INFORME SOBRE LA SOLUCIÓN DE AKAMAI

# Segmentación para entornos de nube híbrida

Contenga los ataques con segmentación para su infraestructura de nube

Ante la creciente migración de aplicaciones y cargas de trabajo a la nube, los equipos encargados de la seguridad y la nube se enfrentan a cada vez más retos. Uno de ellos es trasladar los principios Zero trust y la segmentación a las aplicaciones y las cargas de trabajo en la nube. Con Akamai Guardicore Segmentation, las organizaciones pueden reducir la superficie de ataque y contener los ataques a aplicaciones y cargas de trabajo en sus entornos de nube pública sin necesidad de instalar agentes. La clave para lograrlo reside en unificar en una sola vista una detección automática de las aplicaciones, una visualización completa de los flujos de nube, unas políticas de segmentación precisas y alertas de seguridad de la red.

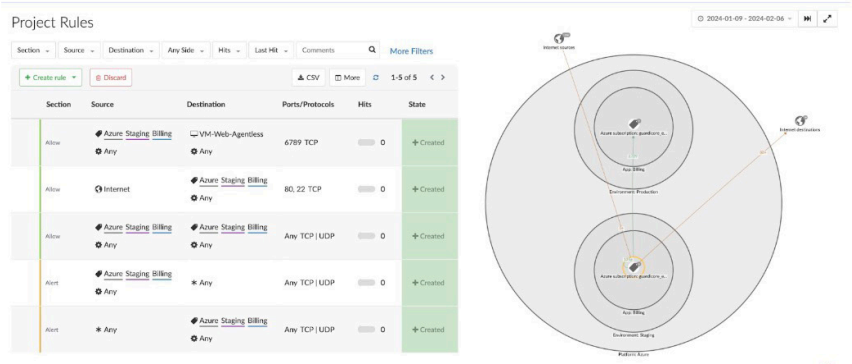
## Retos de seguridad únicos

Las organizaciones actuales confían cada vez más en la nube para gestionar sus sistemas esenciales y almacenar sus datos más valiosos.

Según el informe IBM Cost of a Data Breach 2023 (Coste de la vulneración de datos 2023), el 82 % de las filtraciones se han relacionado con datos almacenados en la nube, ya fuesen nubes públicas, privadas o de los dos tipos. A menudo, los atacantes consiguieron acceder a más de una plataforma en la nube: un 39 % de las vulneraciones abarcaron varios entornos y registraron un coste superior a la media de 4,75 millones de USD.

La naturaleza única y dinámica de la nube implica que sus cargas de trabajo están más expuestas a amenazas externas que los recursos locales. Los equipos de seguridad se enfrentan a una serie de retos únicos:

- **Una visibilidad deficiente.** La visibilidad del proveedor de nube se basa en registros sin procesar de los flujos entre diferentes cargas de trabajo. Si no se comprenden las relaciones entre las distintas cargas de trabajo y aplicaciones dentro de los entornos de nube, resulta casi imposible crear políticas de seguridad eficaces.
- **No hay una política global.** Crear una política coherente en todos los entornos de nube híbrida utilizando solo herramientas de seguridad en la nube nativas es extremadamente complejo. Esto se debe a que cada instancia en la nube tiene sus propios objetos y reglas y, por lo tanto, sus propias políticas, lo que da lugar a fragmentaciones.
- **Ausencia de una gestión unificada.** En la nube, no siempre se prioriza la seguridad, lo que genera fricciones entre los equipos de seguridad y los propietarios de las aplicaciones, que ponen en marcha cargas de trabajo sin tener en cuenta la seguridad.




*Acordonamiento de una aplicación Azure mediante sugerencias de políticas automatizadas*

## Ventajas para su empresa

**Visualice los flujos de la nube con una única interfaz**
Comprenda en profundidad cómo interactúan sus aplicaciones y cargas de trabajo en la nube mediante un mapa dinámico de dependencias de red y aplique fácilmente controles de seguridad.

**Implemente una política de segmentación coherente**
Despliegue una única solución de segmentación que funcione de forma coherente en todos los entornos de nube híbrida y evite soluciones específicas de proveedores que creen silos de seguridad.

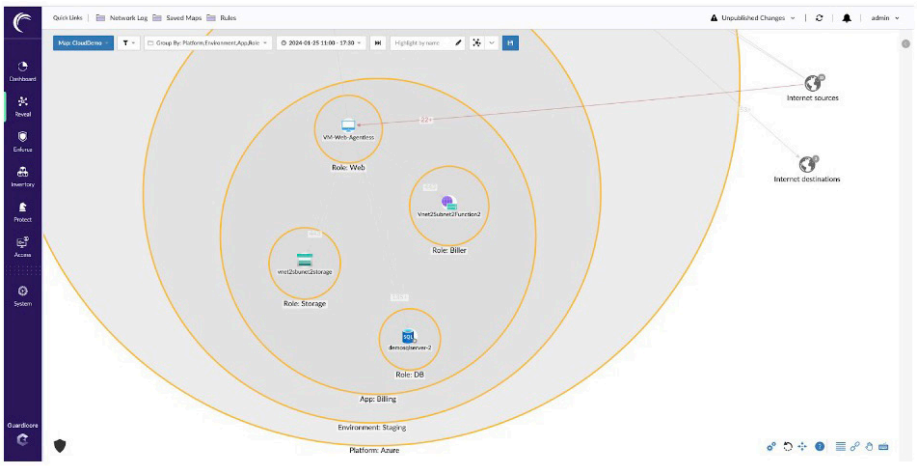
**Detenga las filtraciones**
Adapte las políticas de seguridad de su entorno de nube a cualquier cambio y ahorre a su equipo tener que realizar actualizaciones de forma manual.

## Prevención de amenazas a la seguridad en la nube

Akamai Guardicore Segmentation extiende su segmentación líder del sector a las aplicaciones y cargas de trabajo en la nube. Al ampliar la segmentación a los recursos de nube, cualquier conexión no autorizada se detiene automáticamente, lo que limita el movimiento lateral y los daños causados por filtraciones o incidentes de ransomware.

## Funciones clave

- **Funciones de visibilidad y control integrales, sin agentes y nativas de la nube:** los administradores pueden visualizar las cargas de trabajo de la nube mediante un mapa interactivo de flujos de red casi en tiempo real, comprender las dependencias de las aplicaciones y armonizar los esfuerzos de los equipos de desarrollo y seguridad en términos de control de la seguridad de red en la nube.
- **Un motor de aplicación de políticas híbrido con varios puntos de cumplimiento:** permite a una organización definir el objetivo de la política de red y que el motor de políticas Akamai Guardicore Segmentation decida de forma dinámica qué puntos de cumplimiento se deben usar en el centro de datos, tanto con agente como sin él.
- **Funciones integradas de análisis de reputación y de firewall de inteligencia ante amenazas:** diseñadas para reducir el tiempo de detección y de respuesta ante incidentes en caso de vulneraciones.
- **Flexibilidad y seguridad:** para garantizar que los datos no salgan de su entorno de nube y que la arquitectura de la solución se adapte automáticamente a él.




*Un único mapa para entornos locales y de nube híbrida*

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

 | Asistencia | Publicado en febrero de 2024