Akamai

LIBRO ELECTRÓNICO

Estado de segmentación

Superar los obstáculos de implementación produce resultados transformadores

Sector del e-commerce

Tabla de contenido

Introducción

Los equipos de seguridad de TI, en especial los que se dedican a proteger a las organizaciones de e-commerce, nunca lo han tenido fácil. Dado que, por lo general, los presupuestos son más ajustados y los recursos de seguridad limitados, los expertos en protección empresarial siempre han tenido que hacer más con menos. Pero ahora, los equipos de seguridad se enfrentan a unos atacantes muy motivados y sofisticados, y gestionan infraestructuras cada vez más complejas, por lo que se ven sometidos a una presión mayor que nunca para mitigar los riesgos. Las organizaciones de e-commerce dependen de una presencia online eficaz para funcionar, por lo que una filtración efectuada con éxito, como un ataque de ransomware, podría causar un daño considerable, si no irreparable, a la reputación de la marca y a sus ingresos. Imagine el impacto perjudicial que tendría que las operaciones online, el procesamiento de pedidos o las líneas de producción se detuvieran porque los servidores y sistemas críticos dejaran de estar disponibles debido a un evento de cifrado masivo y una posible extorsión doble mediante exfiltración de datos.

Como muestran los resultados de este informe sobre el estado de la segmentación en el sector del e-commerce, estos ataques también están teniendo un mayor impacto, lo que aumenta la presión sobre los responsables a la hora de elegir las herramientas y soluciones adecuadas a fin de mantener a salvo los datos críticos, sin sacrificar el rendimiento ni añadir gastos operativos. Según el informe, el e-commerce es el sector industrial más atacado de todos los encuestados, lo que pone de relieve la necesidad urgente de prevenir, detectar y responder lo antes posible a los ataques de ransomware para limitar su impacto.

Los encuestados de las organizaciones del sector del e-commerce (con representación de todas las regiones, que abarcan EE. UU., LATAM, EMEA y APAC) coinciden de forma abrumadora en la eficacia de la segmentación a la hora de mantener protegidos los activos de TI. No obstante, el progreso general en su implementación en torno a las aplicaciones, servidores y sistemas empresariales esenciales es menor de lo esperado. Los principales obstáculos a los que se enfrentan las organizaciones de e-commerce son la falta de experiencia para implementar la segmentación de forma eficaz y los complejos requisitos de cumplimiento en materia de datos. Esto demuestra que los equipos no solo están teniendo dificultades para contratar o retener al talento necesario para su sector, sino que también están dedicando un tiempo muy valioso a intentar garantizar el cumplimiento de la legislación, con el consiguiente consumo de unos recursos ya de por sí limitados.

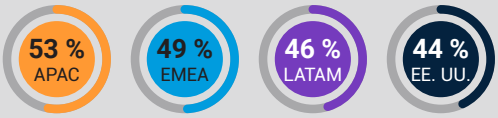
La buena noticia es que con perseverancia (y eligiendo la solución adecuada) se obtienen buenos resultados. Las empresas que lograron segmentar la mayoría de sus activos esenciales en seis áreas clave se beneficiaron del efecto transformador de la segmentación en sus capacidades defensivas, ya que les permitió mitigar y contener los ataques de ransomware 11 horas más rápido que las que solo tenían un activo segmentado. Imagine la diferencia que podrían suponer esas 11 horas no solo para su personal de respuesta a incidentes, sino también para sus clientes y para la reputación de su marca.

El progreso de la segmentación ha sido generalmente lento, pero los que han perseverado han logrado reducir enormemente su riesgo

La segmentación es buena. La microsegmentación es mejor.

La segmentación es un enfoque arquitectónico que divide una red en segmentos más pequeños con el fin de mejorar la seguridad y reducir el riesgo asociado a las redes planas. También se ha utilizado para ayudar a reducir el alcance, el coste y la dificultad de lograr y mantener el cumplimiento de la norma PCI en empresas que se apoyan en el e-commerce.

La microsegmentación es una técnica de seguridad definida por software que divide lógicamente una red en distintos segmentos de seguridad hasta el nivel de carga de trabajo o proceso individual (capa 7). De este modo, los controles de seguridad y la prestación de servicios se pueden definir para cada segmento único a un nivel más detallado que con los métodos de segmentación tradicionales, como las VLAN, las ACL y los firewalls internos, que solo ofrecen control de capa 4. Por eso, el 94 % de los encuestados del sector del e-commerce prefiere las soluciones de segmentación basadas en software a los métodos tradicionales.



Los responsables de la toma de decisiones de seguridad en APAC tienden más a afirmar que la segmentación de red es extremadamente importante para garantizar la seguridad de su organización que los de EMEA, LATAM o EE. UU. Los de LATAM tienden más a afirmar que la microsegmentación es la máxima prioridad (42 %) que sus homólogos de APAC (35 %), EE. UU. (34 %) y EMEA (26 %).

El e-commerce es el sector más afectado y los ataques de ransomware siguen en aumento

El número de ataques de ransomware a empresas de e-commerce (logrados y fallidos) ha sido, de media, 167 en los últimos 12 meses. Esto no solo sitúa al sector del e-commerce a la cabeza de la lista por el número medio de ataques de ransomware, sino que es casi el doble que el sector que le sigue más de cerca (la media del sector de la construcción es de 89 ataques).

Los ciberatacantes tienden más a dirigir sus ataques a organizaciones de e-commerce de EE. UU.: el número de ataques de ransomware en EE. UU. es el más alto de todas las regiones, con 312 ataques de media en los últimos 12 meses, frente a 119 en APAC, 91 en EMEA y 68 en LATAM (figura 1).

Número medio de ataques de ransomware en organizaciones de e-commerce en los últimos 12 meses por región

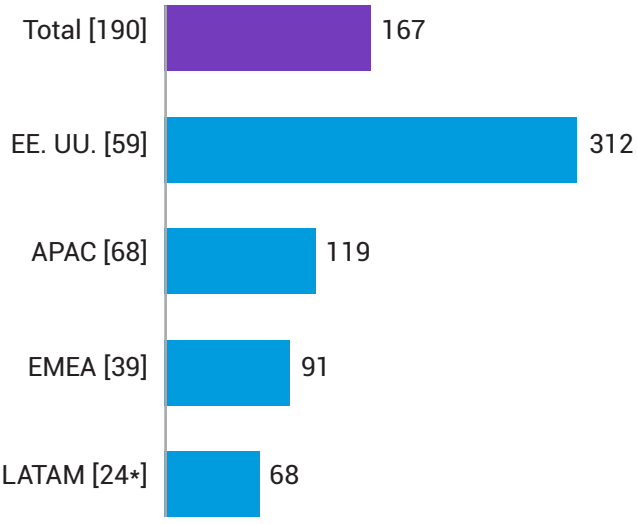


Fig. 1: ¿Cuántos ataques de ransomware se han dirigido a su organización en los últimos 12 meses (independientemente de si han tenido éxito)? El gráfico muestra el número medio de ataques durante los últimos 12 meses, dividido por región, en el sector del e-commerce.

* Atención: Tamaño reducido de la base menor a 30

Aunque los promedios en las regiones fuera de EE. UU. no podrían calificarse como bajos, lo parecen si se comparan con el número de ataques dirigidos a dicho país. Al tener la economía más grande del mundo, EE. UU. es el país más atacado por las bandas de ransomware, y los atacantes suelen poner sus miras en otros países occidentales y de habla inglesa. Las motivaciones geopolíticas también influyen en los países y sectores más afectados. Las organizaciones de e-commerce se encuentran a menudo en el punto de mira, ya que, tradicionalmente, tienen menos madurez en materia de seguridad que otros sectores, como el de los servicios financieros, lo que las convierte en un objetivo más fácil. A esta presión se añade el hecho de que un ataque de ransomware efectuado con éxito puede tener una gran repercusión pública, sobre todo si se produce durante periodos críticos de generación de ingresos como vacaciones, festivales, eventos deportivos, vuelta al colegio u otros momentos de máxima actividad comercial, por lo que es más probable (desde el punto de vista del atacante) que se realice un pago si se interrumpen las operaciones.

A pesar del elevado número de ataques de ransomware que sufren las organizaciones de e-commerce, no se está implementando la segmentación en la medida adecuada. De estas organizaciones, solo el 11 % ha segmentado más de dos áreas, cifra bastante homogénea en todas las regiones. Esto indica que es posible que muchas de estas organizaciones dispongan de recursos limitados más allá de lo necesario para hacer frente a los problemas y ataques a medida que surgen.

Los ataques de ransomware en el sector del e-commerce pueden tener un impacto enorme e inmediato en el negocio (figura 2). Nuestros encuestados mencionaron pérdidas financieras y daños a la reputación, dos factores que suben el listón de forma significativa para los equipos de seguridad de las organizaciones de e-commerce. También se ha observado un aumento en la proporción de encuestados que mencionan unas primas de seguros más elevadas. Esto demuestra el nivel de riesgo en que pueden incurrir las organizaciones de e-commerce, que, a menudo, almacenan datos personales sobre los usuarios y sus hábitos de compra, además de los riesgos relacionados con cuestiones logísticas de inventario o almacenamiento.

Las repercusiones pueden variar según la región: los encuestados de APAC tienden particularmente a destacar las pérdidas financieras, más de la mitad (51 %) frente a la media general del 42 %. Por otro lado, los encuestados de EE. UU. son los que más tienden a señalar el tiempo de inactividad de la red, casi la mitad (49 %) frente a la media general del 39 %. La repercusión más frecuente entre los encuestados de la UE es una moral más baja entre los empleados (41 %, frente al 36 % general).

También vemos el efecto de esta presión en términos de estrategia: el número de organizaciones de e-commerce que actualizan continuamente las estrategias o políticas de ciberseguridad ha aumentado del 3 % en 2021 al 13 % en 2023, no solo en respuesta al ransomware, sino también a una superficie de ataque en constante cambio. La creciente complejidad de la infraestructura a medida que las cargas de trabajo se migran a la nube es solo uno de los factores de riesgo que afectan a las estrategias y a los equipos de seguridad a diario.

Impacto del ransomware y los ciberataques en las organizaciones de e-commerce

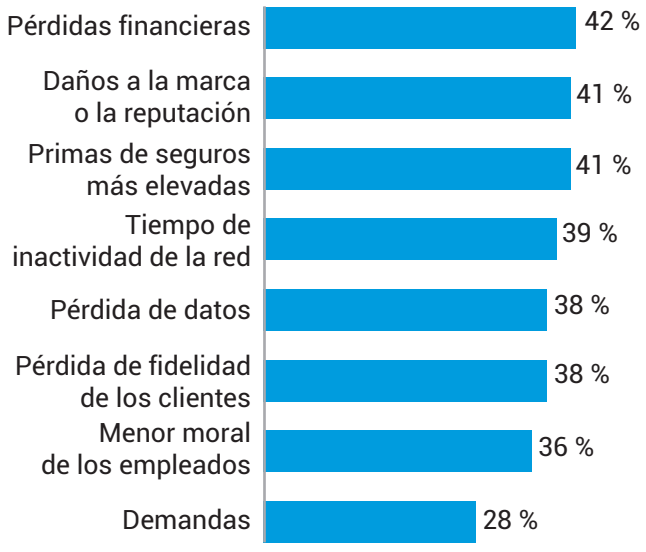


Fig. 2: En el pasado, tras detectarse un ataque de ransomware u otro tipo de ciberataque, ¿cuáles de las siguientes repercusiones ha tenido en su organización? El gráfico no muestra todas las opciones de respuesta y solo se incluyen datos del sector del e-commerce.

La segmentación se reconoce ampliamente como una parte importante de la arquitectura Zero Trust

Nuestros encuestados coinciden en que la segmentación es importante para garantizar la seguridad de sus organizaciones y, en particular, para hacer frente al malware.

Casi la mitad (48 %) afirma que la segmentación es extremadamente importante, y el 89 % considera que es fundamental para poner fin a los peores ataques.

La segmentación también se considera la piedra angular de un marco de seguridad Zero Trust, y la buena noticia para las organizaciones de e-commerce es que ya se han hecho avances en este ámbito. Todas están implementando o han implementado ya un marco de seguridad Zero Trust (100 %), aunque solo algo más de dos de cada cinco (42 %) afirman que su marco Zero Trust está totalmente completo y definido, y se considera maduro. Se trata, por tanto, de un área en la que la segmentación puede ayudar a las organizaciones de e-commerce a avanzar en su transición hacia Zero Trust. Según los datos, las organizaciones de EE. UU. han avanzado mucho más en la implementación de su marco de seguridad Zero Trust: tienden mucho más a afirmar que su implementación de Zero Trust está totalmente completa y definida (63 %) que las de LATAM (46 %), APAC (32 %) y EMEA (23 %).

Las razones para iniciar un proyecto de segmentación de red varían de manera considerable según la región, y "el interés del gobierno por la ciberseguridad" ocupa el primer lugar, con un 41 %. Tanto LATAM como los países de la UE mencionaron las vulnerabilidades de día cero de gran repercusión como los factores más importantes a la hora de adoptar una iniciativa de segmentación (un 44 % y un 42 %, respectivamente). No obstante, los encuestados de la UE tienden mucho más a afirmar que los proyectos se iniciaron porque se trata de una práctica recomendada (41 %, frente al 22 % general). Por otro lado, los encuestados de EE. UU. y APJ tienden más a afirmar que comenzaron debido al interés de su gobierno por la ciberseguridad (41 % y 39 % respectivamente, frente al 35 % general). Los encuestados de APJ también tienden más a afirmar que la migración de aplicaciones esenciales a la nube fue lo que les hizo iniciar sus proyectos (39 %, frente al 32 % general).

La mayoría de los encuestados de las organizaciones de e-commerce aspiran a ir más allá e implementar la microsegmentación, que protege las cargas de trabajo de las aplicaciones a un nivel detallado: el 92 % afirma que la microsegmentación es, al menos, una prioridad alta, y el 34 % la nombra como su prioridad principal. Además, todos (100 %) los responsables de la toma de decisiones de TI y seguridad de este sector afirman que ha sido adoptada por al menos una minoría, lo que indica que se trata de una solución ampliamente conocida por todos, aunque los avances hasta la fecha hayan sido limitados.

Los encuestados también señalan la necesidad de aumentar la visibilidad del entorno de TI de las organizaciones. Las empresas de LATAM afirman que necesitan "mucha más" visibilidad (63 %) de las comunicaciones de red, la ubicación de los activos, etc., para reducir los riesgos. Les siguen las de APAC (56 %), EE. UU. (46 %) y EMEA (44 %).

Las implementaciones son lentas, pero la perseverancia produce resultados transformadores

La cruda realidad es que, incluso con un consenso tan amplio de que la segmentación es la clave para detener los ataques protegiendo los activos de TI, su implementación ha sido lenta, quizá más de lo esperado.

Solo el 11 % de las organizaciones de e-commerce han segmentado más de dos áreas de negocio críticas, y el 48 % iniciaron por última vez un proyecto de segmentación de red hace dos o más años, lo que sugiere que las iniciativas se han estancado.

Las áreas críticas

- Aplicaciones esenciales
- Aplicaciones orientadas al público
- Controladores de dominio
- Terminales
- Servidores
- Activos/datos esenciales del negocio

La lentitud de las implementaciones se explica con mayor claridad si atendemos a los principales obstáculos a los que se enfrentan los encuestados: falta de competencias/experiencia para la segmentación (40 %), requisitos de cumplimiento (40 %) y aumento de los cuellos de botella que afectan al rendimiento (38 %), todos ellos asociados a los métodos de segmentación tradicionales. Cabe señalar que, aunque la falta de recursos o experiencia es la causa principal de retraso en los proyectos de segmentación, existe una escasez de talento en el ámbito de la ciberseguridad y, con la rapidez con la que se producen los cambios en este espacio, es lógico que existan tales carencias.

Las organizaciones de e-commerce de todas las regiones se enfrentan a desafíos: el 100 % de las organizaciones ubicadas en EE. UU. y LATAM afirma tener problemas a la hora de segmentar su red. Casi el mismo número afirma lo mismo en APAC (99 %) y EMEA (97 %).

Sin embargo, cuando se desglosan por región (figura 3), existe cierta variación en el tipo de obstáculos que tienden a encontrarse con más frecuencia. Esto demuestra que ciertos problemas (por ejemplo, la falta de competencias o el cumplimiento) pueden deberse tanto o más a cuestiones locales que a cuestiones globales.

Las organizaciones de EMEA y LATAM citan la falta de competencias y experiencia (54 % en ambos casos) como su mayor desafío a la hora de implementar la segmentación. Para las organizaciones de EE. UU., el mayor desafío es el aumento de los cuellos de botella que afectan al rendimiento (44 %), mientras que, en APAC, son los requisitos de cumplimiento (43 %).

	Problema que más se tiende a experimentar	Segundo y tercer problema que más se tienden a experimentar	
EE. UU. [59]	Aumento de los cuellos de botella que afectan al rendimiento (44 %)	Requisitos de cumplimiento/Disponibilidad limitada de herramientas adecuadas (ambos 41 %)	
LATAM [24*]	Falta de competencias/ experiencia para la segmentación (54 %)	Elevada complejidad del proceso (46 %)	Parte o todo el equipo que se utiliza es propiedad de la empresa/Parte o todo el equipo que se utiliza es antiguo (ambos 38 %)
EMEA [39]	Falta de competencias/ experiencia para la segmentación (54 %)	Disponibilidad limitada de herramientas adecuadas (41 %)	Requisitos de cumplimiento/Parte o todo el equipo que se utiliza es antiguo/ Costes muy elevados (todos 36 %)
APAC [67]	Requisitos de cumplimiento (43 %)	Disponibilidad limitada de herramientas adecuadas/Parte o todo el equipo que se utiliza es propiedad de la empresa/Aumento de los cuellos de botella que afectan al rendimiento (todos 37 %)	

Fig. 3: Si su organización ha tenido o prevé tener problemas al segmentar la red, ¿cuáles han sido o cree que serán? En el gráfico figuran las organizaciones que han segmentado su red en algún momento y se muestran las tres respuestas más seleccionadas por región. Solo se incluyen datos del sector del e-commerce.

* Atención: Tamaño reducido de la base menor a 30

Conclusiones clave: las empresas que han segmentado seis áreas de negocio críticas han reducido en gran medida el riesgo

Proteger y segmentar más activos en el entorno del e-commerce aumenta inmediatamente la seguridad de las organizaciones. Con la solución adecuada, los equipos de seguridad pueden identificar los ataques con mayor rapidez, mejorando así el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR) ante un incidente. Sin embargo, la infrasegmentación de los activos, que suele ser el resultado del uso de tecnologías de segmentación heredadas, puede crear brechas de seguridad y puntos ciegos, lo que deja a la organización en una posición más vulnerable o reactiva. Pero, cuando se hace bien, la segmentación mediante un enfoque definido por software puede ayudar a las organizaciones a gestionar mejor sus superficies de ataque para mantener protegidos los activos esenciales de una forma más eficaz y rentable.

Nuestros resultados muestran que, después de una filtración, la recuperación se produce 11 horas más rápido con la segmentación. Hablemos de cifras: en las organizaciones de e-commerce que han implementado la segmentación en seis áreas críticas, se tarda una media de 3 horas en detener por completo un ataque de ransomware. En aquellas con segmentación en un solo activo, se tarda una media de 14 horas.

Del mismo modo, la segmentación permite contener el movimiento lateral 11 horas más rápido. En aquellas organizaciones que han implementado la segmentación en seis áreas críticas, se tarda una media de tres horas en limitar significativamente el movimiento lateral de un ataque de ransomware. En aquellas con segmentación en un solo activo, se tarda una media de 14 horas.

Piense en la diferencia que supondrían esas 11 horas para su equipo, el daño a la marca y el coste incurrido en cualquiera de las situaciones.

Para detener un ataque

3 horas

El tiempo que se tarda, de media, en detener por completo un ataque de ransomware en aquellas organizaciones que han segmentado los seis activos empresariales. En aquellas que solo han segmentado un activo: **14 horas**

Para limitar el movimiento

3 horas

El tiempo que se tarda, de media, en limitar significativamente el movimiento lateral de un ataque de ransomware en aquellas organizaciones que han segmentado los seis activos empresariales. En aquellas que solo han segmentado un activo: **14 horas**

Cómo una solución de microsegmentación basada en software ayuda a resolver los desafíos

La microsegmentación no solo permite una segmentación más avanzada y detallada, sino que también facilita su implementación.

Las soluciones basadas en software, como Akamai Guardicore Segmentation, se pueden implementar rápidamente sin tener que realizar cambios físicos en la red. No es necesario volver a asignar la dirección IP a los nuevos segmentos ni preocuparse por dónde se encuentran físicamente los servidores y los dispositivos. Esto hace que la solución sea mucho más rápida y fácil de implementar que los enfoques basados en la infræstructura, como los firewalls y las VLAN. Además, dado que la solución no depende del sistema operativo subyacente para la aplicación de políticas, funciona a la perfección en todos los equipos y sistemas operativos: desde servidores bare metal hasta implementaciones multinube, desde tecnología heredada como Windows Server 2003 y Windows XP hasta los últimos sistemas TPV, dispositivos IoT y OT, e incluso tecnología contenedorizada. Esto significa que solo necesita gestionar una única solución con una interfaz para visualizar y controlar las conexiones realizadas por diferentes sistemas operativos y dispositivos en todo el entorno, independientemente de su ubicación física.

Cómo facilita la implementación

Akamai Guardicore Segmentation genera primero una imagen interactiva de todas las conexiones que se realizan en su entorno, lo cual es un componente fundamental para superar los principales obstáculos de la implementación. Además, Akamai ha incorporado en nuestra solución formas activas de superar los cuellos de botella que afectan al rendimiento y los requisitos de cumplimiento.

Los cuellos de botella que afectan al rendimiento no surgen necesariamente de una tensión técnica en el sistema provocada por una solución de segmentación, sino de los cuellos de botella derivados de la plantilla. El tiempo y el esfuerzo que supone tener que segmentar manualmente las áreas de negocio y, a continuación, solucionar manualmente los problemas de esas áreas cuando las cosas no funcionan puede ser tremendo. Akamai trabaja para resolver este problema (y el principal obstáculo para la implementación: la falta de experiencia) reduciendo el tiempo dedicado a la segmentación manual y ofreciendo asistencia técnica y servicios profesionales de primer nivel. Nuestros expertos en segmentación colaboran con usted durante todo el proceso de implementación para garantizar el cumplimiento de sus objetivos de segmentación en su exclusivo entorno de TI.

La asistencia para la implementación también proviene de la propia solución: sus recomendaciones de políticas y etiquetado basadas en IA y sus plantillas de políticas listas para usar para casos de uso comunes ahorran tiempo y clics, simplifican el flujo de trabajo, reducen el tiempo total de implementación de políticas y evitan configuraciones erróneas debido a errores humanos. Uno de nuestros clientes tenía un proyecto de segmentación detallada con una duración estimada de dos años y un presupuesto de más de 1 millón de dólares estadounidenses en costes totales; nosotros pudimos completarlo en tan solo seis semanas con un solo ingeniero, lo que redujo el coste total del proyecto en un 85 %. Esto demuestra que la segmentación detallada se puede implementar rápida y fácilmente, sin sufrir cuellos de botella.

Cómo facilita el cumplimiento

Muchos de nuestros clientes implementan nuestra solución para garantizar y certificar el cumplimiento de una serie de requisitos nacionales e internacionales, como PCI DSS, SWIFT, Sarbanes-Oxley, HIPAA, RGPD y muchos más. Estos requisitos de cumplimiento suelen exigir que los datos dentro del ámbito de aplicación, como el entorno de datos del titular de la tarjeta (CDE) para PCI DSS, estén separados y protegidos de otros sistemas de su entorno. Aunque hacer esto puede resultar extremadamente difícil si se utilizan firewalls y VLAN, nuestra solución basada en software le permite crear segmentos específicamente para los datos dentro del ámbito de aplicación y aplicar reglas de comunicación sobre lo que puede y no puede acceder a esos datos. Con nuestro mapa visual con vistas casi en tiempo real y con perspectiva histórica, puede certificar que cumple estos requisitos mostrando físicamente que los usuarios, sistemas y equipos no autorizados no están accediendo a los datos dentro del ámbito de aplicación.

Persevere con la solución y la asistencia adecuadas para transformar su estrategia de seguridad

La segmentación puede ser extremadamente difícil de implementar. Pero, como muestra este informe, quienes logran implementarla de forma eficaz ven reducciones masivas en su riesgo cibernético. Disponer de una segmentación adecuada limita el movimiento lateral y permite al personal de respuesta a incidentes reaccionar con mayor rapidez durante un ataque. Y después de una filtración, las tareas de recuperación están protegidas y tardan menos tiempo en completarse.

La elección de una solución definida por software diseñada para superar los desafíos comunes de la implementación de la segmentación tradicional, y la colaboración con expertos que están a su disposición a medida que avanza en el proceso, le sitúa en la mejor posición posible para transformar su estrategia de seguridad. Además, cuantas más áreas de negocio segmente, más avanzará en su arquitectura Zero Trust, lo que le permite reducir el riesgo al que se enfrenta actualmente.

Nuestro grupo de estudio

Para elaborar este informe, analizamos las respuestas de 190 encuestados que trabajan en el sector del e-commerce (59 en EE. UU., 39 en EMEA, 68 en APAC y 24 en LATAM).

En el estudio de investigación completo, entrevistamos a 1200 responsables de la toma de decisiones de TI y seguridad de 10 países para medir el progreso que las organizaciones han realizado en la protección de sus entornos, haciendo hincapié en el papel que desempeña la segmentación.

Se les hicieron preguntas sobre sus enfoques de seguridad de TI y sus estrategias de segmentación, así como sobre las amenazas a las que sus organizaciones se habían enfrentado en 2023. Estos datos y resultados nos ofrecen detalles sobre cómo han cambiado las estrategias de seguridad desde 2021 y en dónde se tienen que realizar mejoras todavía.

Se encuestó a personas de países de todo el mundo, como EE. UU., India, México, Brasil, Reino Unido, Francia, Alemania, China, Japón y Australia. Procedían de organizaciones con más de 1000 empleados, así como de una amplia gama de industrias y sectores.

Nota: Esta muestra difería ligeramente de la de 2021. Tamaño de las muestras: 2023: 1200 encuestados; 2021: 1000 encuestados. En 2023, también se entrevistó a personas procedentes de Australia, Japón y China. Los sectores diferían ligeramente de los de 2021. En 2023, nos centramos específicamente en el comercio digital como sector por derecho propio.

Obtenga más información sobre Akamai Guardicore Segmentation

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 cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y www.akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn. Publicado el 24 de mayo.

VansonBourne

Vanson Bourne es una empresa independiente especializada en investigaciones de mercado para el sector tecnológico. La reputación de solidez y credibilidad de sus análisis se basa en principios de investigación rigurosos y en su capacidad para recabar las opiniones de los responsables de la toma de decisiones sénior en los diferentes cargos técnicos y comerciales, en todos los sectores de actividad y en los principales mercados. Para obtener más información, visite www.vansonbourne.com.