INFORME SOBRE LA SOLUCIÓN DE AKAMAI

Plataforma Akamai Guardicore: seguridad Zero Trust

Implementar una solución Zero Trust es un proceso demasiado complejo y caro para la mayoría de las empresas, especialmente cuando las medidas de protección abarcan activos en local y en la nube, y la plantilla trabaja de forma remota o en la oficina. Por eso, la plataforma Akamai Guardicore está diseñada para abordar de forma eficaz todas las facetas de Zero Trust con una sola consola y un solo agente.

A medida que las ciberamenazas se vuelven más sofisticadas y los requisitos normativos más estrictos, las organizaciones tienen que hacer frente a una enorme presión para proteger sus redes sin perder la eficiencia operativa. La plataforma Akamai Guardicore ofrece a las organizaciones una solución Zero Trust con todas las herramientas y capacidades que necesitan para implementar de forma eficaz un modelo de seguridad Zero Trust sólido con el que abordar estos retos.

El diseño de la plataforma Akamai Guardicore es compatible con proyectos Zero Trust, puesto que combina la mejor microsegmentación, el acceso de red Zero Trust (ZTNA), el firewall de DNS y la búsqueda de amenazas en una sola plataforma. De forma conjunta, estos componentes optimizan los esfuerzos de Zero Trust para reducir significativamente la superficie de ataque y reforzar la estrategia de seguridad en toda la empresa.

Plataforma Akamai Guardicore

Microsegmentación

Uno de los componentes clave de la plataforma Akamai Guardicore es la microsegmentación. Tradicionalmente, la seguridad de la red se ha basado en defensas perimetrales que se centran en proteger los límites externos de la red. No obstante, a medida que evolucionan las ciberamenazas, es más que evidente que estas defensas perimetrales ya no son suficientes para protegerse de ataques sofisticados.

Ventajas

Infraestructura consolidada
Implemente rápidamente y amplíe según sus necesidades sin esfuerzo con un impacto mínimo en el rendimiento.

Visibilidad amplia y detallada
Obtenga información completa sobre los recursos de red y las comunicaciones.

Motor de directivas unificado
Simplifique la aplicación de políticas en diversos entornos desde una interfaz de usuario.

Flexibilidad modular
Aproveche los componentes modulares adaptados a sus necesidades empresariales.

Cobertura completa
Proteja todos sus recursos de forma local y en la nube, así como a los usuarios en casa y en la oficina.

Las mejores soluciones
Combine la microsegmentación líder del sector con ZTNA para mejorar la estrategia de seguridad.

Akamai

La microsegmentación adopta un enfoque diferente al dividir la red en segmentos más pequeños y manejables, a los que aplica políticas de seguridad individuales en función del principio de privilegios mínimos. Este enfoque detallado de la seguridad garantiza que, incluso si un segmento se ve comprometido, el resto de la red permanezca protegida. Gracias a Akamai Guardicore Segmentation, todos los activos están protegidos, incluidos los centros de datos locales, las instancias de nube, los sistemas operativos heredados, los dispositivos del IoT y los clústeres de Kubernetes, entre otros, sin tener que cambiar de consola.

Acceso de red Zero Trust

Además de la microsegmentación, la plataforma Akamai Guardicore también ofrece funciones de acceso de red Zero Trust (ZTNA). ZTNA es un modelo de seguridad que incorpora el principio de Zero Trust, lo que significa que, de forma predeterminada, ningún dispositivo o usuario es de confianza, incluso si forman parte de la red corporativa. En su lugar, el acceso a los recursos se concede en función de una estricta verificación de la identidad, el nivel de seguridad del dispositivo y otros factores contextuales. Este enfoque minimiza el riesgo de acceso no autorizado y ayuda a las organizaciones a evitar las filtraciones de datos y las amenazas internas.

Firewall de DNS

Otro de los componentes fundamentales de la plataforma Akamai Guardicore es el firewall de DNS. El sistema de nombres de dominio (DNS) es un componente fundamental de Internet que convierte los nombres de dominio legibles por el ser humano en direcciones IP. No obstante, también es uno de los objetivos más comunes de los ciberataques, puesto que muchas variantes de malware dependen del DNS para comunicarse con servidores de mando y control o para exfiltrar datos. Con un firewall de DNS, las organizaciones pueden bloquear las consultas de DNS maliciosas y evitar que el malware se comunique con dominios malintencionados, lo que reduce el riesgo de sufrir filtraciones de datos y otras ciberamenazas.

Búsqueda de amenazas

Por último, la plataforma Akamai Guardicore incluye un servicio de segmentación adaptable que permite a las organizaciones identificar y mitigar de forma proactiva las amenazas de seguridad antes de que se conviertan en incidentes. La búsqueda de amenazas implica la búsqueda activa de señales de riesgo dentro de la red, como comportamientos anómalos o indicadores de compromiso (IOC). Con la ayuda de herramientas y técnicas de búsqueda de amenazas, las organizaciones pueden mantenerse un paso por delante de los ciberadversarios y proteger sus valiosos activos frente a cualquier daño.

Además de sus capacidades principales, la plataforma Akamai Guardicore cuenta con otras ventajas clave que la diferencian del resto de soluciones de seguridad del mercado. La plataforma proporciona una infraestructura ligera y consolidada que minimiza el exceso de agentes y la fatiga de la consola, lo que permite a las organizaciones implementar y gestionar su pila de seguridad de forma más eficaz. Además, ofrece una visibilidad amplia y completa de los activos de red y las comunicaciones, lo que permite a los profesionales de la seguridad obtener información completa sobre su entorno de red y responder a las amenazas de forma rápida y eficaz.

> En el informe Gartner®, Quick Answer: What is Zero Trust Networking?, Andrew Lerner y John Watts el 13 de septiembre de 2023: “Gartner sugiere implementar la microsegmentación o ZTNA para avanzar hacia una estrategia de red Zero Trust (ZTN)".*

* GARTNER es una marca comercial registrada y una marca de servicio de Gartner, Inc. y/o sus filiales en EE. UU. y otros países, y se usa aquí con permiso. Todos los derechos reservados.

Visite Seguridad Zero Trust de Akamai para obtener más información.