Akamai

WHITE PAPER

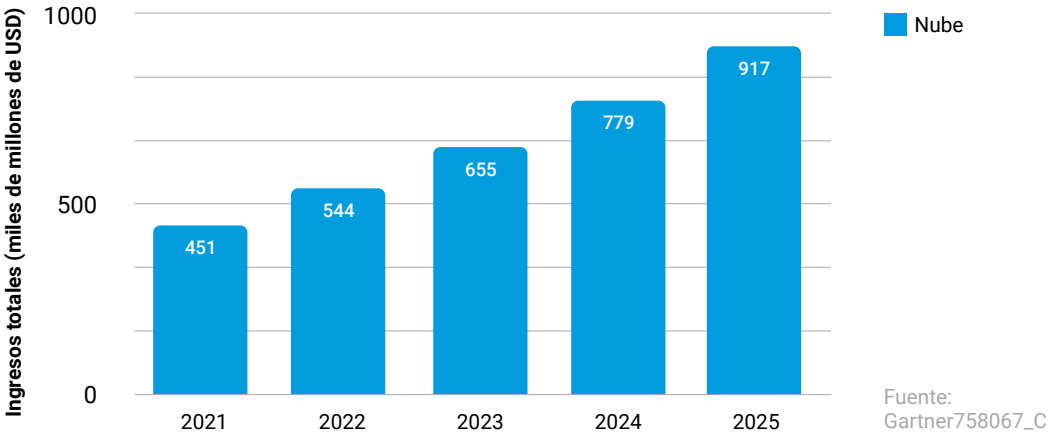
Abrir camino a la microsegmentación

Una guía de estrategia para implementar la microsegmentación en nubes híbridas

Nubes en el horizonte

La migración de grandes cantidades de datos y el tratamiento de datos en la nube (o, más concretamente, en varias nubes) es, sin duda, el mayor cambio en la informática empresarial de la última década. Cada vez más organizaciones están migrando a nubes públicas y, por lo general, a arquitecturas de centros de datos híbridos públicos y privados. Al mismo tiempo, están aprovechando la infraestructura como servicio (IaaS) en la búsqueda de una agilidad cada vez mayor. Gartner, analista tecnológico, prevé que en 2025 poco más de la mitad de todo el gasto de TI en segmentos de mercado objetivo habrá pasado de las soluciones tradicionales a la nube pública, en comparación con el 41 % de 2022, y se espera que el gasto total en la nube pública supere los 900 millones de USD en 2025.[1]

La distinción entre "la nube" y "varias nubes" no es trivial. Cada vez más empresas adoptan plataformas y proveedores de servicios multinube. Una cosa está clara: la idea de un centro de datos empresarial como un espacio físico único y seguro afronta su pronta extinción. Los centros de datos modernos son una combinación cada vez más heterogénea de entornos y tecnologías que combinan servidores físicos, máquinas virtuales y contenedores en instalaciones locales, nubes privadas y proveedores de IaaS de nube pública. Además, estas instalaciones dispares no son estáticas: las organizaciones cambian constantemente los datos y las cargas de trabajo entre sus distintos entornos locales y de nube, según las exigencias que plantean los niveles de tráfico y las necesidades de tratamiento de datos.



Previsión de ingresos por servicios en la nube pública en todo el mundo (miles de millones)

El aumento de la complejidad crea nuevas vulnerabilidades y amplía las superficies de ataque

Los clientes de la nube se benefician, sin duda, de la agilidad, elasticidad y escalabilidad adicionales que les ofrece la IaaS. Estas ventajas son una gran parte de lo que hace que la nube sea tan atractiva. Sin embargo, las desventajas son una complejidad de gestión mucho mayor, una pérdida de visibilidad de las cargas de trabajo en los distintos entornos y, a su vez, un panorama de ciberseguridad inexplorado. Trabajar con varios proveedores de nube significa que los equipos de seguridad tienen que hacer frente a estándares y funciones de seguridad muy diversos. Las herramientas de seguridad tradicionales, diseñadas para servidores y terminales locales, no son capaces de gestionar la escala y la complejidad de la nube. Las herramientas más recientes proporcionadas por los proveedores de IaaS pueden ser eficaces en el entorno del proveedor, pero son de poco valor en una infraestructura de varios proveedores.

Además, incluso en esta era de virtualización, con tantos productos "definidos por software", la mentalidad de seguridad (y, por lo tanto, la mayor parte de la inversión) sigue basándose en la necesidad percibida de bloquear los ataques específicamente en el punto de entrada. No se trata de un descarte de las defensas perimetrales, que siguen siendo muy relevantes para la pila de seguridad de TI, aunque no funcionan tan bien cuando el perímetro cambia constantemente. Los datos y las cargas de trabajo se desplazan entre nubes públicas y privadas, y centros de datos locales, y los usuarios que acceden a ellos trabajan cada vez más desde ubicaciones remotas que pueden o no contar con los controles de seguridad adecuados.

El gran número de vulneraciones de la seguridad informática que se notifican cada año es suficiente para comprender que los atacantes astutos están atravesando las defensas perimetrales a su antojo. Una vez dentro, encuentran una red relativamente plana en la que los activos que residen dentro del perímetro están prácticamente desprotegidos. A pesar de toda la flexibilidad que han adquirido las organizaciones, la complejidad añadida de gestionar y proteger las infraestructuras multinube ha multiplicado exponencialmente la superficie de ataque; con poco o ningún control de comunicación, cada servidor individual se convierte en una superficie de ataque en sí mismo. Como resultado, los atacantes pueden pasar más tiempo desplazándose lateralmente (sin ser detectados) entre las cargas de trabajo de tráfico este-oeste para encontrar los activos más importantes.

La segmentación de la red es una práctica de seguridad bien conocida y establecida, pero hoy en día puede resultar difícil ejecutarla en infraestructuras de TI dinámicas y a escala de nube, donde las cargas de trabajo se comunican y a menudo migran entre segmentos. Los clientes de la nube empresarial han llegado a la conclusión de que necesitan segmentar aún más sus aplicaciones y cargas de trabajo para controlar estrechamente los flujos de comunicación en tiempo real, así como detectar y frustrar las amenazas en el centro de datos antes de que puedan causar daños. Lo que se necesita es una solución que reduzca la complejidad de la seguridad al trabajar de forma coherente a través de los límites de la infraestructura para reducir la superficie de ataque general, lo que permite a los equipos de seguridad detectar más amenazas con mayor rapidez y limitar su propagación.

Aquí entra en juego la microsegmentación.

Definición de la microsegmentación

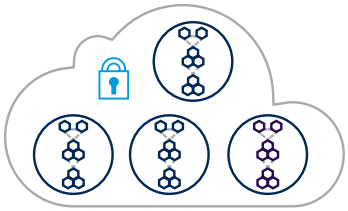
Gartner define la microsegmentación como "el proceso de implementación de aislamiento y segmentación con fines de seguridad en el centro de datos virtual". Además, la microsegmentación "reduce el riesgo de una propagación lateral de ataques avanzados en los centros de datos empresariales y permite a las empresas aplicar políticas de segmentación coherentes en las cargas de trabajo locales y basadas en la nube".[2]

La microsegmentación suele funcionar mediante el establecimiento de políticas de seguridad en torno a aplicaciones individuales o grupos de aplicaciones, independientemente de dónde residan en el centro de datos híbrido. Estas directivas determinan qué aplicaciones y componentes pueden comunicarse entre sí o no. Así pues, cualquier intento de comunicación no autorizada es un indicador instantáneo de una amenaza. En el mejor de los casos, las tecnologías de microsegmentación son independientes de la infraestructura, por lo que las políticas de seguridad pueden seguir protegiendo sus aplicaciones respectivas a medida que se mueven entre entornos de nube.

Áreas de soluciones para la segmentación

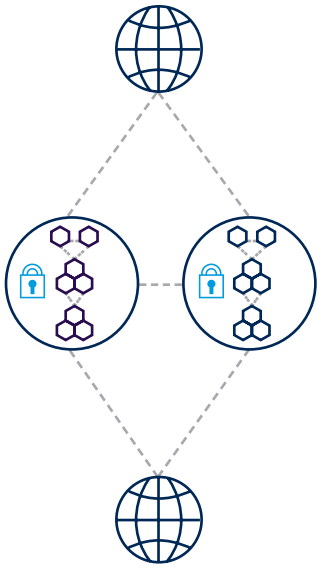
Segmentación de la infraestructura

Protección del tráfico de aplicaciones con una infraestructura concreta.



Segmentación de aplicaciones

Protección del tráfico entre aplicaciones y redes externas.



Microsegmentación

Reglas que protegen el tráfico dentro de aplicaciones con contexto adicional, como la atribución a nivel de proceso.

2 Gartner, "Technology Insight for Microsegmentation", marzo de 2017; "Hype Cycle for Cloud Security 2017", julio de 2017

Justificación de la microsegmentación

Los centros de datos dinámicos actuales exigen que las empresas desvíen su atención de la prevención de intrusiones y la gestión del acceso a las cargas de trabajo y las aplicaciones en sí. Esto parece estar sucediendo a un ritmo acelerado. Incluso en 2017, Gartner comenzó a notar una tendencia hacia "un mayor enfoque en la protección de las cargas de trabajo de los servidores frente a amenazas específicas avanzadas que eluden la protección tradicional basada en perímetros y firmas. Por lo general, estos ataques están motivados económicamente y se dirigen a las cargas de trabajo de servidores y aplicaciones como una forma de llegar a datos o transacciones confidenciales".[3]

Un factor clave de la microsegmentación es la necesidad de proteger las aplicaciones y las cargas de trabajo esenciales. Esto puede parecer simplemente una cuestión de interés propio o de buen juicio empresarial, pero en muchos casos, también resulta obligatorio por las políticas de seguridad y los requisitos normativos.

Los equipos de seguridad necesitan encontrar formas de reducir la superficie de ataque en expansión dentro de los centros de datos, lo que implica reducir la vulnerabilidad de los servidores que ejecutan aplicaciones. Las técnicas de autenticación tradicionales, como el bloqueo de firmas o la inclusión en listas de autorización, son demasiado fáciles de eludir por parte de atacantes sofisticados. La microsegmentación permite a los equipos establecer y aplicar políticas de acceso y comunicación estrictas y detalladas. También debe mejorarse la visibilidad de los flujos de aplicaciones y permitir a los equipos evaluar mejor su situación de seguridad.

¿Necesita microsegmentación?

Responder a unas sencillas preguntas le ayudará a determinar si necesita la microsegmentación.

- ¿Se encuentra en un sector regulado o necesita cumplir con las normativas que rigen la seguridad de los datos y las transacciones?
- ¿Tiene una infraestructura híbrida con cargas de trabajo que abarcan varias nubes?
- ¿Ejecuta aplicaciones en máquinas virtuales o contenedores?
- ¿Nota una pérdida de visibilidad y control de las cargas de trabajo?
- ¿Puede saber, en cualquier momento, si existe una amenaza o hay un ataque en curso en su centro de datos?
- ¿Puede controlar la seguridad en toda su infraestructura a través de una "vista unificada"?

Los cuatro obstáculos principales en el camino

Si los expertos en seguridad están de acuerdo en general sobre la necesidad de la microsegmentación en los centros de datos dinámicos actuales, ¿por qué se considera tan difícil lograr una implementación satisfactoria y eficaz? Las organizaciones que intentan implementar la microsegmentación mediante herramientas convencionales suelen encontrarse con cuatro obstáculos principales:

1. **Falta de visibilidad a nivel de proceso**
   Este es probablemente el primer impedimento que encontrará: no puede proteger lo que no puede ver. La microsegmentación consiste en proteger aplicaciones, tanto individuales como en grupos, y procesos de flujos de trabajo. Los equipos de seguridad necesitan visibilidad de los flujos de tráfico este-oeste reales para entenderlos en contexto. La mayoría de las herramientas no proporcionan ese nivel de detalle.

2. **Falta de compatibilidad con entornos multinube híbridos**
   Las políticas de seguridad de microsegmentación deben poder adaptarse fácilmente a entornos locales y de nube pública, y seguir las cargas de trabajo a medida que se desplazan. Las herramientas diseñadas para funcionar en un entorno específico no son eficaces en entornos híbridos.

3. **Motores de políticas inflexibles**
   Como se señaló anteriormente, los centros de datos actuales no son estáticos. Las medidas de seguridad tampoco pueden serlo: la mentalidad de "configurar y olvidar" ya no sirve. Lamentablemente, las herramientas existentes de los proveedores de nube no ofrecen la flexibilidad necesaria para definir, probar y perfeccionar constantemente las reglas. Este desafío se agrava en las infraestructuras híbridas que requieren diferentes herramientas de gestión de políticas.

4. **Falta de integración con controles complementarios**
   Si se realiza correctamente, la microsegmentación no solo tiene que ver con la protección de los procesos, sino también con la detección de ataques. Sin embargo, las herramientas de microsegmentación de función única no suelen incluir capacidades de detección de infracciones, lo que deja al usuario la tarea de integrar las herramientas y hacer que trabajen juntas de forma eficaz. Este enfoque conlleva un alto riesgo de fracaso.

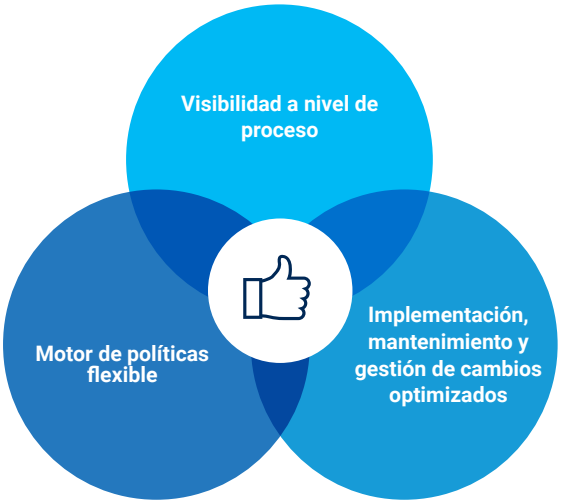
Los proyectos fallidos son la norma, no la excepción

Teniendo en cuenta todos los obstáculos, no es de extrañar que la mayoría de los proyectos de microsegmentación tiendan a tener que soportar ciclos de implementación lentos y potenciales aumentos en los costes, graven los recursos y, en última instancia, no logren sus objetivos. A menudo, las organizaciones tienen dificultades a la hora de averiguar qué hay que segmentar (debido a la falta de visibilidad) y qué nivel de segmentación es necesario. Es posible que pasen meses creando hojas de cálculo de reglas complejas para las comunicaciones a nivel de proceso, sin poder reconocer oportunidades para agrupar aplicaciones y optimizar las políticas. Con demasiada frecuencia, se equivocan, tendiendo a la "sobresegmentación": establecen demasiadas políticas discretas, lo que resulta en una excesiva complejidad de la seguridad, que es precisamente lo que se está intentando superar. Como ha señalado Gartner, "… más del 70 % de los proyectos de segmentación deberán rediseñarse debido a la sobresegmentación".[4]

La sobresegmentación conlleva el riesgo de ralentizar las aplicaciones y, en última instancia, a la empresa. Con todo, la balanza también puede inclinarse al lado contrario, hacia una infrasegmentación, y terminar poniendo en peligro su estrategia de seguridad.

Estrategia para un proceso de microsegmentación satisfactorio

El camino hacia la implementación de la microsegmentación no es una línea recta; hay muchos giros y vueltas a medida que descubre, comprende y controla los flujos de comunicación en su entorno. Los equipos de seguridad necesitan flexibilidad a la hora de desarrollar políticas de seguridad para incorporar constantemente nuevos cambios o adiciones sin interrumpir las aplicaciones. Muchas soluciones ofrecen motores de creación de políticas inflexibles, lo que obliga a los equipos de seguridad a implementar reglas incompletas o ineficaces antes de que estén listos.



Sencillamente, una implementación exitosa es aquella que supera o elude los cuatro obstáculos principales, evitando la complejidad indebida y reduciendo el riesgo de una infrasegmentación o una sobresegmentación al permitir un enfoque por fases. Esto significa tener una solución que cumpla estos requisitos:

- **Visibilidad a nivel de proceso:** los equipos necesitan la capacidad de revelar, recopilar y normalizar todos los flujos este-oeste y norte-sur; herramientas que permitan la detección automática de aplicaciones y la comprensión de sus requisitos de comunicación; y la capacidad de filtrar por varios atributos de aplicación para facilitar el etiquetado y la agrupación de activos que puedan compartir políticas.

- **Un motor de políticas flexible:** debe ser capaz de diseñar simultáneamente prácticas recomendadas y reglas de cumplimiento generales para segmentos grandes y reglas más granulares para microsegmentos. La solución debería permitirle pasar gradualmente de las alertas a la aplicación de las reglas. Además, debería permitirle establecer políticas que funcionen en todas las plataformas, dispositivos y nubes.

- **Implementación, mantenimiento y gestión de cambios optimizados:** el sistema debe facilitar la implementación, el mantenimiento y la modificación de reglas según sea necesario. Debe incorporar funciones integradas de detección de infracciones y respuesta ante incidentes. En última instancia, las políticas deben estar suficientemente bien definidas para poder integrarlas en herramientas de implementación automatizada (CI/CD) para cada nueva aplicación que se lance.

Características ideales de la solución

Por supuesto, hay muchas herramientas de microsegmentación en el mercado y no todas facilitan el proceso explicado. Para garantizar una implementación más fluida y satisfactoria, asegúrese de elegir una solución con estas características:

- **Detección automática de aplicaciones**, con visibilidad completa a nivel de proceso para servidores bare metal, máquinas virtuales y contenedores

- Capacidad de definir **consultas sólidas y extensas** para crear etiquetas contextuales y grupos de objetos

- Un **motor de políticas flexible** con un diseño de reglas inteligente que le ayude a perfeccionar, fortalecer y mantener las políticas

- Una **capacidad integrada de detección de filtraciones con varios métodos** para detectar más amenazas con mayor rapidez y limitar su propagación

- **Soporte de infraestructura híbrida**: una plataforma que funcione con cualquier infraestructura (centros de datos, nubes públicas y privadas, etc.)

Una solución con estas características básicas le pondrá en camino hacia el éxito a la hora de implementar la microsegmentación, le facilitará superar las complejidades y los obstáculos conocidos, y le preparará para aprovechar todas las ventajas empresariales de una infraestructura de nube híbrida flexible sin sacrificar la seguridad.

Los centros de datos híbridos, las plataformas multinube y la IaaS ofrecen a las organizaciones más flexibilidad, escalabilidad y agilidad de lo que sería posible en un centro de datos local "cerrado". Sin embargo, también dejan las aplicaciones y las cargas de trabajo, los activos reales a los que se dirigen los ciberatacantes, más expuestos y vulnerables. Aunque la microsegmentación se considera una práctica recomendada para proteger las cargas de trabajo en la nube, a las empresas les cuesta ponerla en práctica correctamente. La buena noticia es que no tiene que hacerlo todo a la vez. Las soluciones avanzadas de hoy en día, junto con un enfoque paso a paso, hacen que el camino hacia la implementación de la microsegmentación sea mucho más fácil. Eso se traduce en una mayor seguridad para los activos más importantes de su organización.

Obtenga más información sobre la correcta implementación de la microsegmentación en akamai.com/guardicore

1 "Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025". Gartner, 9 de febrero de 2022.

2 Heiser, Jay. "Hype Cycle for Cloud Security, 2017". Gartner, 17 de julio de 2017.

3 MacDonald, Neil. "Market Guide for Cloud Workload Protection Platforms". Gartner, 22 de marzo de 2017.

4 Young, Greg. "Best Practices in Network Segmentation for Security". Gartner, 28 de julio de 2016.

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 seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado el 23 de mayo.