Akamai

WHITE PAPER

Lograr una estrategia Zero Trust madura con Akamai

Cómo las agencias y departamentos federales pueden cumplir el modelo de la CISA con funciones interrelacionadas

Introducción

La seguridad Zero Trust se ha convertido en el estándar de referencia para proteger los datos confidenciales de sistemas gubernamentales, las infraestructuras críticas y los sistemas de seguridad nacional. Las agencias y departamentos federales ya no pueden confiar en los modelos tradicionales de seguridad perimetral para hacer frente a las amenazas modernas. A medida que los ciberdelincuentes aumentan su nivel de sofisticación, valiéndose de técnicas avanzadas como el robo de credenciales, el ransomware y los ataques internos, las organizaciones federales se ven obligadas a adaptar cada vez más su estrategia de seguridad a un marco Zero Trust. No obstante, esta adaptación se ha encontrado con un panorama fragmentado, lo que hace necesario tomar más medidas para proteger los sistemas federales.

El modelo de madurez Zero Trust de la Agencia de Seguridad Cibernética y de la Infraestructura (CISA) ayuda a las agencias y departamentos federales a implementar principios de seguridad que eliminan la confianza implícita y aplican estrictos mecanismos de verificación. El modelo se basa en cinco pilares fundamentales: Identidad, Dispositivos, Redes, Aplicaciones y cargas de trabajo, y Datos. Además, gracias a tres funciones interrelacionadas (Visibilidad y análisis, Automatización y orquestación, y Control) se garantiza el uso de un enfoque integral y coherente ante la ciberseguridad.

Para lograr estos objetivos, es necesario plantearse la microsegmentación como principio básico de la seguridad Zero Trust, como componente fundamental de la defensa de red interna (es decir, de este a oeste). Al segmentar las cargas de trabajo y restringir el movimiento lateral, las organizaciones federales consiguen evitar posibles filtraciones y aplicar políticas Zero Trust. Además, se deben usar soluciones integrales de seguridad de la interfaces de programación de aplicaciones (API) para proteger las comunicaciones externas (es decir, de norte a sur), para garantizar que solo entidades con la autorización necesaria accedan a las aplicaciones gubernamentales.

En este white paper se analizan los pasos esenciales para lograr una estrategia Zero Trust madura, destacando cómo las soluciones de seguridad avanzadas de Akamai, entre ellas Akamai Guardicore Segmentation, Akamai API Security y Akamai Enterprise Application Access, permiten a las agencias y departamentos gubernamentales cumplir las directrices de la CISA y mejorar su estrategia de ciberseguridad.

Cambio de la seguridad perimetral a un modelo Zero Trust

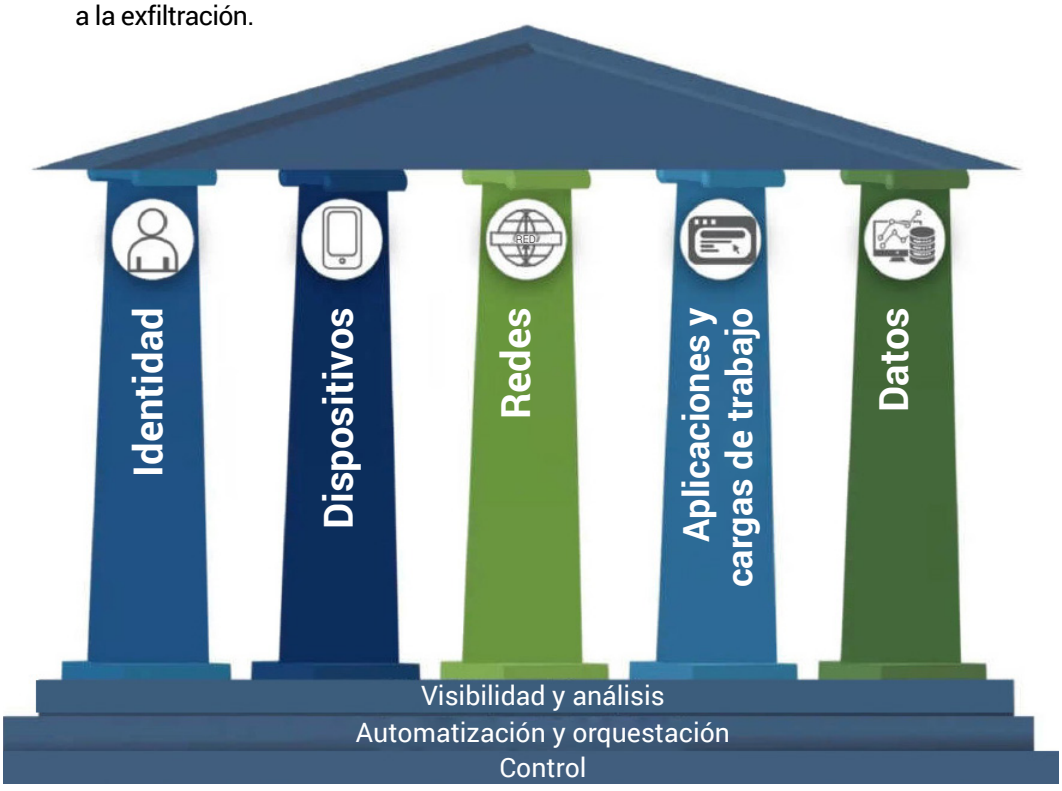
La ciberseguridad tradicional se ha basado en defensas perimetrales, donde se asume que la entidad que se encuentre dentro de la red se puede considerar de confianza. Sin embargo, este modelo ha demostrado en reiteradas ocasiones no ser suficiente ante las ciberamenazas modernas. Los atacantes aprovechan unas credenciales poco seguras y una configuración incorrecta de los ajustes de seguridad, además de utilizar técnicas de movimiento lateral para eludir las defensas tradicionales y acceder a información confidencial.

Zero Trust elimina la confianza implícita, ya que es necesario verificar de forma continua a los usuarios, los dispositivos, las aplicaciones y el tráfico de red. Todas las solicitudes de acceso se autentican, autorizan y supervisan de forma continua según los resultados de las evaluaciones de riesgo en tiempo real. Con este enfoque se reduce drásticamente la superficie de ataque y se evita el acceso no autorizado, incluso si un adversario vulnera parte de la red.

Modelo de madurez Zero Trust de la CISA

El modelo de madurez Zero Trust de la CISA ofrece a las agencias y departamentos federales un plan para que consoliden progresivamente su marco de seguridad (Figura). El modelo se basa en cinco pilares clave:

- **Identidad:** mediante la aplicación de estrictos controles de acceso y medidas de autenticación y autorización para asegurarse de que sean solo los usuarios legítimos los que interactúen con los recursos confidenciales.
- **Dispositivos:** mediante la supervisión, la protección y la validación de terminales para garantizar que se ajusten a las políticas de seguridad antes de que se produzca el acceso a las redes gubernamentales.
- **Redes:** mediante la implementación de la microsegmentación y políticas de control de acceso avanzadas para evitar el movimiento lateral no autorizado.
- **Aplicaciones y cargas de trabajo:** mediante la protección de las aplicaciones y cargas de trabajo con estrictas políticas de acceso basado en la identidad, seguridad en tiempo de ejecución y controles de seguridad de las API.
- **Datos:** mediante la garantía de que los datos gubernamentales confidenciales estén en todo momento cifrados, supervisados y protegidos frente al acceso no autorizado y a la exfiltración.



Pilares del modelo de madurez Zero Trust de la CISA (Fuente: CISA)

Además de estos pilares, en el modelo se integran tres funciones interrelacionadas esenciales que se aplican a todos los componentes de Zero Trust:

- **Visibilidad y análisis:** supervisión continua, registro y detección de anomalías para identificar y mitigar las amenazas en tiempo real.
- **Automatización y orquestación:** automatización de la seguridad basada en IA para aplicar políticas, responder a las amenazas y optimizar los controles de acceso.
- **Control:** mediante la aplicación centralizada de políticas para cumplir en todo momento las normativas federales, como la Ley Federal de Modernización de la Seguridad de la Información (FISMA) y la publicación especial 800-207 del Instituto Nacional de Normas y Tecnología (NIST).

La importancia de la microsegmentación y de la seguridad de las API

En los modelos tradicionales de seguridad de las redes, estas se suelen dividir en grandes segmentos mediante firewalls basados en redes. Si bien con este enfoque se obtiene un cierto nivel de seguridad, no se consigue el nivel de detalle necesario para proteger los entornos modernos distribuidos. En los entornos federales, la segmentación basada en la red suele generar un aprovisionamiento excesivo, donde los usuarios y las aplicaciones tienen acceso a más recursos de los que realmente necesitan. De esta forma se puede dar lugar a oportunidades no deseadas de movimiento lateral. En cuanto los atacantes consiguen acceder a una parte de la red, pueden llegar a áreas donde existe un mayor nivel de confidencialidad sin encontrar prácticamente ningún tipo de resistencia.

El concepto de la microsegmentación da respuesta a este problema, al aplicar un control detallado del tráfico de este a oeste en la red. En un entorno microsegmentado, cada una de las aplicaciones, de las cargas de trabajo o de los servicios está aislado de los demás, y el acceso según políticas concretas. De esta forma se garantiza que los usuarios, los dispositivos y las aplicaciones solo se puedan comunicar con los recursos para los que cuenten con una autorización expresa de acceso. Al implementar la segmentación basada en identidades y con reconocimiento de aplicaciones, la microsegmentación limita los posibles daños provocados por los ciberataques, reduce la superficie de ataque y aplica el principio de Zero Trust.

En lo que respecta al tráfico de la red de norte a sur, las redes federales suelen usar cada vez más API para facilitar la comunicación entre los distintos sistemas. Como resultado, la protección de los terminales de las API se ha convertido en una de las principales prioridades. En los últimos años, los ataques a las API, incluidos los ataques de inyección, el Credential Stuffing y el acceso no autorizado a los datos, han aumentado mucho. Las agencias y los departamentos federales necesitan contar con soluciones de seguridad de las API integrales, que ofrezcan protección de todo el ciclo de vida de las API, y que permitan al personal de seguridad detectar, supervisar y proteger el tráfico de sus API en tiempo real. La detección de las API es especialmente importante. Es habitual tener API que nadie conoce.

Resumen de las soluciones Zero Trust de Akamai

Identidad

Akamai MFA es una solución de identidad de FIDO2 sin clave que protege las cuentas de los empleados del phishing y otros ataques de máquina intermediaria. Garantiza que solo los empleados con una autenticación sólida basada en identidades puedan acceder a las cuentas que poseen. Se deniegan otros accesos y se evita el robo de cuentas de empleados.

Dispositivos

Akamai Guardicore Segmentation es una solución de microsegmentación líder del sector, diseñada para limitar la propagación de este a oeste del ransomware y de otros tipos de malware. Al supervisar y aplicar políticas de forma continua en los dispositivos, Akamai Guardicore Segmentation puede verificar las configuraciones de estos, las instalaciones de software y las posibles vulnerabilidades, garantizando que solo puedan acceder a la red los dispositivos compatibles. Además, la solución ofrece un enfoque sin agentes para proteger los dispositivos del Internet de las cosas (IoT).

Akamai Enterprise Application Access es una solución integral de acceso de red Zero Trust que garantiza que solo los usuarios y dispositivos autenticados puedan acceder a las aplicaciones. Mediante la verificación de la identidad y del perfil de los dispositivos, Enterprise Application Access complementa las funciones de Akamai Guardicore Segmentation. Si se detecta que un dispositivo no cumple la normativa o representa un riesgo de seguridad, Enterprise Application Access puede restringir su acceso a las aplicaciones confidenciales.

Redes

Akamai API Security ofrece a los profesionales que trabajan en seguridad federal una visibilidad completa de todo el entorno de las API, gracias a la detección continua y al análisis en tiempo real del tráfico de norte a sur. La solución detecta API desconocidas, identifica vulnerabilidades y analiza el comportamiento de las API para que los equipos puedan detectar ataques y corregir riesgos en esta superficie de ataque de rápido crecimiento.

Akamai App & API Protector reúne en una única solución el firewall de aplicaciones web (WAF), la mitigación de bots, la seguridad de las API y la protección contra ataques distribuidos de denegación de servicio (DDoS) de capa 7. Identifica rápidamente las vulnerabilidades y mitiga las amenazas en las infraestructuras de toda la red y de las API.

Akamai Secure Internet Access Enterprise es un servicio de nombres de dominio (DNS) seguro basado en la nube que garantiza que los usuarios y dispositivos puedan conectarse a Internet de forma segura, estén donde estén, sin las complejidades y la sobrecarga de gestión asociadas a otras soluciones de seguridad.

Akamai Guardicore Segmentation proporciona un control selectivo del tráfico de red para permitir solo el tráfico legítimo.

Resumen de las soluciones Zero Trust de Akamai

Aplicaciones y cargas de trabajo

Akamai Enterprise Application Access proporciona acceso Zero Trust a los empleados, contratistas externos, partners y usuarios móviles, independientemente de su ubicación.

Akamai Guardicore Segmentation proporciona visibilidad y comprensión de las aplicaciones y cargas de trabajo.

Datos

Akamai Secure Internet Access Enterprise proporciona un acceso seguro a los datos gracias a funciones como el filtrado de contenido, la protección avanzada frente a amenazas y la prevención de la pérdida de datos. Permite la gestión del inventario de datos, evitando el acceso no autorizado y las filtraciones de datos.

Akamai Guardicore Segmentation: clave para la protección del tráfico de este a oeste

Akamai Guardicore Segmentation es una solución de microsegmentación líder diseñada para ayudar a las organizaciones, especialmente agencias y departamentos federales, a implementar controles de seguridad selectivos en los entornos locales y en la nube.

Segmentación detallada de las cargas de trabajo y las aplicaciones

A diferencia de la segmentación tradicional, que controla el acceso a nivel de la red, Akamai Guardicore Segmentation aplica políticas de seguridad a nivel de la aplicación y de la carga de trabajo. De esta forma se garantiza que el acceso esté muy restringido. Por ejemplo, en una agencia federal, una aplicación de recursos humanos (RR. HH.) se puede limitar para comunicarse exclusivamente con su base de datos de RR. HH, concreta, evitando, de esta forma, que los atacantes se muevan lateralmente si se produce una filtración.

Microsegmentación basada en identidades

Akamai Guardicore Segmentation aplica la segmentación tomando como base la identidad del usuario o del dispositivo en lugar de solo direcciones IP. De esta forma, se garantiza que el acceso se otorgue de forma dinámica según el rol, el nivel de confianza y la verificación en tiempo real. Por ejemplo, se puede restringir el acceso de los contratistas externos y los partners solo a los sistemas que necesiten, con lo que se reduce los riesgos relacionados con el acceso no autorizado.

Aplicación dinámica de políticas

Akamai Guardicore Segmentation ajusta de forma continua las políticas de seguridad según factores de tiempo real, como el comportamiento del usuario, el estado del dispositivo y la actividad de red. Si se detecta alguna actividad sospechosa, como un volumen anómalo de transferencias de datos, Akamai Guardicore Segmentation puede restringir el acceso, bloquear el tráfico o informar a los equipos de seguridad de forma automática. Con esta estrategia proactiva se garantiza que las políticas de seguridad se adapten para contrarrestar las amenazas emergentes.

Al integrar la microsegmentación de Akamai Guardicore Segmentation, las organizaciones pueden reforzar sus arquitecturas Zero Trust, minimizar el riesgo y mantener un control de acceso estricto sobre sus redes.

CASO REAL

Akamai Guardicore Segmentation en un entorno federal

Una agencia federal recientemente ha implementado una solución de microsegmentación de Akamai para proteger sus sistemas internos frente a ataques de movimiento lateral. Antes de adoptar Akamai Guardicore Segmentation, la agencia usaba la segmentación tradicional de la red, que permitía pocos detalles y un amplio acceso a los distintos segmentos de la red. De esta forma, había bastante riesgo de que se produjera movimiento lateral si alguna de las partes de la red era objeto de un ataque.

Con Akamai Guardicore Segmentation, la agencia logró lo siguiente:

- Implementar una segmentación detallada: al segmentar las cargas de trabajo a nivel de aplicación, la agencia redujo el riesgo de movimiento lateral y garantizó que todas las aplicaciones pudieran comunicarse exclusivamente con los recursos que necesitaban.
- Aumentar la visibilidad: las herramientas de visualización de la solución han permitido a la agencia contar con información detallada del tráfico interno, para permitir a los equipos de seguridad identificar y mitigar las posibles amenazas en tiempo real.
- Mejorar la seguridad: al integrar Akamai Guardicore Segmentation en sus sistemas de gestión de identidades y control de acceso, la agencia pudo usar Zero Trust en la red, garantizando una supervisión continua del acceso y un ajuste dinámico basado en los resultados de las evaluaciones de riesgo en tiempo real.

Con este ejemplo se demuestra el potencial de Akamai Guardicore Segmentation para mejorar la seguridad de la red, reducir el riesgo de movimiento lateral y garantizar que se concedan los permisos mínimos necesarios en todo momento.

Seguridad de las API: protección del tráfico de norte a sur

Akamai ofrece varias soluciones para garantizar la seguridad de las API. La plataforma de seguridad de las API de Akamai garantiza una visibilidad integral de las interacciones de las API, además de permitir detectar y mitigar automáticamente las amenazas de norte a sur en tiempo real. Gracias al análisis de comportamiento avanzado, las agencias y los departamentos federales pueden:

- **Identificar las API en la sombra** que podrían aprovechar los atacantes.
- **Supervisar los patrones de tráfico de las API** para detectar los intentos de acceso no autorizado.
- **Implementar la limitación de la velocidad de las API** para evitar el abuso y los ataques de denegación de servicio.
- **Identificar API olvidadas, descuidadas o desconocidas** para detectar posibles rutas de ataque.
- **Realizar un inventario de todas sus API** independientemente de la configuración o el tipo, incluidas RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC y gRPC.

Akamai Secure Internet Access Enterprise es un firewall del sistema de DNS basado en la nube diseñado para ayudar a los equipos de seguridad a garantizar que todos los usuarios y dispositivos, tanto dentro como fuera de la red, puedan conectarse a Internet de forma segura. Bloquea de forma proactiva las solicitudes de DNS maliciosas, como el malware, el ransomware, el phishing y la exfiltración de datos de DNS de bajo rendimiento. Secure Internet Access Enterprise reduce la complejidad de la seguridad, ya que no es necesario implementar, gestionar ni actualizar ningún dispositivo. El uso de la solución es sencillo e intuitivo.

Akamai App & API Protector detecta y mitiga las amenazas dirigidas a aplicaciones y API que se ejecutan a través de Akamai Cloud, además de bloquear cualquier tráfico que contenga posibles amenazas desenmascaradas por Akamai API Security. Si se implementan juntas, las protecciones de API de Akamai ofrecen una visibilidad completa y continua de las API, lo que permite que su personal de seguridad detecte, audite y responda a los problemas de seguridad de las API en todo el entorno de aplicaciones.

Uso de funciones interrelacionadas con Zero Trust

Uno de los principales retos de las arquitecturas Zero Trust es el riesgo de crear silos tecnológicos. Cada uno de los silos suele funcionar de forma independiente, lo que genera controles de seguridad, aplicaciones de políticas y detección de amenazas fragmentados. Esto nos demuestra la gran importancia que tiene la integración en todas las capas de seguridad.

En el caso de las agencias y departamentos federales que gestionan datos altamente confidenciales e infraestructuras complejas, este contexto fragmentado puede plantear importantes riesgos de seguridad. Los atacantes pueden aprovechar la falta de visibilidad entre los distintos silos (o pilares) o la aplicación incoherente de políticas en los distintos sistemas. Para mitigar estos riesgos, las organizaciones federales deben adoptar un modelo de seguridad unificado y para todos los pilares, donde se integren visibilidad, control y automatización en todos ellos, garantizando una aplicación coherente de las políticas y una reducción de las brechas que podrían aprovechar los adversarios.

Si se quiere conseguir un modelo de seguridad unificado, la integración entre los pilares debe centrarse en las tres áreas interrelacionadas del modelo de madurez Zero Trust de la CISA: Visibilidad y análisis, Automatización y orquestación, y Control. Estos elementos resultan esenciales para usar una arquitectura Zero Trust, donde el acceso y los permisos se ajustan de forma dinámica en todos los pilares en función de los resultados de las evaluaciones de riesgos en tiempo real.

Visibilidad y análisis

La visibilidad es fundamental para detectar las amenazas, entender el comportamiento del usuario y aplicar políticas de seguridad dinámicas en todos los pilares. Si no cuentan con una visibilidad completa de la forma en que las identidades, los dispositivos, las aplicaciones y los datos interactúan, los equipos de seguridad se quedan a oscuras, con lo que les resultará difícil detectar los comportamientos anómalos o los intentos de accesos no autorizados. Las soluciones de Akamai ofrecen visibilidad global de todos los pilares.

- Akamai Guardicore Segmentation supervisa el tráfico de red de las cargas de datos segmentadas, permitiendo una visibilidad del tráfico de este a oeste y detectando cualquier intento que se produzca de movimiento lateral en la red.
- Enterprise Application Access proporciona información sobre los patrones de acceso a las aplicaciones, realizando un seguimiento de cómo interactúan los usuarios con aplicaciones confidenciales, y garantizando que el acceso se ajuste de forma dinámica según los datos que se tengan del contexto.

Al integrar estas funciones, las agencias federales pueden correlacionar los datos de todos los pilares, obteniendo una visión unificada de los eventos de seguridad. Cuando un usuario solicita acceso a una aplicación, las soluciones de Akamai comprueban no solo la identidad del usuario sino también la seguridad del dispositivo, la red que se usa y el comportamiento en tiempo real de la aplicación, permitiendo a los equipos de seguridad detectar más rápidamente las posibles amenazas, minimizar el riesgo de derivación de privilegios, así como garantizar que los permisos se ajusten de forma dinámica como respuesta a los resultados de las evaluaciones de riesgos en tiempo real.

Automatización y orquestación

Responder a los incidentes y aplicar políticas en varios sistemas se puede convertir en un proceso manual muy lento. Con Zero Trust, las políticas de seguridad se tienen que aplicar de forma dinámica en todos los pilares, para lo que se necesita un gran nivel de automatización y orquestación. De esta forma, a medida que cambien los niveles de riesgo, se garantiza que los permisos se ajusten inmediatamente al nivel mínimo necesario, con lo que se reducen las posibilidades de que se produzca un error humano o de que se tarde en responder. Las soluciones de Akamai incluyen flujos de trabajo automatizados para ofrecer seguridad de las identidades, la red y las aplicaciones.

- Akamai Guardicore Segmentation ofrece microsegmentación automática, que ajusta de forma dinámica las políticas de segmentación de red en función de patrones de tráfico en tiempo real y de las anomalías detectadas. De esta forma, cualquier actividad sospechosa que se produzca en la red se aísla de forma rápida, evitando el movimiento lateral.
- Enterprise Application Access automatiza el proceso de protección del acceso a las aplicaciones, lo que garantiza que los usuarios solo puedan acceder a las aplicaciones mediante un proxy seguro, así como que los permisos se vayan actualizando de forma continua en función de cómo vayan cambiando los factores de riesgo.

Al automatizar estos procesos, las agencias y los departamentos federales pueden garantizar que la aplicación de las políticas de seguridad se realice de manera uniforme y rápida, con lo que se reducen las oportunidades para los atacantes.

Control

El control es la base de cualquier estrategia de seguridad, ya que garantiza una aplicación uniforme de las políticas y que se cumplan los requisitos de conformidad. En un modelo que se aplique a todos los pilares, el control debe garantizar que todas las medidas de seguridad se ajusten a los principios de Zero Trust. Gracias a las soluciones de Akamai, las agencias pueden implementar políticas de control que se apliquen a todos los pilares.

- Control de identidades: garantía de que los controles de acceso basados en identidad se aplican de manera uniforme en los distintos dispositivos, aplicaciones y redes, así como de que los permisos de acceso se revisan de forma periódica y se actualizan en función de los resultados de las evaluaciones de riesgos en tiempo real.
- Control de la red: aplicación de la segmentación de la red y de políticas de supervisión del tráfico en los distintos entornos, incluidas las infraestructuras locales, en la nube e híbridas; Akamai Guardicore Segmentation permite a las agencias definir políticas de segmentación de la red y garantizar que se apliquen de manera uniforme en toda la infraestructura.
- Control de los datos: protección de los datos confidenciales al garantizar que el acceso se restrinja basándose en los privilegios mínimos y que todas las transferencias de datos se supervisen de forma continua para detectar los accesos no autorizados o las actividades sospechosas.

Las tecnologías de Akamai se han diseñado para interactuar perfectamente y ofrecer a las agencias federales una arquitectura de seguridad totalmente integrada, válida para todos los pilares y compatible con Zero Trust.

CASO REAL

Integración en todos los pilares en una agencia federal

Una importante agencia federal se enfrentaba a importantes desafíos debido a unos políticas de seguridad fragmentadas en sus capas de identidad, red y aplicación. Existían sistemas distintos para gestionar la verificación de las identidades, el acceso a las aplicaciones y la segmentación de la red, lo que generaba una aplicación poco coherente de las políticas de seguridad, así como brechas de visibilidad.

Al adoptar las soluciones integradas de Akamai, la agencia pudo:

- **Combinar la seguridad de las identidades y las aplicaciones:** se integró la solución de gestión de acceso, credenciales e identidades (ICAM) de Akamai, Enterprise Application Access, para garantizar que el acceso a la aplicación se autenticara en todo momento basándose en datos de identidades en tiempo real. Esto permitió a la agencia ajustar de forma dinámica los permisos de la aplicación según el comportamiento del usuario y el estado del dispositivo.
- **Aplicar la segmentación dinámica de la red:** se implementó Akamai Guardicore Segmentation para segmentar el tráfico de la red en función del acceso a aplicaciones e identidades, impidiendo el movimiento lateral en los distintos sistemas confidenciales y garantizando una actualización continua de los permisos en función de los resultados de evaluaciones de riesgos en tiempo real.
- **Mejorar la visibilidad y la automatización:** la agencia pudo tener una visibilidad completa de su estrategia de seguridad y automatizar la aplicación de políticas en todos los pilares gracias a las herramientas de automatización y análisis integrados de Akamai.

Como resultado, pudo reducir su superficie de ataque y los tiempos de respuesta ante incidentes, además de lograr cumplir todas las normativas de seguridad federales. Este caso viene a demostrar el potencial de la integración en todos los pilares para transformar una arquitectura de seguridad fragmentada en un modelo de seguridad dinámico y cohesivo compatible con Zero Trust.

Conclusión

Las seguridad Zero Trust ya no es una opción. Resulta esencial para proteger a las agencias federales frente a sofisticadas ciberamenazas. Con la microsegmentación, la seguridad de las API y unos estrictos controles de identidades, las agencias y los departamentos federales pueden reducir de forma drástica el riesgo, pero seguir cumpliendo las normativas federales sobre ciberseguridad.

Akamai ofrece un conjunto completo de soluciones Zero Trust, entre ellas Akamai Guardicore Segmentation, Akamai API Security y Akamai Secure Internet Access Enterprise, para que las agencias puedan adoptar una estrategia de seguridad proactiva y adaptable. Al elegir a Akamai y su experiencia, las organizaciones federales pueden realizar una transición más rápida a Zero Trust y garantizar la resiliencia a largo plazo en lo relativo a la seguridad.

Ha llegado el momento de que las agencias federales actúen. Al integrar las soluciones de seguridad de Akamai, las agencias pueden lograr adoptar el modelo de madurez Zero Trust, mitigar los riesgos cibernéticos y proteger los activos digitales más esenciales de la nación.

Contacte con Akamai hoy mismo para obtener más información sobre nuestras soluciones de seguridad integradoras.

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Aprovechando la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn. Publicado en abril de 2025.