WHITE PAPER

Convierta el cumplimiento en una ventaja competitiva con la seguridad de Akamai

Un enfoque basado en cuatro pilares para reforzar la seguridad y tener todo preparado para las auditorías

Céntrese en cuatro pilares de seguridad para allanar el camino hacia el cumplimiento

Hoy en día, las organizaciones de todo el mundo se encuentran inmersas en un laberinto de normativas cada vez más desafiante, desde el RGPD y la HIPAA hasta el PCI DSS y una creciente variedad de normativas regionales. Pero demostrar la preparación para el cumplimiento no solo consiste en satisfacer a los reguladores, sino que se ha vuelto esencial para mantener la confianza de los clientes y las partes interesadas internas, como los altos cargos y la junta directiva.

De hecho, las implicaciones de los fallos de cumplimiento van mucho más allá de las sanciones normativas directas. Los costes del incumplimiento incluyen la interrupción de la actividad empresarial durante las fases de investigación y corrección, el daño a la reputación y el aumento de la exposición legal. Si una organización incumple las exigencias de cumplimiento, puede provocar pérdidas de ingresos a causa del abandono de los clientes y costes operativos significativos, ya que los recursos se desvían a la corrección en lugar de a la innovación. En 2024, las 35 filtraciones más importantes de todo el mundo acumularon 3000 millones de dólares en sanciones, y 23 de ellas citaron las infracciones vinculadas a las normas del Reglamento General de Protección de Datos (RGPD) de la Unión Europea como la causa, según Forrester.

En el pasado, los equipos de seguridad trabajaban en el cumplimiento a medida que surgían normativas nuevas. Sin embargo, ahora que la tecnología avanza rápidamente y los ataques aumentan y son más intensos, el cumplimiento debe formar parte del debate a la hora de evaluar las herramientas y los modelos de madurez. Los equipos deben preguntarse lo siguiente: "¿Cómo me ayudarán mis opciones de seguridad actuales a cumplir los requisitos de cumplimiento ahora y en el futuro?"

En Akamai, ayudamos a los clientes a responder a esa pregunta centrando la conversación en cuatro pilares de las prácticas recomendadas de seguridad que, naturalmente, también promueven áreas clave de preparación para el cumplimiento. Estos pilares son los siguientes:

- Obtención de visibilidad en todo el entorno de TI
- Prevención del movimiento lateral (en redes, aplicaciones y API)
- Prevención del acceso no autorizado
- Protección de los datos confidenciales y la información de la cuenta de los usuarios

El resultado es una clara ventaja competitiva. Las organizaciones no solo están más seguras, sino que están mejor preparadas para superar los obstáculos en materia de normativas. Al ser más seguras y cumplir con las normativas, también pueden ganarse mejor la confianza de los clientes y del liderazgo interno.

Pilar 1

Obtención de visibilidad en todo el entorno de TI

La base de la preparación para el cumplimiento comienza con una visibilidad completa de todos los activos digitales. Las organizaciones no pueden proteger lo que no pueden ver, y los reguladores necesitan cada vez más pruebas de un inventario completo de activos, una supervisión continua y un conocimiento de las amenazas.

No es tan fácil. Según un estudio reciente de Forrester, el 52 % de las empresas financieras están de acuerdo o muy de acuerdo en que carecen de una visibilidad completa de su entorno de TI. Desafortunadamente, ningún sector es inmune a las consecuencias del incumplimiento normativo. Entre 2023 y 2024, el número de organizaciones que pagaron más de 100 000 USD en sanciones aumentó casi un 20 %.

Para muchas organizaciones, el desafío de la visibilidad reside en supervisar el tráfico de red y las API. A continuación, se muestran algunos estándares y normativas que exigen una visión clara del riesgo:

- El Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) contiene directrices para confirmar que el software de una empresa utiliza de forma segura las funciones de los componentes externos, como las API que transmiten datos de pago desde una aplicación móvil al sistema de un banco.
- Estándares como la norma IEC 27001 de la Organización Internacional de Normalización (ISO) exigen la separación de datos y de instalaciones de tratamiento de datos en caso de que un atacante entre en la red.
- La Ley de Seguridad de Datos de la República Popular China exige controles de seguridad sólidos para garantizar el acceso a la información personal de los clientes a través de tecnologías que intercambian datos confidenciales entre diferentes sistemas de TI.

Muchas empresas tienen herramientas o procesos que pueden cumplir algunos de estos requisitos. Sin embargo, a medida que se expanden a los entornos informáticos híbridos y a través de las distintas zonas geográficas, la supervisión se vuelve mucho más difícil. Esto es especialmente cierto en el caso de las API. Según el estudio de Akamai, solo el 27 % de expertos en seguridad que tienen inventarios de API completos saben cuáles exponen datos confidenciales, lo que supone un descenso con respecto al ya preocupante 40 % registrado en 2023.

En última instancia, las organizaciones necesitan saber dónde se encuentran sus datos confidenciales y qué acceso se tiene a ellos para saber dónde centrar sus esfuerzos de seguridad. Esto requiere visibilidad de:

- qué activos se comunican con la red (con vistas en tiempo real e históricas), incluidos los procesos de capa 7 y el tráfico del Edge, en entornos locales y de nube híbrida;
- el inventario de API, incluidas las API en la sombra y zombis, que muestra dónde se integran con el código y las fuentes de tráfico; y
- JavaScript del lado del cliente, que es especialmente importante para los requisitos más recientes de PCI DSS.

La cartera de productos de Akamai puede ayudar a los equipos de seguridad a obtener la visibilidad que necesitan.

Akamai Guardicore Segmentation puede identificar y visualizar los activos que se comunican dentro de la red en todo el entorno de TI, incluidos los detalles del proceso de capa 7, el hash y la línea de comandos. También ofrece visibilidad histórica para obtener una validación durante las auditorías de cumplimiento que le ayudarán a demostrar que los activos del ámbito de aplicación no se han visto comprometidos. Las visualizaciones del tráfico norte-sur y este-oeste también muestran dónde se está produciendo el acceso.

API Security proporciona un inventario en tiempo real de las API que las organizaciones necesitan para cumplir con la normativa y puede ayudar a identificar dónde y cuándo pueden fluir los datos sin cifrar a través de las API.

App & API Protector ofrece visibilidad en el nivel de aplicación, incluido el inventario de API, la detección de la exposición de datos confidenciales y el análisis del tráfico en tiempo real.

Client-Side Protection & Compliance proporciona la visibilidad de los scripts del lado del cliente que requiere PCI DSS v4.

Una organización sanitaria implementó Akamai Guardicore Segmentation para abordar los requisitos de cumplimiento de HIPAA y SOC 2. Proporcionó vistas valiosas de los flujos de tráfico entre diferentes aplicaciones. El equipo de seguridad podía inspeccionar detalles muy precisos más allá de los registros de capa 4: los ID de usuario, las entradas de línea de comandos e incluso las correlaciones entre servicios.

Pilar 2

Prevención del movimiento lateral

Al igual que los propios equipos de seguridad, muchos reguladores aceptan que, incluso con una estrategia de seguridad sólida, se puede producir una vulneración, y buscan garantías de que las empresas puedan limitar el daño que se produce en caso de que ocurra. Por ejemplo:

- El artículo 32 del RGPD exige "la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia continuas de los sistemas y servicios de tratamiento" y "la capacidad de garantizar la disponibilidad y el acceso a los datos personales en el momento necesario si se produce una incidencia técnica o física".
- De forma similar, PCI DSS v4 requiere a las organizaciones "Implementar firewalls para proteger los datos del titular de la tarjeta de crédito y asegurarse de que los firewalls están configurados para restringir las conexiones entre redes de confianza y no fiables".
- **La Organización Internacional de Normalización/Comisión Electrotécnica Internacional (**ISO**/IEC) 27001** exige que se separe la información y las instalaciones de tratamiento de datos para proteger la confidencialidad, integridad y disponibilidad de la información.

Aunque la mayoría de las organizaciones tienen implementado algún tipo de firewall, limitar el movimiento lateral una vez que un agente malicioso está dentro de la red requiere un mayor nivel de control. Esto hace que la microsegmentación, preferiblemente definida por software, sea una herramienta clave para lograr el cumplimiento. Akamai está bien posicionada para abordar las preocupaciones de los auditores en materia de movimiento lateral.

Akamai Guardicore Segmentation proporciona los límites del movimiento lateral que las organizaciones necesitan para cumplir la normativa. Las plantillas de políticas listas para usar facilitan la aplicación rápida de las iniciativas relacionadas con el cumplimiento con los controles detallados de capa 7. Y como están definidas por software, pueden proporcionar el mismo nivel de protección detallada, independientemente de la ubicación de los activos. Además, su capacidad para identificar las aplicaciones que se comunican dentro de la red y los intentos de comunicación entre zonas segmentadas proporcionan a los auditores otro nivel de confianza en su capacidad para mitigar las amenazas.

Los atacantes están encontrando nuevas oportunidades para el movimiento lateral gracias a la proliferación de las API, especialmente los terminales de API que son vulnerables a los ataques de autorización a nivel de objeto comprometida (BOLA). Los atacantes pueden manipular los ID de objeto en las solicitudes de API para permitir el movimiento lateral en la red. Una vez dentro, los atacantes pueden omitir la autorización, escalar los privilegios y obtener acceso a los datos de los clientes.

Akamai API Security puede marcar las API que exponen datos confidenciales sin la autenticación adecuada e identificar las API con controles de acceso débiles o con errores de configuración que podrían dar lugar a un acceso a los datos no autorizado y a un movimiento lateral. La integración con el firewall de aplicaciones web (WAF) de Akamai también permite a API Security bloquear las amenazas maliciosas en tiempo real.

Un cliente de Akamai, una organización global de servicios financieros, implementó API Security porque tenía problemas con API desconocidas en su entorno. La implementación ha reducido drásticamente la proliferación de API y ha mejorado sus niveles de cumplimiento, ya que Akamai API Security clasifica los datos confidenciales para ayudar a cumplir normativas como el RGPD y la HIPAA, entre otras. Durante las auditorías normativas, estas implementaciones sirven como prueba directa de que la empresa ha tomado las medidas técnicas adecuadas.

Las amenazas de hoy en día de la IA son los obstáculos normativos del mañana

Hoy en día, cualquier examen de las defensas de ciberseguridad de una organización debe abordar el espectro de la IA. La rápida proliferación de aplicaciones basadas en IA, los modelos de lenguaje de gran tamaño (LLM) y las API vinculadas a la IA generativa han introducido nuevas vulnerabilidades de las que muchas organizaciones aún no son conscientes. Entre los ejemplos de este tipo de aplicaciones se incluyen los chatbots basados en IA, los motores de recomendaciones del retail, las herramientas de diagnóstico de estado y los motores de decisión de riesgos. Mientras tanto, los atacantes aprovechan la IA para lanzar ataques más sofisticados.

Y en cualquier lugar en el que surjan amenazas a las operaciones empresariales y al público, es probable que surjan nuevas normativas.

Las organizaciones que buscan proteger sus inversiones en IA, sus datos y sus clientes acuden a Akamai para buscar ayuda. Como proveedor de seguridad con un sólido historial de cumplimiento de los requisitos actuales de visibilidad, movimiento lateral y control de acceso, Akamai ha invertido de forma proactiva en satisfacer los requisitos de la IA del futuro. Akamai ha desarrollado capacidades avanzadas de IA para reforzar sus soluciones de seguridad y ahora ha introducido una solución para ayudar a las organizaciones a proteger sus propias inversiones en IA.

Akamai Firewall for AI proporciona una seguridad integral para las aplicaciones basadas en IA, ya que identifica y mitiga las amenazas y los ataques específicos de la IA para los que las herramientas de seguridad tradicionales no están diseñadas para abordar. Entre las protecciones específicas de Firewall for AI se incluyen las siguientes:

- **Defensa contra inyecciones de instrucciones**: Protege contra los atacantes que manipulan los modelos de IA mediante la introducción de datos engañosos.
- **Prevención de pérdida de datos (DLP)**: Detecta y bloquea las filtraciones de datos confidenciales en las respuestas generadas por IA, y protege contra la recepción de datos confidenciales en las solicitudes.
- **Filtrado de contenido tóxico e inapropiado**: Detecta los discursos de odio, la información engañosa y el contenido ofensivo antes de su difusión.
- **Seguridad de la IA frente a adversarios**: Protege contra la ejecución remota de código, los ataques de puerta trasera y los ataques de envenenamiento de datos.
- **Mitigación de la denegación de servicio**: Mitiga los ataques de denegación de servicio basados en IA, puesto que controla el abuso de consultas y la sobrecarga del modelo.

Además, Firewall for AI ayuda a las organizaciones a cumplir las directrices existentes de privacidad, seguridad y protección. Mediante la aplicación de políticas de seguridad específicas para la IA, las empresas pueden mitigar los riesgos relacionados con las normativas de protección de datos, el uso ético de la IA y los requisitos de gobernanza corporativa.

Pilar 3

Prevención del acceso no autorizado

El control del acceso a los sistemas y datos confidenciales representa una piedra angular del cumplimiento en prácticamente todos los marcos normativos. Las organizaciones deben comprender su estrategia de seguridad de aplicaciones y API, y prevenir el acceso no autorizado y el uso indebido. Esto exige autenticar a los usuarios de forma adecuada, autorizar el acceso según sea necesario y mantener registros detallados de todas las actividades de acceso.

Para obtener un control de acceso completo que cumpla los requisitos normativos, las organizaciones deben abordar tres desafíos clave. La cartera de productos de seguridad de Akamai puede ayudar a ofrecer defensas exhaustivas que aborden cada una de ellos:

1. **Obtención de una comprensión completa de su estrategia de seguridad de aplicaciones y API**

Akamai App & API Protector permite a las organizaciones aplicar políticas de tráfico en todos los entornos en los que se ejecutan, mientras que Akamai API Security puede alertar a una organización de cualquier actividad inusual, acceso no autorizado a los datos o errores de configuración, todas ellas consideraciones clave para los auditores. Por su parte, Akamai Guardicore Segmentation puede realizar un seguimiento de todas las aplicaciones que se comunican dentro de la red y establecer una referencia para la actividad.

2. **Supervisión del comportamiento de los usuarios y limitación del acceso a la información confidencial**

Akamai Guardicore Segmentation limita el acceso dentro de la red en función de la identidad del usuario, mientras que **App & API Protector** aplica políticas de tráfico con detección de amenazas basada en IA para evitar infracciones. Por último, **Client-Side Protection & Compliance** supervisa el comportamiento de ejecución de JavaScript para mitigar los ataques del lado del cliente.

3. **Detección y limitación de la actividad fraudulenta**

API Security puede ayudar a detectar comportamientos anómalos de las API y controles de autenticación con errores de configuración para bloquear ataques de alto riesgo. Akamai Guardicore Segmentation protege la red al marcar y bloquear las conexiones sospechosas que puedan indicar actividades fraudulentas. App & API Protector detecta y mitiga las amenazas identificadas por OWASP para reducir aún más el riesgo de fraude.

NIS2 y protección del acceso

La Directiva sobre Seguridad de las Redes y los Sistemas Informáticos (NIS2) actualizada está diseñada para crear un nivel común de ciberseguridad en todos los Estados miembros de la UE. Entre las recientes adiciones a la NIS2 se encuentra el requisito de que las empresas deben crear un sistema de gestión de la seguridad de la información que evalúe a las personas, las políticas y la tecnología para proteger los datos confidenciales y garantizar la resiliencia operativa. NIS2 también incluye un mayor énfasis en proteger las cadenas de suministro de TI y las relaciones con proveedores externos.

Pilar 4

Protección de los datos confidenciales y la información de la cuenta de los usuarios

El pilar final de un enfoque integral de preparación para las normativas exige que las organizaciones tengan planes para los datos confidenciales. La protección de los datos de clientes, pacientes, socios, etc., es el núcleo de la mayoría de las normativas centradas en la seguridad.

Por ejemplo, la Ley sobre Protección de Datos Personales de Japón exige evaluaciones de impacto de la protección de datos que puedan identificar y mitigar los riesgos de las tecnologías que realizan el tratamiento de grandes volúmenes de datos personales o que implican actividades de tratamiento de datos de alto riesgo.

En el caso de las instituciones financieras de EE. UU., el Consejo Federal de Certificación de Instituciones Financieras (FFIEC) requiere controles que garanticen que las API solo permitan el acceso a datos específicos para usuarios autorizados a través de seguridad por capas, por ejemplo, supervisión, registro y notificación.

Abordar este pilar comienza con la detección de amenazas. **App & API Protector**, la solución de protección de API y aplicaciones web de Akamai, ofrece la primera capa de defensa, mientras que **Akamai Guardicore Segmentation** supervisa y segmenta el tráfico norte-sur y este-oeste. La **cartera de soluciones de protección contra los bots y la usurpación** de Akamai añade una capa adicional de seguridad contra amenazas automatizadas y ataques humanos.

Sin embargo, para identificar correctamente las amenazas, las organizaciones también deben comprender el comportamiento de referencia dentro de su red. A continuación, se muestra cómo las capacidades de seguridad de Akamai pueden proporcionar esta información esencial:

- Akamai API Security y Akamai Guardicore Segmentation, respectivamente, proporcionan la comprensión de referencia de las API y las aplicaciones que se comunican dentro de la red para detectar cualquier comportamiento anómalo.
- Adaptive Security Engine, una tecnología fundamental de App & API Protector, aprende los patrones de ataque mediante el uso de datos locales y globales para realizar ajustes específicos del cliente en las protecciones y adaptarse a las amenazas futuras.
- Akamai Hunt, un servicio gestionado de búsqueda de amenazas que aprovecha el equipo de investigación de expertos de Akamai, permite a las empresas adoptar un enfoque más proactivo en materia de defensa.

DORA y la seguridad de datos

La Ley de Resiliencia Operativa Digital (DORA) tiene como objetivo ayudar a las empresas financieras que operan en los Estados miembros de la UE a contener ciberataques y recuperarse de ellos. Con la ley DORA, el sector tendrá un marco vinculante y amplio de gestión de riesgos para las tecnologías de la información y las comunicaciones (TIC). El artículo 3 de la ley DORA obliga a las organizaciones a utilizar soluciones y procesos basados en TIC que:

- minimizan los riesgos relacionados con los datos, el acceso no autorizado y los defectos técnicos;
- previenen la falta de disponibilidad de los datos, la pérdida de los datos y las infracciones de integridad y confidencialidad; y
- garantizan la seguridad de la transferencia de datos.

Desde el silo de cumplimiento hasta la ventaja competitiva

Los programas de cumplimiento eficaces deben demostrar el impacto empresarial más allá de simplemente "marcar la casilla" en los requisitos normativos. Las organizaciones que implementan las soluciones de seguridad centradas en el cumplimiento de Akamai han informado de mejoras cuantificables en tres dimensiones clave.

Reducción de costes de cumplimiento

Las organizaciones con programas de cumplimiento maduros suelen gastar menos en actividades de cumplimiento que aquellas con enfoques ad hoc. La automatización de la recopilación de pruebas a través de plataformas de seguridad integradas puede reducir significativamente el tiempo de preparación de las auditorías, al igual que la consolidación de soluciones puntuales en una plataforma completa.

Mejora de la estrategia antes los riesgos

Más allá de la reducción de costes, las mejoras en el cumplimiento deben ofrecer una reducción de riesgos cuantificable. Las organizaciones que implementan las soluciones de segmentación de Akamai pueden restringir las rutas de movimiento lateral vulnerables, abordando directamente los requisitos de cumplimiento clave y reduciendo al mismo tiempo el riesgo de la organización.

Las completas funciones de supervisión mejoran la visibilidad, lo que se traduce directamente en la reducción de riesgos al eliminar los puntos ciegos en los que las infracciones de cumplimiento podrían pasar desapercibidas.

Eficiencia operativa

La tercera dimensión del impacto del cumplimiento implica mejoras en la eficiencia operativa. Los controles aprobados previamente y los patrones de seguridad coherentes pueden traducirse en aprobaciones de seguridad significativamente más rápidas para las nuevas aplicaciones. Esto mejora la satisfacción de los desarrolladores al reducir la fricción en los procesos de revisión de la seguridad y acelerar el tiempo de comercialización de las nuevas aplicaciones.

Ajuste del cumplimiento

A medida que los requisitos normativos evolucionan y las organizaciones crecen, necesitan un enfoque de cumplimiento que se pueda adaptar. La cartera de productos de seguridad integrada de Akamai proporciona la base para una estrategia de cumplimiento que anticipa las tendencias normativas y se adapta al crecimiento de la organización.

- Los marcos de políticas configurables se pueden adaptar a los nuevos requisitos sin necesidad de tener que volver a diseñarlos de forma significativa, mientras que las capacidades de generación de informes extensibles pueden adaptarse a los requisitos de pruebas emergentes a medida que evolucionan las normativas.
- La implementación automatizada de políticas para nuevos activos garantiza que la cobertura de cumplimiento se extienda automáticamente a medida que la empresa se expande.
- Las capacidades de gestión centralizadas mantienen una visibilidad completa independientemente de la escala, mientras que la compatibilidad integral con las API permite automatizar los procesos de cumplimiento para gestionar la creciente complejidad.

Además, las organizaciones deben ser proactivas a la hora de establecer un ritmo regular para revisar las normativas y actualizar sus controles de cumplimiento en consecuencia. Akamai proporciona actualizaciones periódicas a nuestras soluciones de seguridad, diseñadas específicamente para abordar los requisitos de cumplimiento en constante evolución, lo que garantiza que los clientes mantengan un cumplimiento continuo independientemente de los cambios normativos.

Conclusión: El cumplimiento como factor diferenciador de la competencia

El cumplimiento eficaz ya no se limita a satisfacer los requisitos normativos, sino que representa un imperativo empresarial estratégico que afecta directamente al rendimiento de la organización, la confianza del cliente y el posicionamiento competitivo. Independientemente de su sector o región, un enfoque proactivo hacia el cumplimiento garantiza una estrategia de seguridad sólida y ágil.

Mediante la implementación de un enfoque de seguridad integrado en los cuatro pilares de la preparación para el cumplimiento (visibilidad en todo el entorno de TI, prevención del movimiento lateral, prevención del acceso no autorizado y protección de los datos confidenciales y la información de la cuenta de los usuarios), las organizaciones pueden establecer una base de cumplimiento sostenible que ofrezca un valor empresarial cuantificable que vaya más allá del cumplimiento de las normativas.

Las organizaciones que han logrado el mayor éxito son aquellas que han transformado el cumplimiento para que pase de ser un coste necesario para hacer negocios a ser una ventaja estratégica que permite la transformación digital al tiempo que protege lo más importante: la confianza del cliente, la integridad de los datos y la reputación empresarial.

Póngase en contacto con nosotros para descubrir cómo Akamai puede ayudar a su organización.

Contactar con nosotros

| Publicado en julio de 2025