Akamai

WHITE PAPER

Estado de la segmentación de 2023

Una vez superados los obstáculos de la implementación, llega la transformación

Tabla de contenido

Introducción

Los departamentos de seguridad de TI nunca lo han tenido fácil. Sin embargo, ahora los atacantes son cada vez más sofisticados, y combinan técnicas para plantear amenazas más grandes y frecuentes, lo que somete a los equipos de seguridad a mayor presión que nunca. Ninguna empresa puede operar sin una presencia online, y una filtración puede causar un daño considerable, si no irreparable, a la reputación y a los ingresos.

Como demuestran los resultados de este informe, estos ataques también están teniendo un mayor impacto, lo que aumenta la presión sobre los responsables de la seguridad para que elijan las soluciones adecuadas y mantengan todo el entorno protegido, sin sacrificar el rendimiento general ni la innovación.

Al actualizar los resultados de este informe, que comprenden el periodo que va desde 2021 hasta la actualidad, intentamos averiguar si la segmentación era la solución elegida y si era eficaz. Los 1200 encuestados coincidieron de forma abrumadora en la eficacia de la segmentación a la hora de mantener protegidos los activos, pero su progreso general en la implementación de la misma en torno a los activos y aplicaciones empresariales esenciales fue inferior a lo esperado. En todas las zonas geográficas, el principal obstáculo ha sido la falta de experiencia a la hora de implementar la segmentación, lo que sugiere que los equipos podrían dudar a la hora de embarcarse en un proyecto que podría afectar al rendimiento, especialmente dada la creciente complejidad de los entornos de TI.

La buena noticia es que la perseverancia tiene su recompensa. La segmentación demostró tener un efecto transformador en la defensa para aquellos que habían segmentado la mayoría de sus activos esenciales, ya que les permitió mitigar y contener el ransomware 11 horas más rápido que aquellos que solo tenían un activo segmentado. Imagine la diferencia que esas 11 horas marcan para su equipo, sus clientes, la reputación de su marca y los ingresos.

Los ataques de ransomware siguen aumentando, al igual que su impacto

El número de ataques de ransomware (logrados o fallidos) se ha duplicado en los últimos dos años, pasando de 43 de media en 2021 a 86 en 2023. Entre el primer trimestre de 2022 y el primer trimestre de 2023 se observó un aumento aún mayor gracias a los datos recopilados de los sitios de filtración de aproximadamente 90 grupos de ransomware diferentes. Publicado en agosto de 2023, el informe El ransomware en movimiento: Evolución de las técnicas de explotación y la búsqueda activa de día cero cita que el uso de vulnerabilidades de día cero y de primer día ha dado lugar a un aumento del 143 % en el total de víctimas de ransomware de todo el mundo.

No es de extrañar que las organizaciones estadounidenses sigan enfrentándose al mayor número de amenazas de ransomware (figura 1): los equipos de seguridad de TI y los responsables de la toma de decisiones de ese país han informado de una media de 115 ataques de ransomware en los últimos 12 meses, la mayor cantidad con respecto de los datos medidos en cualquier país.

Número medio de ataques de ransomware en los últimos 12 meses por país

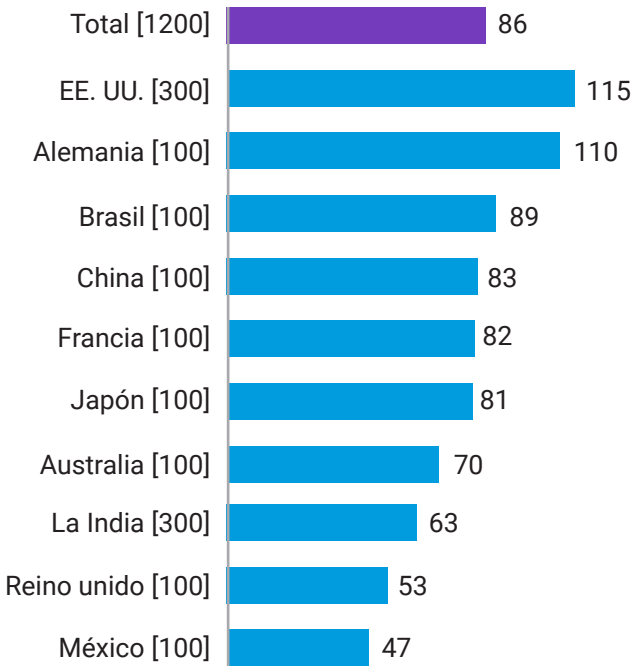

Fig. 1: ¿Cuántos ataques de ransomware se han dirigido a su organización en los últimos 12 meses (independientemente de si han tenido éxito o no)? [1200]; solo se muestra el número medio de ataques durante los últimos 12 meses; dividido por países.

Teniendo en cuenta que EE. UU. es uno de los dos países con menos probabilidades de haber implementado la segmentación en más de dos áreas de negocio críticas (figura 2), su clasificación superior en ataques de ransomware y su clasificación inferior en la implementación de la segmentación podrían estar relacionadas.

Por supuesto, el elevado número de ataques de ransomware en EE. UU. puede atribuirse a una serie de factores, incluidos la notoriedad de las filtraciones importantes como la que un grupo de ciberdelincuencia ruso cometió contra agencias federales en 2023 y la proliferación de dispositivos del Internet de las cosas (IoT) en Estados Unidos (2000 millones más que China, que ocupa el segundo lugar). El ransomware para el IoT (R4IoT) ataca los dispositivos vulnerables del IoT, como las cámaras IP, para obtener acceso inicial y, a continuación, se mueve lateralmente en una red de TI, aprovechando las prácticas de seguridad defectuosas para mantener como rehenes los procesos críticos.

Los ataques de ransomware no solo son más frecuentes en todo el mundo en 2023 que en 2021, sino que su impacto es mayor (figura 3), y nuestros encuestados indican un aumento del tiempo de inactividad de la red, la pérdida de datos y el daño a la reputación, lo que sube significativamente el listón para los equipos de seguridad. Vemos el efecto de esta presión también en términos de estrategia: el número de organizaciones que actualizan continuamente las estrategias o políticas de ciberseguridad ha aumentado del 5 % en 2021 al 13 % en 2023, no solo en respuesta al ransomware, sino también a una superficie de ataque en constante cambio. Los equipos de trabajo dispersos a nivel geográfico y la migración de aplicaciones y datos a la nube son solo dos factores que afectan diariamente a la estrategia de seguridad.

Organizaciones que han segmentado más de dos activos/áreas por país

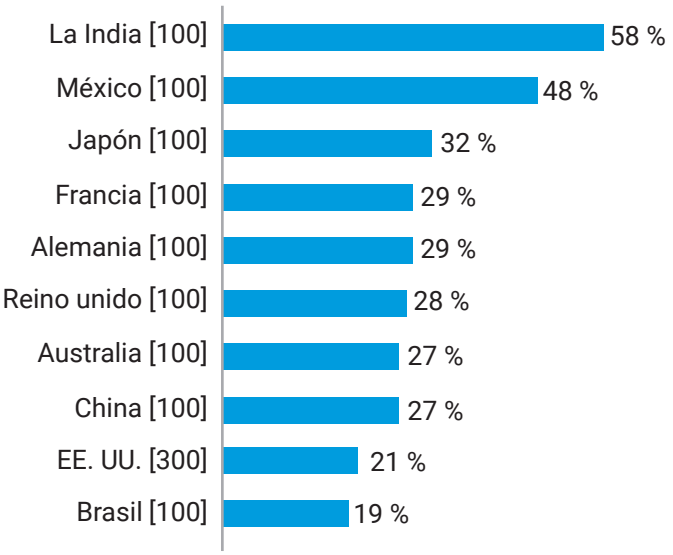

Fig. 2: Para cada una de las siguientes medidas de seguridad de TI, ¿qué activos protegen, si es que protegen alguno? [1200]; solo se muestran las respuestas para la medida de seguridad de la segmentación y los porcentajes de organizaciones que utilizan la segmentación para proteger los activos clave; dividido por países.

Impacto del ransomware y los ciberataques

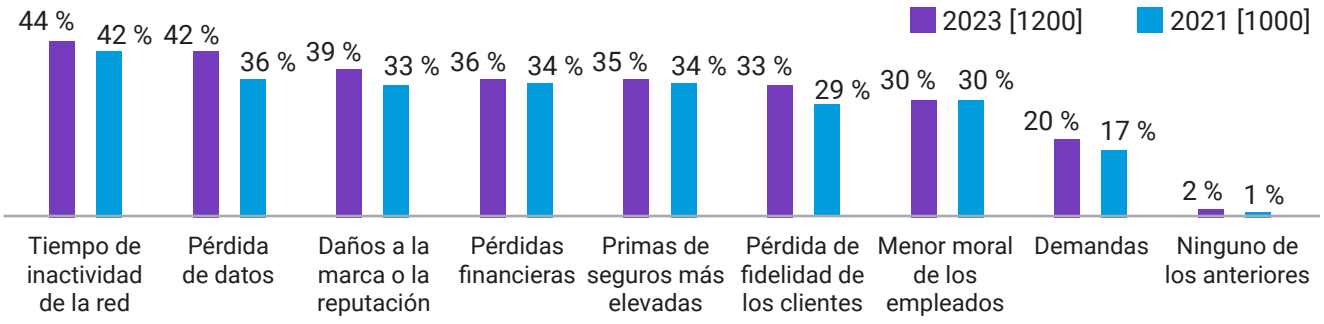

Fig. 3: En el pasado, cuando su organización ha detectado ataques de ransomware u otros ciberataques, ¿cuáles de los siguientes impactos ha tenido en su organización? [Tamaños básicos en el gráfico]; no se muestran todas las opciones de respuesta; dividido por datos históricos.

Conclusiones regionales

Es más probable que los ciberatacantes dirijan sus ataques a las organizaciones ubicadas en las regiones de América: el número total de ataques de ransomware es mayor en América, con 96 ataques de media en los últimos 12 meses, en comparación con 83 en países de EMEA y 75 en países de APAC.

La segmentación y la microsegmentación se consideran más importantes en países de APAC y América que en países de EMEA: los equipos de seguridad de TI y los responsables de la toma de decisiones de países de APAC (62 %) y América (60 %) son más propensos a afirmar que la segmentación de la red es extremadamente importante para garantizar la seguridad de su organización que los de los países de EMEA (53 %).

Los de los países de América tienen más probabilidades de afirmar que la microsegmentación es la prioridad principal (41 %) que sus homólogos de los países de APAC (35 %) o EMEA (23 %).

Es más probable que las organizaciones de los países de EMEA no hayan implementado la segmentación en absoluto: es mucho más probable que las organizaciones digan que no se han segmentado activos esenciales en países de EMEA (10 %) que en los de APAC (4 %) o América (1 %).

Las tasas de implementación más lentas, es decir, aquellas sin áreas segmentadas, se observaron en el Reino Unido (23 %), y los equipos antiguos se notificaron como el principal obstáculo (46 %).

Las organizaciones de los países de APAC son las que más segmentan: es más probable que las organizaciones de los países de APAC hayan segmentado más de dos activos esenciales (36 %) que las de los países de EMEA (29 %) o América (26 %).

Las organizaciones de todas las regiones se enfrentan a desafíos: el 97 % de las organizaciones ubicadas en América afirma tener problemas a la hora de segmentar su red. Una cantidad similar dijo lo mismo en países de EMEA (94%) y APAC (97%).

Las organizaciones de los países de EMEA y APAC citan la falta de competencias y experiencia (38 % y 43 % respectivamente) como su mayor obstáculo para la segmentación. Para las organizaciones de América, el mayor obstáculo es el aumento de los cuellos de botella que afectan al rendimiento (41 %).

Más organizaciones ubicadas en América consideran que sus marcos de seguridad Zero Trust son maduros: es más probable que las organizaciones de América declaren que su implementación de la arquitectura Zero Trust está totalmente completa y definida (49 %) que las de los países de APAC (35 %) o EMEA (33 %).

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

Nuestros encuestados están de acuerdo en que la segmentación es importante para garantizar que su organización esté segura, especialmente a la hora de abordar el malware. En todos los sectores, el 93 % cree que es fundamental para frustrar los ataques, cifra que aumenta hasta el 99 % para los encuestados de los sectores de fabricación y producción. Esto podría deberse al hecho de que esos sectores dependen en gran medida de una serie de terceros en su cadena de suministro, por lo que una interrupción puede tener efectos masivos en cascada en el negocio.

La segmentación también contribuye en gran medida a un marco Zero Trust. Al citar los motivos por los que su organización inició un proyecto de segmentación, la tercera respuesta más común fue la decisión avanzar en la arquitectura Zero Trust: casi todas las organizaciones que han segmentado están implementando o ya han implementado un marco de seguridad Zero Trust (99 %), aunque solo dos de cada cinco (40 %) afirman que su marco Zero Trust está totalmente definido y completo.

En todo el mundo, la mayoría de los encuestados aspiran a ir más allá e implementar la microsegmentación, que protege las cargas de trabajo de las aplicaciones en un nivel detallado: el 89 % afirma que la microsegmentación es, al menos, una prioridad alta, y el 34 % la nombra como su prioridad principal. Además, el 97 % de los equipos de seguridad de TI y los responsables de la toma de decisiones afirma que al menos una minoría de su sector la ha adoptado. Esta cifra se reduce al 80 % para los encuestados del sector público (excluida la atención médica), una diferencia que puede atribuirse a presupuestos más ajustados y a la infraestructura heredada, y que plantean mayores obstáculos para implementar la protección en el nivel de cargas de trabajo de la microsegmentación.

Microsegmentación

Porcentaje de los equipos de seguridad de TI y los responsables de la toma de decisiones que afirma que al menos una minoría de su sector ha adoptado la microsegmentación.

Sin embargo, el sector público se beneficiaría enormemente de la implementación de técnicas de seguridad avanzadas, como la microsegmentación. Debido a que los sistemas de este sector no están diseñados necesariamente para interactuar entre sí, carecen de interoperabilidad, lo que aumenta tanto las probabilidades de que se produzcan errores humanos como las probabilidades de que un ciberataque tenga éxito.

En el nivel de segmentación, el 15 % de los encuestados del sector público afirma no tener segmentación, aunque el 93 % reconoce su importancia. Esto representa el nivel de implementación más bajo por sector, siendo el mayor obstáculo los requisitos de conformidad (52 %).

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 el rendimiento y la seguridad.

La microsegmentación divide una red en segmentos en el nivel de carga de trabajo individual, de modo que los controles de seguridad y la prestación de servicios se pueden definir para cada segmento único.

Las implementaciones son lentas, pero la perseverancia produce resultados transformadores

La dura realidad es que, incluso con un acuerdo tan amplio respecto a que la segmentación es la clave para detener los ataques, la implementación de la segmentación ha sido lenta. Mucho más lenta de lo esperado. En 2023, solo el 30 % de las organizaciones se ha segmentado en más de dos áreas de negocio críticas (en comparación con el 25 % de 2021), mientras que el 44 % afirma haber iniciado un proyecto de segmentación de red hace dos años o más, lo que sugiere que las iniciativas se han estancado.

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 (39 %), aumento de los cuellos de botella que afectan al rendimiento (39 %) y requisitos de conformidad (38 %; figura 4). Casi todos los encuestados se han encontrado con los mismos retos en mayor o menor medida, independientemente de su sector o país. Cabe señalar que, aunque la falta de competencias 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.

A pesar del lento progreso, las tasas de segmentación están aumentando gradualmente en general. El porcentaje de organizaciones con aplicaciones/datos empresariales esenciales segmentados aumentó un 12 % y el de los servidores segmentados aumentó un 8 % entre 2021 y 2023.

Obstáculos detectados al segmentar la red

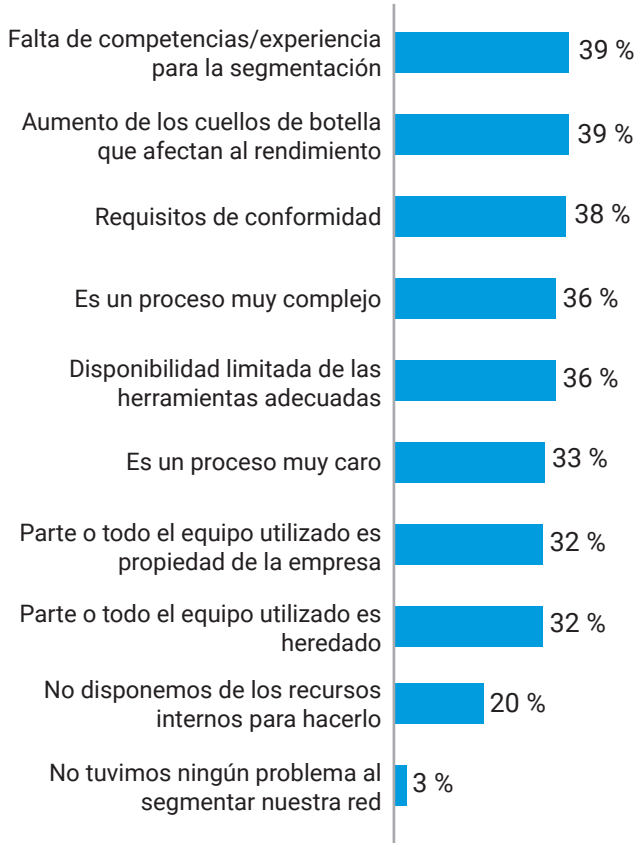

Fig. 4: ¿Qué problemas ha tenido su organización o prevé que tendrá al segmentar la red? [1187]; solo se muestra a aquellos que han segmentado su red en algún momento, no se muestran todas las opciones de respuesta.

Conclusión: la segmentación de seis áreas de negocio críticas reduce enormemente el riesgo

Proteger y segmentar más activos aumenta inmediatamente la seguridad de las organizaciones. Los equipos de seguridad tienen mayor capacidad para identificar los ataques y pueden responder de forma mucho más eficaz. Es probable que la implementación de estrategias de segmentación inmaduras o mal definidas solo aumente el riesgo de una organización, pero cuando se hace correctamente, la segmentación compensa claramente todos los obstáculos que hay que superar para implementarla.

Nuestros resultados muestran que después de una filtración, la recuperación se produce 11 horas más rápido con la segmentación. Hagamos los cálculos: para aquellos que han implementado la segmentación en seis áreas críticas, se tarda una media de cuatro horas en detener completamente un ataque de ransomware; para aquellos con segmentación en un solo activo, se necesitan 15 horas.

Del mismo modo, la segmentación permite limitar el movimiento lateral 11 horas más rápido. Para aquellos 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. Para aquellos con segmentación en un solo activo, se tarda una media de 14 horas.

Piense en la diferencia que suponen 11 horas para su equipo y para contener los costes y los daños a la marca en cualquier escenario.

Para detener un ataque

4 horas

El tiempo que se tarda, de media, en detener por completo un ataque de ransomware para aquellos que han segmentado los seis activos empresariales

Para aquellos que solo han segmentado un activo: **15 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 para aquellos que han segmentado los seis activos empresariales

Para aquellos 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 Guardicore Segmentation de Akamai, 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 infraestructura, como los firewalls y las VLAN. Además, dado que la solución utiliza su propio controlador en propiedad para la aplicación de políticas, funciona a la perfección en máquinas y sistemas operativos: desde servidores bare metal hasta implementaciones multinube, desde tecnología heredada como Windows Server 2003 hasta los últimos dispositivos IoT/OT y 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

La microsegmentación 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 abordar los cuellos de botella que afectan al rendimiento y los requisitos de conformidad.

Los cuellos de botella que afectan al rendimiento no surgen necesariamente de ningún motivo técnico en un sistema causado por una solución de segmentación, sino de los cuellos de botella derivados de la plantilla y que surgen por la necesidad de segmentar manualmente las áreas de negocio y, a continuación, solucionar manualmente esas áreas cuando las cosas se rompen. Akamai trabaja para resolver este problema (y para resolver el principal obstáculo para la implementación: la falta de experiencia) reduciendo la necesidad de realizar la segmentación manualmente 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 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 la conformidad

Muchos de nuestros clientes implementan nuestra solución para garantizar y certificar la conformidad con una serie de requisitos nacionales e internacionales, como PCI-DSS, SWIFT, Sarbanes-Oxley, HIPAA, RGPD y muchos más. Estos requisitos de conformidad suelen exigir que los datos dentro del ámbito de aplicación se separen 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 su conformidad con estos requisitos mostrando físicamente que los usuarios 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 de las amenazas y le permite reaccionar más rápido durante una filtración activa. Y después de una filtración, las tareas de recuperación están protegidas y tardan menos tiempo en completarse.

La elección de una solución diseñada para superar los desafíos comunes de la implementación de la segmentación, 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 y garantizar una defensa de primera línea contra futuros vectores de amenazas.

Nuestro grupo de estudio

Entrevistamos a 1200 responsables de la toma de decisiones de TI y seguridad de 10 países con el fin de medir el progreso que las organizaciones han realizado en la protección de sus entornos, centrándose 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 resultados nos proporcionan información útil sobre cómo han cambiado las estrategias de seguridad desde 2021 y en dónde se tienen que realizar mejoras todavía.

Entrevistamos a personal de seguridad y responsables de la toma de decisiones de EE. UU., México, Brasil, Reino Unido, Francia, Alemania, China, India, Japón y Australia. Todos ellos trabajaban para organizaciones con más de 1000 empleados de una amplia variedad de sectores.

Nota: Esta muestra difería ligeramente de la de 2021. Tamaños de la muestra — 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 Guardicore Segmentation de Akamai

Akamai protege la experiencia de sus clientes, 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, proteger las aplicaciones y las API, y proteger su infraestructura, 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 X, antes Twitter, y LinkedIn. Publicado el 23 de octubre.

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.