

INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Akamai Guardicore Segmentation

Detenga el movimiento lateral con controles exhaustivos de visibilidad y microsegmentación

La infraestructura de TI empresarial sigue evolucionando de los centros de datos locales tradicionales a las arquitecturas de nube y nube híbrida, con una combinación de plataformas y modelos de implementación de aplicaciones. Aunque esta transformación digital ayuda a muchas organizaciones a lograr una mayor agilidad empresarial, reducir los costes de infraestructura y permitir el trabajo remoto, también crea una superficie de ataque mayor y más compleja que no cuenta con un perímetro bien definido. Todos los servidores, máquinas virtuales, instancias de nube y terminales son un posible punto de exposición, y con la prevalencia de amenazas como el ransomware y las vulnerabilidades de día cero, los atacantes cada vez tienden más a avanzar lateralmente hacia objetivos de mayor valor cuando encuentran la forma de entrar.

Akamai Guardicore Segmentation proporciona el método más sencillo, rápido e intuitivo para aplicar los principios Zero Trust en su red. La solución se ha diseñado para detener el movimiento lateral mediante la visualización de la actividad en sus entornos de TI, la implementación de políticas de microsegmentación precisas y la detección rápida de posibles filtraciones.

Características principales de la solución

Segmentación exhaustiva basada en IA

Implemente políticas con unos pocos clics con ayuda de recomendaciones de IA, plantillas para solución de problemas de ransomware y otros casos de uso habituales, además de atributos de carga de trabajo precisos, como procesos, usuarios y nombres de dominio.

Visibilidad en tiempo real o de registros anteriores

Asigne flujos y dependencias de las aplicaciones hasta niveles de usuario y proceso en tiempo real o basándose en registros anteriores.

Gran compatibilidad con plataformas

Englobe los sistemas operativos modernos y heredados mediante servidores bare metal, máquinas virtuales, contenedores, IoT e instancias en la nube.

Etiquetado flexible de activos

Consiga una mayor visibilidad y un mejor cumplimiento añadiendo información contextual detallada para personalizar el etiquetado y automatícelo integrándolo todo con herramientas de orquestación y bases de datos de gestión de la configuración.

Múltiples métodos de protección

Integre las funciones de detección de brechas, defensa e inteligencia contra amenazas para reducir el tiempo de respuesta ante incidentes.

VENTAJAS PARA SU EMPRESA



Prevención del ransomware



Implantación de Zero Trust



Aceleración del cumplimiento



Acordonamiento de las aplicaciones críticas



Migración segura a la nube



Protección de los trabajadores remotos



Protección de los terminales



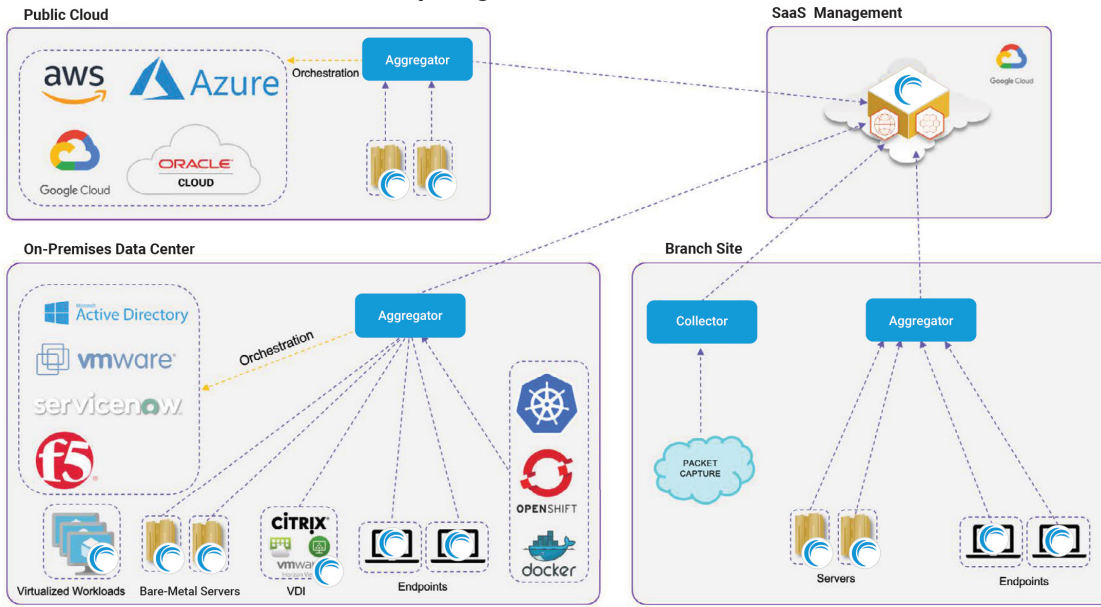
Seguridad más allá de los firewalls internos



Cómo funciona

Akamai Guardicore Segmentation recopila información detallada sobre la infraestructura de TI de una organización mediante una combinación de sensores basados en agentes, recopiladores de datos basados en red, registros de flujo de nubes privadas virtuales de proveedores de nube e integraciones que habilitan la funcionalidad sin agente. Se añade contexto relevante a esta información a través de un proceso de etiquetado flexible y altamente automatizado que incluye la integración con fuentes de datos existentes, como sistemas de orquestación y bases de datos de gestión de la configuración.

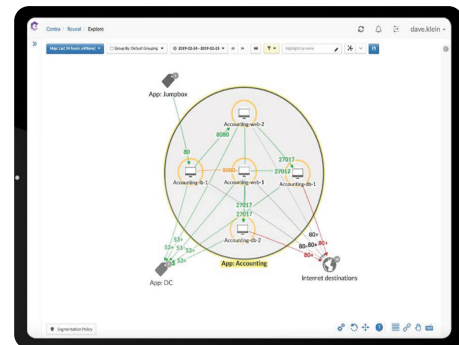
Topología de la infraestructura



La mayoría de los clientes utiliza la gestión basada en SaaS, pero también hay opciones de gestión in situ.

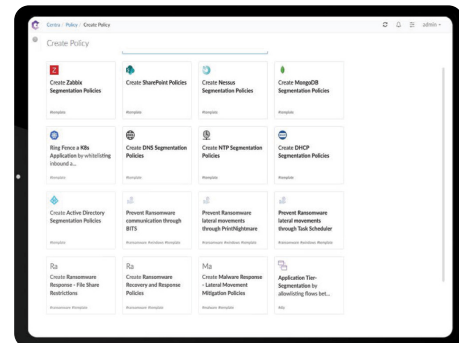
Mapa de red

El resultado es un mapa dinámico de toda la infraestructura de TI que permite a los equipos de seguridad ver la actividad con gran detalle a nivel de usuario y proceso en tiempo real o de registros anteriores. Gracias a esta información detallada y a los flujos de trabajo de políticas basados en IA, la creación de políticas de segmentación resulta rápida e intuitiva y se basa en el contexto real de la carga de trabajo.



Plantillas

Resulta sencillo crear políticas con plantillas prediseñadas para los casos de uso más comunes. La aplicación de políticas es totalmente independiente de la infraestructura subyacente, de modo que las políticas de seguridad se pueden crear o modificar sin cambios complejos en la red ni tiempo de inactividad. Además, las políticas siguen la carga de trabajo sin importar dónde se encuentre, ya sea en los centros de datos locales o en los entornos de nube pública. Nuestras funciones de segmentación se complementan con un sofisticado conjunto de opciones de detección de brechas y defensa contra amenazas, así como con **Akamai Hunt**, nuestro servicio gestionado de búsqueda de amenazas.



Protección integral a escala



En cualquier entorno

Proteja las cargas de trabajo en entornos de TI complejos con una combinación de cargas de trabajo locales, máquinas virtuales, sistemas heredados, contenedores y orquestación, instancias de nube pública/privada e IoT/OT.



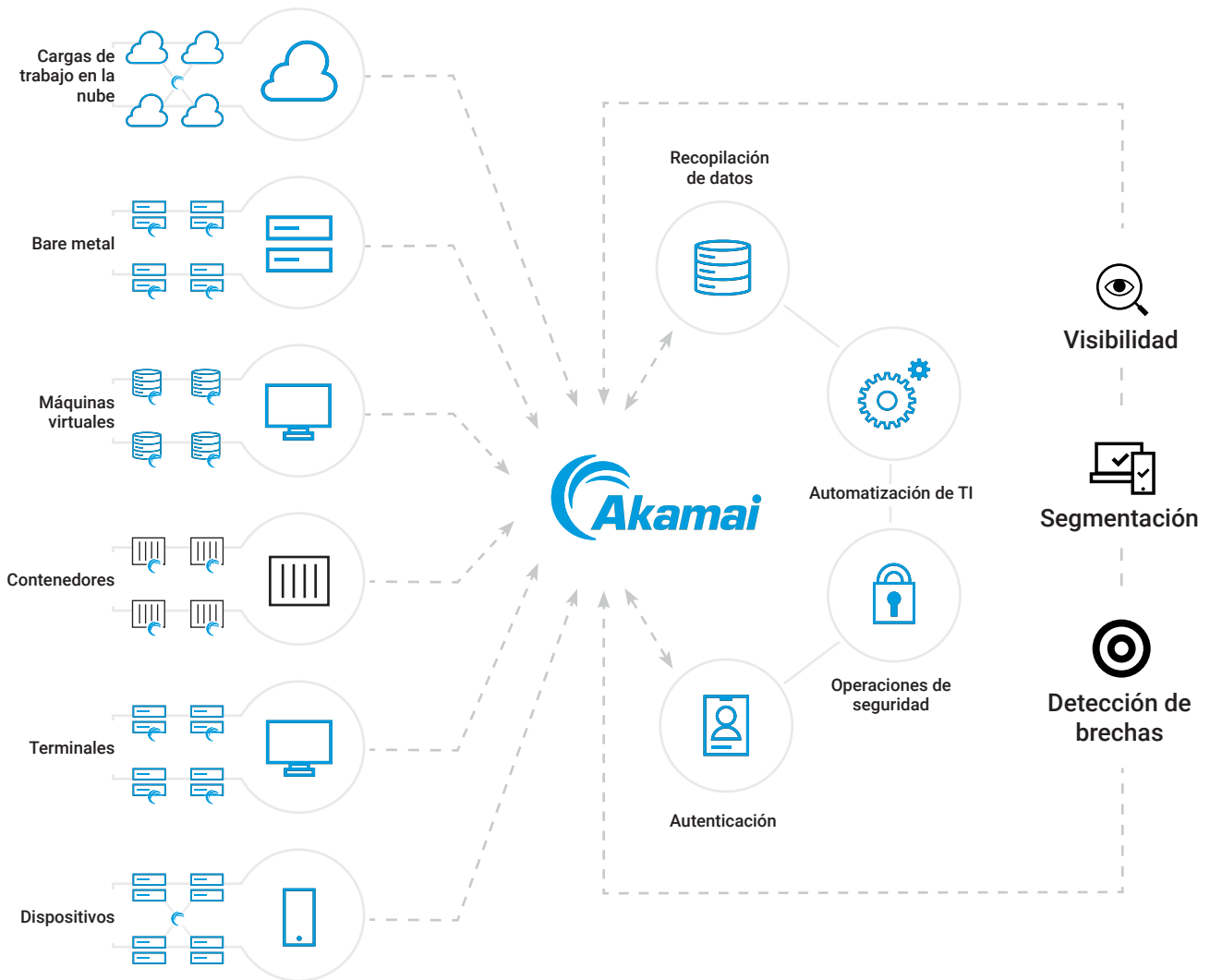
Una seguridad simplificada

Simplifique la gestión de la seguridad con una plataforma que proporciona visualización de red, segmentación, defensa contra amenazas, funciones de detección de brechas e implantación guiada de políticas para iniciativas Zero Trust.



Rendimiento y escalabilidad empresarial

Comience con la protección de sus activos digitales más importantes y amplíe para proteger toda su empresa sin complicaciones, cambios en la infraestructura ni cuellos de botella de rendimiento.



Plataformas y tecnologías compatibles

- Akamai Guardicore Segmentation está diseñado para integrarse con su infraestructura actual.
- La compatibilidad con los diferentes sistemas operativos se amplía continuamente para adaptarse a las exigencias de nuestros clientes.
- Consulte nuestra [página de partners tecnológicos](#) para obtener una lista completa de las integraciones que hemos llevado a cabo.

Sistemas operativos

Linux



Apple



Microsoft



Unix



Proveedores de nube pública



Hipervisores



Orquestación de hipervisores



Puertas de enlace de seguridad



Orquestación de contenedores y motores



Navegadores para consola web



Requisitos mínimos de memoria y sistema

Management Server 32 GB RAM, 8 vCPUs, 530 GB	Aggregator 4 GB RAM, 4 vCPUs, 30 GB
Deception Server 32 GB RAM, 8 vCPUs, 100 GB	ESC Collector 2 GB RAM, 2 vCPUs, 30 GB

INTELLIGENCE-SHARING EXPORT PROTOCOLS

STIX, Syslog, SMTP, CEF, Open REST API

Para obtener más información sobre Akamai Guardicore Segmentation o para solicitar una demostración personalizada del producto, visite akamai.com/guardicore.