Akamai

WHITE PAPER

11 capacidades fundamentales de detección y respuesta de API

Desarrollando su estrategia de seguridad de API

Introducción

Las API desempeñan un papel fundamental en todas las aplicaciones que su organización crea para los clientes, utiliza internamente y pone a disposición de distribuidores y proveedores. Su trabajo consiste en intercambiar información (a menudo datos confidenciales) entre tecnologías. Están ubicadas no solo en las aplicaciones, sino también en las migraciones a la nube, las herramientas de IA generativa y la cadena de suministro digital.

El desafío es que las API también han ocupado un lugar destacado en la superficie de ataque de su organización.

Dado que las empresas innovan a toda prisa, las API se desarrollan con rapidez, no se prueban lo suficiente y se envían a la fase de producción con errores de configuración y sin controles de seguridad. Es más, estas API proliferan hasta el punto de que los equipos de seguridad carecen de visibilidad en cuanto a gran parte de sus infraestructuras de API. Y sin una visibilidad adecuada, las organizaciones:

1. No pueden detectar las API que no se gestionan, quedan olvidadas y que siguen expuestas sin estar controladas a datos confidenciales, a Internet y a los atacantes.
2. Por lo tanto, no pueden evaluar los riesgos que representan las API: por ejemplo, tan solo el 27 % de las empresas con inventarios de API completos conocen cuáles transfieren datos confidenciales, en comparación con el 40 % en 2023.
3. Acaban con una superficie de ataque repleta de vulnerabilidades centradas en las API que los atacantes aprovechan con frecuencia (y a menudo con facilidad).

Hasta hace poco, las organizaciones se sentían cómodas confiando en una lista de herramientas de uso común para gestionar las API y obtener una protección básica. Sin embargo, dado que el 84 % de las organizaciones ha experimentado un incidente de seguridad relacionado con las API en los últimos 12 meses, frente al 78 % registrado en 2023, algo debe cambiar.

A medida los ataques a las API aumentan en número y sofisticación, es hora de evaluar la posibilidad de añadir nuevas capas de protección a herramientas como las puertas de enlace de API, los firewalls de aplicaciones web (WAF) y las plataformas de protección de aplicaciones web y API (WAAP).

Estas nuevas capas deberían proporcionar una mayor visibilidad de todas las API de su entorno y sus riesgos, incluida la gran parte de las API que no se gestionan, como las siguientes:

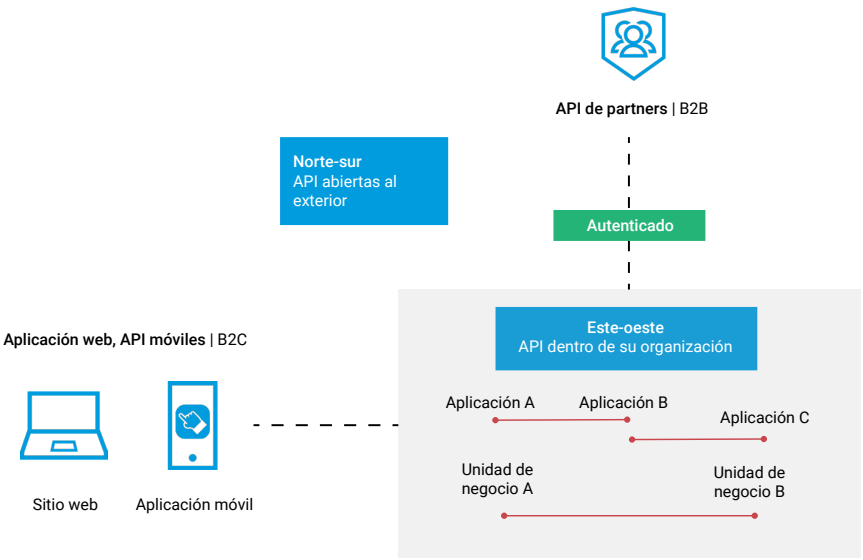
- API zombis que deberían haberse retirado, pero que permanecen activas;
- API en la sombra que no están documentadas y que deben eliminarse o incorporarse a procesos de gobernanza formales.

Las organizaciones también necesitan capacidades más específicas para detectar y combatir el abuso y los ataques de API, incluidas todas las amenazas detalladas en la lista de los 10 principales riesgos de seguridad de las API según OWASP. Además, con la mirada puesta en la búsqueda y corrección de vulnerabilidades a lo largo de todo el ciclo de vida de una API, las empresas deberían adoptar pruebas de seguridad rigurosas y en tiempo real para las API, desde las primeras fases de desarrollo hasta la de producción.

¿Significa esto que hay que añadir una nueva herramienta a la lista para cada problema que surja? No. Digamos que se trata más bien de garantizar que una orquesta tenga a los músicos adecuados para el trabajo, y que toquen siempre las notas adecuadas en los momentos adecuados, y con una coordinación precisa con sus homólogos.

Cuando piense en cómo añadir nuevas capas a su pila de protección de API, plantéese el enfoque de defensa en profundidad que los equipos de seguridad aplican a otras amenazas: por ejemplo, implementar un conjunto de controles para detectar, prevenir y mitigar los efectos de un ataque de ransomware. Así es exactamente como las organizaciones deberían pensar con respecto de las API.

En este white paper, exploraremos 11 capacidades esenciales que puede integrar en su estrategia de seguridad de API, y nos centraremos en la detección y respuesta ante amenazas de API.



El contexto es fundamental

¿Dónde encaja la detección y respuesta ante amenazas de API en una estrategia de seguridad de API?

Es probable que haya observado de primera mano que las API han modificado la forma de operar de las empresas, ya que posibilitan más casos de uso, aceleran el cambio, transportan más datos confidenciales y están abiertas a más usuarios. No es de extrañar que las organizaciones hayan creado muchos más canales de API que interfaces de aplicaciones web. Y el riesgo se complica a medida que estas API que proliferan se integran con volúmenes cada vez mayores de datos empresariales básicos y lógica empresarial.

Dada la prevalencia de las API en las innumerables tecnologías que los equipos de seguridad ya protegen (es decir, las aplicaciones), la mayoría de las categorías de productos de seguridad son compatibles con las API de alguna manera. Sin embargo, las API y las aplicaciones no son lo mismo; incluso aparecen como activos diferentes en algunos marcos de cumplimiento. No basta con añadir capacidades puntuales de protección de amenazas a API a, por ejemplo, un producto de seguridad de aplicaciones existente. Las API merecen más atención de la que suelen recibir en la mayoría de las organizaciones. Los equipos de seguridad de hoy en día deben ver las API como una clase de activos independiente con un conjunto distinto de atributos de riesgo y buscar capacidades esenciales para ver y proteger cada API a escala.

En el pasado, si una organización tenía un inventario de API y algunas herramientas básicas para su gestión y protección, tenían muchas posibilidades de prevenir una serie conocida de ataques de API comunes. Lamentablemente, los atacantes de hoy en día a menudo innovan igual que hacen las empresas, con un enfoque similar en la mejora continua.

- Los agentes maliciosos están haciendo todo lo posible por evolucionar sus tácticas de forma lógica para eludir las herramientas en las que saben que la mayoría de las organizaciones confían para defender las API.
- De manera similar a cómo la mayoría de las empresas utilizan la IA, los atacantes están aumentando sus limitadas capacidades humanas con la ayuda ininterrumpida de las capacidades de IA generativa.
- Cada vez más, los atacantes buscan eslabones débiles en la cadena de suministro digital conectada a las API de una empresa, como los partners B2B de una empresa que tal vez no estén priorizando la protección de estas API.

Por ejemplo, algunos tipos de abuso de API proceden de clientes y partners a los que se les han otorgado credenciales de API, pero las utilizan de formas no autorizadas. También hay maneras de piratear credenciales de API o tokens de seguridad aparentemente legítimos. Las vulnerabilidades ocultas en las implementaciones de cliente de API son otro vector de ataque que los atacantes pueden aprovechar para explotar las API de formas que las herramientas de seguridad tradicionales no son capaces de detectar.

Lo bueno es que las organizaciones ya tienen a su disposición las capacidades fundamentales a gran escala que se necesitan para proteger las API de métodos de ataque en rápida evolución. Siga leyendo para obtener más información sobre 11 capacidades clave con las que su equipo puede empezar a tomar medidas para proteger sus API (y los datos que intercambian) de los ataques.

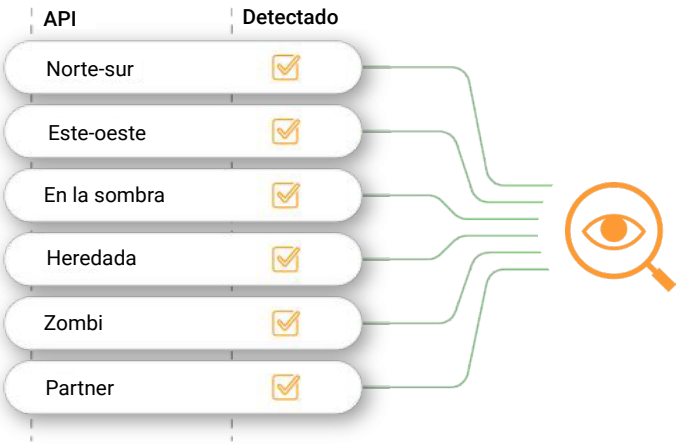
Capacidad crítica n.º 1
Gestión de la estrategia y detección continua de API

Un inventario completo y continuamente actualizado de las API en uso en toda la organización es la base esencial de cualquier estrategia de seguridad de API. Esto se debe a la sencilla razón de que una organización no puede proteger lo que no sabe que tiene en su entorno. Muchos productos de seguridad de API afirman contar con cierto nivel de detección de API, pero su funcionamiento se limita a una vez al día o a petición. Es importante asegurarse de que las capacidades de detección de API de la plataforma incluyan:

- detección automatizada y continua de API en todo momento, incluida la detección de API que solo se utilizan una vez (la detección una vez al día o a petición no es suficiente);
- detección de las API de diferentes tecnologías e infraestructuras;
- detección de API recién implementadas y comparación con el conjunto de API bien documentadas para identificar las API en la sombra;
- puntuación de riesgos de cada servicio de API y terminal, lo que ayuda a los equipos de seguridad y desarrollo a ir al grano y a priorizar las API con el mayor impacto potencial si se ven comprometidas;
- detección de instancias de vulnerabilidades conocidas de API, como las que se describen en la lista de los 10 principales riesgos de seguridad de API según OWASP.

Mejora de la visibilidad

No pierda nunca de vista su inventario de API



Capacidad crítica n.º 2
Visualización del comportamiento de las API

La capacidad de visualizar el comportamiento real de las API (llamadas a las API) es fundamental para las plataformas de seguridad de API. Esta capacidad es necesaria para que las partes interesadas clave de seguridad, desarrollo y operaciones puedan ver y comprender cómo se están utilizando las API o si se está abusando de ellas, de modo que puedan comunicarse con los equipos e investigar los casos. Las funciones de visualización específicas que deben tener son:

- **Investigación:** cualquier alerta debe ofrecer la capacidad de inspeccionar la actividad original de la API, llamada por llamada, para identificar qué elemento específico ha activado la alerta.
- **Fidelidad y enriquecimiento de datos:** respecto a cada llamada a la API, debe ser posible identificar qué usuario la ha realizado, qué operación ha utilizado, a qué registros ha accedido o cuáles ha manipulado, qué encabezados y parámetros se han utilizado, etc.
- **Privacidad de datos:** aunque la fidelidad de los datos es importante, los datos confidenciales no se pueden almacenar en reposo. Una solución debe analizar el tráfico y enviar únicamente los metadatos relevantes para actualizar los paneles de control.

Capacidad crítica n.º 3

Detección de los intentos de abuso de las API a través del contexto en las entidades de usuario

Los equipos de seguridad necesitan contar con la capacidad de realizar un seguimiento de la actividad maliciosa en entidades como las direcciones IP y las entidades de procesos empresariales como los ID de pago. Esto puede ser extremadamente valioso cuando se combina con capacidades para correlacionar ataques de diferentes IP en instancias en las que otros identificadores relevantes pueden ofrecer contexto para el abuso de las API.

Supongamos que un usuario desconocido llama a la API de una empresa de retail con /api/getpaymentID/50 como su ID. En este escenario, el equipo de seguridad del retailer sabe que todos los demás usuarios de la plataforma de la empresa están vinculados a un tipo de ID de pago. Si un analista de seguridad ve que, de repente, el usuario desconocido está realizando llamadas repetidas, ajustando moderadamente cada vez el número de ID (/api/getPaymentID/51 … 52 … 53 … 54), este es un indicador clave de intento de abuso de API.

Disponer de información en tiempo real sobre el comportamiento atípico de los usuarios puede marcar la diferencia entre un intento de filtración frustrado y un ataque de API victorioso.

943 162 $

El coste promedio para corregir incidentes de seguridad de API, según los directores de seguridad de la información (CISO), los directores de TI (CIO) y los directores de tecnología (CTO) residentes en EE. UU. que informaron haber experimentado eventos de este tipo en los últimos 12 meses.

Obtenga más información sobre las opiniones y experiencias de las empresas de su sector en el Estudio sobre el impacto de la seguridad de API de 2024.

Capacidad crítica n.º 4
Análisis y detección de comportamiento

Si bien el análisis de las llamadas de API individuales de las entidades de usuario, o incluso de las sesiones individuales, puede ayudar a los equipos de seguridad, es importante contar con una detección completa de amenazas de API centrada en el panorama general. Busque capacidades que le permitan obtener una comprensión profunda de los patrones y las anomalías de comportamiento en toda la infraestructura de API. Para determinar si el comportamiento de una API es anómalo, lo que indicaría que podría haberse vulnerado, se debe analizar el uso de la API durante periodos de tiempo más largos y en el marco de un contexto base creado mediante un seguimiento exhaustivo del comportamiento durante periodos de tiempo prolongados. Esto proporciona a los equipos de seguridad una referencia básica fiable cuando supervisan continuamente el comportamiento para detectar anomalías.

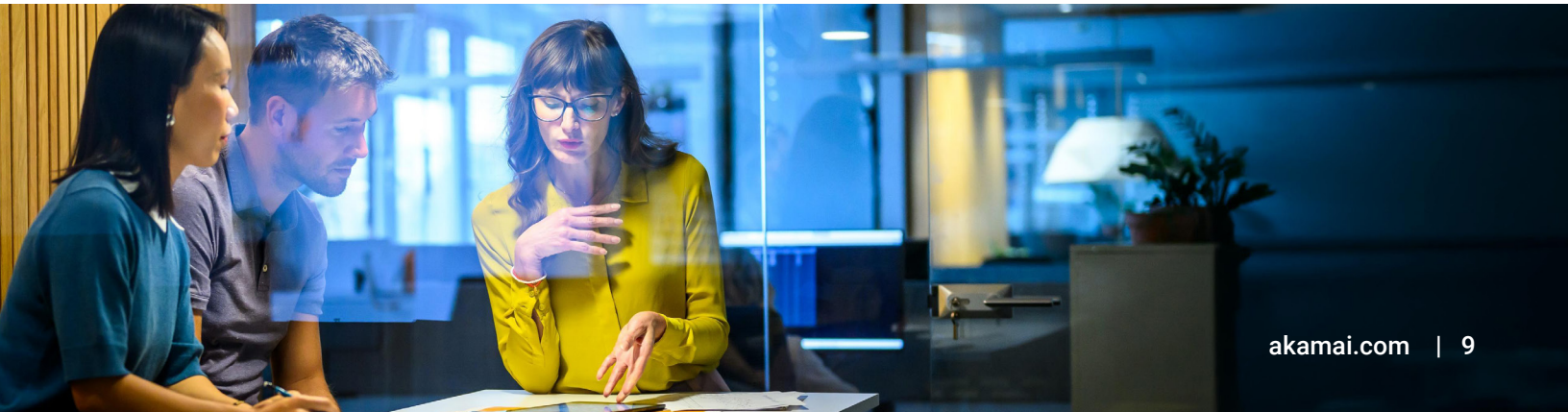
Capacidad crítica n.º 5
Detección de desviaciones de las especificaciones de API

Las API están en constante cambio debido a la naturaleza cambiante de la demanda del mercado y los requisitos empresariales. Como resultado, las organizaciones lanzan continuamente nuevas implementaciones de terminales para satisfacer las necesidades empresariales en rápida evolución, corregir errores e introducir mejoras técnicas. La actualización de la documentación de las API en sincronía con estos cambios, en función de las especificaciones de API, es fundamental, y se debe prestar especial atención a garantizar que el tráfico de las API siempre esté en consonancia con sus especificaciones.

Para hacer que las API sean resistentes contra el abuso y los ataques, las organizaciones deben buscar funciones capaces de detectar posibles desviaciones con respecto a las especificaciones de las API. Esto ayuda a las empresas a detectar cualquier discrepancia o brecha en la documentación de las API mediante la comparación continua del tráfico de API en tiempo real con las especificaciones definidas.

Si la función detecta cualquier discrepancia o acceso no documentado a los terminales en la fase de producción, puede alertar a los desarrolladores y a los equipos de seguridad, lo que les permite:

- anticiparse a los problemas antes de que se conviertan en graves;
- asegurarse de que las API funcionan como se espera;
- reforzar la seguridad de las aplicaciones que funcionan con estas API;
- mantener la integridad del ecosistema de API de la empresa.



Capacidad crítica n.º 6
Seguridad de API B2B y este-oeste

El área en la que más aumenta el uso de API son los casos de uso B2B, tanto internos como externos. La seguridad debe abarcar las API B2B de máquina a máquina, incluidas las instancias norte-sur (orientadas al exterior) y este-oeste (orientadas al interior).

Aunque las plataformas WAAP y WAF ofrecen protección a las aplicaciones web B2C, algunos de los tipos más sensibles de actividad de API, como la de las API este-oeste internas o la funcionalidad de aplicaciones de propiedad expuestas a los partners a través de API B2B, pueden estar en peligro incluso al pasar por WAAP.

A menudo, una vez que un usuario se autentica en una API de partner B2B, se supone que es seguro y no se aplica ningún otro método de supervisión. Esto constituye una carencia crítica de la estrategia de seguridad de API de muchas organizaciones. Para proporcionar una imagen completa de la actividad de las API y del panorama de amenazas general, las organizaciones deben aplicar un enfoque que proporcione visibilidad, capacidad de observación y supervisión eficaces de todos los casos de uso.

Capacidad crítica n.º 7
Alertas útiles con contexto

Una vez que una organización tiene visibilidad de toda la actividad de sus API y análisis de comportamiento a gran escala, las alertas sobre la actividad de las API son mucho más útiles. Pero ¿cómo puede asegurarse de que está centrando la atención y los recursos en las verdaderas amenazas de API? Un motor de confianza para los ataques puede utilizar algoritmos avanzados de aprendizaje automático entrenados para evaluar señales externas e internas, incluido el comportamiento de las API, patrones de tráfico de red, datos de geolocalización, fuentes de inteligencia sobre amenazas y otros factores contextuales, para determinar el nivel de confianza en que un incidente durante el tiempo de ejecución detectado es el resultado de una actividad maliciosa. Esta capacidad puede ayudar a un equipo de seguridad a centrarse rápidamente en las amenazas críticas y debe complementarse con funciones que crean flujos automáticos de corrección y notificación para ataques de alta probabilidad.

Capacidad crítica n.º 8
Respuestas personalizadas y automatizadas

Los enfoques tradicionales de API en línea pueden automatizar acciones para bloquear posibles ataques contra las API, con la salvedad de que las organizaciones deben ser capaces de identificar el ataque. Dado que el análisis de comportamiento y la detección de anomalías de las API se realizan a lo largo del tiempo con un contexto empresarial mucho mayor, la profundidad de la detección permite identificar anomalías. Esto posibilita una amplia gama de respuestas automatizadas y personalizadas, que se pueden aplicar con gran precisión. Veamos algunos ejemplos:

- Bloquear o limitar el tráfico en las puertas de enlace de API y los filtros en el Edge de la red de distribución de contenido (CDN) compatibles.
- Enviar notificaciones por correo electrónico a las partes interesadas de la empresa y el departamento de seguridad.
- Crear incidencias para desarrolladores.
- Activar webhooks.

¿Qué pueden hacer las organizaciones para ayudar a sus desbordados equipos de seguridad a maximizar su capacidad a medida que aumentan las amenazas de API? Busque funciones de automatización que mejoren la eficiencia y la productividad simplificando la creación y gestión de flujos de trabajo multitarea. Las funciones de automatización deben ofrecer una interfaz de diseñador visual sin código capaz de crear procesos de respuesta a eventos complejos y sincronizar datos relacionados con incidentes entre las soluciones de seguridad de API principales e innumerables servicios de terceros, incluidos ServiceNow, Jira y Azure DevOps.

Capacidad crítica n.º 9
Análisis del tráfico de API

Las organizaciones necesitan capacidades siempre activas para registrar, visualizar y analizar el tráfico de API en sus entornos sin implementar un lago de datos. Al registrar flujos de datos de API que coincidan con criterios específicos en los entornos de aplicaciones, incluida la actividad típica y anómala de las API, las organizaciones pueden detectar las amenazas de forma más eficaz y gestionar al mismo tiempo la exposición al riesgo de usuarios sospechosos y comportamientos inusuales de las API. Es importante contar con funciones de auditoría de tráfico de API que se puedan personalizar para un caso de uso concreto y que permitan a las organizaciones capturar y retener el tráfico de acuerdo con filtros y reglas predeterminados.

Capacidad crítica n.º 10
Pruebas de API rigurosas y en tiempo real

Debido a las prisas por innovar, las organizaciones envían las API a la fase de producción con vulnerabilidades y defectos de diseño que a menudo pasan desapercibidos. Las organizaciones pueden evitar estos problemas adoptando un enfoque "shift-left" para las pruebas de API en la fase de desarrollo. Entre las capacidades principales se incluyen las siguientes:

- ejecución de pruebas automatizadas que simulan tráfico malicioso, incluidos los tipos que se indican en la lista de los 10 principales riesgos de seguridad de API según OWASP;
- análisis de las especificaciones de las API con respecto a las políticas y normativas de gobernanza establecidas;
- pruebas de las API bajo demanda o como parte de un proceso de integración e implementación continuas (CI/CD).

Capacidad crítica n.º 11
Protección independiente de la plataforma

Por lo general, los servicios de API los implementan diferentes grupos de una organización, que suelen utilizar un conjunto diverso de plataformas y tecnologías. Por ejemplo, algunas API se implementan localmente, mientras que otras se ejecutan en la nube pública. A menudo, las organizaciones utilizan tecnologías intermedias, como proxies inversos, puertas de enlace de API, WAF y CDN, lo que ofrece valor empresarial, pero genera complejidad respecto a la visibilidad de las API.

La capacidad de acceder a los datos de actividad de API de cada una de estas tecnologías es imprescindible. Un enfoque de protección frente a las amenazas contra las API que no dependa de la plataforma garantiza que su organización siempre tenga una visión completa de toda la actividad de las API, independientemente de las particularidades de implementación o de la infraestructura en uso. Esto ofrecerá:

- protección para todos los departamentos, empresas adquiridas y entornos;
- protección tanto para las API autorizadas como las que se usen en la sombra, tanto si utilizan la puerta de enlace de API como si no.

Un enfoque de protección que no dependa de la plataforma también ampliará la visibilidad más allá de las API que manejan tráfico norte-sur, incluidas las API públicas, las de partners y las internas que manejan tráfico este-oeste.

Garantizar que la visibilidad de su plataforma de protección contra amenazas de API sea lo más amplia posible protegerá su organización contra las amenazas internas y el abuso de API por parte de organizaciones de partners, así como contra los riesgos de atacantes externos.

Conclusión

Las API son un componente clave de la capacidad de las organizaciones para prestar servicio a los clientes, generar ingresos y trabajar de forma eficiente en la economía actual cada vez más digital y centrada en la nube. Sin embargo, su crecimiento continuo, su proximidad a los datos confidenciales y la falta de controles de seguridad las convierte en una fuente de riesgos.

Akamai API Security proporciona las 11 capacidades esenciales que se describen en este white paper, y ayuda a las organizaciones a desarrollar sus enfoques actuales con capacidades esenciales, como las siguientes:

- Detección de API
- Evaluación de riesgos (incluida la exposición a datos confidenciales)
- Detección de abuso y ataques de API
- Pruebas de API para detectar riesgos y vulnerabilidades de seguridad

Obtenga más información sobre cómo protegerse frente a los 10 principales riesgos de seguridad de API según OWASP.

Descubra cómo podemos ayudarle con esta demostración de Akamai API Security personalizada.

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Gracias a la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, anteriormente conocido como Twitter, y en LinkedIn. Publicado en enero de 2025.