LIBRO ELECTRÓNICO

Superar los obstáculos de implementación para proteger los sistemas bancarios esenciales

Informe sobre el estado global de la segmentación

Tabla de contenido

Introducción

La protección del sector de los servicios financieros siempre ha planteado desafíos importantes y únicos para los equipos de seguridad de TI. Sin embargo, con unos atacantes cada vez más sofisticados y que combinan diferentes técnicas para lanzar amenazas más grandes y frecuentes, los equipos de seguridad de las instituciones de servicios financieros se ven sometidos a una mayor presión que nunca. Las operaciones de estas instituciones dependen de su presencia digital, por lo que 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 arriesgarse a exponer grandes cantidades de datos confidenciales.

Los encuestados de las instituciones de servicios financieros (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, pero su progreso general en la implementación de la misma en torno a los activos y aplicaciones empresariales esenciales es menor de lo esperado. El principal obstáculo al que se han enfrentado ha sido el aumento de los cuellos de botella, lo que sugiere que los equipos pueden haber estado reaccionando a las amenazas sin el tiempo o el apoyo necesarios para comprender y mitigar por completo el impacto en el rendimiento derivado de estos cambios.

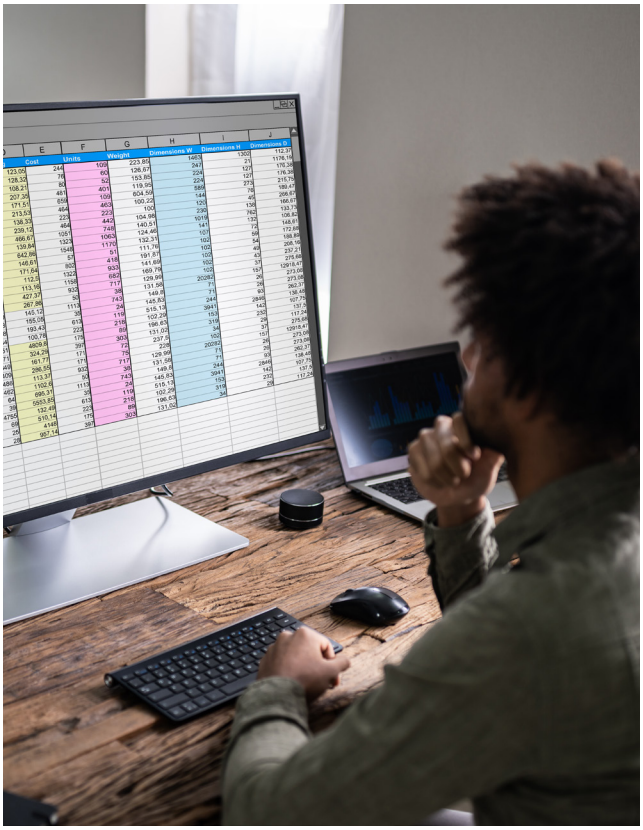
La buena noticia es que la perseverancia tiene su recompensa. La segmentación demostró tener un efecto transformador en la defensa para aquellos que habían segmentado la mayoría de sus activos esenciales, ya que les permitió mitigar y contener el ransomware 13 horas más rápido que aquellos que solo tenían un activo segmentado. Imagine la diferencia que esas 13 horas pueden suponer para su equipo, sus clientes y su reputación.

El resultado: 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 el rendimiento y la seguridad.

La microsegmentación es una técnica de seguridad que permite dividir lógicamente una red en distintos segmentos de seguridad hasta el nivel de carga de trabajo individual. De este modo, los controles de seguridad y la prestación de servicios se pueden definir para cada segmento único.



Los ataques de ransomware, y sus efectos, siguen aumentando

El número de ataques de ransomware a instituciones de servicios financieros (tanto logrados como fallidos) ha aumentado en casi un 50 % en los últimos dos años, pasando de 43 de media en 2021 a 62 en 2023. A pesar de las sólidas medidas de seguridad por las que es conocido el sector, estas cifras indican la existencia de una vulnerabilidad crítica que no se puede pasar por alto. Es evidente que el sector de los servicios financieros no es inmune a la amenaza del ransomware, por lo que bajar la guardia no es una opción.

De media, las instituciones de servicios financieros de la región APAC han sido objeto del mayor número de ataques de ransomware (73), mientras que la región LATAM ha sido la que menos ha recibido (48, figura 1).

Número medio de ataques de ransomware en el sector de los servicios financieros durante los últimos 12 meses por región

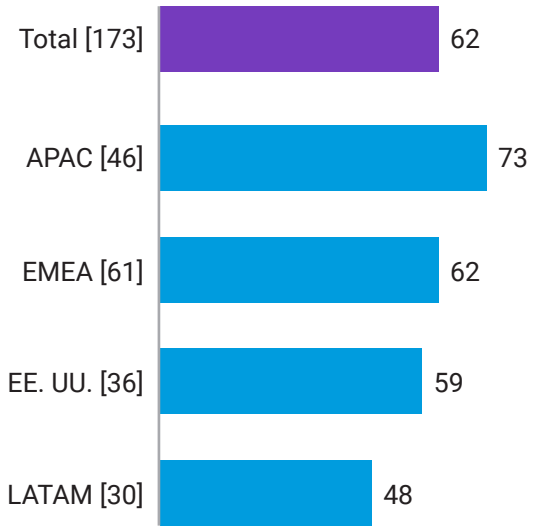


Fig. 1: ¿Cuántos ataques de ransomware se han dirigido a su organización en los últimos 12 meses (independientemente de si han tenido éxito)? El gráfico muestra el número medio de ataques durante los últimos 12 meses, dividido por región (se muestran las cifras base), en el sector de los servicios financieros.

Puesto que la mayoría de las instituciones de servicios financieros operan a escala global, el mayor número de ataques dirigidos en APAC podría deberse a que los hackers consideran que los ataques en esta región son más rentables. No obstante, esto no significa que las instituciones financieras de otras regiones sean más seguras, sino que pueden tender más a sufrir ataques laterales que se originen en otro lugar.

Además, los encuestados de la región LATAM son los que más tienden a indicar que su institución financiera ha segmentado más de dos activos, seguidos de los de APAC. Esto demuestra que las instituciones financieras de APAC pueden estar intentando aumentar la segmentación debido a la cantidad de ataques de ransomware que están recibiendo.

Organizaciones que han segmentado más de dos activos o áreas por región dentro del sector de los servicios financieros

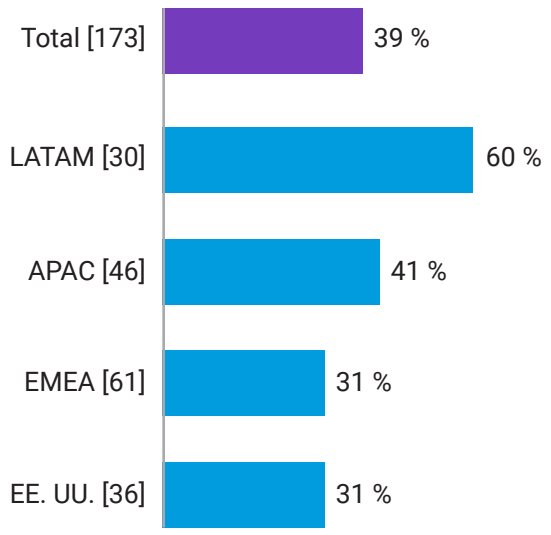


Fig. 2: Para cada una de las siguientes medidas de seguridad de TI, ¿qué activos protegen, si es que protegen alguno? El gráfico solo muestra las respuestas para la medida de seguridad de la segmentación y los porcentajes de organizaciones que utilizan la segmentación para proteger activos clave, divididos por región (se muestran las cifras base) y solo para el sector de los servicios financieros.

Los ataques de ransomware no solo son más frecuentes 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 y de la pérdida de datos, lo que sube significativamente el listón para los equipos de seguridad. También se ha observado un aumento en la proporción de encuestados que declaran primas de seguros más elevadas, sobre todo entre los encuestados de EE. UU. (56 %). Estos datos demuestran el nivel de riesgo en que pueden incurrir las instituciones financieras, puesto que a menudo no solo almacenan datos de personas, sino también de empresas.

También vemos el efecto de esta presión en términos de estrategia: el número de instituciones de servicios financieros que actualizan continuamente las estrategias o políticas de ciberseguridad ha aumentado del 3 % en 2021 al 18 % en 2023, no solo en respuesta al ransomware, sino también a una superficie de ataque en constante cambio. La dispersión de las aplicaciones y los equipos de trabajo a nivel geográfico, así como la migración de datos a la nube, son solo dos factores que afectan diariamente a la estrategia de seguridad.

Impacto del ransomware y los ciberataques en las instituciones de servicios financieros

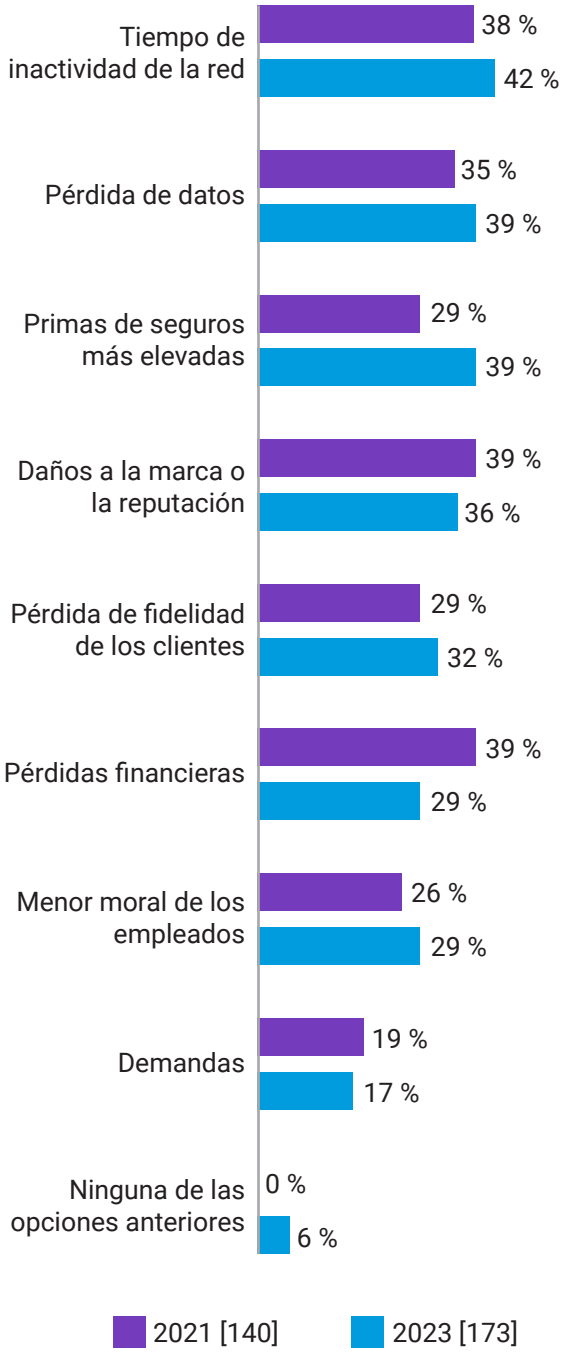


Fig. 3: En el pasado, tras detectarse ataques de ransomware u otro tipo de ciberataques, ¿cuáles de los siguientes impactos ha tenido en su organización? El gráfico muestra el tamaño de la base por año, dividido por datos históricos. Solo se muestran los datos del sector de los servicios financieros y no se incluyen todas las opciones de respuesta.

La segmentación es la piedra angular de Zero Trust

Nuestros encuestados del sector de los servicios financieros están de acuerdo en que la segmentación es importante para garantizar la seguridad de su organización, especialmente a la hora de combatir el malware: el 66 % afirma que es extremadamente importante y el 92 % considera que es fundamental para poner fin a los peores ataques.

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 respuesta más común fue querer desarrollar el modelo Zero Trust: casi todas las organizaciones que han segmentado están implementando o han implementado ya un marco de seguridad Zero Trust (99 %), aunque menos de la mitad (47 %) afirman que su marco Zero Trust está totalmente definido y completo y, por lo tanto, maduro.

La mayoría de los encuestados de las instituciones de servicios financieros aspiran a ir más allá e implementar la microsegmentación, que protege las cargas de trabajo de las aplicaciones a un nivel detallado: el 88 % afirma que la microsegmentación es al menos una prioridad alta, y el 39 % la nombra como su prioridad principal. Los encuestados de la región LATAM son los que más tienden a considerarla como una de las principales prioridades (50 %), mientras que los de EMEA son los que menos tienden a compartir esa opinión (31 %). El hecho de que los encuestados de LATAM tiendan más a considerar la microsegmentación como una de las principales prioridades se refleja en su rendimiento (figura 1), lo que demuestra que las organizaciones que dan prioridad a la microsegmentación pueden esperar recoger los frutos.

Además, el 99 % de los responsables de la toma de decisiones de TI en este sector afirma que la microsegmentación ha sido adoptada por al menos una minoría, lo que indica que se trata de una solución ampliamente conocida.

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, su implementación ha sido lenta. Mucho más lenta de lo esperado. En 2023, solo el 39 % de las instituciones de servicios financieros ha segmentado más de dos áreas de negocio críticas (en comparación con el 26 % de 2021), mientras que el 45 % 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: mayores cuellos de botella en el rendimiento (41 %), falta de competencias/experiencia para la segmentación (39 %) y requisitos de cumplimiento (35 %). Cabe señalar que, aunque la falta de competencias o recursos es una de las causas principales de retrasos 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.

Sin embargo, cuando se desglosan por región (véase la figura 4), existe cierta variación en el tipo de obstáculos que tienden a encontrarse con mayor frecuencia. Esto demuestra que ciertos problemas pueden deberse en igual o incluso mayor medida a las condiciones locales (por ejemplo, la falta de competencias en EE. UU. o los problemas de cumplimiento en APAC) que a cuestiones globales.

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 17 %, y el de los servidores segmentados también aumentó un 17 % entre 2021 y 2023. Estos aumentos superan la media general observada en todos los sectores (12 y 8 %, respectivamente), lo que demuestra que los departamentos de TI de las instituciones de servicios financieros son algo mejores a la hora de superar obstáculos que los del resto de sectores. Esto podría deberse a que los estrictos requisitos de cumplimiento mencionados anteriormente requieren un nivel de seguridad cada vez mayor. También podría estar relacionado con las primas de seguros más elevadas a las que se han estado enfrentando las instituciones de servicios financieros: es posible que las aseguradoras estén imponiendo a sus clientes el requisito de abordar determinados problemas lo más rápido posible.

Obstáculos encontrados al segmentar la red en el sector de los servicios financieros: tres principales por región

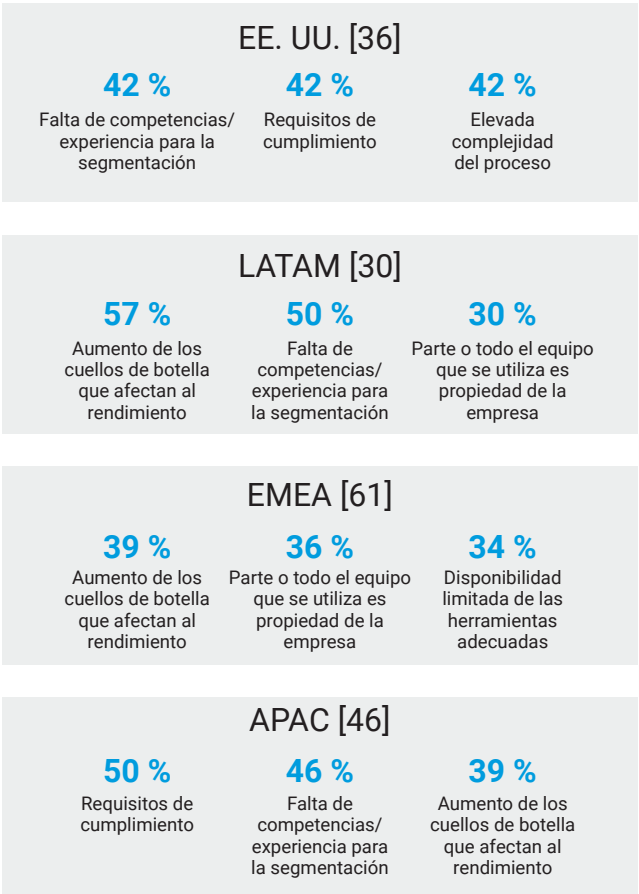


Fig. 4: ¿Qué problemas ha tenido su organización o prevé que tendrá al segmentar la red? El gráfico muestra el tamaño de la base por región. La pregunta solo se hizo a los encuestados que habían segmentado su red en algún momento. Solo se muestran las tres respuestas principales por región y solo se incluyen datos del sector de los servicios financieros.

Las empresas que han segmentado seis áreas de negocio críticas han reducido en gran medida el riesgo

Proteger y segmentar más activos aumenta inmediatamente la seguridad de las instituciones financieras. Los equipos de seguridad tienen mayor capacidad para identificar los ataques y pueden responder de forma mucho más eficaz. La implementación de estrategias de segmentación inmaduras o mal definidas solo aumenta la vulnerabilidad; no obstante, si se realiza correctamente, la segmentación mejora la ciberresiliencia y evita que los ciberataques provoquen fallos empresariales importantes al impedir que el ransomware y las filtraciones se propaguen a sistemas y datos críticos.

Nuestros resultados muestran que, después de una filtración, la recuperación se produce 13 horas más rápido con la segmentación.

Hablemos de cifras: en las instituciones de servicios financieros que han implementado la segmentación en seis áreas esenciales, 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 16 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 11-13 horas para su equipo, el daño a la marca y el coste incurrido según la situación.

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: **16 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

Las instituciones financieras buscan mejorar la escalabilidad, sacar partido a las inversiones existentes, optimizar los costes y mejorar la agilidad y la flexibilidad migrando las cargas de trabajo a la nube, a menudo integrando los centros de datos locales con nubes privadas o públicas. Las soluciones de segmentación definida por software, como Akamai Guardicore Segmentation, han surgido como un enfoque flexible, optimizado y rentable de la seguridad a nivel de aplicación que acelera drásticamente la implementación, simplifica el mantenimiento y mitiga eficazmente las amenazas. Al ser más rápida y fácil de implementar que los enfoques basados en infraestructura, como firewalls y VLAN, esta solución permite a las instituciones financieras ampliar la escala de la seguridad al tiempo que satisfacen las crecientes exigencias empresariales y proporcionan una experiencia de cliente innovadora con tecnologías de vanguardia. Además, se integra a la perfección en distintos sistemas y entornos para proporcionar una gestión y un control centralizados, desde servidores bare metal hasta implementaciones multinube y sistemas heredados. Por tanto, ofrece una solución unificada para visualizar y controlar las conexiones de todo el entorno, independientemente de la 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 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 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 los problemas de esas áreas cuando las cosas no funcionan. 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 el cumplimiento

Muchos de nuestros clientes implementan nuestra solución para garantizar y certificar la conformidad con una serie de requisitos de cumplimiento, como PCI-DSS, SWIFT, Sarbanes-Oxley, RGPD, DORA y muchos más. Estos requisitos normativos 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 que cumple 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 compleja. Sin embargo, como se muestra en este informe, quienes consiguen implementarla de forma eficaz disfrutan de una seguridad de red mejorada, un mayor rendimiento de la red, un mejor cumplimiento y una gestión de la red simplificada. Disponer de una segmentación adecuada limita el movimiento lateral de las amenazas y le permite reaccionar más rápido durante una filtración. 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.

Conclusiones regionales

La segmentación y la microsegmentación son más importantes en las regiones EMEA y EE. UU. que en LATAM: los responsables de la toma de decisiones de seguridad de TI de EMEA (70 %) y EE. UU. (60 %) tienden más a afirmar que la segmentación de la red es extremadamente importante para garantizar la seguridad de su organización que los de LATAM (57 %).

Las organizaciones de la región LATAM tienden más a señalar la segmentación como su principal prioridad: (50 %) a diferencia de sus homólogos en EE. UU. (42 %), APAC (41 %) y EMEA (31 %).

Las organizaciones de EMEA tienden más a no haber implementado la segmentación en absoluto: las instituciones de EMEA tienden más a afirmar que no se ha segmentado ningún activo esencial (7 %); el resto de regiones han implementado en cierto grado la segmentación.

Las organizaciones de la región LATAM son las que más tienden a haber hecho el mayor avance con la segmentación: las organizaciones de servicios financieros de LATAM tienden más a haber segmentado más de dos activos esenciales (60 %) que las de las regiones APAC (41 %), EMEA (31 %) y EE. UU. (31 %).

Las organizaciones de todas las regiones se enfrentan a desafíos: El 98 % de las instituciones de APAC afirma tener problemas a la hora de segmentar su red, y una cantidad similar afirmó lo mismo en EE. UU. (97 %). En EMEA y LATAM, el porcentaje es algo menor (89 y 87 %, respectivamente).

Las instituciones de servicios financieros en LATAM cuentan con bastante más experiencia en la implementación del marco de seguridad Zero Trust: las organizaciones de LATAM tienden más a declarar que su implementación de la arquitectura Zero Trust está totalmente completa y definida (57 %) que las de EMEA (48 %), EE. UU. (47 %) y APAC (41 %).

Nuestro grupo de estudio

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.

Para elaborar este informe, analizamos las respuestas de 173 (2023) y 140 (2021) participantes que trabajan en el sector de los servicios financieros.

Obtenga más información sobre Akamai Guardicore Segmentation

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. 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. Puede obtener más información sobre las soluciones de Akamai para las instituciones financieras en akamai.com/finserv y akamai.com/blog. También puede seguir a Akamai Technologies en X, anteriormente conocido como Twitter, y en 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.