión inusual a una IP externa extraña desde un dispositivo de escritorio dentro de la empresa, comprobó que esta comunicación estaba revelando datos públicos confidenciales, a los que podía acceder un delincuente para recopilar material para futuros ataques de spear phishing e incluso para suplantar identidades. La visibilidad total que ofrece Darktrace en tiempo real reveló este peligroso punto ciego y permitió al equipo de seguridad corregir el error de configuración.

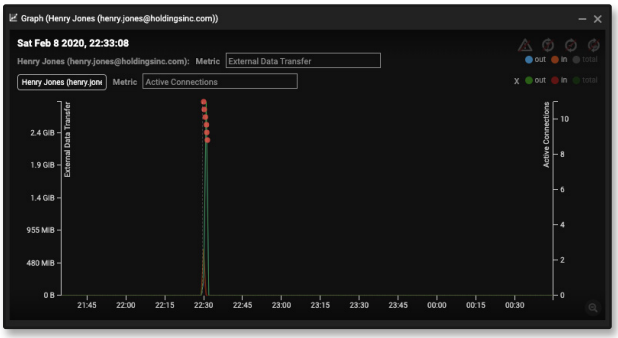


Figura 17: El Threat Visualizer mostrando la transferencia externa de más de 2GB de datos

Instalación inadvertida de malware de criptominería

Darktrace detectó el error de un ingeniero junior de DevOps de una multinacional con cargas de trabajo en AWS y Azure, que aprovechaba sistemas de contenedores como Docker y Kubernetes. El ingeniero descargó accidentalmente una actualización que incluía un malware de criptominería que infectó múltiples sistemas de producción de la nube.

Tras la infección inicial, el malware comenzó a enviar señales a un servidor de comando y control externo que fueron inmediatamente detectadas por Darktrace. Con la conexión externa establecida y las instrucciones de la misión de ataque entregadas, la infección del malware de criptominería fue capaz de propagarse rápidamente por la amplia infraestructura de la nube de la organización, a la velocidad de la máquina, infectando 20 servidores de la nube en menos de 15 segundos.

Gracias a la IA de Darktrace, el entorno de la nube de esta empresa había dejado de ser un punto ciego y se disponía de una vista dinámica y unificada de la vasta infraestructura híbrida y multinube, lo que permitió al equipo de seguridad contener el ataque en cuestión de minutos, en vez de horas o días. Aunque el ataque ocurrió a la velocidad de la máquina, Darktrace lo detectó en una fase suficientemente temprana, mucho antes de que los costos pudieran comenzar a dispararse.

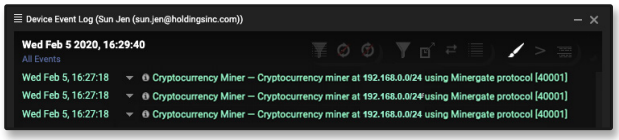


Figura 18: El malware de criptominería detectado en tiempo real.

IP expuesta en Azure

Una empresa de fabricación líder de Europa utilizaba un servidor de Microsoft Azure para almacenar archivos con información detallada de los productos y proyecciones de ventas. A pesar de que los archivos que había en el servidor y la IP raíz estaban protegidos mediante nombre de usuario y contraseña, estos datos confidenciales se habían dejado sin cifrar. Se detectó una actividad anómala cuando un dispositivo descargó un archivo en formato ZIP desde una dirección IP externa extraña que Darktrace clasificó como muy anómala.

Posteriormente, se descubrió que la dirección IP externa pertenecía a un servidor de Microsoft Azure recientemente configurado y que el archivo en formato ZIP era accesible para cualquier persona que conociera la URL, algo que podría haberse obtenido con solo interceptar el tráfico de la red, interna o externamente. Unos delincuentes más dedicados podrían incluso haber obtenido el parámetro 'clave' de la URL del archivo mediante un ataque de fuerza bruta.

La pérdida o filtración de estos archivos confidenciales podría haber puesto en riesgo toda la línea de productos, pero al informar sobre este incidente tan pronto como fue detectado, Darktrace contribuyó a impedir la pérdida de una valiosa propiedad intelectual y ayudó al equipo de seguridad a revisar sus prácticas de almacenamiento de datos en la nube con el objetivo de mejorar la protección de la información de sus productos en el futuro.

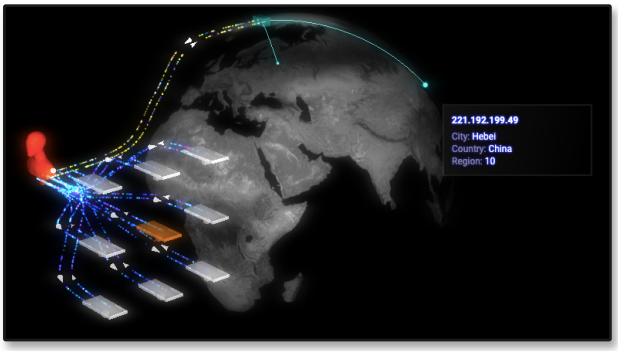


Figura 19: Darktrace mostrando la ubicación de la dirección IP inusual

Ingeniero de DevOps demasiado entusiasta

En un grupo de seguros, un ingeniero de DevOps trataba de construir una infraestructura paralela de respaldo dentro de la 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 respaldo. Sin embargo, el costo de funcionamiento del sistema habría sido de varios millones de dólares anuales.

El ingeniero de DevOps desconocía los costos asociados con el proyecto y no informó a la dirección sobre sus actividades. Cuando se puso en marcha la infraestructura de la nube, los costos comenzaron a elevarse. Pese a ello, la IA de Darktrace alertó sobre este comportamiento inusual y el equipo de seguridad fue capaz de adoptar inmediatamente medidas preventivas.

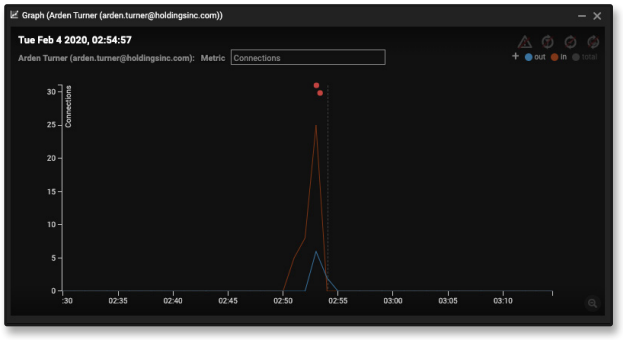


Figura 20: El Threat Visualizer mostrando un gran aumento en el número de conexiones internas y externas

Escenarios de implementación

Nube híbrida (IaaS)

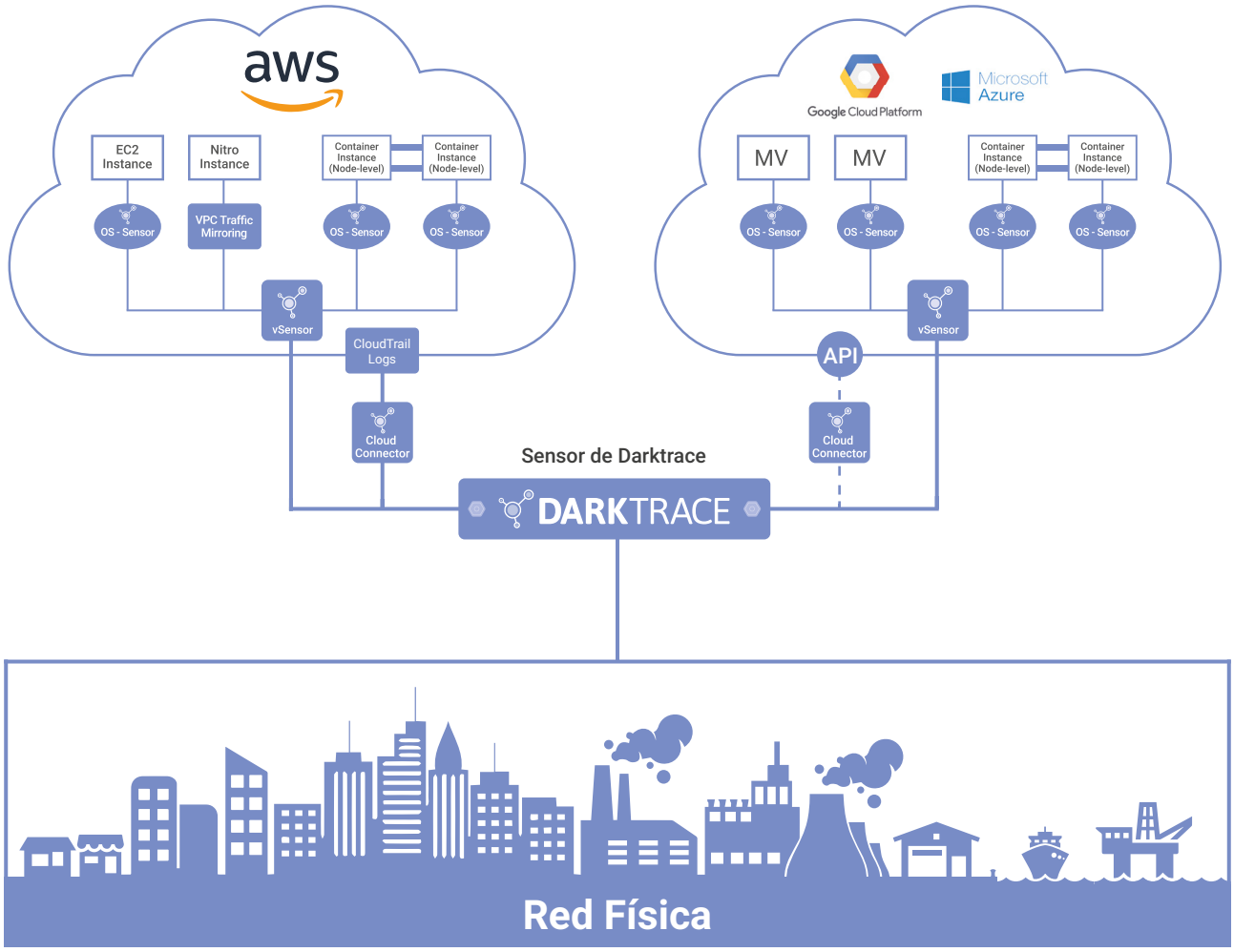
Para las organizaciones que poseen infraestructuras de nube híbrida, Darktrace implementa sensores virtuales o 'vSensor' que capturan el tráfico de la nube en tiempo real y lo correlacionan con el resto de la empresa.

En AWS, los vSensor capturan el tráfico en tiempo real desde instancias Nitro a través de VPC Traffic Mirroring. Los metadatos de AWS Nitro pueden capturarse directamente, sin necesidad de sensores adicionales a nivel de servidor. Para otras instancias, que no son instancias Nitro, Darktrace implementa sensores OS en cada punto de conexión –cada sensor OS envía el tráfico a un vSensor local que, a su vez, envía los metadatos relevantes al sensor maestro de Darktrace en la nube o en la red corporativa para su análisis.

En Azure, GCP y otros, Darktrace implementa los vSensor y los sensores OS para capturar el tráfico en tiempo real, tal y 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 de administradores de sistemas a nivel de API como, por ejemplo, la actividad de inicio de sesión y la creación de recursos.

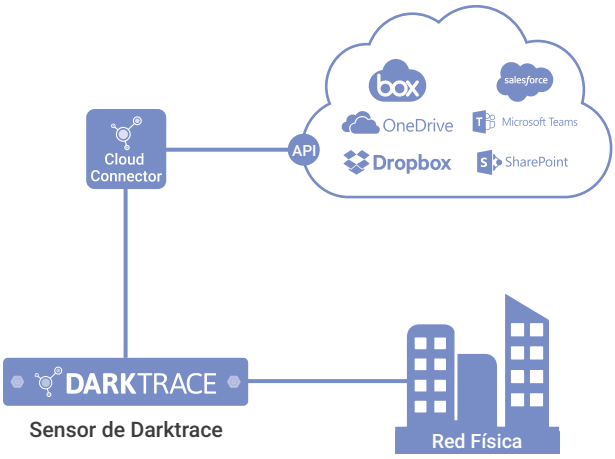
Por último, Darktrace captura el tráfico de contenedores en Docker y Kubernetes a través de un sensor OS especializado, que envía de manera parecida los datos a un vSensor local que, a su vez, los envía al sensor maestro de Darktrace para su análisis.



Nube híbrida (SaaS)

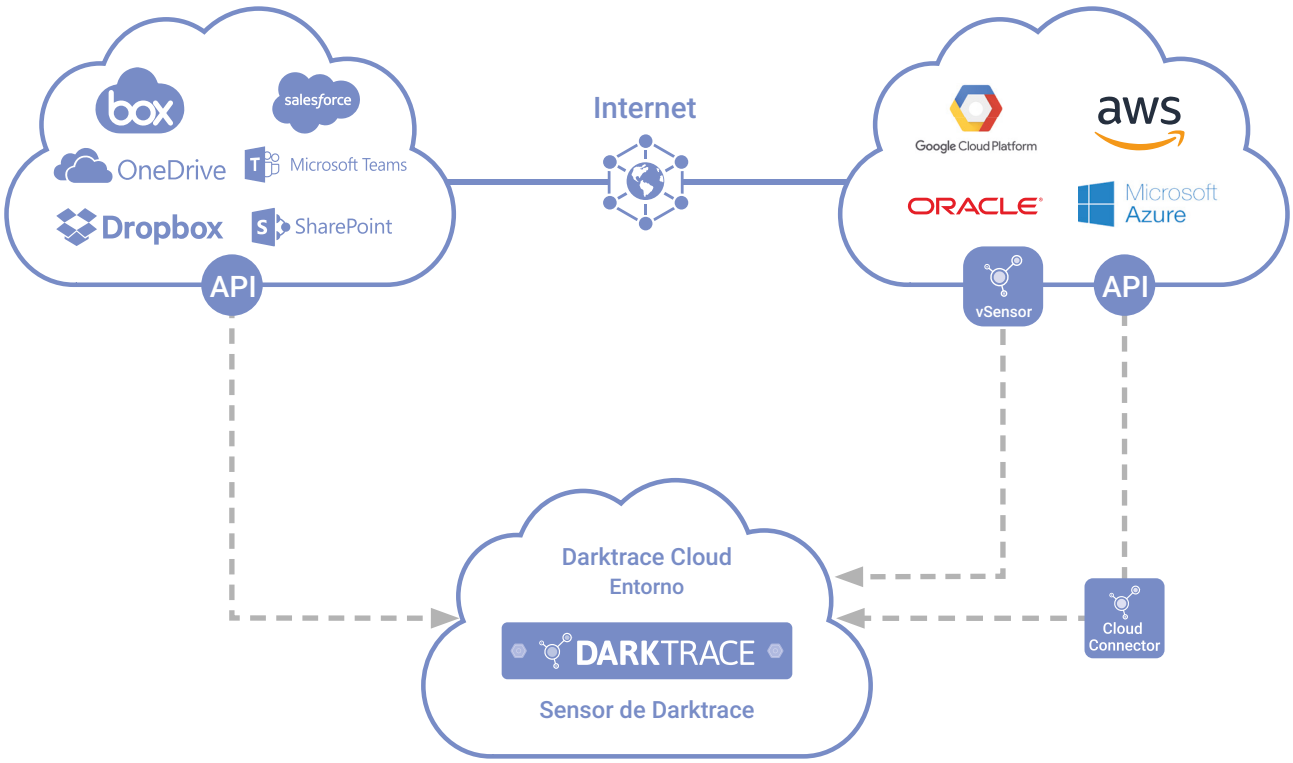
Para implementaciones de SaaS híbrido, los conectores de Darktrace se instalan de forma remota en el sensor maestro de Darktrace (ya sea físico o en la nube) para interrogar las API de seguridad de las soluciones de SaaS relevantes. Esto incluye Office 365, Salesforce, Dropbox, Box, Egnyte y muchos más.

Una vez que se han implementado los conectores, Darktrace analiza y correlaciona continuamente los datos de SaaS con el tráfico del resto de la empresa en una vista unificada.



Solo en la nube (IaaS y/o SaaS).

Si un cliente aprovecha la nube, pero carece de una red física, Darktrace puede entregar una implementación solo en la nube como un servicio dedicado. Para implementaciones que se realizan solo en la nube, Darktrace gestiona un sensor maestro en la nube que recibe el tráfico desde sensores y conectores en los entornos de IaaS y/o SaaS del cliente.



Conclusión

A medida que las organizaciones confían cada vez más en los servicios de la nube y en las aplicaciones de SaaS para racionalizar sus prácticas empresariales, el paradigma familiar del perímetro de la red se ha disuelto, dejando en su estela un patrimonio digital poroso y siempre cambiante que se mueve a la velocidad y escala de la infraestructura digital.

Mientras que las ventajas que ofrece la computación en la nube garantizarán la continuación de migraciones, los retos únicos de seguridad que plantea la nube requerirán de tecnologías con capacidad de autoaprendizaje que puedan moverse a la velocidad y escala de las implementaciones en la nube. Además, la creciente aparición de entornos híbridos y multinube requiere una única plataforma de seguridad con capacidad para correlacionar la actividad en tiempo real a través de estos diversos sistemas.

El liderazgo mundial de Darktrace en el campo de la inteligencia artificial para ciberseguridad convierte a esta solución probada en la más eficaz para detectar amenazas sin precedentes e incidentes cibernéticos anómalos en cualquier lugar de la nube. En lugar de basarse en reglas y políticas predefinidas, la tecnología adopta la incertidumbre inherente en el actual complejo entorno digital.

Ya se trate de un intruso malicioso, un delincuente lanzando un ataque para robar datos confidenciales en contenedores de prueba o un error de configuración importante que pueda ser aprovechado en el futuro, la plataforma de ciber IA de Darktrace ayuda a eliminar puntos ciegos y a proteger sus datos, dondequiera que residan.

Conclusiones clave

- Aprende 'la forma de ser' para detectar amenazas basadas en la nube que pasan desapercibidas para otras herramientas
- Correlaciona la actividad a través de entornos híbridos y multinube
- Ofrece visibilidad total en tiempo real que deja a los atacantes sin lugares para esconderse

> Darktrace representa una nueva frontera en la ciberdefensa basada en IA. Nuestro equipo tiene ahora cobertura completa en tiempo real a través de nuestras aplicaciones de SaaS y contenedores en la nube.

– CIO, Ciudad de Las Vegas

Acerca de Darktrace

Darktrace es la empresa líder mundial en ciber IA y creadora de la tecnología de **Autonomous Response** (Respuesta Autónoma). La IA de auto-aprendizaje se ha modelado en **el sistema humano** y es utilizado por más de 4.000 organizaciones para proteger contra las amenazas dirigidas hacia la **Nube**, **correo electrónico**, **IoT** (Internet de las cosas), **redes** y **sistemas industriales**.

La empresa tiene más de 1.300 empleados y cuenta con sede en San Francisco y Cambridge, Reino Unido. Cada 3 segundos, la IA de Darktrace defiende contra una amenaza cibernética, evitando que causen daños.

Contáctenos

América Latina: +55 11 97242 2011

Norteamérica: +1 (415) 229 9100

Europa: +44 (0) 1223 394 100

Asia-Pacífico: +65 6804 5010

info@darktrace.com | darktrace.com

@darktrace