White paper

Cumplimiento de NIS2 en la era de la IA

Cuatro desafíos clave para las organizaciones y cómo resolverlos mediante la segmentación

Akamai Security

Akamai Security

Contenido

Resumen ejecutivo 3

Contención rápida de las brechas de seguridad 5

Protección frente a riesgos en la cadena de suministro 7

Continuidad operativa y reducción de las interrupciones 8

Auditorías, cumplimiento normativo e informes más sencillos 10

Un resumen rápido 12

Resumen ejecutivo

Con la Directiva NIS2, la ciberseguridad ha pasado a ocupar un lugar prioritario en los consejos de administración europeos, que ahora afrontan responsabilidad personal y un plazo de solo 24 horas para notificar incidentes. Cuando los ataques basados en IA reducen de días a minutos el tiempo que transcurre hasta la explotación, ya no basta con proteger el perímetro ni con adoptar un enfoque estático del cumplimiento.

En una economía hiperconectada, no es realista pensar que se pueden detener todos los ataques. Las organizaciones necesitan una protección dinámica que contenga las amenazas en tiempo real y permita demostrar de inmediato hasta dónde se ha extendido una brecha de seguridad, para ayudar a proteger a los directivos frente a posibles reclamaciones de responsabilidad.

En este documento abordamos cuatro áreas especialmente críticas para las organizaciones que trabajan en el cumplimiento de NIS2.

1. Demostrar que pueden limitar el impacto de una brecha
2. Contar con garantías sobre la seguridad de la cadena de suministro
3. Tener capacidad para garantizar la continuidad del negocio
4. Informar rápidamente sobre los detalles y el impacto de cualquier ataque

En este documento mostramos cómo una segmentación bien implantada permite hacer frente a estos cuatro desafíos gracias a una contención rápida y automatizada, al mantenimiento de la continuidad del negocio y al apoyo a las iniciativas de cumplimiento de NIS2.

Demostrar el cumplimiento y la responsabilidad

Con NIS2, la ciberseguridad ha ganado protagonismo en los consejos de administración de toda Europa, un avance fundamental para proteger la continuidad de los servicios críticos. Hoy, cuando las amenazas actúan a velocidad de máquina y dejan atrás a las defensas humanas, ya no basta con proteger el perímetro ni con limitarse a marcar casillas de cumplimiento.

Ahora, el verdadero desafío para las organizaciones afectadas es: ¿Cómo *demuestra* que sus defensas internas funcionan?

Cuando los directivos responden personalmente y los incidentes significativos deben notificarse en un plazo de 24 horas, ya no basta con demostrar el cumplimiento en un momento determinado: este enfoque se ha convertido en un riesgo en sí mismo. La resiliencia operativa de verdad requiere una contención dinámica del riesgo capaz de responder a un entorno en el que la IA y el ransomware han comprimido de días a minutos el tiempo disponible antes de que se produzca la explotación.

Una segmentación moderna y avanzada puede dar respuesta a todos estos desafíos. Los enfoques tradicionales se apoyaban en infraestructuras complejas y estáticas que avanzaban al ritmo de la intervención humana y que ya no son suficientes para las necesidades actuales de las organizaciones, entre ellas:

- Una red de protección que no solo supervise las amenazas, sino que las contenga de forma activa antes de que provoquen consecuencias graves
- Un marco automatizado y adaptable para la contención de riesgos
- Análisis continuo de la exposición

Según los estudios, la región EMEA registra la mayor incidencia de ransomware del mundo y, al mismo tiempo, el nivel más bajo de madurez en segmentación. Los atacantes aprovechan las vulnerabilidades más rápido de lo que los equipos pueden corregirlas. A esto se suma la dificultad de las organizaciones para integrar sistemas heredados en entornos de trabajo híbridos y en un contexto de expansión basada en la IA.

Akamai Guardicore Segmentation cambia este enfoque por completo: Permite delimitar rápidamente el alcance de una brecha de seguridad dentro del plazo de 24 horas exigido por NIS2 y proporciona pruebas que ayudan a los directivos a cumplir sus obligaciones de cumplimiento normativo y rendición de cuentas.

Cuatro desafíos clave para el cumplimiento de NIS2 en la era de la IA

1. Contener rápidamente las brechas de seguridad
2. Mitigar los riesgos de la cadena de suministro
3. Garantizar la continuidad del negocio
4. Simplificar auditorías e informes

En este documento se abordan estos retos específicos y se explica cómo la segmentación favorece el cumplimiento normativo, protege a los directivos y ayuda a garantizar la continuidad de los servicios esenciales.

1. Contención rápida de las brechas de seguridad

El desafío

Con NIS2, las empresas deben poder demostrar que pueden contener una brecha de seguridad antes de que cause un impacto social o económico, utilizando "medidas técnicas adecuadas y proporcionadas".

Algunos de los obstáculos más comunes para cumplir NIS2 son:

- Equipos de seguridad separados por silos, con herramientas distintas para los entornos nativos de la nube y los centros de datos locales, lo que dificulta obtener una visión completa
- Dificultad para priorizar amenazas ante el gran volumen de alertas generadas por las herramientas de seguridad, muchas de ellas sin contexto de negocio
- Rápido movimiento lateral de los ataques basados en IA, que se propagan antes de que los equipos internos puedan detectarlos y responder
- Puntos de control rígidos en la red que no pueden adaptarse a la segmentación de cargas de trabajo dinámicas, entornos Kubernetes o tráfico este-oeste en la nube
- Capacidades de análisis de exposición y respuesta (ExAR) separadas de los mecanismos que aplican las políticas, lo que impide contener los riesgos de forma automática
- Políticas que quedan desactualizadas a medida que cambia la infraestructura y dejan abiertas vías de exposición no identificadas

A medida que aumenta el uso de la IA en tareas de alto valor, cobra aún más importancia adoptar un modelo de seguridad que priorice la contención y evite que una brecha de seguridad se propague más allá del punto en el que se produjo inicialmente. Los equipos necesitan una mejor priorización para poder centrarse en contener los activos realmente peligrosos, en lugar de perder tiempo interpretando puntuaciones de gravedad.

Cómo ayuda la segmentación

Frente a ataques basados en IA, la contención basada en IA permite reaccionar mucho más rápido. Para ello, hemos creado Akamai Guardicore Segmentation, una plataforma definida por software que pone los activos en el centro de la estrategia de seguridad. Está preparada para infraestructuras de nube híbrida y opera en la nube, centros de datos, Kubernetes, entornos de tecnología operativa (OT) y cargas de trabajo de IA. La plataforma recopila telemetría en todos los niveles, desde los paquetes de red hasta los procesos del sistema operativo y las solicitudes DNS, para que la segmentación se base en el comportamiento real y se ajuste continuamente a nuevas vías de exposición.

Las alertas se ordenan según el posible alcance del incidente y su impacto en el negocio, lo que ayuda a evitar la saturación por exceso de alertas. Akamai Guardicore Segmentation convierte directamente los resultados del análisis en políticas automatizadas que contienen las amenazas antes de que se propaguen. Gracias a la IA, se acelera el análisis de dependencias que tantas veces retrasa los proyectos de segmentación tradicionales.

Ya no se trata de detener todos los ataques, sino de impedir que se extiendan más de lo necesario. Con Akamai Guardicore Segmentation, una brecha de seguridad puede quedar contenida según la segmentación definida y, a partir de ahí, pueden adoptarse las medidas de mitigación necesarias, incluida la notificación en tiempo y forma conforme a NIS2.

2. Protección frente a riesgos en la cadena de suministro

El desafío

Hasta ahora, los incidentes de seguridad causados por un proveedor directo, un contratista de mantenimiento o un proveedor de nube solían tratarse como problemas externos y gestionarse mediante contratos, mecanismos legales y seguros. NIS2 elimina esa posibilidad. La alta dirección debe garantizar el cumplimiento de NIS2, incluida la seguridad de la cadena de suministro, y puede asumir responsabilidades si la organización no cumple.

Cómo ayuda la segmentación

Una buena segmentación permite mantener la actividad con normalidad aunque un socio externo se vea comprometido. En lugar de depender de VPN y otros controles de acceso perimetrales —que pueden abrir un acceso demasiado amplio si se vulneran—, las organizaciones deben permitir a los proveedores acceder solo a los servidores y aplicaciones que necesitan para prestar el servicio contratado.

Akamai Guardicore Segmentation hace que este proceso sea sencillo mediante una microsegmentación basada en la identidad y en los activos. Los equipos de seguridad pueden aplicar políticas muy precisas según la identidad del usuario y las etiquetas de las aplicaciones, para que una credencial comprometida de un proveedor solo tenga acceso a la carga de trabajo y al puerto expresamente autorizados, reduciendo al mínimo el riesgo de movimiento lateral hacia infraestructuras críticas.

Un aspecto clave es que la visualización en tiempo real de la plataforma ofrece a reguladores y auditores pruebas claras de que las conexiones de terceros están sujetas al principio de mínimo privilegio y se mantienen aisladas de forma demostrable. En el caso de conexiones con proveedores de mayor riesgo, la segmentación multifactioral (MFS) de Akamai Guardicore Segmentation añade una capa adicional de protección al incorporar la autenticación multifactor (MFA) directamente a la política de segmentación. En lugar de confiar en una única autenticación perimetral, la identidad del proveedor se comprueba en cada conexión y para cada servicio o puerto específico al que intenta acceder.

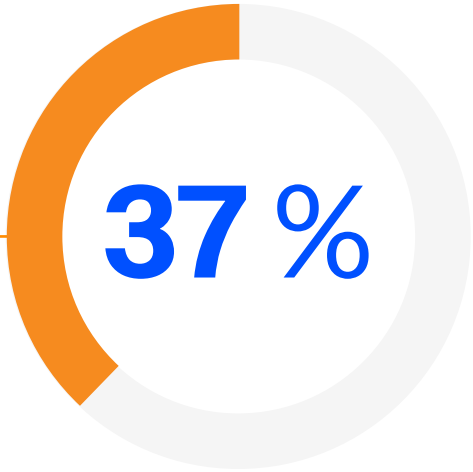
3. Continuidad operativa y reducción de las interrupciones

El desafío

NIS2 no se limita a la privacidad de los datos. También tiene como objetivo garantizar la seguridad de servicios críticos en sectores como las finanzas, la energía, el agua y el transporte, todos ellos golpeados por brechas de ciberseguridad en los últimos años. Estos incidentes han puesto en riesgo la economía, las infraestructuras críticas y la seguridad pública. Además, provocan importantes consecuencias internas para las organizaciones afectadas. A menudo, lo que más expone a una empresa a interrupciones prolongadas es el tiempo que transcurre hasta detectar un incidente y reaccionar.

La microsegmentación permite acelerar esa respuesta y, al mismo tiempo, apoyar el cumplimiento de NIS2. Pero sabemos que el temor a *provocar* interrupciones en la actividad es el principal obstáculo para dar ese paso. Si solo el 37 % de las empresas gestiona la segmentación de forma conjunta entre los equipos de seguridad e infraestructura, es evidente que en muchos casos sigue existiendo una gestión por silos que frena la capacidad de actuar.

El 37 % de las empresas afirma que los equipos de seguridad e infraestructura comparten la responsabilidad de la segmentación



Cómo ayuda la segmentación

Para reducir el riesgo empresarial, la segmentación puede combinarse con detección, respuesta y análisis de exposición automatizados. Al comprender cómo se comportan las aplicaciones, la plataforma puede ver cómo se comunican realmente y detectar qué activos están de verdad expuestos y pueden ser explotados. Después, puede automatizar las acciones que normalmente tendrían que ejecutarse manualmente durante un incidente.

Akamai Guardicore Segmentation es la primera plataforma que permite automatizar este proceso. Y, dado que uno de los principales temores es afectar al funcionamiento de las aplicaciones, Akamai utiliza un modelo de implantación que simula primero los cambios antes de aplicarlos. Antes de aplicarse, las políticas de seguridad se ejecutan en modo borrador con tráfico real, de modo que los equipos pueden comprobar matemáticamente que una regla no afectará a las aplicaciones antes de activar el bloqueo. Esto permite dedicar menos tiempo a crear reglas y aplicarlas con seguridad, agilizando la adopción de Zero Trust y reduciendo los costes.

La plataforma ofrece un portal para los responsables de las aplicaciones, desde el que los gestores de las unidades de negocio pueden revisar y validar reglas de conexión concretas. Esta colaboración entre departamentos permite aplicar las estrictas medidas de contención de NIS2 sin interrumpir la actividad.

Además, Akamai Guardicore Segmentation ayuda a adoptar la IA de forma segura, evitando que los modelos de alto valor y los datos sensibles queden expuestos a accesos laterales innecesarios a medida que aumenta la infraestructura de GPU. Evita que el ataque se propague y reduce drásticamente sus consecuencias.

El sistema aprende de forma continua cómo se comportan las aplicaciones, analiza sus dependencias y genera políticas de segmentación precisas para que los equipos las revisen y aprueben. Desde un único plano de control, estas políticas se aplican de forma coherente en entornos locales, de nube y de contenedores, y evita las brechas de seguridad que provocan las arquitecturas aisladas.

4. Auditorías, cumplimiento normativo e informes más sencillos

El desafío

Los altos directivos responden ahora personalmente del cumplimiento de NIS2, y las organizaciones están obligadas a notificar cualquier incidente significativo en un plazo de 24 horas desde que tengan constancia de él. Tanto los auditores como la alta dirección necesitan tener la certeza, de forma continua, de que los controles pueden contener amenazas reales.

Sin embargo, los informes tradicionales de ciberseguridad para la dirección suelen limitarse a enumerar alertas y vulnerabilidades. Una larga lista de vulnerabilidades sin corregir no ayuda al consejo a saber cuáles suponen de verdad un riesgo para las funciones esenciales del negocio. Las herramientas tradicionales de terminales pueden aislar un solo equipo, pero no tienen la visibilidad de red ni el contexto de las cargas de trabajo necesarios para contener rápidamente una brecha de seguridad en una infraestructura de nube híbrida o de centro de datos.

Los mapas estáticos y los flujos de tráfico en bruto de las herramientas antiguas no muestran cuál es el riesgo real. Ya no basta con demostrar que las herramientas se han implantado. La dirección necesita saber dónde existe exposición, por dónde podría avanzar un ataque y disponer de pruebas de que los controles de seguridad están reduciendo el riesgo operativo de forma continua.

> **Cuando la ANSSI [Agencia Nacional de Ciberseguridad de Francia] exige la notificación de un incidente en 24 horas, no hay margen para emplear tres días en identificar manualmente la red y determinar qué activos han resultado afectados. Es imprescindible contar con visibilidad inmediata y verificable sobre el alcance de la brecha.**
>
> Yann Fralo, gerente regional de ventas de Akamai

Cómo ayuda la segmentación

Las organizaciones necesitan una plataforma de segmentación capaz de transformar la telemetría técnica en informes claros para la dirección y centrados en el riesgo. De este modo, se satisfacen los principales requisitos de auditoría de NIS2 y, al mismo tiempo, se consigue una reducción cuantificable del riesgo para el negocio.

Akamai ofrece una respuesta a esta necesidad. Las organizaciones pueden acreditar con facilidad el control de entornos híbridos y regulados sin depender de documentación manual ni de reglas rígidas y difíciles de mantener. En lugar de obligar a los auditores a revisar miles de líneas de código de firewall, Akamai Guardicore Segmentation ofrece una representación visual, intuitiva y en tiempo real que demuestra que los entornos están aislados y que se aplica el principio de mínimo privilegio.

Por su parte, Insight Query con ExAR permite a los equipos hacer consultas sencillas en lenguaje natural y conocer al instante hasta dónde puede extenderse un incidente. Proporciona justo los datos necesarios para cumplir el plazo de 24 horas de NIS2 sin tener que dedicar días al análisis forense manual.

También permite avanzar mucho más rápido en la adopción de la microsegmentación. Mientras que los enfoques tradicionales pueden tardar años, Akamai Guardicore Segmentation utiliza etiquetado y plantillas basados en IA para lograr en semanas una segmentación preparada para NIS2 y reducir así el tiempo durante el que el consejo está expuesto a riesgos regulatorios.

Por último, aporta la infraestructura de contención necesaria para proteger clústeres de entrenamiento de IA de alto valor frente a riesgos como una mayor propagación de los incidentes, la exfiltración no autorizada de datos y el acceso indebido a modelos.

Un resumen rápido

Desafíos relacionados con la NIS2	Artículo relacionado con la NIS2	Enfoque tradicional	Akamai Guardicore Segmentation
Contención de brechas de seguridad	Artículos 21 (1) y 21 (2) (f)	Los perímetros estáticos y los puntos de control no tienen en cuenta el tráfico este-oeste en entornos de nube y Kubernetes	Microsegmentación definida por software y centrada en los activos que detiene el movimiento lateral
Seguridad de la cadena de suministro	Artículo 21 (2) (d)	Tratar las vulnerabilidades de los proveedores como un riesgo jurídico o asegurable	Acceso Zero Trust definido por software y basado en el principio de mínimo privilegio, que restringe estrictamente el acceso de terceros a los activos de servidor asignados Autenticación multifactorial (MFA) de nivel de conexión, de modo que el robo de credenciales por sí solo no permita obtener acceso
Continuidad operativa	Artículo 21(2)(c)	Parálisis en la toma de decisiones por temor a afectar a la actividad empresarial	Un motor de implantación basado en la simulación que permite probar las políticas en modo borrador con tráfico real
Responsabilidad	Artículo 23	La identificación manual de los activos comprometidos en la red requiere varios días	Determinación inmediata del alcance de una brecha de seguridad mediante lenguaje natural y rápida aplicación de políticas para cumplir el plazo de notificación de 24 horas Asignación visual en tiempo real para sustituir las líneas de código

Microsegmentación para contener brechas de seguridad mediante IA

La Directiva NIS2 ha trasladado la responsabilidad personal hasta los consejos de administración. Y, en lo que respecta a los ciberataques, la IA ha cambiado radicalmente las reglas del juego. Las vulnerabilidades pueden descubrirse y explotarse en cuestión de minutos, dejando a las organizaciones sin el margen de respuesta del que disponían antes. En una economía global hiperconectada, la huella digital de una organización ya no termina en su propia red: también incluye la cadena de suministro, los entornos cloud, las redes OT y los clústeres de entrenamiento de IA de alto valor. Todo está estrechamente interconectado.

Las organizaciones actuales requieren un mecanismo de protección dinámico y automatizado que garantice la continuidad operativa ante una brecha de seguridad y proporcione evidencias casi inmediatas de una contención rápida.

La segmentación granular puede resolver eficazmente estos desafíos, pero cualquier plataforma adoptada debe responder al panorama actual de la ciberseguridad y estar preparada para su evolución.

Akamai Guardicore Segmentation es una plataforma de microsegmentación de referencia que ayuda a las organizaciones a protegerse frente a ciberamenazas cada vez más sofisticadas y a avanzar en el cumplimiento de NIS2. Permite contener brechas de seguridad rápidamente mediante IA, reducir el riesgo asociado a la cadena de suministro, adoptar la microsegmentación con más agilidad que con las herramientas tradicionales y mantener la continuidad del negocio sin generar interrupciones.

Replantear la seguridad

Akamai Guardicore Segmentation cambia por completo el enfoque al agilizar la adopción de la microsegmentación y pasar de intentar impedir todos los ataques a controlar hasta dónde pueden extenderse.

Ayuda a cumplir NIS2 en cuatro áreas fundamentales:

Contención rápida de brechas de seguridad con IA

La plataforma analiza telemetría en todos los niveles de las cargas de trabajo híbridas y mantiene los activos en el centro de la estrategia. De este modo, puede aislar automáticamente las amenazas según su impacto en el negocio y frenar su movimiento lateral.

Protección frente a riesgos en la cadena de suministro

Akamai Guardicore Segmentation permite que los proveedores accedan solo a los servidores imprescindibles y ofrece una representación visual clara que demuestra que la infraestructura crítica está debidamente aislada.

Continuidad operativa

Para evitar que el temor a interrumpir la actividad frene la adopción de medidas, la plataforma simula primero los cambios antes de aplicarlos. Así, los equipos de seguridad pueden comprobar matemáticamente las reglas con tráfico real antes de activarlas.

Auditorías e informes más sencillos

Akamai Guardicore Segmentation ofrece mapas visuales en tiempo real que permiten demostrar fácilmente a los auditores que los entornos están debidamente aislados. También convierte los datos técnicos en informes claros para la dirección, centrados en el riesgo y capaces de demostrar de forma continua el cumplimiento normativo.

En la era de la IA, no podemos evitar todos los ataques, pero sí controlar hasta dónde llegan sus consecuencias.

Acelere su camino hacia NIS2 con microsegmentación automatizada. Conozca Akamai Guardicore Segmentation en acción y descubra cómo asegurar activos críticos en minutos.

Solicite una evaluación personalizada.

Aviso: La información proporcionada aquí se incluye solo con fines informativos generales. No debe interpretarse como un consejo legal y no supone ningún compromiso por parte de Akamai. Las leyes y normativas pueden variar, y las interpretaciones legales pueden cambiar con el tiempo. No se garantiza la exactitud, integridad o idoneidad de la información proporcionada. Si necesita consejo legal o tiene preguntas concretas en este sentido, consulte a un profesional del sector jurídico cualificado que le proporcionará asesoramiento específico sobre su situación y jurisdicción.

Akamai es la empresa de ciberseguridad y cloud computing que potencia y protege los negocios online. Nuestras soluciones de seguridad líderes en el mercado, nuestra inteligencia contra ciberamenazas consolidada y nuestro equipo de operaciones globales proporcionan una defensa en profundidad para proteger los datos y las aplicaciones empresariales en cualquier lugar. Las soluciones integrales de cloud computing de Akamai garantizan el rendimiento y una buena relación calidad-precio en la plataforma más distribuida del mundo. Las grandes empresas confían en Akamai, ya que les ofrece una fiabilidad, una escalabilidad y una experiencia inigualables en el sector, idóneas para crecer con seguridad. Obtenga más información en akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn. Publicado en agosto de 2026.