WHITE PAPER

Exploración de casos de uso clave de microsegmentación

Por John Grady, analista sénior de Enterprise Strategy Group

Enero de 2023

Este documento técnico de Enterprise Strategy Group fue encargado por Akamai y se distribuye bajo licencia de TechTarget, Inc.

Contenido

Resumen ejecutivo

El modelo Zero Trust se ha hecho omnipresente en el sector de la ciberseguridad. Sin embargo, la extensión de la iniciativa y los puntos de vista enfrentados en torno a lo que es más importante para la estrategia han generado confusión sobre dónde empezar y qué herramientas respaldan mejor este marco. Aunque no hay una sola ruta hacia Zero Trust, la estrategia depende en última instancia de garantizar que los recursos y las entidades solo puedan comunicarse entre sí cuando lo permita expresamente una política, lo que señala la importancia de la microsegmentación.

El uso de herramientas de microsegmentación es bastante limitado en la actualidad, pero se espera que aumente bastante como reconocimiento a la importancia fundamental de la microsegmentación para Zero Trust y su aplicabilidad a una variedad de casos de uso. Tanto si las organizaciones se están planteando el uso de Zero Trust para evitar amenazas, fomentar la eficiencia en la empresa o modernizar su enfoque de seguridad general, la microsegmentación puede ser de ayuda. En concreto, el enfoque de la microsegmentación basado en software y respaldado por inteligencia artificial de Akamai ofrece una visibilidad detallada y permite a las organizaciones evitar el movimiento lateral, detener los ataques de ransomware y aplicar los principios de Zero Trust de forma coherente en todo el entorno.

Tanto si las organizaciones se están planteando el uso de Zero Trust para evitar amenazas, fomentar la eficiencia en la empresa o modernizar su enfoque de seguridad general, la microsegmentación puede ser de ayuda.

El modelo Zero Trust gana impulso, pero es fundamental establecer prioridades claras

La complejidad de los entornos empresariales sigue aumentando debido al cambio de los recursos a la nube, el afianzamiento de los modelos de negocio digitales y una distribución de los usuarios cada vez mayor. Estos cambios dificultan por naturaleza el trabajo del equipo de ciberseguridad, ya que los atacantes buscan colarse por las brechas en las defensas para iniciar ataques de ransomware, robar información de los clientes o exfiltrar datos confidenciales de propiedad intelectual. Lamentablemente, los enfoques de seguridad tradicionales basados en controles perimetrales altamente permisivos ya no pueden hacer frente a estas realidades, lo que fuerza a los equipos de seguridad a volver a evaluar sus estrategias. Además, los ataques crecen en número y sofisticación, lo que hace imposible para los equipos de seguridad estar al tanto de todas las posibles amenazas, solucionarlas y aplicar parches.

Estos problemas han llevado a muchos al concepto de Zero Trust. Aunque no son nuevas, las estrategias Zero Trust han despertado un gran interés en las organizaciones como ruta hacia un enfoque de la ciberseguridad más dinámico, de privilegios mínimos y basado en riesgos. Un enfoque Zero Trust elimina la confianza implícita del entorno y valida continuamente cada interacción digital. Como resultado, dicho enfoque debería ofrecer a los equipos de seguridad una mayor confianza en que sus recursos, usuarios y dispositivos seguirán estando protegidos y disponibles. Sin embargo, la amplia aplicabilidad del modelo Zero Trust, sumada a los puntos de vista a veces en conflicto y las definiciones sobre lo que es, ha generado confusión y puede hacer que a las organizaciones les resulte difícil identificar un punto de inicio.

La evaluación de las prioridades de la organización y los resultados deseados puede ayudar a limitar el enfoque y determinar por dónde empezar en una iniciativa Zero Trust. Existen diversos impulsores empresariales que empujan a las organizaciones hacia el modelo Zero Trust (véase la figura 1).[1] Según el 51 % de los encuestados ,el objetivo más habitual es la modernización de la ciberseguridad. El gobierno federal de

La estrategia Zero Trust depende de garantizar que los recursos y las entidades solo puedan comunicarse entre sí cuando lo permita expresamente una política.

[1] Fuente: Enterprise Strategy Group Survey Results, *The State of Zero Trust Security Strategies,* mayo de 2021.

EE. UU. ha destacado esta mentalidad a través de las órdenes ejecutivas sobre ciberseguridad publicadas por la administración Biden, que incluían la arquitectura Zero Trust en sus requisitos de modernización. Aunque no están específicamente dirigidas al sector privado, estas órdenes pueden servir de orientación para los equipos de seguridad fuera del gobierno federal. Otros objetivos estratégicos de Zero Trust incluyen respaldar la transformación digital (35 %) y acelerar la adopción de la nube (34 %). Estos factores resaltan las expectativas que tienen muchas organizaciones de que el equipo de seguridad ayude al negocio, en lugar de simplemente proteger los activos. También son habituales objetivos tácticos como reducir el número de incidentes de seguridad (43 %), permitir un acceso remoto seguro (41 %), simplificar el cumplimiento (31 %) y prevenir la exfiltración de datos (30 %).

Figura 1. Impulsores de Zero Trust

Fuente: Enterprise Strategy Group, una división de TechTarget, Inc.

En algunos casos, limitar el enfoque inicial de un proyecto de Zero Trust puede ayudar sin duda al equipo de seguridad a identificar las herramientas necesarias para respaldar la estrategia. Por ejemplo, si el objetivo es mejorar el acceso remoto seguro para los empleados y terceros, muchos llegarán al acceso de red Zero Trust (ZTNA). En ese caso, también pueden entrar en juego las herramientas de gestión de identidades, como la autenticación de varios factores (MFA). Sin embargo, algunos impulsores pueden dejar los requisitos de tecnología abiertos a interpretación y, muchas organizaciones, incluso después de limitar el enfoque, se centran en varios objetivos. En estas situaciones, es importante que las organizaciones identifiquen las herramientas y prácticas que pueden respaldar una variedad de casos de uso y resultados.

Actualmente, la microsegmentación se infrautiliza al respaldar un modelo Zero Trust

Aunque no hay una sola ruta hacia Zero Trust, la estrategia depende en última instancia de garantizar que los recursos y las entidades solo puedan comunicarse entre sí cuando lo permita expresamente una política. Esto significa que un elemento clave para la filosofía Zero Trust de cualquier organización debería ser la capacidad de garantizar la segmentación adecuada de los activos para ayudar a limitar el impacto de los ataques que tengan éxito. Esto podría aplicarse a un objetivo general, como la modernización de la ciberseguridad, o un objetivo más centrado, como la prevención de la exfiltración de datos.

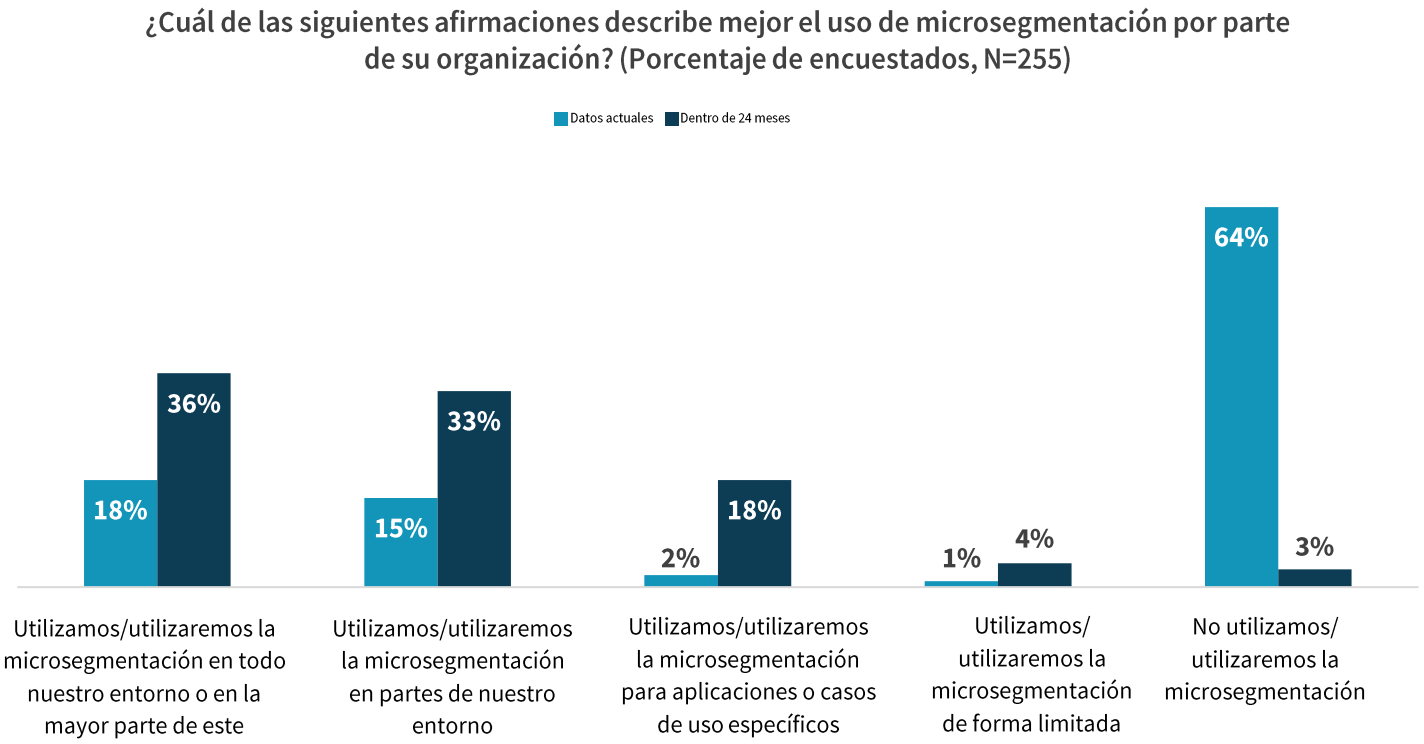
Sin embargo, en el entorno actual, la segmentación general no suele ser suficiente, y se requiere una segmentación más específica para proteger adecuadamente los activos de la empresa. Las arquitecturas de aplicaciones modernas a menudo dependen de cargas de trabajo distribuidas en varias instancias de servidor y, en algunos casos, varios entornos de nube. La segmentación de los recursos en función de una ubicación ha quedado obsoleta y no soluciona los desafíos a los que se enfrentan los equipos de seguridad en la actualidad.

Históricamente, las organizaciones han dudado un poco de la adopción de herramientas de microsegmentación. Una investigación de Enterprise Strategy Group (ESG) de TechTarget ha observado que el 28 % de las organizaciones creen que la microsegmentación es demasiado compleja. Sin embargo, es probable que esto se deba en gran parte a que los equipos de seguridad utilizan las herramientas de microsegmentación incorrectas. En concreto, la investigación de ESG ha determinado que el 55 % de las organizaciones afirman usar herramientas basadas en infraestructura para la microsegmentación, como firewalls, mientras que solo el 8 % utilizan herramientas basadas en host.[2] Los firewalls no pueden forzar la aplicación de las políticas específicas necesarias para que la microsegmentación tenga éxito. Además, estas herramientas ofrecen una visibilidad limitada de las cargas de trabajo de las aplicaciones y tienen dificultades para solucionar de manera coherente todos los aspectos del entorno en las ubicaciones locales y en la nube.

Esto ha provocado una infrautilización de la microsegmentación. A pesar de su importancia para el modelo Zero Trust, solo el 36 % de las organizaciones utilizan microsegmentación en la actualidad, de acuerdo con la investigación de ESG (véase la figura 2). La buena noticia es que muchas organizaciones reconocen que esta es una brecha importante en sus defensas. Como resultado, el 91 % de ellas tienen previsto usar la microsegmentación en el plazo de 24 meses.[3] En última instancia, la microsegmentación consolida y refuerza los beneficios clave del modelo Zero Trust al respaldar las redes físicas, virtuales y en la nube frente a las amenazas tanto externas como internas, y debería ser un componente principal de cualquier estrategia Zero Trust.

[2] Fuente: Enterprise Strategy Group Complete Survey Results, *Network Security Trends in Hybrid Cloud Environments,* diciembre de 2021.
[3] Ibid.

Figura 2. Adopción de la microsegmentación



Fuente: Enterprise Strategy Group, una división de TechTarget, Inc.

Casos de uso clave de microsegmentación

La microsegmentación puede aplicarse a una amplia variedad de casos de uso de Zero Trust, lo que es un motivo importante de que se enfatice más que nunca. Sin embargo, lo principal es que la microsegmentación ofrece un buen punto de partida en un viaje hacia el modelo Zero Trust, ya que puede proteger los activos más críticos de una organización, especialmente si la solución utilizada ofrece una visibilidad muy detallada de las relaciones entre cargas de trabajo y entidades. El desarrollo de una base de flujos de tráfico y dependencias es el fundamento de cualquier esfuerzo de Zero Trust como primer paso hacia la eliminación de la confianza implícita sin interrumpir el negocio. Este enfoque permite a los equipos de seguridad proteger rápidamente sus activos más críticos para ayudar a limitar el impacto en caso de filtración mientras está en curso una implementación de Zero Trust. Con esta garantía, los equipos de seguridad pueden centrar su atención en algunos de los otros casos de uso que respalda la microsegmentación.

Prevención de amenazas

Zero Trust es un marco de seguridad y el objetivo de la seguridad es proteger la organización de las ciberamenazas. Por eso, algunos de los principales casos de uso de la microsegmentación se centran en prevenir las amenazas y limitar su impacto en los recursos corporativos, en concreto los siguientes:

- Protección de los activos críticos. Los equipos de seguridad deben sopesar y equilibrar los riesgos cuando deciden dónde priorizar las protecciones. Las aplicaciones de alto valor que contienen información regulada de los clientes, de propiedad intelectual y confidencial deben recibir más atención y unos mayores controles de seguridad debido al posible impacto que puede tener que estos sistemas estén en riesgo. Con la microsegmentación, los equipos de seguridad pueden asegurarse de que estas aplicaciones y las cargas de trabajo de las que se componen estén totalmente separadas del resto de la infraestructura.
- Limitación del movimiento lateral. Un principio poco apreciado del modelo Zero Trust es trabajar con una mentalidad de "dar por sentado las filtraciones", asumiendo que los adversarios tienen acceso a la red corporativa. La proliferación de terminales tradicionales, servidores, recursos en la nube e, incluso, dispositivos inteligentes hace que las intrusiones sean inevitables. Como resultado, limitar el radio de explosión de un posible ataque a través de la microsegmentación puede acabar con la capacidad de los potenciales atacantes para moverse lateralmente por la red.

Protección contra el ransomware

La continua prevalencia del ransomware y el impacto de estos ataques han convertido el problema en uno de nivel ejecutivo, o incluso directivo. Aunque la preparación contra el ransomware requiere no solo una seguridad sólida, sino también unas buenas capacidades de protección de datos y respuesta a incidentes, la microsegmentación puede ayudar a las organizaciones a asegurarse de que están bien preparadas para hacer frente a un ataque. A menudo, los atacantes se dirigen a la información confidencial y los sistemas en el transcurso de un ataque, para después penetrar en el entorno y tomarse su tiempo para hacer un reconocimiento. Cuando se utiliza la microsegmentación para proteger los activos críticos y limitar el movimiento lateral, los atacantes tienen menos libertad para moverse por el entorno. Además, cuando se detecta un ataque de ransomware, una organización que utiliza microsegmentación puede desconectar rápidamente las vías de comunicación que utilizan los atacantes y aislar los servidores infectados para evitar que el ataque se siga propagando.

- Detección y respuesta a amenazas. En caso de ataque, el tiempo es esencial. Las herramientas de microsegmentación pueden ayudar a los equipos de seguridad a responder de forma rápida y eficaz, ya que pueden conocer rápidamente las posibles vías de ataque en función de las relaciones entre aplicaciones, bloquear los puertos que utilizan los atacantes durante un ataque y aislar rápidamente los sistemas afectados del resto de la red. También contienen el ataque en su punto de entrada inicial.

Promover la eficiencia en toda la empresa

Aunque el primer objetivo del equipo de seguridad es proteger el entorno, las directrices actuales también exigen que se haga de manera que no afecte a la eficiencia del negocio. Además, cuando los equipos de seguridad pueden ayudar realmente a habilitar a sus compañeros, la empresa está mejor preparada para ello. Esto puede tener varios significados, pero entre algunos de los más habituales se incluyen:

- Respaldar la adopción de la nube. El cambio a la nube no es ninguna novedad, pero las preocupaciones en torno a la seguridad siguen siendo primordiales para muchas organizaciones. Algunas de ellas se deben a la falta de familiaridad con los controles de seguridad nativos de las plataformas de infraestructura como servicio, y otras a las incoherencias de seguridad que pueden producirse en los entornos de nube híbrida. La microsegmentación aporta a las organizaciones una mayor confianza, ya que los controles se pueden utilizar en todos los aspectos del entorno y ofrecer una mejor coherencia de la seguridad en situaciones de nube híbrida.

- Permitir la modernización de las aplicaciones. Además del cambio a la nube, la adopción de arquitecturas de aplicaciones modernas, como contenedores, se sigue acelerando. Estos modelos permiten a los equipos de aplicaciones diseñar, crear e implementar las aplicaciones con mayor rapidez que nunca. Las herramientas que pueden garantizar la protección de estos recursos, y lo hacen sin limitar la velocidad de los desarrolladores, crean un impacto positivo en la empresa. Las herramientas de microsegmentación que ofrecen visibilidad de los flujos de tráfico en entornos de contenedores y aplican automáticamente políticas de segmentación al trasladar los contenedores a un entorno en línea o moverlos pueden ayudar a los equipos de desarrollo a garantizar que sus aplicaciones estén protegidas.

- Agilizar el cumplimiento. Los problemas normativos requieren cada vez más tiempo, presupuesto y atención de una organización. Aislar los riesgos de seguridad lo máximo posible para limitar los posibles problemas, como las filtraciones de privacidad de datos o la pérdida de información de identificación personal, puede hacer que el proceso resulte mucho menos pesado. La microsegmentación puede garantizar que los sistemas sujetos a obligaciones de cumplimiento se aíslen del resto del entorno, lo que puede aligerar la carga de los equipos de seguridad.

Segmentación Zero Trust

Uno de los aspectos más atractivos de la microsegmentación es que puede ofrecer un valor inmediato a las organizaciones cuando se centra en casos de uso muy específicos. La capacidad de empezar con listas de denegación, protección de aplicaciones críticas, segmentación del entorno y otras políticas menos complicadas que ofrecen un valor rápido con relativa facilidad puede ser atractiva para muchos. Pocas organizaciones, si es que hay alguna, implementan una estrategia de microsegmentación completa en toda la empresa a la vez. Pero, a medida que la microsegmentación se implemente más ampliamente en todo el entorno en el ámbito de una iniciativa Zero Trust, muchas organizaciones empezarán a adoptar la segmentación Zero Trust. Esta combina los casos de uso y los resultados positivos mencionados anteriormente, ya que las organizaciones pueden mantener una visibilidad completa y detallada de los flujos de tráfico, proteger sus activos más confidenciales, evitar el movimiento lateral y responder rápidamente a las amenazas, al tiempo que habilita mejor los negocios. Aunque no es el punto de partida de muchos proyectos de microsegmentación, debería verse como un objetivo al que aspirar con el tiempo.

El enfoque de Akamai para la microsegmentación

La solución Akamai Guardicore Segmentation es un enfoque de microsegmentación basado en software, diseñado para impedir que las amenazas se desplacen lateralmente en el entorno digital.

Es importante que las organizaciones tengan en cuenta que, aunque la microsegmentación es un aspecto importante del modelo Zero Trust, también hay otros componentes clave, que requieren otras tecnologías que ayuden a la detección y respuesta a amenazas, la identidad, la seguridad de los datos, etc. Evaluar, seleccionar y trabajar con proveedores de tecnología es un proceso metódico orientado a los detalles que puede marcar la diferencia entre cumplir los objetivos de ciberseguridad de la organización y algo que consume dinero, tiempo y recursos de mano de obra. Como resultado, considerar herramientas de microsegmentación que ofrezcan un amplio conjunto de integraciones y capacidades de uso compartido de señales puede ayudar a desarrollar una estrategia Zero Trust más allá de la microsegmentación, además de reducir la complejidad operativa.

Akamai, una empresa consolidada en infraestructuras de red, ha convertido la microsegmentación y el modelo Zero Trust en componentes fundamentales de su cartera de soluciones. El conocimiento que tiene la empresa de los requisitos de las infraestructuras empresariales tanto en entornos locales como en la nube incluye experiencia en detección y solución de los posibles desafíos de ciberseguridad.

Akamai Guardicore Segmentation es una solución de microsegmentación basada en software, diseñada para impedir que las amenazas se desplacen lateralmente en el entorno digital. Utiliza una visibilidad detallada para aplicar los principios de Zero Trust a nivel de red, lo que ayuda a las organizaciones a visualizar la actividad y el movimiento dentro del entorno físico o virtual. Su marco de segmentación basado en inteligencia artificial utiliza plantillas integradas para detectar y detener las incursiones, como el ransomware, los ataques basados en terminales y los ataques remotos orientados a los empleados. Se puede utilizar en una variedad de plataformas, que incluyen servidores bare metal, máquinas virtuales, contenedores, dispositivos IoT e instancias en la nube.

Akamai Guardicore Segmentation recopila una gran cantidad de información sobre la infraestructura subyacente de varias formas, como sensores basados en agente, recopilación de datos basada en la red, registros de flujos de nube privada virtual e integraciones que fomentan la funcionalidad sin agentes. La asignación dinámica ofrece a los administradores una vista integral de las actividades con una granularidad general. Gracias a la experiencia de Akamai en entornos de red empresariales, Akamai Guardicore Segmentation se ha diseñado para ofrecer escalabilidad empresarial y un rendimiento constante que permiten identificar y esquivar las fuentes de cuellos de botella de tráfico.

Conclusión

La microsegmentación no es una tecnología nueva. En realidad, puede que se haya adelantado a su tiempo. Sin embargo, no puede sobrestimarse la importancia de la microsegmentación para proteger los entornos multinube híbridos modernos y, específicamente, para poner en funcionamiento las estrategias Zero Trust. La microsegmentación ofrece la flexibilidad, agilidad y eficiencia necesarias para habilitar Zero Trust en un número de casos de uso esenciales para el negocio protegiéndolo todo, desde la infraestructura crítica y la propiedad intelectual, hasta las identidades y las credenciales. La experiencia de Akamai en infraestructura de red, segmentación y microsegmentación lo convierten en un candidato viable para ayudar a planificar, crear, implementar e incluso gestionar una infraestructura segura creada basándose en mentalidades y herramientas de microsegmentación.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group es una empresa de análisis, investigación y estrategia tecnológica integrada que ofrece servicios de inteligencia de mercado, conocimientos prácticos y contenidos de salida al mercado a la comunidad global de TI.

www.esg-global.com contact@esg-global.com 508.482.0188