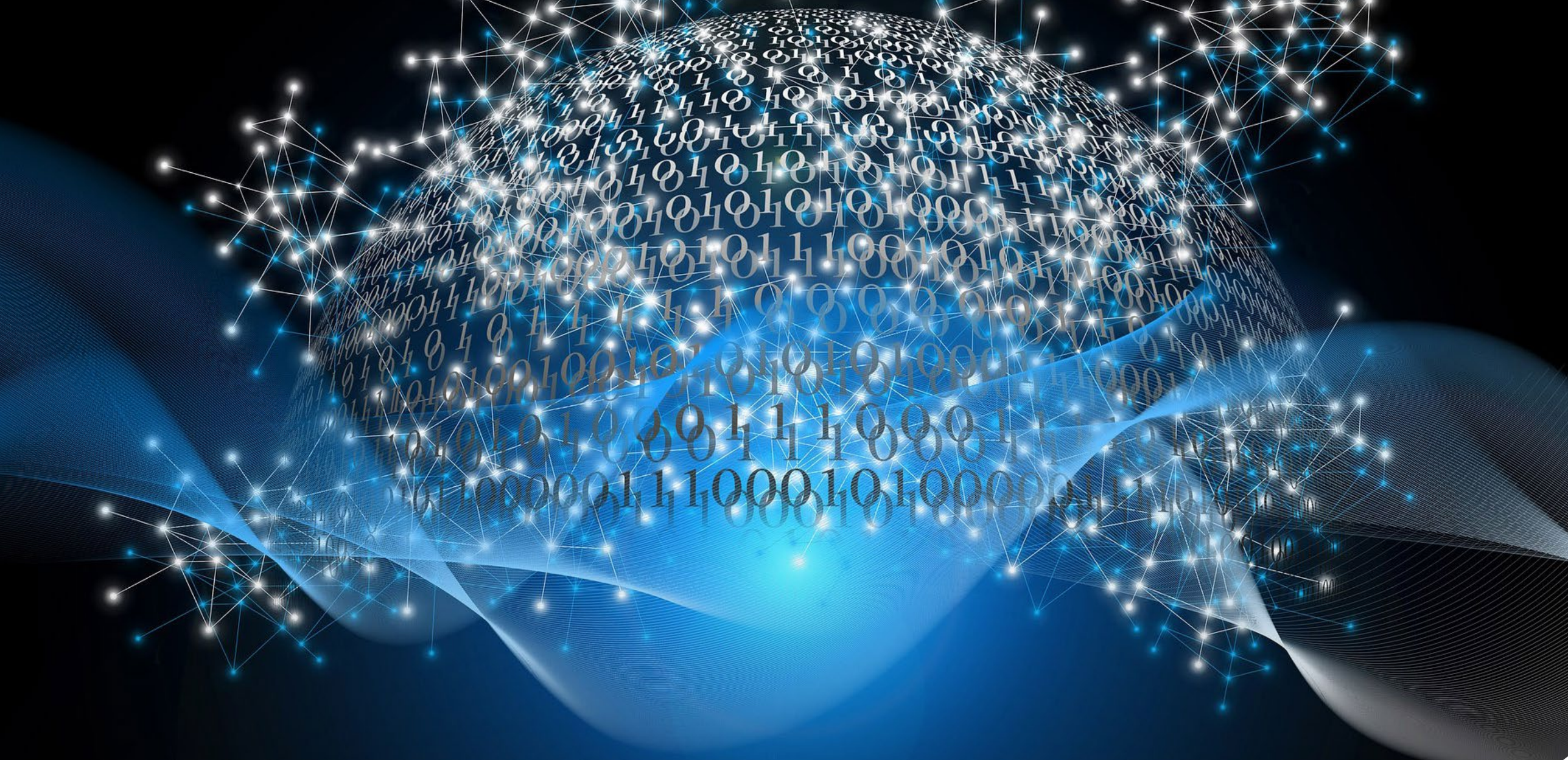


Microsegmentación, clave para la seguridad empresarial

Elaborado por:

itResearch

Para:

zscaler

Microsegmentación, clave para la seguridad empresarial

La microsegmentación es un método para crear zonas seguras en centros de datos y despliegues en la nube que permite a las empresas aislar cargas de trabajo entre sí y protegerlas individualmente. Su objetivo es hacer que la seguridad de la red sea más granular.

La segmentación de la red no es nueva. Las empresas han confiado en firewalls, redes de área local virtuales (VLAN) y listas de control de acceso (ACL) para la segmentación de la red durante años. Con la microsegmentación, las políticas se aplican a cargas de trabajo individuales para una mayor resistencia a los ataques.

La granularidad que ofrece la microsegmentación es esencial en un momento en que la mayoría de las organizaciones están adoptando servicios en la nube y nuevas opciones de implementación, como contenedores, que hacen que la seguridad perimetral tradicional sea cada vez menos relevante.

Y es que a pesar de los diferentes tipos de protección [firewalls, IPS, etc] los ataques están logrando penetrar el perímetro y las infracciones continúan ocurriendo. El problema principal es que una vez que un ataque sobrepasa el perímetro de la red, existen pocos controles laterales para evitar que las amenazas se extiendan. La mejor manera de resolver esto es adoptar un modelo de seguridad microgranular más estricto con la capacidad de vincular la seguridad a las cargas de trabajo individuales y la agilidad para aprovisionar políticas automáticamente.

'LAS TÉCNICAS DE MICROSEGMENTACIÓN TIENEN QUE SER ALTAMENTE AUTOMATIZADAS' (MIGUEL ÁNGEL MARTOS, ZSCALER)

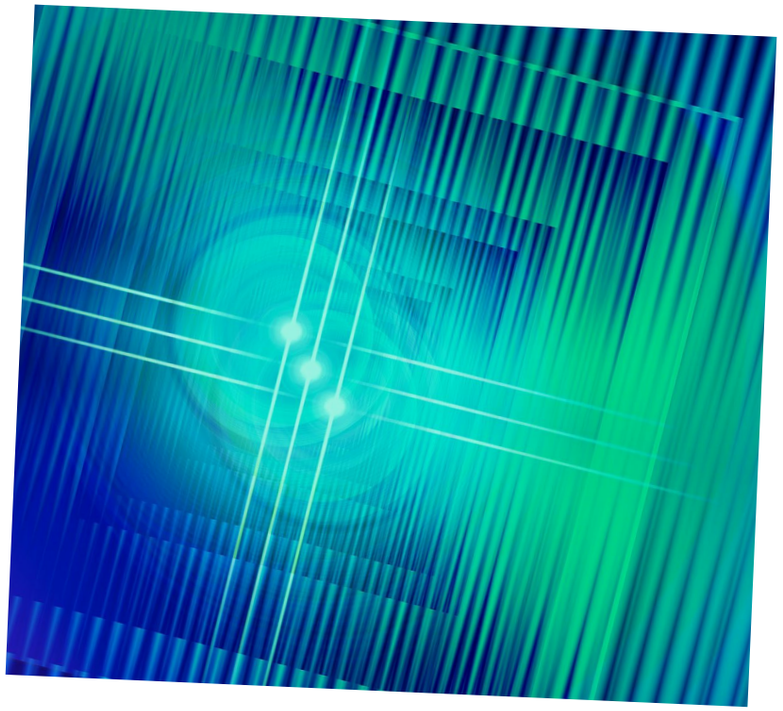
CLICAR PARA VER EL VÍDEO

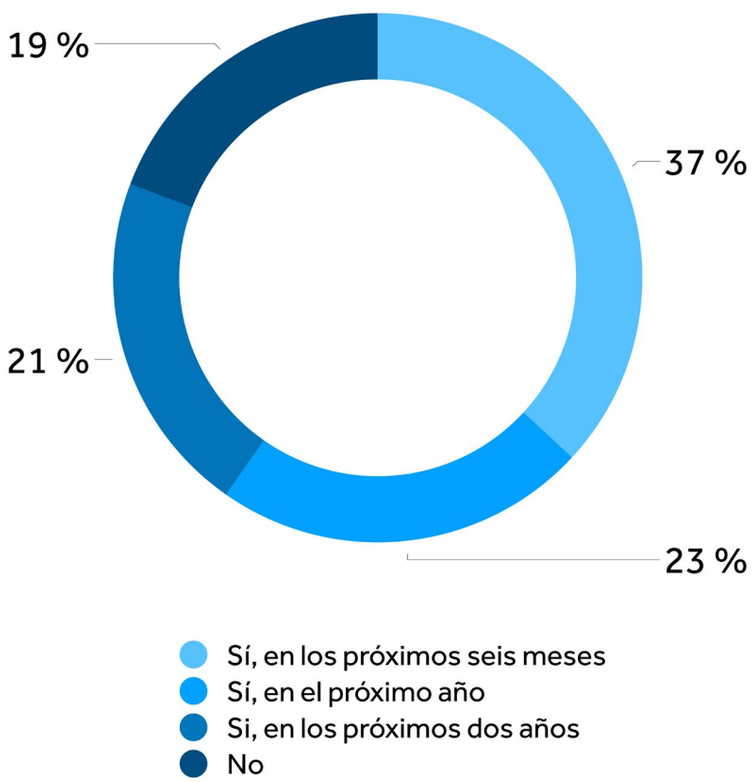
Se prevé que el mercado de microsegmentación alcanzará los 2.700 millones de dólares para 2025, con un crecimiento medio anual del 23.4% durante 2020-2025. Algunos de los factores que están impulsando este mercado son una mayor conciencia para proteger el entorno de la nube, el aumento del coste de los ciberataques y un mayor aumento del uso de aplicaciones, dispositivos conectados y dispositivos móviles, según datos de Industry ARC.

IT Digital Security, en colaboración con Zscaler, ha realizado una encuesta entre profesionales españoles durante los meses de junio y julio de 2021 para conocer la visión que los profesionales de las empresas tienen acerca de la microsegmentación, qué viene a solucionar, que beneficios aporta, qué características deben tener las soluciones que lo permitan o cómo impacta en la seguridad.

"Si bien el concepto de microsegmentación en la superficie es fácil (hay que crear segmentos separados para microservicios), ponerlo en su lugar a menudo parece demasiado complejo, más aún con las conexiones internas. Sin embargo, uno de los mayores beneficios de la microsegmentación es la facilidad de escalar y cambiar las políticas. Al utilizar esta estrategia como base, su empresa ahora tiene la agilidad necesaria para realizar cambios internos (en empleados, dispositivos, cargas de trabajo y aplicaciones) para reaccionar a las necesidades comerciales cambiantes. Con la microsegmentación y la confianza cero, se crea la seguridad y la flexibilidad necesarias para el mundo actual".

Carlos Asún, CISO, Food Delivery Brands





¿Está considerando implementar microsegmentación como parte de su estrategia de seguridad para el datacenter?

Como decíamos, la microsegmentación es una forma de crear zonas seguras en los centros de datos y despliegues cloud que te permiten aislar cargas de trabajo y protegerlas individualmente, de forma que cuanto más pequeños son los segmentos, más se reduce la superficie de ataque y por tanto menor el riesgo para las empresas.

Según la encuesta realizada por IT Digital Security, la empresa española está más que dispuesta a adoptar microsegmentación como parte de su estrategia se seguridad para el centro de datos, aunque lo harán a diferentes velocidades.

Del 80,6% que consideran la adopción, la mayor parte, un 36,8% implementarán la microsegmentación en los próximos seis meses, un 22,8% la considera en el próximo año y un 21% en los próximos dos años.

Un 19,2% no considera la implementación de la microsegmentación asociada a la seguridad.

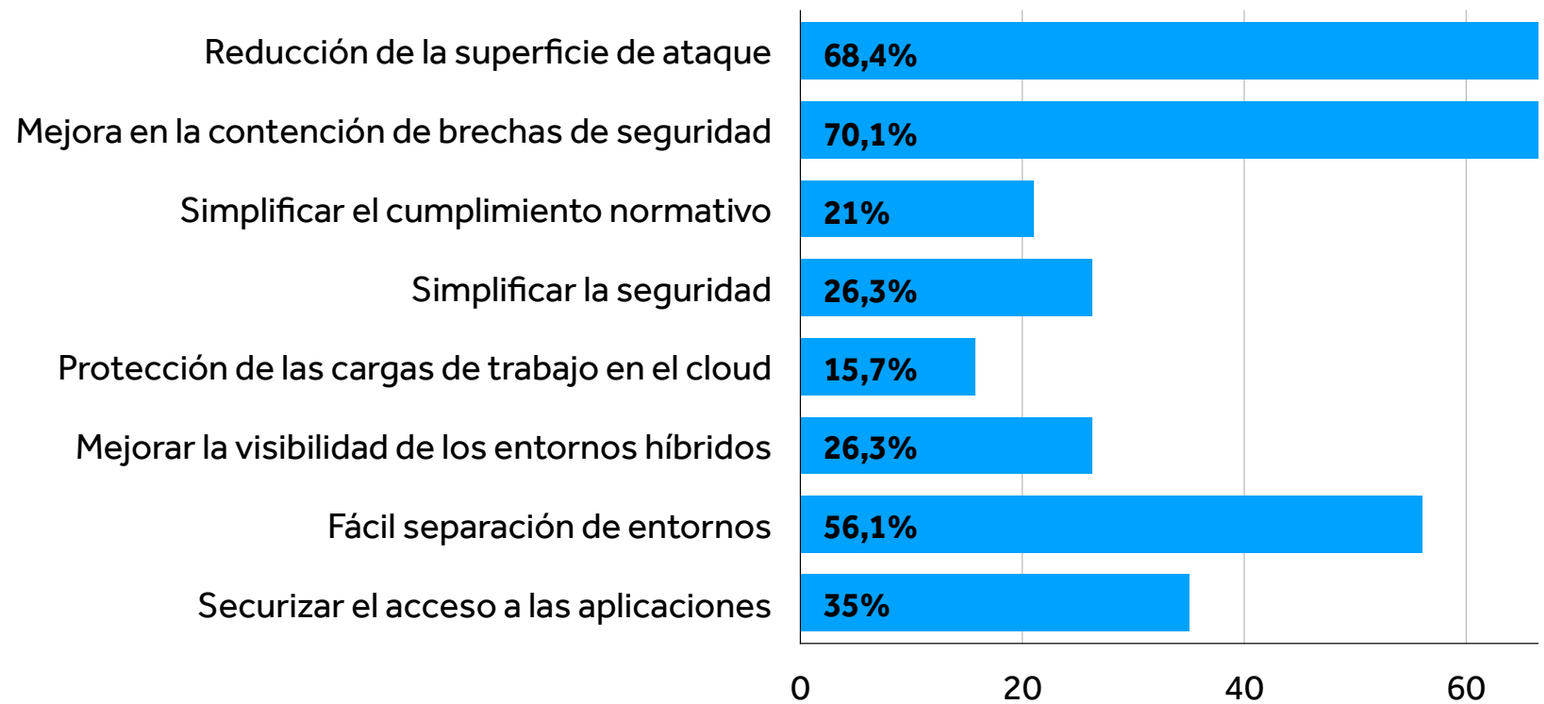
¿Qué objetivos cree que puede lograr con un proyecto de microsegmentación?

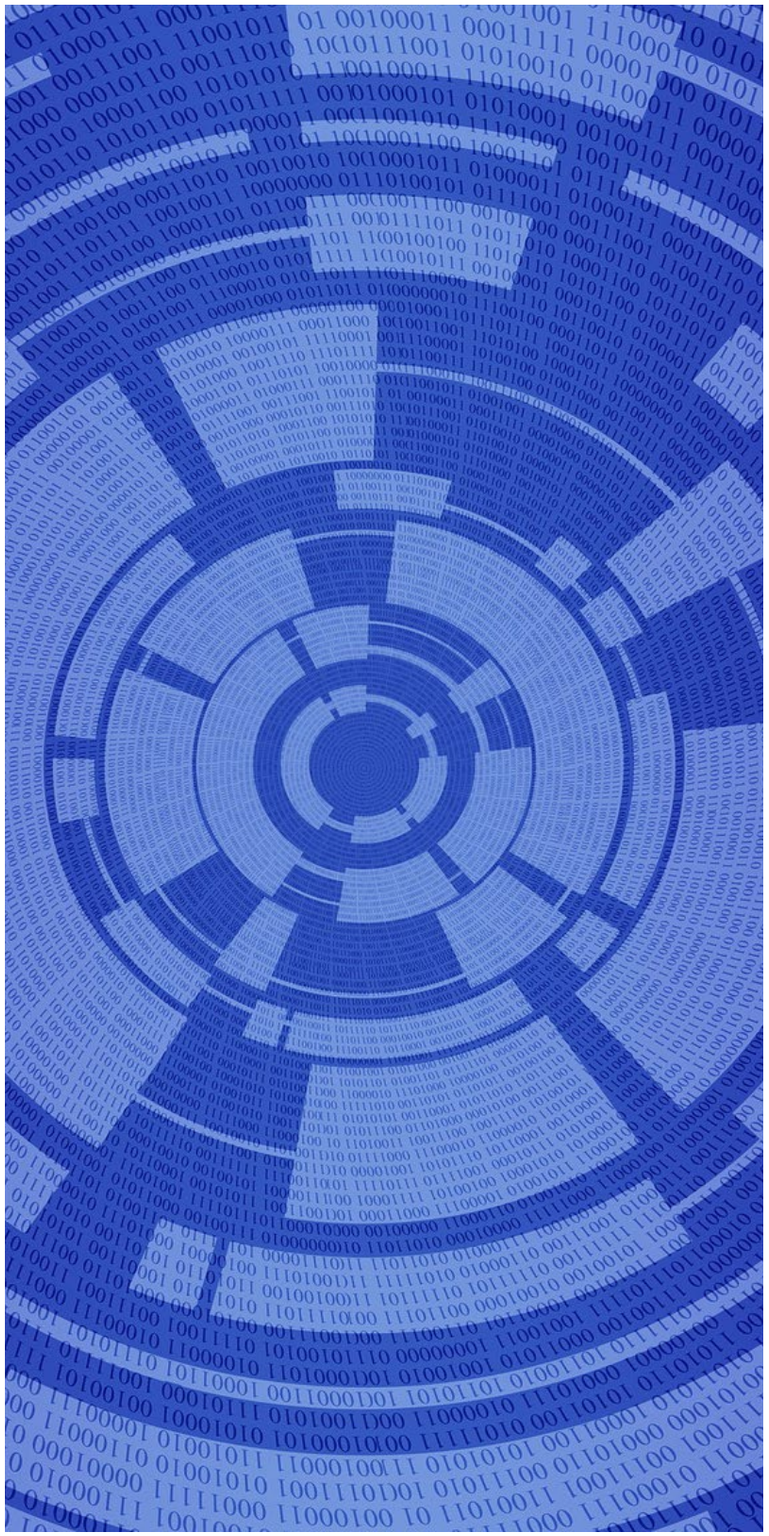
La microsegmentación ofrece a las empresas un mayor control sobre la comunicación este-oeste, o comunicación lateral que se produce dentro de las empresas. Un tráfico que ya no pasa por las herramientas de seguridad centradas en el perímetro. Si se producen infracciones, la microsegmentación limita la posible exploración lateral de las redes por parte de los ciberdelincuentes.

La mejora en la contención de las brechas de seguridad es, para el 70,1% de los encuestados, el principal objetivo que persiguen en un proyecto de microsegmentación, seguido de la reducción de la superficie de ataque (68,4%). La fácil separación de entornos es el tercer objetivo más destacado para un 56,1%, que también valoran positivamente la posibilidad de securizar el acceso a las aplicaciones (35%) mediante la microsegmentación.

El objetivo menos valorado de los propuestos es la protección de las cargas de trabajo en el cloud (15,7), así como la posibilidad de simplificar el cumplimiento normativo (21%).

Existe un empate entre simplificar la seguridad y la mejora de la visibilidad de los entornos híbridos (26,3%) como posibles objetivos de un proyecto de microsegmentación.





¿Cuáles son las principales características que debería tener una solución de microsegmentación para hacer viable su despliegue?

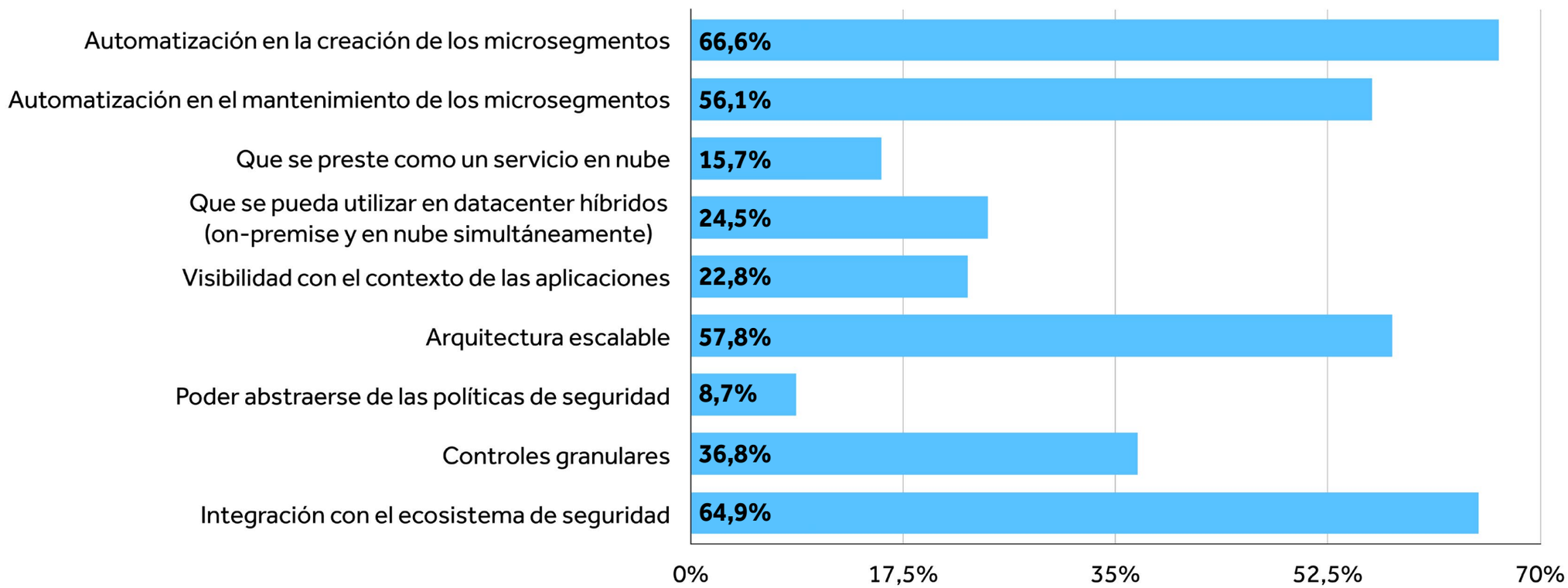
La microsegmentación permite políticas de seguridad más flexibles y precisas que se pueden asignar hasta el nivel de carga de trabajo. Estos controles minuciosos aseguran que los atacantes se enfrenten a menos debilidades potenciales para explotar, incluso cuando aumenta el número teórico de posibles puntos de ataque.

Las tres características más valoradas que debe tener una solución de microsegmentación según los encuestados son: la automatización en la creación de los microsegmentos (66,6%); su integración con el ecosistema de seguridad (64,9) y la automatización en el mantenimiento de esos microsegmentos creados (56,1%).

También se toma en consideración que sea una arquitectura escalable (57,8%) e incluso que se puedan aplicar controles granulares (36,8%).

Similares respuestas han tenido el que una solución de microsegmentación pueda ser utilizada en datacenter híbridos (on-premise y en nube simultáneamente) y que ofrezca visibilidad con el contexto de aplicaciones, para un 24,5% y un 22,8% de los encuestados respectivamente.

A pesar del interés que despierta el as-a-service, que se preste como un servicio en nube ha sido escogido por un 15,7% de los encuestados como una de las características que debería tener una solución de microsegmentación para hacer viable su despliegue. La opción que menos interés ha despertado es el que pueda abstraerse de las políticas de seguridad (8,7%)



Microsegmentación, clave para la seguridad empresarial

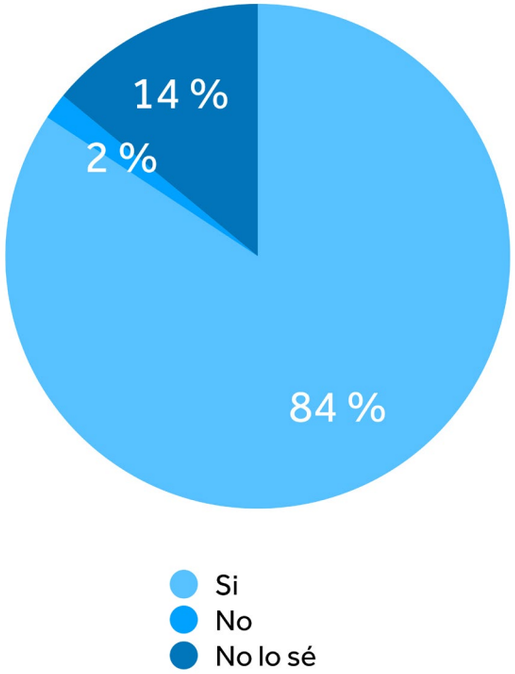
"La Microsegmentación ayuda a aislar los diferentes entornos que tenemos en una empresa permitiendo avanzar en el paradigma de Zero Trust o desconfianza total. Aislar los sistemas nos permite NO proporcionar accesos que quizás antes teníamos que realizar una segmentación más compleja a nivel de red, sin embargo, ahora, con la microsegmentación nos facilita esta labor y podemos aislar de forma eficiente cada uno de los entornos. No quiero dejar de comentar que la microsegmentación también permite una monitorización más sencilla, con lo que facilita encontrar posibles fallos más rápidamente".

Jose María Pulgar Gutierrez, CISO Responsable Oficina Técnica Seguridad de la Información, Bosonit

¿Cree que la microsegmentación le puede ayudar a implementar o extender su estrategia Zero Trust?

Rotunda es la afirmación de que la microsegmetación ayuda en la implementación de una estrategia de Zero Trust. Así lo consideran el 84,2% de los encuestados.

Un 14% no lo tienen claro, mientras que un mero 1,7% no creen que la microsegmentación ayude a extender un marco de seguridad que requiere que las organizaciones autentiquen y autoricen a todos los usuarios y dispositivos dentro y fuera del perímetro antes de permitir el acceso a aplicaciones y datos.

La microsegmentación es un método para crear segmentos de red de forma lógica y controlar completamente el tráfico dentro y entre los segmentos. Proporciona la capacidad de controlar las cargas de trabajo en un centro de datos o un entorno de múltiples nubes con controles de políticas granulares y restringe la propagación de amenazas laterales en el centro de datos.

Uno de los principios clave de un enfoque de confianza cero es nunca confiar y siempre verificar primero. La microsegmentación a nivel de host permite a los equipos de seguridad aislar entornos y segmentar cargas de trabajo y aplicaciones distribuidas. Una vez segmentadas, las políticas de seguridad detalladas se pueden aplicar en función de un enfoque de confianza cero.