INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Firewall de DNS de Akamai Guardicore

Visibilidad y control completos del tráfico de DNS de las cargas de trabajo

El sistema de nombres de dominio (DNS) es esencial para los servicios de Internet, pero no diferencia entre solicitudes benignas y maliciosas. Por tanto, las empresas han implementado firewalls de DNS para inspeccionar las consultas del DNS, bloquear los dominios dañinos y resolver los seguros. Sin embargo, dado que el uso de DNS abarca cargas de trabajo, servidores y otros dispositivos conectados, la falta de visibilidad y control sobre este tráfico de DNS conlleva riesgos de seguridad adicionales.

Segmentación unificada y un firewall de DNS

Akamai Guardicore Segmentation, combinada con el firewall de DNS de Akamai Guardicore, ofrece una defensa sólida para su red. Al bloquear las solicitudes de DNS maliciosas y aislar los segmentos de red críticos, esta integración reduce significativamente la superficie de ataque y evita la propagación de amenazas. Este enfoque de doble capa mejora la seguridad, garantiza el cumplimiento y mantiene la eficiencia operativa, lo que lo convierte en una solución esencial para una protección de red fiable.

Cómo funciona el firewall de DNS de Akamai Guardicore

El firewall de DNS de Akamai Guardicore se puede activar en cuestión de minutos para ofrecer seguridad y reducir la complejidad sin afectar al rendimiento. Todos los dominios solicitados se cotejan con la información sobre amenazas en tiempo real de Akamai, y las solicitudes de dominios maliciosos se bloquean automáticamente. El uso de DNS como capa de seguridad inicial bloquea de forma proactiva las amenazas en las primeras fases de intrusión antes de establecer cualquier conexión IP. Además, el DNS está diseñado para ser eficaz en la mayoría de los puertos y protocolos, con el fin de proteger incluso frente al malware que no utilice los puertos y protocolos web estándar.

Cuando se bloquea una solicitud de DNS, se crea un incidente que proporciona a los equipos de seguridad y búsqueda de amenazas información detallada sobre por qué se ha bloqueado la amenaza, el origen y el destino de la solicitud, que se pueden visualizar en un mapa, y detalles sobre los indicadores de riesgo.

Ventajas para su empresa

Protección integral contra amenazas
Al filtrar el tráfico de DNS en el perímetro de la red y al aplicar la microsegmentación a nivel de red interno, las empresas pueden defenderse de manera eficaz frente a los intentos de malware, phishing, mando y control y filtración de datos.

Eficacia mejorada en la búsqueda de amenazas
Los incidentes ayudan a los equipos de seguridad a detectar, analizar y responder mejor a las amenazas emergentes, lo que minimiza el impacto de las infracciones y refuerza las defensas generales de ciberseguridad.

Visibilidad y contexto mejorados
La combinación del firewall de DNS y la microsegmentación proporciona una mayor visibilidad de los patrones de tráfico de DNS para identificar posibles amenazas e infracciones de políticas.

Gestión simplificada
La integración de un firewall de DNS con microsegmentación optimiza la gestión de seguridad, ya que proporciona una supervisión, aplicación y creación de políticas unificadas. Esto reduce la complejidad y los gastos operativos, lo que permite a las empresas gestionar de forma eficaz su infraestructura de seguridad.

Cloud Security Intelligence de Akamai

El firewall de DNS de Akamai Guardicore, avalado por Cloud Security Intelligence de Akamai, proporciona información en tiempo real sobre las amenazas y los riesgos que estas pueden suponer para las empresas. La inteligencia ante amenazas de Akamai está diseñada para proteger contra los peligros actuales o relevantes que puedan afectar a su empresa y para minimizar el número de alertas por falsos positivos que deben investigar los equipos de seguridad. Esta inteligencia se basa en los datos recopilados ininterrumpidamente por Akamai Connected Cloud, que puede llegar a gestionar hasta un 30 % del tráfico web mundial y distribuye hasta 14 billones de consultas de DNS diarias. La inteligencia de Akamai se complementa con cientos de fuentes de información externas sobre amenazas, y el resultado de dicha combinación se analiza y se mantiene continuamente utilizando técnicas de análisis de comportamiento avanzadas, inteligencia artificial y algoritmos propios. A medida que se van identificando nuevas amenazas, se van agregando al conjunto de datos de inteligencia contra amenazas para ofrecer una protección en tiempo real.

Akamai Connected Cloud

El servicio de firewall de DNS de Akamai Guardicore se basa en Akamai Connected Cloud, la plataforma más distribuida del mundo para cloud computing, seguridad y entrega de contenido. Akamai Connected Cloud ofrece un acuerdo de nivel de servicio del 100 % de disponibilidad y garantiza una fiabilidad óptima para la seguridad web de una empresa.

Visite Seguridad Zero Trust de Akamai para obtener más información.

©2024 Akamai Technologies | Asistencia |
| Publicado en septiembre de 2024