Segmentación basada en software

Un enfoque desde dentro para lograr una seguridad absoluta

TABLA DE CONTENIDO

Superación de los firewalls heredados	03
Solucionado: 3 problemas de los firewalls heredados	04
4 aspectos básicos de la segmentación	09
Mito frente a realidad: 5 mitos sobre la segmentación desmontados	10
Reducción del riesgo en el interior	11
Lista de comprobación Zero Trust: 6 maneras de obtener control explícito	13
Conclusión	14

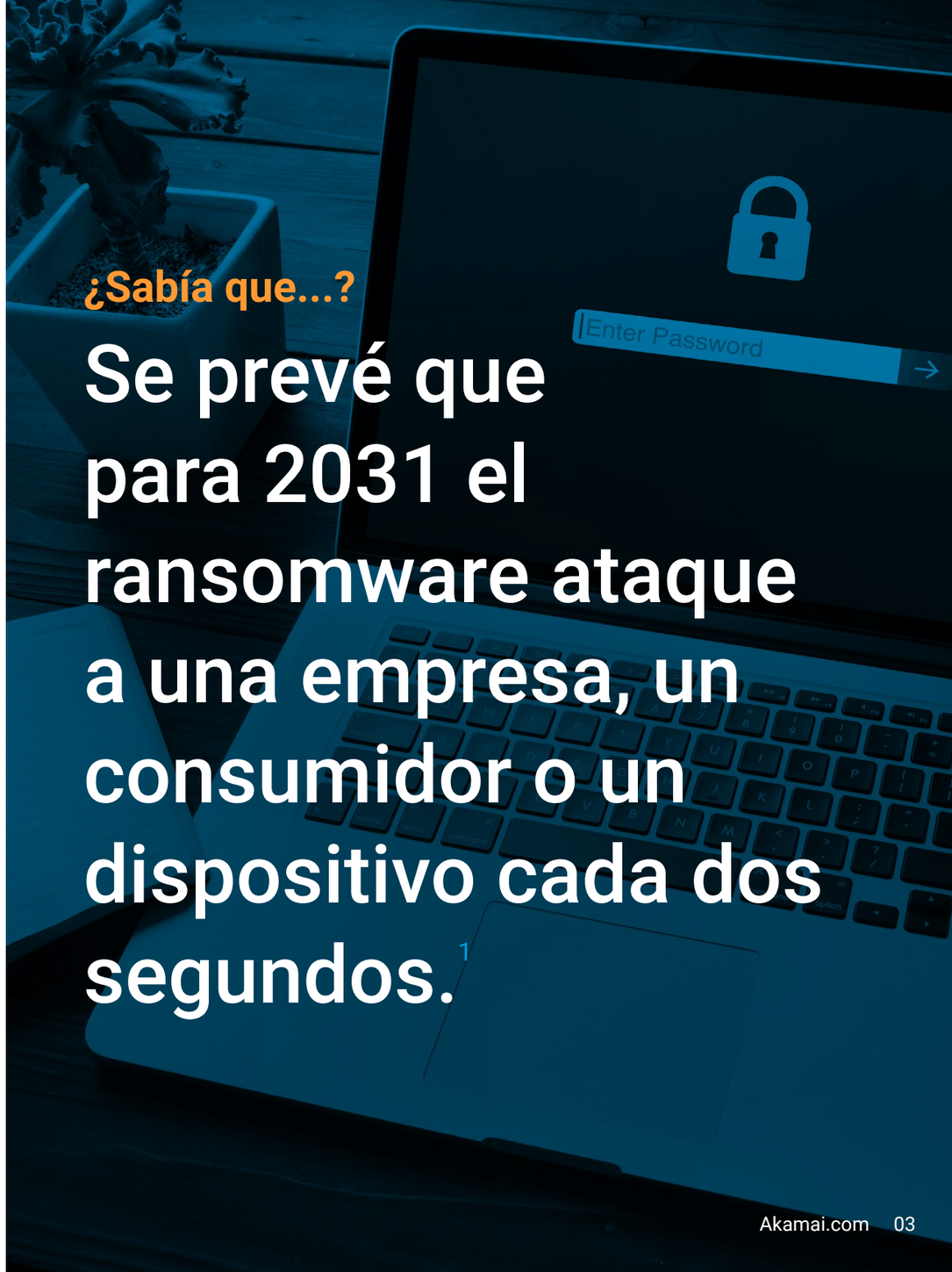
Superación de los firewalls heredados

Ya sabemos que está cansado de sus firewalls antiguos en las instalaciones. Los entornos de TI y los requisitos de seguridad han evolucionado tanto que, en la actualidad, se encuentran a años luz del propósito inicial para el que se habían diseñado. Además, el panorama de la ciberseguridad también ha cambiado: los métodos de ataque son más sofisticados y los ciberdelincuentes son más numerosos. Una arquitectura basada en dispositivos, con décadas de antigüedad, es sencillamente incapaz de hacer frente a las técnicas de ataque más recientes, como los malware, los ataques de botnet, los esquemas de phishing, la ingeniería social o la extorsión en torno a los datos.

Sin embargo, a pesar del sinfín de problemas que presentan —son caros, no ofrecen movilidad y carecen de visibilidad, entre otros muchos— la realidad es que los firewalls heredados no van a desaparecer a corto plazo. Esto se debe a que ejercen una función importante en el perímetro al gestionar el tráfico norte-sur y actuar a modo de coraza para toda la organización.

Sin embargo, los firewalls no pueden gestionar el tráfico este-oeste en los centros de datos in situ y en la nube.

La segmentación basada en software es perfecta para esa tarea.



¿Sabía que...?

Se prevé que para 2031 el ransomware ataque a una empresa, un consumidor o un dispositivo cada dos segundos.[1]

Solucionado:

3 problemas de los firewalls heredados

1. El problema: **Falta de visibilidad**

   La falta de visibilidad sobre el flujo de datos dificulta la implementación y el mantenimiento de las reglas. Debido a esto, los firewalls suelen tener conjuntos de reglas muy largos y muchas de esas reglas son demasiado laxas, o incluso innecesarias.

La solución

Busque soluciones que integren un mapa visual, la clasificación de activos y la asignación de dependencias de aplicaciones con la creación y la gestión de políticas.

Solucionado:

3 problemas de los firewalls heredados

2. El problema: Los firewalls son difíciles de mantener

Los propietarios de aplicaciones y los administradores de firewall no suelen conocer los protocolos y puertos IP que son necesarios para las comunicaciones. Esto hace que la administración de firewalls se convierta en un proceso de solución de problemas repetitivo.

La solución

En lugar de utilizar los componentes de la red fija, como las IP y los puertos, como punto de partida para diseñar las políticas, trate de diseñarlas basándose en atributos importantes, como el proceso que utiliza una aplicación, los nombres de dominio completos (FQDN) y la identidad de usuario. De esta manera, los atributos siguen siendo los mismos y las políticas seguirán funcionando, incluso si introduce un cambio en su centro de datos o mueve su carga de trabajo a la nube.

Solucionado:

3 problemas de los firewalls heredados

3. El problema: Los firewalls carecen de agilidad

Cualquier cambio que desee hacer en un firewall normalmente requiere tiempo de inactividad programado. Cuando el propietario de una aplicación necesita realizar un cambio, puede tener que esperar una semana o más a que el cambio se revise e implemente durante un periodo de mantenimiento.

La solución

Los departamentos de TI modernos han abandonado los modelos en que los cambios tienen lugar en períodos de mantenimiento programados y han empezado a utilizar modelos de DevOps que permiten introducir aplicaciones y actualizarlas continuamente. Busque una solución tecnológica que pueda automatizarse con las mismas herramientas de DevOps que ya utiliza para las aplicaciones. De esta forma, a medida que las aplicaciones evolucionan, el enfoque de seguridad se adapta a estos cambios.

Puede llevarla donde quiera

Hablemos sobre la forma tradicional de hacer las cosas: es compleja y no se adapta a los cambios. El enfoque tradicional para administrar firewalls heredados se basa en la segmentación de la ubicación, algo que no se puede cambiar con facilidad. Normalmente, se basa en una dirección IP integrada como código fuente o dirigida a un centro de datos. Esto significa que, para proteger un elemento tras el firewall, debe moverlo físicamente, lo que implica un proceso lento, arriesgado y que requiere muchos recursos. ¿Migración a la nube? ¿Visibilidad? ¿Seguridad adecuada? Olvídese de todo esto.

Deje los firewalls heredados donde están. Respire profundamente y abra la puerta a nuevas tecnologías. La segmentación basada en software es adaptable y se puede implementar junto a los firewalls existentes con facilidad. También le permite hacer cambios en su entorno, centro de datos y red, así como establecer políticas en función de lo que vea. La carga de trabajo y las políticas pueden aplicarse en cualquier entorno, ya sea la nube, el centro de datos u otra ubicación. Además, puede aplicar y adaptar su política de seguridad sin realizar cambios en la red y sin tiempo de inactividad del sistema.

Identifique los segmentos internos

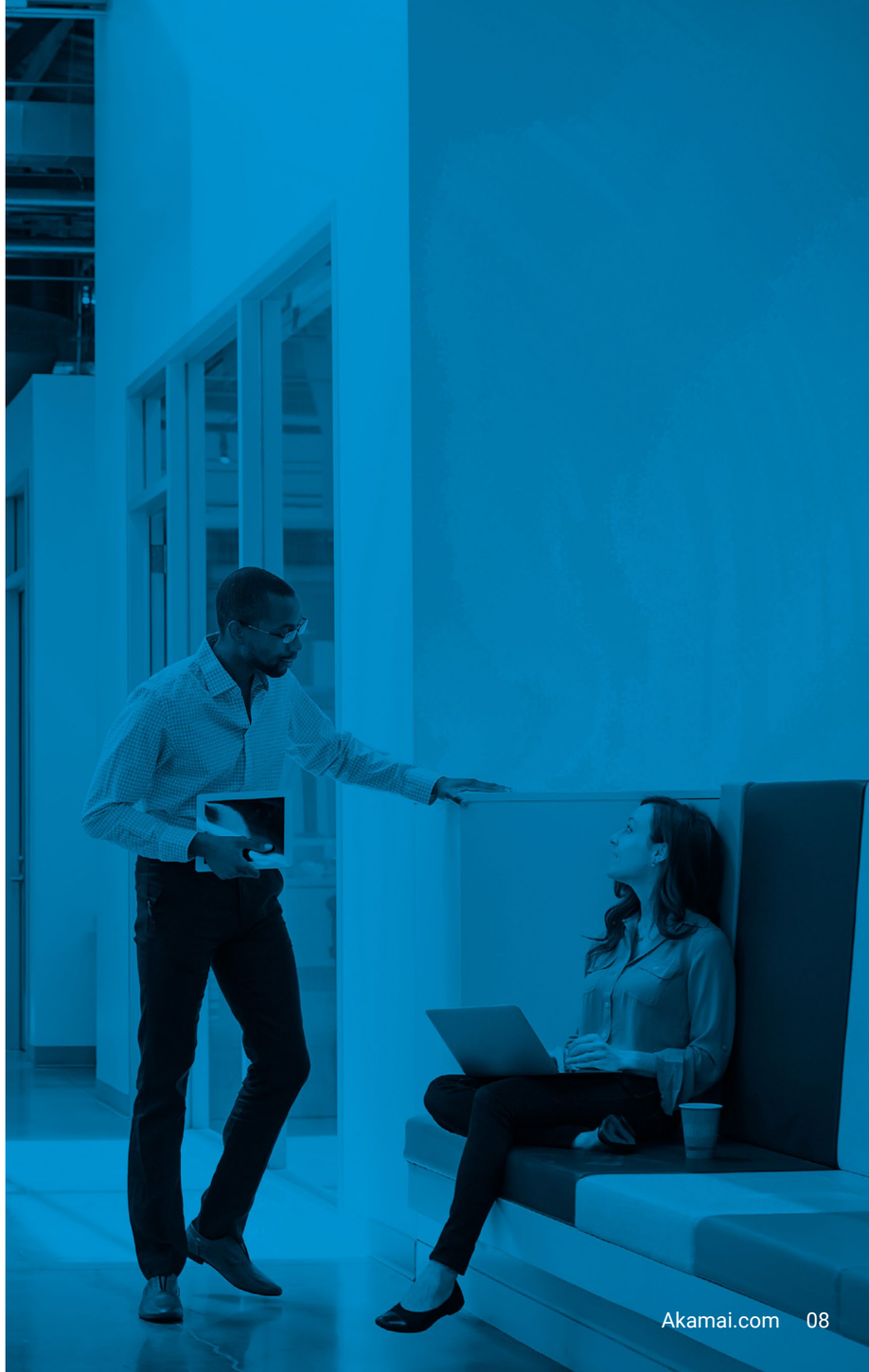
¿Confiaría en algo que no puede ver? Suponemos que no. Sin embargo, es precisamente eso lo que está haciendo cuando establece políticas de seguridad detrás de un firewall, ya que no puede ver lo que hay detrás de él. Es como mirar un edificio, pero sin poder ver a la gente que hay dentro.

La segmentación basada en software no deja nada al azar. Divide las piezas para que sea consciente de toda la actividad en la que están involucradas sus cargas de trabajo. Una vez que sabe lo que hay dentro de su entorno, puede diseñar un plan y estructurar los segmentos de forma que tenga sentido y sea eficaz en función de sus casos de uso específicos.

Obtenga seguridad más allá del perímetro

Los firewalls heredados no se diseñaron para el cambio. Aunque cumplen una función importante en el perímetro, como la protección contra DDoS y el filtrado y la inspección del tráfico, es difícil garantizar la seguridad dentro de la red con este tipo de protección. ¿Por qué sucede esto? Los firewalls se implementaron como puntos de estrangulamiento naturales, así que cada intento de segmentación trae consigo obstáculos operativos, como la necesidad de cambiar y eliminar redes y aplicaciones. Este es un proceso tedioso y que requiere un uso intensivo de recursos.

La segmentación basada en software puede ayudarle a superar estos desafíos operacionales y le permite desarrollar sus prácticas de seguridad más allá de los terminales y el perímetro. En primer lugar, cuenta con un enfoque de firewall distribuido (en vez de utilizar puntos de estrangulamiento). En segundo lugar, gira en torno a la carga de trabajo, lo que le permite recopilar datos del sistema host y utilizarlos después para clasificar los activos y utilizar un enfoque más detallado para las reglas, como políticas y contenido a nivel de proceso. En general, la segmentación basada en software es una forma más adaptable y precisa de proteger los activos esenciales dentro de la red y requiere menos esfuerzo y recursos que los firewalls.



4 aspectos básicos de la segmentación

La segmentación es más importante que nunca. Las superficies de ataque son más amplias. Existen ataques sofisticados, como el ransomware, que se mueven lateralmente después de una filtración. Por ello, debe pensar en las dependencias de las aplicaciones más allá del perímetro. Sin embargo, la segmentación no tiene un único enfoque.

A continuación, se describen cuatro tipos comunes de segmentación.

1. Segmentación de entorno

Separa los sistemas en diferentes entornos de desarrollo, como desarrollo, control de calidad (QA), staging y producción. Esta es una versión general de la segmentación cuyo objetivo final es separar los sistemas en diferentes entornos para garantizar que el acceso se limita solo a las aplicaciones y a los usuarios necesarios. Muchas iniciativas de cumplimiento normativo exigen la garantía de que los sistemas ajenos a la producción no puedan acceder a los sistemas de producción.

2. Segmentación de red

Es una práctica de arquitectura que consiste en dividir una red en varias subredes, cada una de las cuales es a su vez un segmento de red más pequeño. La segmentación de la red proporciona a los operadores de TI una herramienta para controlar mejor el tráfico de la red, impulsar el rendimiento y mejorar la seguridad.

3. Microsegmentación

Es una forma de segmentación más precisa que se utiliza para aislar las cargas de trabajo entre sí y protegerlas de forma individual. Esto incluye la capacidad de establecer reglas de segmentación para elementos como procesos, contenedores, usuarios, nombres de dominio y dispositivos. Este enfoque es excelente para controlar el tráfico este-oeste y protegerse del movimiento lateral.

4. Segmentación basada en identidades

Va un paso más allá de la capacidad de la microsegmentación para proteger un único terminal, dispositivo, carga de trabajo o contenedor y posibilita la creación de reglas dinámicas que evalúan la identidad (puede ser el usuario, el dispositivo o el contexto) para determinar si autorizar o no la comunicación. Las políticas de segmentación basadas en identidades además de establecerse en función de la IP o el puerto pueden utilizar ajustes más específicos como las etiquetas, el tipo de sistema operativo o las características de la aplicación.

Mito frente a realidad: 5 mitos sobre la segmentación desmontados

Mito 1

Los proyectos de segmentación son excesivamente complejos y duran demasiado tiempo.

Realidad: Tener visibilidad y una comprensión clara de lo que sucede dentro de su entorno reduce el tiempo necesario para completar un proyecto de segmentación, que pasará de meses a semanas o incluso días. Las tecnologías de segmentación modernas también pueden utilizar inteligencia artificial (IA) para acelerar aún más el proceso.

Mito 2

Los proyectos de segmentación requieren cambios en la infraestructura de la red y provocan tiempo de inactividad.

Realidad: La segmentación basada en software separa la seguridad de la infraestructura, por lo que la segmentación puede llevarse a cabo de manera independiente sin que ello conlleve tiempo de inactividad o cambios en la infraestructura subyacente.

Mito 3

La segmentación bloquea el tráfico legítimo en mi red.

Realidad: Visualizar su entorno y utilizar políticas de segmentación basada en software le permiten ver el efecto que estas políticas tendrán en sus actividades empresariales antes de activar la adopción en tiempo real.

Mito 4

La segmentación obstaculiza el acceso del usuario y provoca latencia innecesaria.

Realidad: Al usar políticas distribuidas de segmentación basada en software, en lugar de puntos de estrangulamiento específicos por los que debe pasar todo el tráfico, se elimina la aparición de cuellos de botella en la red. Además, las políticas más precisas, con reconocimiento de aplicaciones e identidades, reducen el riesgo de que haya problemas accidentales de acceso del usuario.

Mito 5

No puedo utilizar las mismas herramientas de segmentación en la nube y en los entornos locales.

Realidad: Si separa las políticas de segmentación de la infraestructura, las políticas que utilice en el centro de datos también pueden funcionar en la nube.

Akamai

Reducción del riesgo en el interior

Las filtraciones son inevitables. Además, pueden paralizar su negocio, poner en riesgo sus datos, dañar la imagen de su marca y provocarle pérdidas millonarias.

¿Todavía piensa que los firewalls son suficiente? Piénselo otra vez. Cuando un ciberdelincuente consigue acceder a una red, un entorno o un centro de datos, utiliza el movimiento lateral para robar datos y causar estragos, como hacerse con el control de servidores de aplicaciones o acceder a servidores de bases de datos.

De hecho, en la actualidad, el 70 % de todos los ataques incluye algún tipo de movimiento lateral.[2]

Los firewalls consideran que el movimiento lateral es tráfico legítimo dentro de una red, mientras que la segmentación basada en software detiene su avance en seco. Por ello, la segmentación basada en software debe ser un componente fundamental de su programa de seguridad, ya que le permite restringir el movimiento lateral y, en caso de una filtración, obstaculizar el movimiento del ciberdelincuente por el entorno. De este modo, tiene margen de respuesta para proteger los datos y las aplicaciones esenciales, disminuir el tiempo de permanencia e incluso detectar al atacante. Este enfoque es más escalable y sencillo de usar, y le permite implementar rápidamente la segmentación sin hacer cambios en la red o los sistemas.

La seguridad Zero Trust no tiene por qué ser compleja

El enfoque Zero Trust se centra en saber quién hace qué a quién y cómo lo hace. Es decir, tener un control explícito sobre los actores y sus acciones dentro de la red.

Al otorgar a un usuario acceso a cualquier ubicación dentro de la red, automáticamente otorga demasiada confianza y pone en peligro a toda su organización. Tenga en cuenta que los empleados cometen errores con frecuencia, lo que podría tener graves consecuencias de seguridad. Algunos incluso tienen intenciones maliciosas.

Además, más allá de las redes y dispositivos VPN, existen muchos puntos de entrada al centro de datos que debe tener en cuenta. Por ejemplo, los atacantes pueden acceder a una red a través del servidor de producción (como ocurrió en la filtración de SolarWinds), una aplicación orientada a Internet vulnerable o una VPN vulnerable. En ese caso, confía en un servidor solo porque está dentro de la red, pero, en la práctica, el atacante puede acceder a cualquier sitio y moverse lateralmente sin restricciones.

Para implantar un enfoque Zero Trust en su red de producción, debe bloquear toda actividad que no esté permitida explícitamente.

Esto es algo que los firewalls heredados no pueden hacer de forma precisa porque es necesario identificar atributos a un nivel más profundo que los puertos y las direcciones IP.

Por su parte, la segmentación basada en software le permite ver lo que sucede en detalle y crear políticas precisas y comprensibles para el usuario, que incluyen la identidad.

Lista de comprobación Zero Trust: 6 maneras de obtener control explícito

Simplifiquemos la idea. La confianza se basa en el tamaño del segmento: cuanto más pequeño sea el segmento, más protegidos estarán los datos, los activos y las aplicaciones fundamentales. A continuación, le mostramos los seis pasos que debe seguir para adoptar un enfoque Zero Trust sin complejidad operativa.

1 Identifique sus datos confidenciales con etiquetas de visualización.

2 Asigne los flujos de los datos confidenciales con ayuda de mapas de flujo y dependencias automatizados.

3 Diseñe microperímetros Zero Trust con las herramientas adecuadas para definir rápidamente cualquier política de segmentación o microsegmentación.

4 Supervise constantemente el ecosistema Zero Trust gracias a la supervisión y los análisis en tiempo real.

5 Adopte la automatización y la orquestación de la seguridad con las API y las integraciones tecnológicas.

6 Disponga de capacidades para retirar la confianza a algo o alguien para que, si se produce un ataque, pueda retirar fácilmente la confianza a cualquier máquina con atributos preestablecidos, independientemente del usuario o el segmento.

Conclusión

Llegado a este punto, probablemente se esté preguntando cómo puede dejar atrás sus soluciones tradicionales para reforzar su estrategia de seguridad dentro de la red.

No se preocupe.

Deje los firewalls heredados donde están; cumplen su función protegiendo el perímetro de la red, aunque no aporten mucho más.

Lo más importante es lo que reside en el centro de su organización: los activos digitales, los datos y las aplicaciones que se encuentran más allá del perímetro y vertebran su infraestructura corporativa. Adoptar un enfoque desde dentro, implementar la segmentación basada en software y construir un marco Zero Trust le ofrecerán la visibilidad y el control que necesita para detectar y detener el movimiento lateral, aplicar políticas precisas y adaptables y evitar que los ciberataques como el ransomware se propaguen por la red.

Solicite una demostración u **obtenga más información** sobre cómo la segmentación puede ayudar con el ransomware, el enfoque Zero Trust, la seguridad en la nube y mucho más.

1 Cybersecurity Ventures. 2022 Who's Who In Ransomware Report. Conceal, 2022.

2 Tom Kellerman y Greg Foss. Global Incident Response Threat Report. VMware Carbon Black, octubre de 2020.

3 "2023 Cyber Security Statistics Trends & Data". PurpleSec, 22 de febrero de 2023.

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. 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 Twitter y LinkedIn. Publicado el 23 de junio