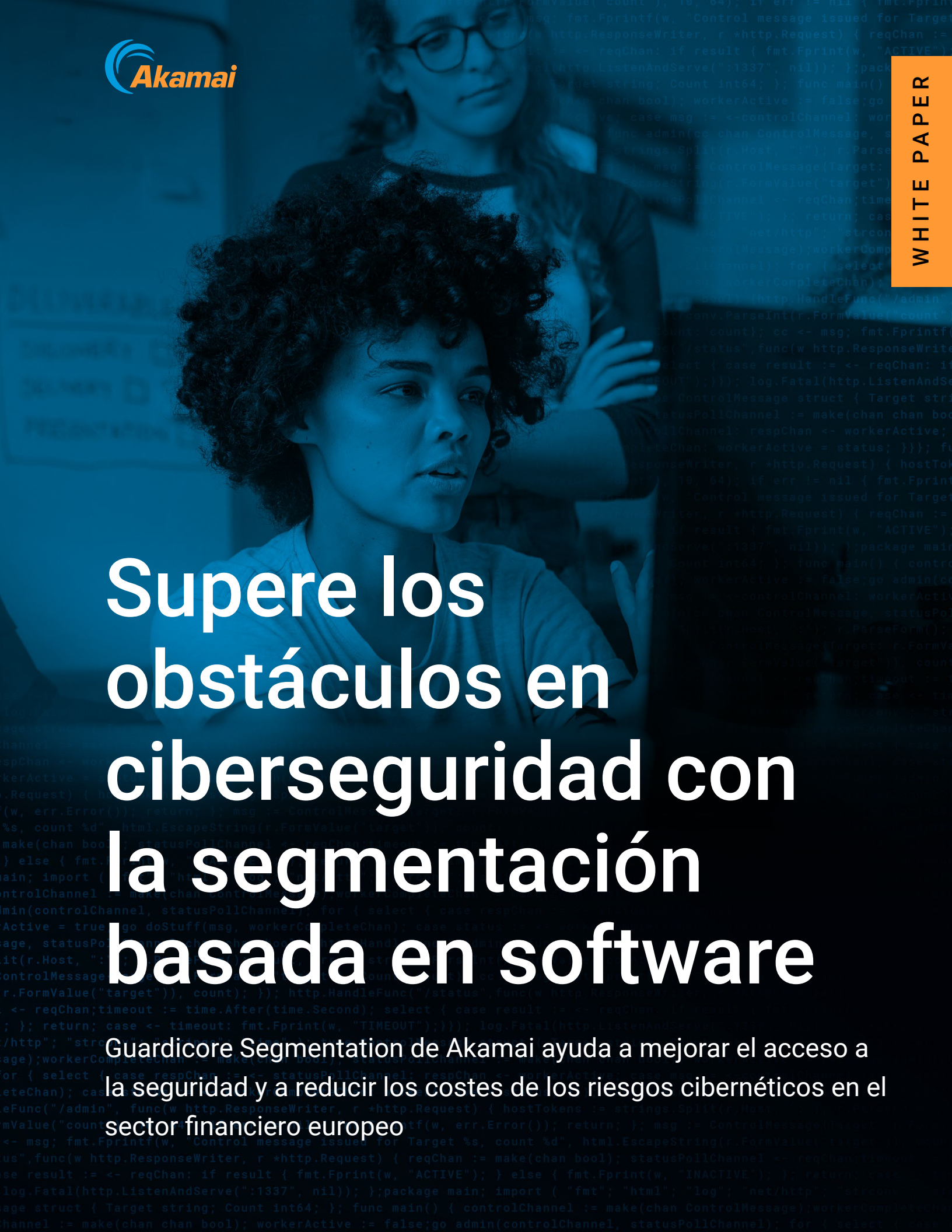
Akamai

WHITE PAPER



Supere los obstáculos en ciberseguridad con la segmentación basada en software

Guardicore Segmentation de Akamai ayuda a mejorar el acceso a la seguridad y a reducir los costes de los riesgos cibernéticos en el sector financiero europeo

Descripción general

El sector financiero es una parte crucial de la economía de la Unión Europea; algunos Gobiernos y reguladores europeos consideran que los sistemas financieros son una infraestructura crítica. Los productos y servicios que proporcionan las organizaciones de servicios financieros dependen en gran medida de los sistemas de TI de alta disponibilidad y del acceso oportuno a la información mediante múltiples canales y partes.

Sin embargo, los ataques de ransomware y criptominería han demostrado la rapidez con la que los atacantes pueden desestabilizar esta infraestructura crítica durante días o incluso semanas, posiblemente propagándose a terceros y homólogos conectados.

Es vital que las instituciones financieras europeas adopten capacidades digitales de vanguardia en la búsqueda de la competitividad y la captación y fidelización de clientes. Con todo, los requisitos normativos en aumento en cuanto respecta a los controles de seguridad y la elaboración de informes están ralentizando significativamente la velocidad de adopción de la nube. El Reglamento General de Protección de Datos (RGPD) de la Unión Europea, por ejemplo, puede imponer multas de hasta el 4 % de la facturación global a aquellas empresas que no protejan a sus clientes.[1]

Además, normativas recientes como el programa de seguridad de clientes de la sociedad para las telecomunicaciones financieras interbancarias internacionales (SWIFT CSP) y las expectativas de supervisión de la ciberresiliencia del Banco Central Europeo (CROE del BCE) exigen específicamente una segmentación más detallada de la red.

Los enfoques tradicionales de segmentación y sus procedimientos manuales asociados no son un enfoque viable para seguir el ritmo de la innovación tecnológica, el aumento de los riesgos de seguridad y las normativas cada vez más estrictas.

Las organizaciones no solo deben adoptar nuevas herramientas, sino que también han de cambiar radicalmente sus procesos de seguridad y segmentación para posibilitar una mayor sencillez, transparencia y automatización.

En este documento se tratan los siguientes temas:

- Los principales retos en materia de ciberseguridad a los que se enfrenta el sector financiero europeo hoy en día
- Cómo los bancos y las instituciones financieras pueden abordar estos riesgos con un enfoque rentable y directo de la segmentación
- Cómo el enfoque de Guardicore Segmentation de Akamai ayuda a las empresas a simplificar sus procesos de seguridad, reduciendo significativamente los costes y acelerando el cumplimiento

La ciberseguridad actual es compleja y su gestión es costosa

Aunque las instituciones financieras y los bancos europeos están comprometidos con la seguridad organizativa y la protección de los datos de los clientes, evolucionar en pro de una estrategia de seguridad más sólida no es un proceso fácil en el mundo actual de riesgos en constante evolución, necesidades de acceso de terceros y requisitos de cumplimiento.

El aumento del riesgo cibernético incrementa las pérdidas monetarias

Los riesgos asociados con los delitos cibernéticos son particularmente graves para las instituciones financieras. El sector financiero ya es el segundo que más invierte en combatir ataques, con un coste medio de 5,72 millones de USD por filtración de datos.[2]

Lograr una estrategia de seguridad sólida también es caro. La aplicación de controles de seguridad para proteger no solo varias plataformas, sino también el acceso de terceros, que es fundamental para la prestación de servicios empresariales, es una tarea compleja. Esto conlleva un aumento significativo de los costes de infraestructura y mano de obra.

El cumplimiento normativo es más costoso

Las empresas de servicios financieros de Europa han observado un aumento espectacular en el coste, el tiempo y los recursos generales necesarios para garantizar el cumplimiento. Aunque las normativas ayudan a asegurar la estabilidad del sector financiero, la introducción continua de nuevas normas de ciberseguridad está afectando a la rentabilidad y al crecimiento al ralentizar la transformación digital y requerir inversiones sustanciales.

El aumento de la presión para endurecer las políticas comenzó con el RGPD, seguido de la Directiva sobre Ciberseguridad (SRI), las directrices CROE del BCE y, más recientemente, el Reglamento sobre la Ciberseguridad de la UE. En conjunto, con la incorporación de mandatos de proveedores, como el SWIFT CSP, lograr el cumplimiento actualmente implica abordar un gran número de requisitos técnicos e informativos.

Por lo tanto, conforme actualizan su tecnología, los bancos y las instituciones financieras también necesitan encontrar formas de simplificar la gestión y reducir los costes operativos relacionados con la ciberseguridad y el cumplimiento.

Vulnerabilidades de seguridad derivadas de la interacción con terceros y mercados financieros

La segunda Directiva sobre Servicios de Pago de la UE (PSD2), destinada a mejorar la comodidad y la transparencia para el usuario, amplió la tipificación de los riesgos del acceso de terceros y de los datos personales. También hay una presión creciente, por parte de los homólogos del sector y los reguladores, para aumentar la eficiencia y la transparencia en los procesos empresariales y tecnológicos.

Las exigencias por parte de los clientes en torno a la seguridad, la movilidad y los nuevos servicios han dado lugar a una mayor dependencia de las infraestructuras de TI y comunicaciones de terceros, los proveedores externos y sus cadenas de suministro.

Con unos entornos más conectados que nunca, la protección de todos los tipos de comunicaciones, incluidas las transacciones interbancarias e intrabancarias automatizadas, requiere muchos recursos.

Hoy en día, una sola filtración en el centro de datos de una de las partes podría tener un efecto dominó, ya que los atacantes solo tendrían que explotar un único activo para moverse lateralmente entre las partes interconectadas, incluidas las instituciones financieras homólogas y los mercados financieros, poniendo en peligro la seguridad y la continuidad empresarial de todo el ecosistema europeo de servicios financieros.

La nube híbrida exige un nuevo enfoque de seguridad

Los mandatos de cumplimiento, junto con las [3] directrices de la Autoridad Bancaria Europea, están conformando las tendencias de adopción de la nube en el sector financiero. Aunque la adopción de la nube está en aumento en Europa, las normativas han incrementado la complejidad de la migración de los sistemas locales.

Por este motivo, es más probable que las empresas europeas conserven sus funciones principales en las instalaciones y adopten entornos de nube híbrida, en lugar de optar por entornos de nube integral. Muchos bancos también han comenzado a utilizar varios proveedores de servicios en la nube, lo que ha resultado en una infraestructura multinube.

No obstante, las organizaciones suelen buscar algo más que aumentar la seguridad. También quieren ahorrar costes y mejorar la eficiencia operativa mediante la modificación de procesos. Así, la automatización y la modernización de procesos se convierten en la clave del éxito.

Afronte los principales desafíos de ciberseguridad con la visibilidad y segmentación de la red

El tema común a todos estos desafíos es la necesidad de aislar de forma segura las aplicaciones y las cargas de trabajo esenciales, lo que comúnmente se conoce como segmentación. Esto permite a las instituciones financieras lograr la seguridad a escala según las necesidades empresariales y demostrar un enfoque basado en el riesgo que se ajusta a los requisitos normativos.

Los firewalls heredados no son la respuesta

Existen varias razones por las que la segmentación no se ha adoptado y desplegado más ampliamente en las instituciones financieras y los bancos europeos.

Mantenimiento y uso intensivo de recursos: muchos profesionales de TI y seguridad se muestran reacios a llevar a cabo iniciativas de segmentación, alegando que requieren demasiado tiempo y numerosos equipos y recursos. Esta vacilación es comprensible, ya que los métodos tradicionales tienden a ser tan complicados como lentos. Por ejemplo, la configuración de VLAN, ACL y firewalls en diversas ubicaciones y entornos suele ser un proceso laborioso, lento y propenso a errores. Además, los métodos tradicionales dependen en gran medida de datos de identidad poco fiables, como las direcciones IP, que tienen poco significado y pueden cambiar con frecuencia.

Falta de visibilidad: las organizaciones se ven aún más obstaculizadas por la falta de visibilidad del tráfico de este a oeste, lo que dificulta la identificación de dependencias entre segmentos y la creación de normas de segmentación que no perturben componentes críticos. Incluso cuando se utilizan derivaciones de tráfico o tecnologías similares, la vista resultante a menudo carece del contexto y las traducciones sofisticadas necesarias entre las direcciones IP y los puertos. En entornos dinámicos, como los sistemas de plataforma como servicio (PaaS), es prácticamente imposible.

Dependencia de la infraestructura: si las cargas de trabajo se extienden a la nube, lo que es cada vez más común, el proceso se complica aún más. La colocación de un firewall de hardware en cada punto de salida de datos tiene un coste prohibitivo. Las complejas configuraciones de red plantean más desafíos de gestión. Estas son necesarias para satisfacer las demandas de entornos diversos con activos virtualizados o heredados, junto con la nube y los contenedores.

> "En algunas áreas, el régimen regulatorio ha tenido dificultades a la hora de mantener el ritmo de la innovación tecnológica, como también ha sucedido con los marcos de gestión y control de riesgos de las empresas".
>
> — Perspectivas regulatorias de los mercados financieros en 2023, Centro para la Estrategia Regulatoria en EMEA de Deloitte

Introducción de un cambio fundamental en el proceso

Incluso las organizaciones de servicios financieros de tamaño medio con unos pocos cientos de servidores pueden generar miles de partidas de políticas de segmentación. La gestión manual de estos elementos resulta ineficaz, especialmente en entornos con distribución de aplicaciones automatizada, utilizando herramientas como Jenkins y ciclos de CI/CD en los que el contexto es fundamental.

Por este motivo, Guardicore Segmentation de Akamai va un paso más allá y ayuda a las organizaciones a cambiar sus ciclos de creación y actualización de políticas de un proceso fundamentalmente manual a uno automatizado.

Con Guardicore Segmentation, una vez que se automatiza el perfilado de una aplicación y se asignan todas las dependencias, la creación y las actualizaciones de reglas se pueden convertir en un proceso repetible en el que las partes interesadas y los propietarios de las aplicaciones solo necesitan aprobar las políticas generadas automáticamente. Esto elimina casi por completo la necesidad de intervención manual, que puede ralentizar los proyectos de forma significativa, y reduce el riesgo de configuraciones defectuosas y errores humanos.

La creación automatizada de reglas mantiene la coherencia estructural de las reglas y la escalabilidad de la propia política, lo que se traduce en un firewall más optimizado.

Acelere la transformación de TI para crear un verdadero entorno Zero Trust

Las instituciones financieras no deben permitir que los procesos manuales y los recursos limitados les impidan lograr la segmentación a escala. Un verdadero entorno Zero Trust no solo requiere la tecnología adecuada, sino también la modernización de los procesos de creación, cambio y mantenimiento de políticas de seguridad.

Los firewalls basados en software o en host han surgido como un enfoque sencillo y rentable de la seguridad a nivel de aplicación. Este enfoque acelera drásticamente la implementación, simplifica el mantenimiento continuo y, en última instancia, es más eficaz para mitigar las amenazas. Guardicore Segmentation de Akamai se ha creado desde cero para hacer la segmentación sencilla, rentable y rápida para organizaciones de todos los tamaños.

La solución proporciona un mapa visual de todas las aplicaciones del centro de datos y sus dependencias. A continuación, los operadores de seguridad pueden crear y aplicar políticas de seguridad en el nivel de procesos individuales y de red para aislar y segmentar aplicaciones y activos esenciales. Este enfoque de superposición definida por software es independiente de la infraestructura subyacente y protege las cargas de trabajo que abarcan las instalaciones locales, los sistemas heredados, las máquinas virtuales, los contenedores, las nubes, etc. Las políticas se pueden crear en torno a aplicaciones individuales o agrupadas de forma lógica, independientemente de su ubicación. Estas políticas determinan qué componentes pueden o no comunicarse entre sí, lo que sienta las bases de un enfoque de seguridad Zero Trust.

Reduzca eficazmente los riesgos y los costes cibernéticos

Las instituciones financieras que utilizan Guardicore Segmentation de Akamai descubren que pueden dar respuesta a algunos de sus problemas de seguridad más apremiantes y, a la vez, reducir los costes en un breve periodo de tiempo:

Reduzca los costes de los riesgos cibernéticos mediante la aplicación de la adecuada seguridad de la red y las prácticas recomendadas en entornos cada vez más complejos e interconectados.

Simplifique la gestión del cumplimiento mediante políticas de segmentación y visibilidad contextual granulares para asignar y aislar rápidamente los activos relacionados con la conformidad y las aplicaciones esenciales para el negocio. Al utilizar un enfoque de panel único, una institución financiera puede demostrar razonablemente que está tomando medidas para proteger los activos críticos, mitigar el riesgo de fraude y proteger la privacidad del cliente.

Proteja el acceso de terceros mediante la aplicación de rutas para el tráfico de terceros con segmentación basada en identidades, que aísla y restringe a los usuarios que navegan por la red. Esto aumenta la seguridad en torno a las interacciones de terceros y en el mercado financiero, lo que impide que los atacantes consigan propagar su actividad desde otro sistema comprometido.

Aísle los sistemas de transferencia y pago de la TI general para cumplir los requisitos de los sistemas electrónicos de transferencia y pago, en particular SWIFT, que exigen la separación estricta de los servicios SWIFT del entorno de TI general de una institución. La segmentación granular permite a los equipos de TI de los bancos establecer límites basados en el contexto (usuario, dominio) alrededor de la "zona" de un proveedor de servicios para restringir aún más el acceso no autorizado.

Migre a la nube de forma rápida y segura mediante la asignación de cargas de trabajo y el inventario de todas las aplicaciones esenciales y sus dependencias antes de la migración. Las políticas de acordonamiento pueden utilizar estos mapas como base para una seguridad coherente que siga las cargas de trabajo durante todo el proceso de migración. Este enfoque permite una migración a la nube más rápida y segura, manteniendo los mismos controles de seguridad, independientemente de los cambios en las aplicaciones o en la infraestructura.

Garantice la continuidad empresarial con una mitigación eficaz de las infracciones mediante una visibilidad detallada del tráfico este-oeste y los indicadores de infracciones para alertar sobre movimientos anómalos y detener a los atacantes antes de que exfiltren datos financieros y confidenciales de los clientes.

Reduzca el riesgo mediante la limitación del movimiento lateral; actualmente, la mayoría del tráfico del centro de datos se mueve lateralmente entre las aplicaciones (este-oeste), en lugar de entrar en el centro de datos desde el exterior (norte-sur). Establecer límites internos mediante la delimitación de aplicaciones y sistemas esenciales para el negocio reduce eficazmente la superficie de ataque, lo que protege contra la propagación lateral de los ataques y limita los daños en caso de vulneración.

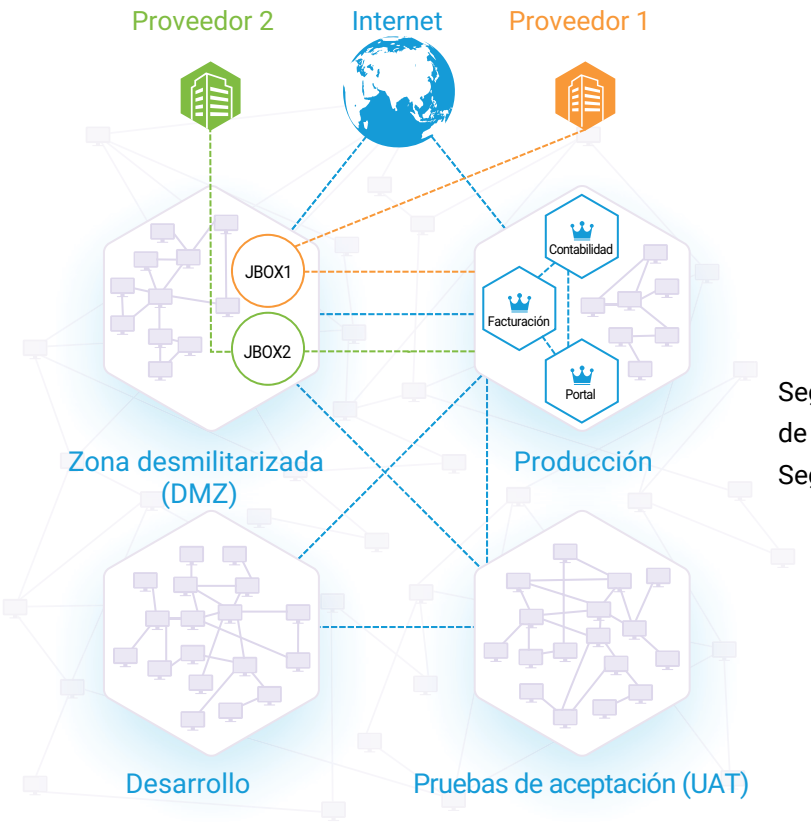
Caso real: Reducción de los costes de cumplimiento en un gran banco multinacional europeo

Un gran banco europeo buscaba un nuevo enfoque eficiente de segmentación de la red, necesario para cumplir con los requisitos técnicos de varias agencias reguladoras, incluidos el Banco de la Reserva Federal de Nueva York (FRBNY), la Autoridad Monetaria de Singapur (MAS), el BCE y otros.

El uso por parte del banco de los enfoques tradicionales de segmentación, las reglas de firewall y las VLAN estaba resultando ineficaz, lo que se traducía en altos costes anuales por incumplimiento. También estaba afectando a las operaciones de TI, dados el tiempo de inactividad de producción y la cantidad de recursos necesarios para crear y actualizar las políticas.

Era necesario dar con un enfoque más rentable y fácil de implementar para lograr los objetivos de segmentación del banco. El requisito clave de la nueva solución era minimizar el impacto en la infraestructura y los recursos del banco, al tiempo que se garantizaba el pleno cumplimiento de las normativas pertinentes.

Tras un exhaustivo proceso de evaluación que incluía a diversos proveedores, los responsables de la toma de decisiones de los equipos de infraestructura y seguridad de TI del banco llegaron a un consenso: Guardicore Segmentation de Akamai ofrecía la transición más rápida y directa hacia la microsegmentación.



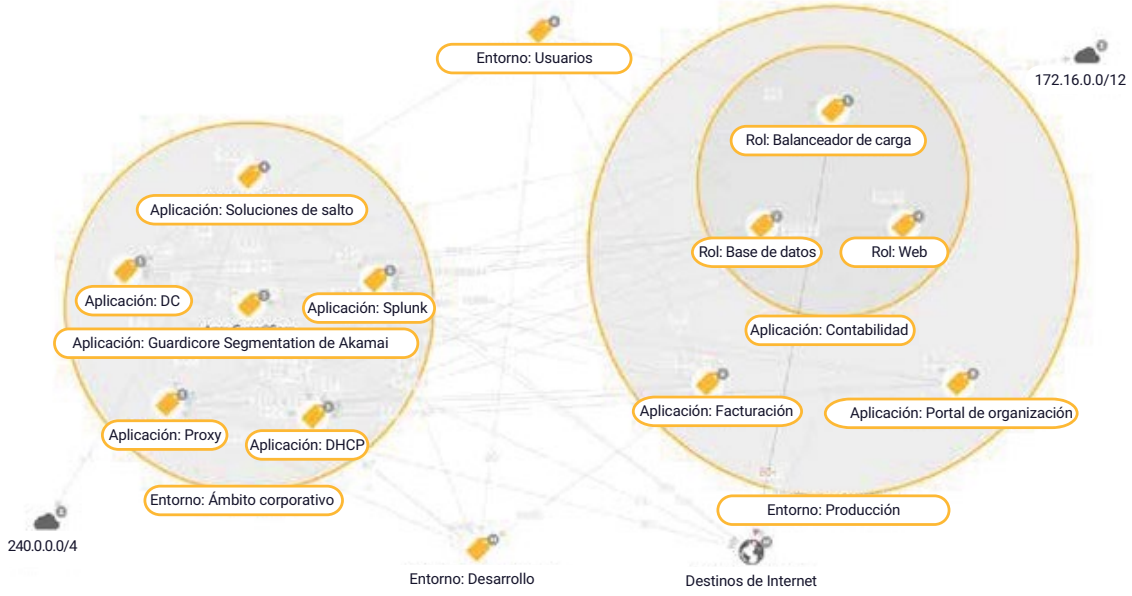
Segmentación de entornos y control de acceso de terceros con Guardicore Segmentation de Akamai

Simplificación y aceleración de la segmentación

El banco implementó Guardicore Segmentation de Akamai en varias regiones y tipos de infraestructuras de TI, incluidos contenedores. Como no era necesario hacer cambios en las aplicaciones, no hubo tiempo de inactividad en el entorno de producción. Además, permitió al banco obtener rápidamente visibilidad centralizada de las cargas de trabajo del centro de datos y aislar los entornos de producción, prueba y desarrollo. Con Guardicore Segmentation, el cliente también pudo restringir el acceso a los servidores a impresoras, otros dispositivos del Internet de las cosas (IoT) y usuarios no autorizados.

El proyecto se completó en menos de tres meses. La duración fue 10 veces menor que la que se había estimado inicialmente con los métodos de segmentación tradicionales. Mediante la representación rápida del entorno y la creación de políticas basadas en la información recopilada, el banco mejoró su estrategia de seguridad y pudo atender a los requisitos de conformidad normativa de más de 10 000 activos no conformes. La rápida implementación se tradujo en una reducción del riesgo y un importante ahorro de costes y recursos.

El equipo de servicios profesionales de Akamai ayudó al banco a transformar completamente sus procesos de segmentación. En la actualidad, las políticas de segmentación y etiquetado de activos están totalmente automatizadas e integradas en los procesos de desarrollo e implementación de aplicaciones. La creación de etiquetas, la gestión de cambios, los incidentes de seguridad y las solicitudes de servicio están completamente integradas en los flujos de trabajo de ServiceNow. El cliente quedó muy satisfecho con los resultados y el valor de la plataforma, así como con los equipos de servicios técnicos especializados de Akamai.



Obtenga más información sobre Guardicore Segmentation de Akamai en akamai.com/guardicore

1 "What are the GDPR Fines?" GDPR.eu, 13 de febrero de 2019.

2 "Cost of a data breach 2022", IBM.

3 "A comprehensive guide to cloud adoption in Europe's banking sector", Techerati, 31 de octubre de 2019.

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 seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado el 23 de junio.