

Líder del sector publicitario adopta el modelo Zero Trust

La empresa pudo optar a cobertura asegurativa por riesgos cibernéticos, evitó ataques y mejoró la protección de su propiedad intelectual mediante la microsegmentación.



Seguro cibernético
afianzado



Amenazas detectadas



Ataques mitigados

Marcas y telespectadores, conectados

Este líder mundial en publicidad de televisión conectada ayuda a las marcas a llegar a audiencias de streaming fragmentadas y rentabilizar al máximo el gasto publicitario. Cuando la empresa quiso optar a un seguro cibernético, implementó [Akamai Guardicore Segmentation](#) para reforzar sus medidas de seguridad.

Cualificación para el ciberseguro

Como empresa pionera, no es de extrañar que sea especialmente protectora con su propiedad intelectual (PI). Al igual que otras empresas modernas, esa PI podría quedar expuesta en caso de que un bot o un hacker se infiltrasen en sus aplicaciones o servidores internos.

Para mitigar el impacto financiero de una posible filtración, su empresa matriz le instó a adquirir un seguro cibernético. Con el aumento de los [ciberataques](#), las aseguradoras evalúan el nivel de ciberseguridad de las empresas antes de asignarles una póliza. Teniendo esto en cuenta, la empresa decidió implementar la segmentación interna.



Advertising
Leader

Ubicación

Estados Unidos

Sector

Medios de comunicación
y entretenimiento

Solución

[Akamai Guardicore
Segmentation](#)

Implementación de controles de segmentación internos

La empresa encontró la solución en Akamai Guardicore Segmentation, que ofrece microsegmentación basada en software. Diseñada para impedir que los atacantes puedan **moverse lateralmente** por el entorno digital, Akamai Guardicore Segmentation es un componente clave para proteger los activos de PI de la empresa. Mediante la microsegmentación, separa los servidores, las aplicaciones y las cargas de trabajo que contienen activos de PI del resto de su infraestructura.

Al utilizar esta solución para proteger los activos esenciales y restringir el movimiento lateral, la empresa garantiza un entorno de TI donde los atacantes no pueden moverse fácilmente. Con una visibilidad exhaustiva de sus movimientos, tanto en el entorno físico como virtual, es posible detener a los atacantes de raíz.

Detección y prevención de los ataques de ransomware

Para confirmar que Akamai Guardicore Segmentation era su mejor apuesta, la empresa decidió realizar una prueba de concepto (PoC), durante la cual la solución de Akamai detectó numerosos atacantes e incluso un incidente de ransomware.

Después de ver el potencial de Akamai Guardicore Segmentation para proteger su entorno, la empresa supo que había encontrado la solución perfecta. Ahora tiene previsto segmentar más de 3000 servidores (una combinación de Linux, bare metal y en la nube) y aproximadamente 1500 contenedores (Docker y Kubernetes).

