Akamai

WHITE PAPER

# Replantearse los firewalls

## El argumento económico convincente para utilizar la segmentación basada en software

# Resumen ejecutivo

¿Por qué los equipos de red y seguridad siguen confiando en firewalls heredados para segmentar la red interna? A medida que proliferan las aplicaciones y los segmentos protegidos por políticas, los firewalls físicos están demostrando ser demasiado complejos, inflexibles e ineficaces para hacer frente a los desafíos de seguridad de los entornos de nube híbrida cada vez más dinámicos de hoy en día. Además, son mucho más caros de lo que los equipos se imaginan. Además del enorme coste inicial de los firewalls y el hardware, hay muchos costes posteriores significativos debido a la gestión de proyectos, la mano de obra y el mantenimiento, además del riesgo bastante real de una exposición prolongada de los activos debido a los largos tiempos de implementación. Si las empresas modernas quieren aprovechar las ventajas de la metodología Agile DevOps, una rápida implementación de aplicaciones y la nube, tiene que haber una forma mejor de proteger los activos críticos con la segmentación. Y ahora la hay: con la segmentación basada en software. Es más fácil, más rápida, más eficaz y, como demostrará claramente este documento, ofrece una seguridad óptima con un TCO mucho menor que los métodos de segmentación tradicionales.

# Introducción

Hoy en día, vemos tres fuerzas convergentes que impulsan la demanda de una forma más detallada de segmentar redes y activos individuales. En primer lugar, Agile DevOps y otros modelos de entrega rápida están poniendo el énfasis en la implementación acelerada de aplicaciones en producción. Inevitablemente, esto requiere la creación de zonas más seguras con políticas más precisas. En segundo lugar, a medida que las organizaciones migran a la nube y adoptan infraestructuras de TI híbridas, sus aplicaciones suelen migrar entre diferentes entornos, lo que aumenta el tráfico entre segmentos en la red. Y, en tercer lugar, la rápida proliferación de aplicaciones debido al desarrollo ágil está creando una superficie de ataque cada vez mayor que los hackers pueden aprovechar.

# Firewalls para la segmentación: una solución obsoleta

Dadas estas condiciones, una dependencia estricta de las VLAN y los firewalls para fines de segmentación se está volviendo insostenible. Desde una perspectiva puramente técnica, la configuración de varias instalaciones de VLAN y firewalls de forma que sigan el ritmo del desarrollo de aplicaciones es compleja y engorrosa. Este enfoque también es costoso en términos de personal, ya que quita a demasiados miembros del equipo de los proyectos de seguridad de mayor prioridad. El tiempo de implementación es otro problema, ya que aumenta el riesgo de exposición prolongada de los activos y la vulnerabilidad. Y, sobre todo, la implementación resulta extremadamente cara, no solo por el coste inicial de los firewalls y el nuevo hardware para que admitan tráfico adicional, sino también por los costes asociados a la gestión, las modificaciones y el mantenimiento continuos de las instalaciones.

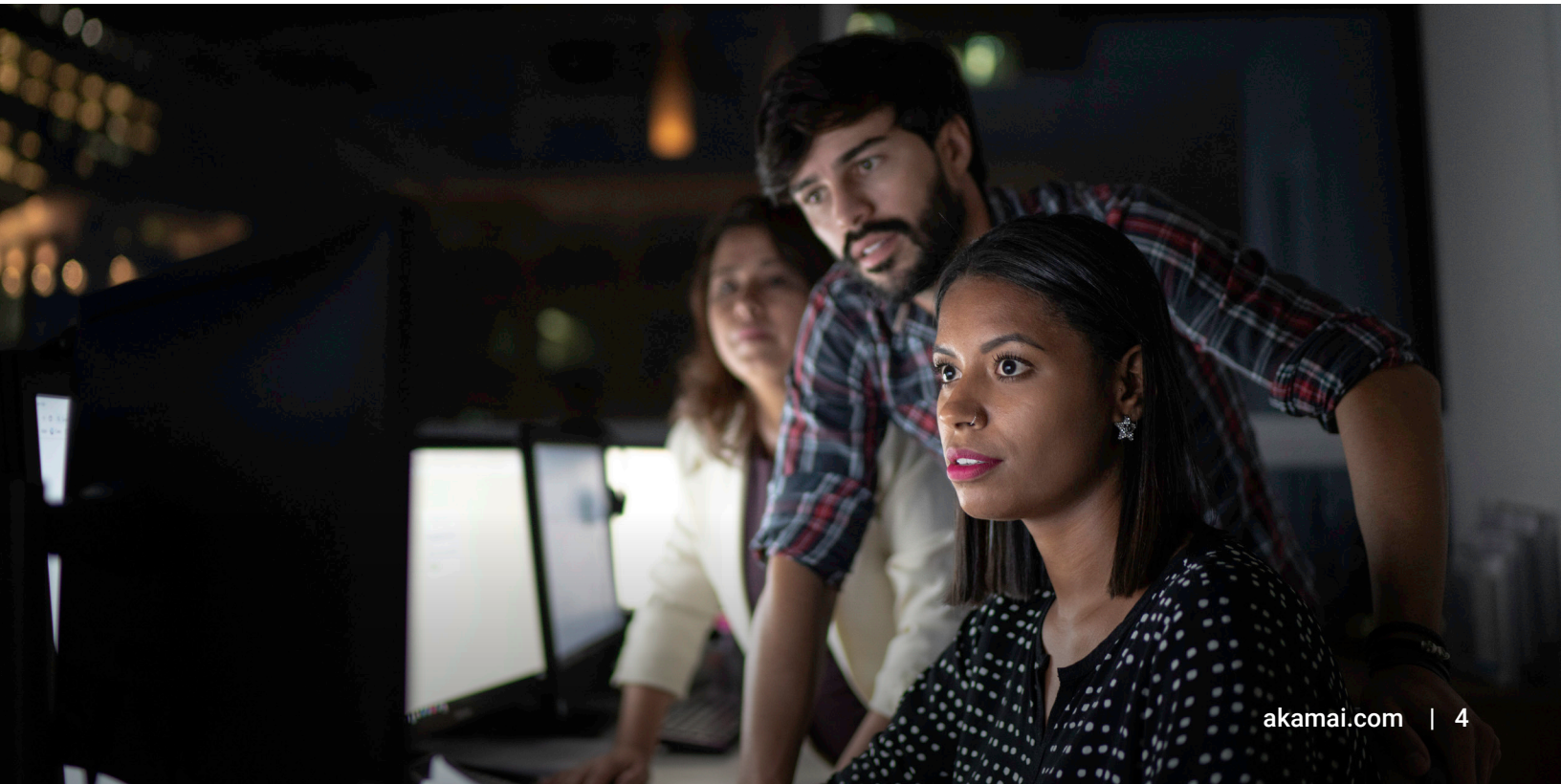
En pocas palabras, los enfoques tradicionales de segmentación de la red han llegado a un callejón sin salida. En concreto, a medida que las organizaciones buscan la manera de aprovechar los entornos híbridos y de nube dinámicos, la dependencia de firewalls internos para la seguridad limita su agilidad, la velocidad de creación y aplicación de políticas, y la capacidad de escalar sus operaciones de forma segura. La necesidad de buscar una alternativa de segmentación moderna, optimizada, menos costosa y, en última instancia, más eficaz a los firewalls heredados nunca había sido tan urgente. Aquí es donde entra en juego la segmentación basada en software.

La necesidad de buscar una alternativa de segmentación moderna, optimizada, menos costosa y más eficaz a los firewalls heredados nunca había sido tan urgente.

# El esfuerzo: la costosa tarea de gestionar los firewalls

Antes de profundizar en las ventajas de la segmentación basada en software, es útil contrastarla con el statu quo. A medida que una empresa crece, también lo hace el número de aplicaciones y la cantidad de tráfico de datos asociado, lo que impulsa la demanda de segmentos de red adicionales y políticas de seguridad más complejas. Si depende de VLAN protegidas por firewall, cada nueva implementación debe añadirse a cada puerto troncal del switch a través del cual fluye el tráfico entre segmentos. También es necesario crear una subred IP para cada nueva VLAN. Asimismo, se debe crear una subinterfaz para el firewall. A continuación, es necesario crear políticas de firewalls. Cada uno de estos cambios suele requerir aprobaciones, plazos de mantenimiento y la posibilidad de que se produzca tiempo de inactividad, lo que supone un mayor riesgo de interrupciones en la red.

La incorporación de VLAN y firewalls conlleva un proceso complejo de varios pasos en el que participan hasta cinco equipos, responsables por separado de la conmutación, el enrutamiento, la implementación de firewalls, los servidores ESXi y la creación de políticas de seguridad. Todo esto se suma a la duración de la implementación, expone a la organización a un riesgo prolongado y aumenta los costes de software, hardware y mano de obra. Además, desde el punto de vista del ingeniero, se trata de un trabajo de alto riesgo y baja recompensa, un gran esfuerzo a cambio de muy pocas ganancias, que quita tiempo y recursos que son necesarios para otras actividades de gestión de riesgos de alta prioridad. Lamentablemente, pocos de los pasos del proceso de gestión de cambios dentro del entorno de VLAN con firewalls se prestan a la automatización.



# La solución: segmentación basada en software en tres sencillos pasos

La tecnología tradicional de firewalls perimetral nunca se diseñó para satisfacer las demandas más precisas y con limitaciones de ancho de banda de la segmentación interna detallada. La segmentación basada en software ha surgido en los últimos años como una alternativa viable, más rápida, más eficaz y de menor coste para satisfacer la demanda de segmentos de red en mayor cantidad y más ajustados en los entornos dinámicos de hoy en día. En la base a la hora de implementar la segmentación basada en software está el concepto de "firewall distribuido", que es mucho más ágil y fácil de gestionar que un dispositivo de firewall de red tradicional.

> La segmentación basada en software permite una implementación hasta **10 o incluso 20 veces más rápida** que la de los firewalls tradicionales; necesita mucho menos personal y no hay prácticamente tiempo de inactividad ni interrupciones.

Un ejemplo líder del sector de una solución de segmentación basada en software es Guardicore Segmentation de Akamai. En comparación con el largo, costoso y complejo proceso de implementación de un firewall para la VLAN, nuestra solución de segmentación basada en software solo consta de tres pasos:

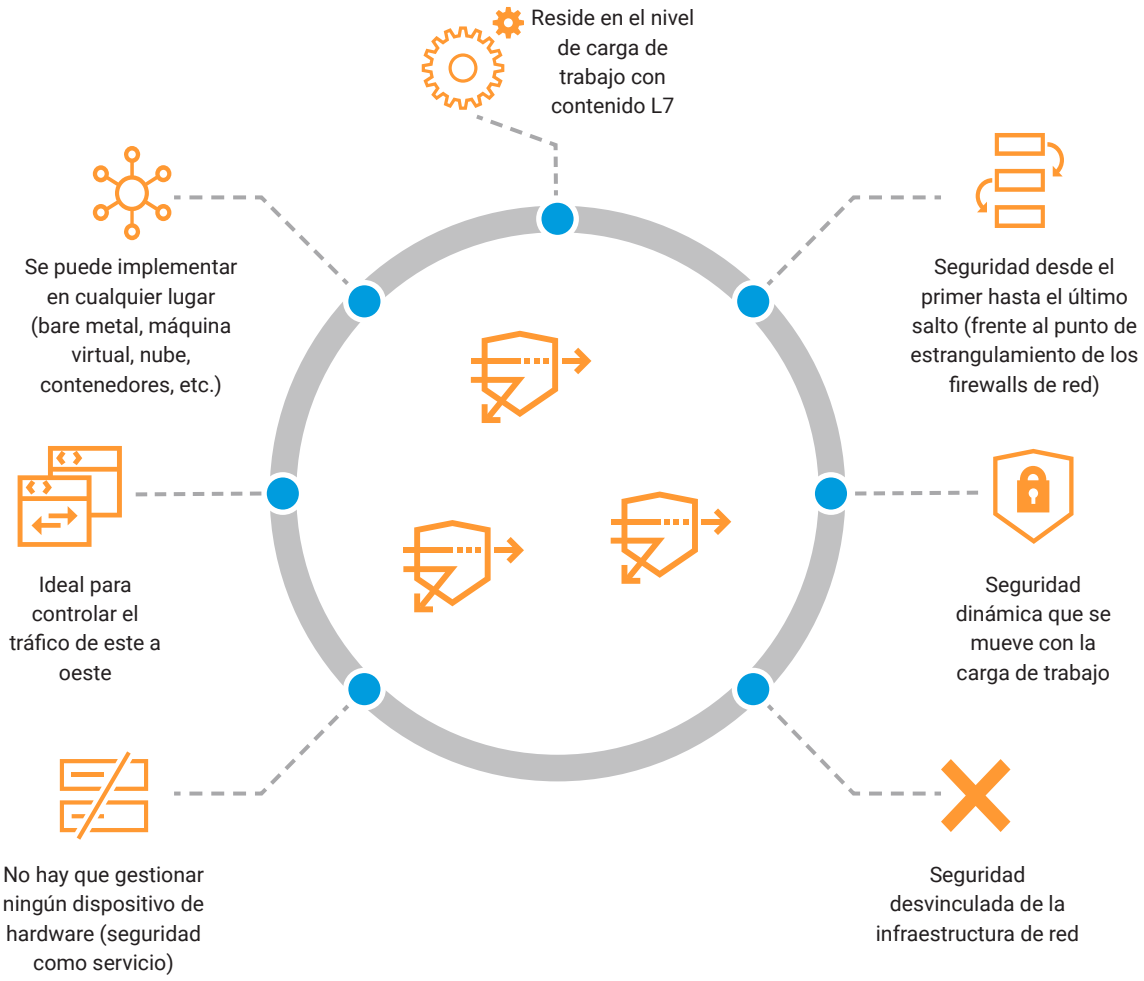
1. **Identificar y etiquetar activos:** un obstáculo importante que se encuentra durante el proceso tradicional de implementación de firewalls es la falta de visibilidad de los activos que se deben proteger. Guardicore Segmentation de Akamai incluye una función de visualización que permite a los operadores identificar y etiquetar todas las aplicaciones y sus dependencias que se ejecutan en la infraestructura de una organización.

2. **Visualizar y agrupar por etiquetas:** una vez conseguida la visibilidad contextual, los operadores pueden organizar las aplicaciones en grupos lógicos en función de sus etiquetas y asignar las dependencias entre ellas. Nuestro proceso de etiquetado es muy flexible y le permite agrupar las aplicaciones en función de su propio contexto empresarial, utilizando la terminología con la que ya está familiarizado.

3. **Crear políticas:** a continuación, los operadores pueden crear políticas de seguridad detalladas que dicten qué aplicaciones pueden comunicarse entre sí en función de los flujos reales observados. Las plantillas de políticas integradas para casos de uso comunes simplifican aún más el proceso. Ahora, las aplicaciones y los flujos de trabajo se segmentan eficazmente entre sí, independientemente de dónde se encuentren en el entorno.

La implementación de la segmentación basada en software es 10 o incluso 20 veces más rápida que la de los firewalls tradicionales; necesita mucho menos personal y no hay prácticamente tiempo de inactividad ni interrupciones. Además, una vez que haya comenzado el proceso de visualización y segmentación, podrá dividir su red más fácilmente o añadir diferentes políticas basadas en etiquetas, automatizar procesos, abordar incidentes de seguridad y realizar cambios rápidos en respuesta a los requisitos empresariales o normativos.

## Ventajas del firewall distribuido



# Caso real: Un procesador de alimentos de gran tamaño consigue un ahorro del 85 % en la segmentación

Un importante procesador de productos de carne de cerdo de EE. UU. necesitaba segmentar 45 aplicaciones con una media de cinco servidores por aplicación, implementados en dos ubicaciones. El objetivo de la empresa era eliminar sus redes planas con una interrupción mínima del servicio y establecer políticas lo antes posible.

Tras revisar las alternativas, la empresa eligió la solución de segmentación basada en software de Akamai. Aunque la velocidad y la simplicidad de la implementación influyeron en la decisión, el factor decisivo fue un análisis que mostraba un ahorro de más de 900 000 USD (o lo que es lo mismo, un ahorro del 85 %) en un periodo de tres años, en comparación con la protección de las VLAN con un proveedor líder de firewall. Específicamente:

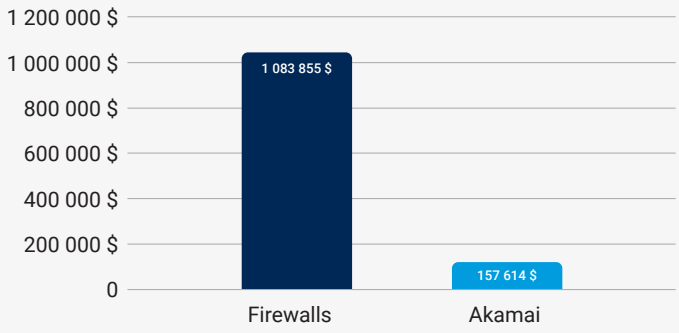
- El coste de la licencia de Guardicore Segmentation de Akamai fue un 55 % inferior al coste del hardware para una implementación de firewall para la VLAN.
- El coste de la mano de obra, basado en una estimación de 2000 USD a la semana, fue un 93 % inferior con Akamai que con un proyecto de VLAN de duración mucho mayor.

Además, Akamai pudo satisfacer la necesidad del cliente de implementar políticas rápidamente, protegiendo 45 aplicaciones sin interrupciones en tan solo seis semanas.

**TCO del firewall***
**1 083 855 $**

**TCO de Akamai***
**157 614 $**
-926 241 $

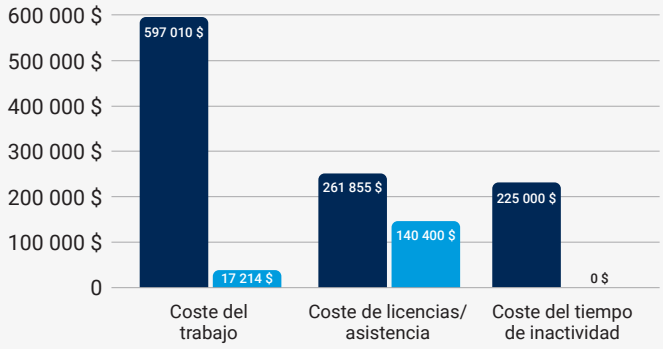
* Coste durante un periodo de 3 años




**Coste del trabajo de Akamai***
**17 214 $**
-579 796 $

**Coste de licencias/asistencia de Akamai***
**140 400 $**
-121 455 $

**Coste del tiempo de inactividad de Akamai***
**0 $**
-255 000 $



# El resultado

## La segmentación basada en software ofrece tres ventajas clave con respecto a los métodos tradicionales de firewall:

**Reducción de riesgos más eficaz:** al permitir una segmentación rápida de las aplicaciones en un nivel muy detallado, la segmentación basada en software reduce enormemente la superficie de ataque. Al aprovechar los principios de Zero Trust, que requieren la autenticación estricta de cualquier usuario, dispositivo o aplicación que intente acceder a un activo de la red, la segmentación basada en software impide el movimiento lateral de las amenazas dentro del centro de datos o el entorno de red. Esto mitiga aún más el impacto de las filtraciones de datos, ya que los atacantes no pueden tomar el control de ningún proceso, incluso si han logrado superar las defensas perimetrales. También permite a las empresas cumplir de forma más rápida con las normativas que exigen el aislamiento absoluto de las aplicaciones críticas y confidenciales del tráfico general de la red.

**Aceleración hacia una estrategia de seguridad óptima:** en resumen, la segmentación basada en software le protege mejor y de manera más rápida, lo que permite a los equipos de seguridad adaptarse al ritmo de implementación ágil de aplicaciones de DevOps y garantizar que todas las aplicaciones en producción estén protegidas correctamente. También permite que haya menos recursos (técnicos o humanos) involucrados en proyectos de segmentación durante largos periodos de tiempo. Los equipos pueden dedicar su tiempo a otras iniciativas importantes.

**Reducción del coste total de propiedad:** este es el resultado final real, y probablemente la ventaja más significativa desde una perspectiva empresarial. La segmentación basada en software se puede lograr con inversiones en bienes de equipo (CAPEX) mucho menores que las que se necesitan al adquirir dispositivos de firewall y otro hardware. También se traduce en una disminución de los gastos de explotación (OPEX) lo largo del tiempo en forma de ahorro en mano de obra y recursos para el mantenimiento y la gestión continuos.

Solo con estas medidas, en una comparación paralela entre la segmentación basada en software y una solución de firewall para 10 segmentos de aplicaciones, se demostró que el enfoque de Akamai ofrecía un ahorro total potencial del 85 %, que asciende a 1 millón de dólares aproximadamente.

Por supuesto, aunque se puede esperar un ahorro cuantificable en la primera semana de implementación, el coste total de propiedad (TCO) implica mucho más que el precio de compra inicial o los costes continuos. Aunque pueda no parecer del todo evidente, la segmentación basada en software produce ahorros sustanciales al eliminar prácticamente el tiempo de inactividad y la interrupción del servicio. Además, las empresas evitarán las pérdidas financieras derivadas de las filtraciones de datos, así como las sanciones por incumplimiento. Además, reducen en gran medida el riesgo de daños a la reputación y la pérdida de negocio a raíz de una filtración. Los equipos y los recursos de TI encargados de gestionar los cambios de firewall pueden reasignarse a proyectos más productivos. Todos estos factores de coste contribuyen a reducir el TCO y a mejorar los resultados para aquellos que optan por una solución de segmentación basada en software.

# Caso real: Un gran banco internacional se enfrenta a sanciones por incumplimiento y recurre a Guardicore Segmentation de Akamai

Tras una auditoría en la que se descubrió que había riesgos de seguridad en sus redes planas, y con la necesidad de enfrentarse a un conjunto de nuevas normativas que requieren una segmentación más estricta, una importante institución financiera europea inició un proyecto de segmentación mediante VLAN y reglas de firewall. El proyecto consumía mucho tiempo y requería el uso de varios equipos y partes interesadas, lo que provocó tiempos de inactividad en la producción y ambigüedades en relación con las políticas. Como resultado, el banco estaba pagando multas por no cumplir con las normativas, a lo que se sumaban los altos costes de la implementación.

El equipo de TI analizó rápidamente las soluciones alternativas y quedó impresionado con el nivel de automatización que Akamai podría aportar a sus operaciones de seguridad. El banco implementó Guardicore Segmentation de Akamai en varias regiones y tipos de infraestructuras de TI. El proyecto tardó menos de tres meses en implementarse, un tiempo 10 veces menor al que se había estimado inicialmente con los métodos de segmentación tradicionales. El banco no solo mejoró su estrategia de seguridad, sino que también satisfizo los requisitos de cumplimiento para más de 10 000 activos. La rápida implementación se tradujo en una reducción acelerada del riesgo, junto con un ahorro considerable de costes y recursos internos.

## Gran banco internacional

**Objetivo del proyecto:**

Separación de los procesos de desarrollo/producción/pruebas de aceptación (UAT)

**Alcance del proyecto:**

1. Restringir el tráfico entre entornos de producción y de no producción
2. Preparación para el acordonamiento de aplicaciones

## Segmentación heredada

- Progreso extremadamente lento
- Errores de auditorías, multas y errores de producción
- Interrupciones en la producción debido al tiempo de inactividad de las aplicaciones

**Tiempo:** 2 años con firewalls/VLAN

## Impacto de Akamai

- Segmentación de 10 000 activos que no cumplen con los estándares
- Sin tiempo de inactividad de las aplicaciones
- Implementación 10 veces más rápida
- Reducción del esfuerzo manual con DevOps

**Tiempo:** 6 meses
**Personas:** 3 arquitectos

# Conclusión: haga cuentas

Los firewalls no están obsoletos. No hay duda de que desempeñan un papel a la hora de proteger el perímetro de la red. Pero en los entornos dinámicos de hoy en día, el perímetro se ha convertido en un concepto algo amorfo. Para lograr el equilibrio necesario entre seguridad y agilidad, las organizaciones deben ser capaces de proteger sus activos digitales no solo en el nivel de red L4, sino en el nivel de aplicación L7, en concreto, en el nivel de procesos individuales. Y, para ello, los firewalls no solo son inadecuados, sino que, en realidad, obstaculizan el progreso. El intento de segmentación detallada con firewalls supone una enorme pérdida de recursos humanos, técnicos y financieros.

En comparación con los firewalls, se ha demostrado que la segmentación basada en software reduce en gran medida los riesgos de seguridad y el tiempo de amortización global con un TCO considerablemente inferior al de los enfoques tradicionales, lo que se traduce en un mayor retorno de la inversión (ROI) que se consigue más rápido. No se trata de una visión futurista: la segmentación basada en software ha llegado y está ofreciendo actualmente estas ventajas a organizaciones de una amplia gama de sectores.

# Un estudio sobre la evolución de TI

La historia de la tecnología se puede resumir en un flujo constante de mejoras, simplificación y reducción de costes. La segmentación no es una excepción.

Pensemos en el ejemplo del almacenamiento, que en apenas dos décadas evolucionó de los disquetes a las memorias USB, luego al almacenamiento conectado a la red (NAS) y, finalmente, al almacenamiento en la nube. O en el tiempo de ejecución de los recursos informáticos, que evolucionó de los servidores a las máquinas virtuales, del cloud computing a los contenedores y, en última instancia, a la informática sin servidor. En cada caso, los factores clave fueron el ahorro de costes y el aumento de la flexibilidad. Y, por supuesto, los rápidos avances tecnológicos hicieron posible la evolución.

La evolución de la segmentación de los dispositivos de firewall físicos a los firewalls distribuidos basados en software, desvinculados de la red, es similar. Y los factores subyacentes son los mismos: la reducción de costes y el aumento de la flexibilidad (lo que se traduce en velocidad de implementación), al tiempo que se mejora constantemente la eficacia de las políticas de seguridad con un enfoque más detallado compatible con el modelo Zero Trust.

Ha llegado el momento de que los equipos de redes y seguridad adopten un nuevo modelo de seguridad con segmentación, como claramente se ha hecho en otros sectores de la tecnología. El firewall físico para la segmentación lleva el mismo camino que el disquete.

## ¿Desea ver nuestra solución en acción?

## Solicite una demostración hoy mismo: akamai.com/guardicore