Akamai

WHITE PAPER

# Protección de las cargas de trabajo en AWS con una segmentación exhaustiva: seguridad más sencilla y rápida

# Introducción

## No deje que las preocupaciones sobre la seguridad impidan la adopción de la nube. Una única solución puede gestionar la visibilidad, la prevención del movimiento lateral y la detección y respuesta a filtraciones de activos y recursos en AWS.

Las ventajas de utilizar recursos de plataforma como servicio (PaaS) en Amazon Web Services (AWS) y migrar cargas de trabajo esenciales fuera de las instalaciones son evidentes: permite eliminar los costes de infraestructura y el mantenimiento, mejorar la escalabilidad y la elasticidad con recursos y potencia casi ilimitados, y utilizar las últimas innovaciones, como el aprendizaje automático y la IA, para mejorar el rendimiento y los análisis. Sin embargo, los problemas de seguridad están frenando a muchas empresas, especialmente porque los recursos en la nube son algunos de los principales objetivos de los ciberataques.

# El desafío de la seguridad en AWS

Cuando se trata de un entorno completamente nuevo, no es de extrañar que tenga que volver a replantearse la seguridad desde cero. Puede que sea un usuario nuevo que no esté familiarizado con la nube o que esté realizando una migración desde un proveedor diferente, que haya elegido una nueva solución híbrida o que quiera añadir AWS a su ecosistema existente. En cualquier caso, la nube requiere su propio conjunto de herramientas específicas para gestionar los desafíos únicos que presenta esta infraestructura. Algunos factores son comunes para todos los proveedores de nube, mientras que otros serán exclusivos de Microsoft Azure, Google Cloud Platform o AWS. A continuación, se muestran algunas de las principales preocupaciones de las empresas que utilizan la nube o la nube híbrida con tecnología de AWS.

**Comprensión de la responsabilidad compartida:** al trasladar sus cargas de trabajo a AWS o al aprovechar sus recursos de PaaS integrados, debe reconocer que todavía tiene una gran responsabilidad. Tendrá que proteger los datos, las aplicaciones y las plataformas de los clientes. La falta de comprensión del modelo de responsabilidad compartida es la razón por la que Gartner predice que el 99 % de los fallos de seguridad en la nube serán culpa del cliente en 2025.

**Falta de visibilidad:** no puede controlar lo que no puede ver. En la nube, la visibilidad es mucho más complicada, especialmente cuando se trata de proteger y visualizar el tráfico de red que se mueve tanto de este a oeste como de norte a sur. No basta con examinar simplemente los flujos. Sus activos críticos pueden estar repartidos entre varias cuentas de AWS, contenedores o grupos de seguridad de red; sin contextualizar todo esto, puede que sea imposible obtener una visión precisa de los flujos e interdependencias.

**Control limitado para la creación de políticas:** si su empresa está acostumbrada a disponer de información sobre la capa 7 en el entorno local, no querrá retroceder a la visibilidad de la capa 4 simplemente: ahora que sus cargas de trabajo están en la nube, perdería esa información detallada y el control. Los grupos de seguridad de Amazon admiten el control del tráfico hasta la capa 4. Sin embargo, con la visibilidad y el control de la capa 7, independientemente de la infraestructura subyacente, puede hacer algo más que depender únicamente de puertos e IP, que son en gran medida insuficientes para la detección de filtraciones o la solución de problemas.

**Seguridad de contenedores:** AWS utiliza los grupos de seguridad de Amazon para aplicar la política de seguridad de contenedores, pero esto se limita a los clústeres en lugar de a los módulos individuales. Para obtener una visión completa de las comunicaciones, necesita una solución capaz de reconocer el contexto de una red superpuesta que se esté ejecutando y de desglosar de forma detallada hasta el nivel de módulo. Todo se vuelve más complejo cuando quiere crear políticas de red que incluyan tanto a las máquinas virtuales (VM) como a los contenedores, lo que obliga a menudo a las organizaciones a gestionar dos conjuntos de controles de seguridad.

**Adopción de PaaS:** existe una tendencia significativa hacia la adopción de recursos de PaaS además de la migración de cargas de trabajo esenciales a la nube, lo que refleja las necesidades en constante evolución de las organizaciones centradas en la nube. Sin embargo, estos recursos de PaaS no admiten agentes, por lo que la mayoría de las soluciones de seguridad basadas en agentes son demasiado limitadas para hacer llegar una protección completa a dichos recursos. Esto puede dar lugar a una política de seguridad de la nube fragmentada, lo que genera gastos adicionales para sus equipos y puede dejar brechas de seguridad que pueden ser explotadas por los atacantes.

## Aborde estos problemas con una plataforma de seguridad todo en uno

Amazon proporciona ciertas herramientas integradas, como los grupos de seguridad de Amazon, que ayudan a combatir algunos de los desafíos de la migración de su infraestructura a la nube. Animamos a las organizaciones a sacar el máximo partido a la gestión de acceso e identidades (IAM) de AWS, usando grupos para asignar los permisos, rotando las credenciales de forma periódica y utilizando los grupos de IAM para garantizar la simplicidad. Sin embargo, estas herramientas por sí solas son solo un punto de partida en la dinámica nube pública actual, especialmente si se considera un entorno híbrido que cubre cualquier cosa, desde infraestructura heredada hasta tecnología de contenedores y recursos de PaaS empleados en diferentes entornos de nube pública.

Una solución de seguridad sofisticada le permitirá complementar lo que AWS proporciona con una tecnología que elimina los puntos ciegos y que funciona a la perfección con el resto de su pila de seguridad, incluso en un entorno híbrido. Esto es lo que ofrece Akamai.

## Visibilidad completa de las instancias de AWS

Cuanto más compleja sea su infraestructura de TI, más importante será el hecho de contar con una visibilidad completa y automatizada. Los movimientos, las adiciones, los cambios y las eliminaciones manuales no solo son poco fiables y propensos a brechas y errores, sino que también suponen una ralentización y, por lo tanto, una barrera para la adopción de la nube. Por el contrario, una visibilidad mejorada y automatizada detectará todas las aplicaciones y flujos, lo que añadirá visibilidad de sus instancias hasta el nivel de proceso individual.

Akamai Guardicore Segmentation, la oferta principal de la plataforma Akamai Guardicore para Zero Trust, incluye una potente API de AWS que extrae datos de orquestación junto con un componente dedicado para recopilar información de activos, flujos y etiquetas, lo que le proporciona un contexto valioso que puede utilizar para el etiquetado y la asignación de aplicaciones. A medida que establece la referencia de su infraestructura, dispone de los detalles que necesita para comprender perfectamente cómo se comunican las aplicaciones entre sí, dónde se encuentran las interdependencias y cómo se deben crear las políticas para posibilitar una mayor fluidez y agilidad. En lugar de tener una solución de seguridad independiente para cada proveedor o entorno de nube, los usuarios pueden visualizar la información de la nube nativa y los datos específicos de AWS en el mismo panel. Nuestra solución funciona en todas las plataformas, infraestructuras y nubes, por lo que puede tener la tranquilidad de que no habrá puntos ciegos.

## Segmentación y aplicación: una política que sigue la carga de trabajo

Una vez que haya conseguido esta "vista unificada" en todos sus entornos, puede empezar a diseñar e implementar la política de seguridad. La política de aplicaciones va más allá de lo que los grupos de seguridad de Amazon pueden conseguir por sí solos, ya que proporciona un nivel de detalle de la capa 7 (en lugar de la capa 4). Aunque algunas organizaciones intentan utilizar firewalls de última generación en el entorno local para limitar el movimiento lateral, esto solo admite la segmentación generalizada del tráfico de este a oeste. Resulta increíblemente difícil como solución para los controles de segmentación detallados debido a la necesidad de realizar cambios enormes en la infraestructura y la red para redirigir el tráfico a través del firewall. Aunque fuera una opción para el entorno local, también deja a las organizaciones con el problema de mantener este nivel de control en la nube.

La microsegmentación de capa 7 es la respuesta, con políticas creadas para cargas de trabajo dinámicas, sin necesidad de cambiar en absoluto la infraestructura de red subyacente. Dado que la política se adapta a la carga de trabajo, hemos eliminado la necesidad de realizar cambios manuales y hemos mejorado la capacidad de su organización para aumentar la agilidad y adoptar los procesos de DevOps en constante cambio. Una política de microsegmentación puede simplificar un entorno híbrido mediante la aplicación de reglas en regiones, VPC, contenedores, VM y de forma local, todo ello con una expresión de política coherente. Ya solo con la visibilidad que proporcionamos, puede definir y aplicar políticas de segmentación en cuestión de minutos. El proceso de creación de políticas también mejora con recomendaciones automáticas que proporcionan los mejores protocolos de seguridad en la nube pública.

## Detección de filtraciones y respuesta a incidentes en la nube de AWS

Con Akamai, puede llevar la seguridad de AWS más allá de la segmentación o la visibilidad. La detección de infracciones de políticas es una parte importante de la detección de filtraciones, ya que le permite responder a una posible ciberamenaza en tiempo real, con detalles en el nivel de aplicaciones. Ofrecemos varios métodos de detección de filtraciones que le pueden alertar inmediatamente de actividades maliciosas en un entorno de nube híbrida.

- **Análisis de reputación:** detecte automáticamente información sospechosa en los flujos, desde nombres de dominio y direcciones IP hasta hashes de archivos y líneas de comandos.
- **Engaño dinámico:** atraiga a los atacantes sin su conocimiento, desviándolos a un entorno que sea un señuelo de gran interacción y en el que pueda aprender de forma segura del comportamiento que muestran.
- **Herramientas para acelerar la respuesta a incidentes:** integre con AWS para enviar cualquier infracción de políticas o incidente de seguridad en tiempo real al centro de seguridad de AWS.
- **Búsqueda personalizada de amenazas:** saque partido a la infraestructura y a la inteligencia global frente a amenazas de Akamai para detener las amenazas más evasivas de su entorno de nube híbrida con nuestro servicio Akamai Hunt.

# Agrupación de todas las soluciones para mejorar la seguridad en AWS (y no solo en AWS)

Aprovechar las ventajas de la nube pública no tiene por qué significar que deba conformarse con una seguridad, una visibilidad o un control menores de los que su organización disfruta en el entorno local. Con Akamai, puede obtener una visibilidad completa de sus activos y recursos de AWS y de toda su infraestructura al completo. Gracias a este mapa básico, se simplifica la creación de políticas y se mejoran las medidas de seguridad existentes para proporcionar un control detallado sin necesidad de intervención manual. Los complementos de detección de infracciones y respuesta a incidentes le ofrecen una solución de seguridad integral única que cubre todas sus bases en la nube de AWS y más.

## Visite akamai.com/guardicore para obtener más información.

**Acerca de la seguridad de Akamai**

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, antes conocido como Twitter, y LinkedIn. Publicado en noviembre de 2024.