INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

# Akamai Guardicore Segmentation

**Detenga el movimiento lateral con controles de visibilidad y microsegmentación precisos**

La infraestructura de TI empresarial continúa evolucionando desde centros de datos locales tradicionales hasta arquitecturas en la nube y en la nube híbrida, con una mezcla de plataformas y modelos de implementación de aplicaciones. Aunque esta transformación digital ayuda a muchas organizaciones a lograr una mayor agilidad empresarial, reducir los costos de infraestructura y permitir el trabajo remoto, también crea una superficie de ataque más grande y compleja que no tiene un perímetro bien definido. Cada máquina virtual, instancia de nube, extremo y servidor individual ahora es un posible punto de exposición. Con la prevalencia de amenazas como el ransomware y las vulnerabilidades de día cero, los atacantes se están volviendo cada vez más expertos en avanzar lateralmente hacia objetivos de alto valor cuando encuentran una forma de entrar.

Akamai Guardicore Segmentation proporciona la manera más simple, rápida e intuitiva de implementar los principios de confianza cero dentro de su red. Está diseñado para detener el movimiento lateral mediante la visualización de la actividad dentro de sus entornos de TI, la implementación de políticas de microsegmentación precisas y la detección de posibles vulneraciones rápidamente.

## VENTAJAS PARA SU EMPRESA

- Evitación del ransomware
- Logro de Zero Trust
- Agilización del cumplimiento
- Seguridad integral para aplicaciones esenciales
- Migraciones seguras en la nube
- Resguardo de la fuerza de trabajo remota
- Protección de extremos
- Movimiento más allá de los firewalls internos

## Capacidades principales de la solución

### Segmentación precisa impulsada por IA

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

### Visibilidad histórica y en tiempo real

Asigne las dependencias de la aplicación y los flujos hacia los niveles de usuario y proceso en tiempo real o de manera histórica.

### Amplia compatibilidad con la plataforma

Abarque sistemas operativos modernos y antiguos en servidores sin SO, máquinas virtuales, contenedores, IoT e instancias de nube.

### Etiquetado flexible de activos

Agregue contexto enriquecido con una jerarquía de etiquetado personalizable para visibilidad y aplicación, además de integración en herramientas de organización y bases de datos de administración de configuración para etiquetado automatizado.

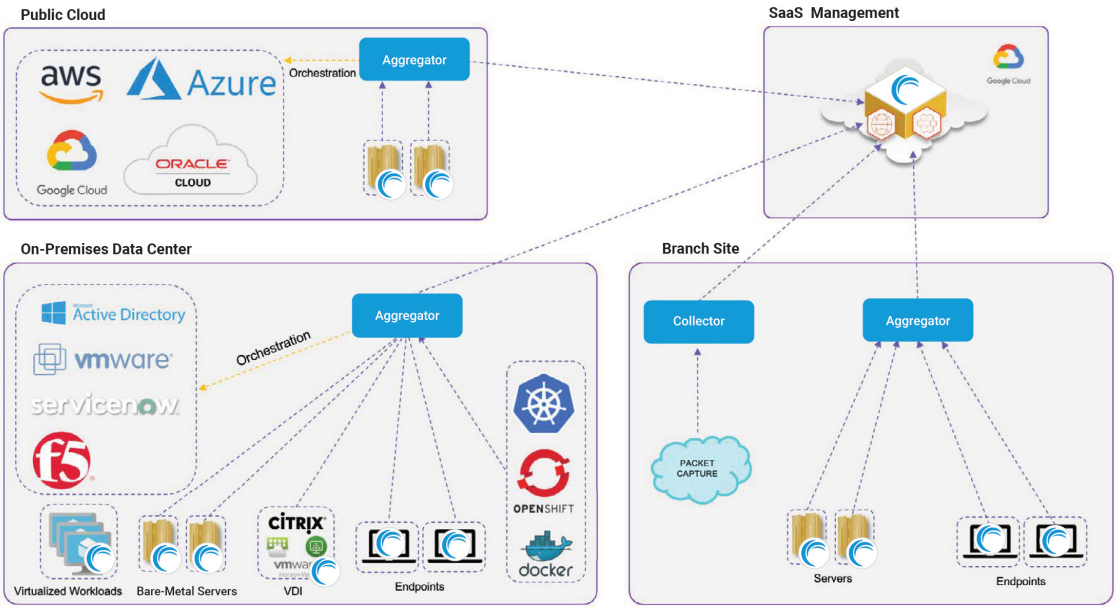
### Múltiples métodos de protección

Integre inteligencia de amenazas, defensa y capacidades de detección de vulneraciones para reducir el tiempo de respuesta ante incidentes.

## Cómo funciona

Akamai Guardicore Segmentation recopila información detallada sobre la infraestructura de TI de una organización a través de una combinación de sensores basados en agentes, recopiladores de datos basados en red, registros de flujo de nube privada virtual de proveedores de nube e integraciones que permiten la funcionalidad sin agente. Se agrega el contexto relevante a esta información a través de un proceso de etiquetado flexible y altamente automatizado que incluye la integración en las fuentes de datos existentes, tales como los sistemas de organización y las bases de datos de administración de la configuración.

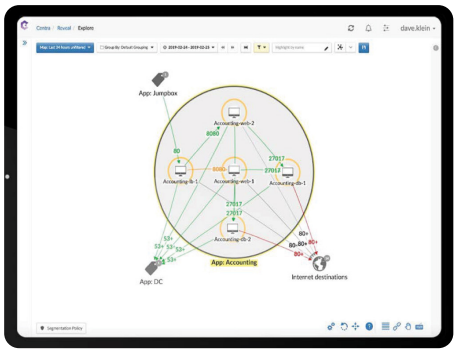
### Topología de infraestructura




La mayoría de los clientes utiliza la administración de SaaS, pero también están disponibles las opciones de administración en las instalaciones.

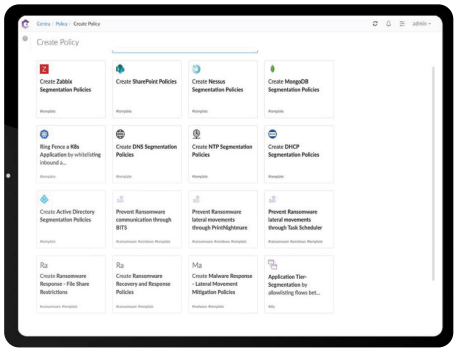
### Mapa de red

El resultado es un mapa dinámico de toda la infraestructura de TI que permite a los equipos de seguridad ver la actividad con precisión a nivel de usuario y proceso en tiempo real o de manera histórica. Estos detalles, combinados con flujos de trabajo de políticas basados en IA, permiten que la creación de políticas de segmentación sea rápida, intuitiva y basada en el contexto de la carga de trabajo real.



### Plantillas

La creación de políticas se simplifica con plantillas prediseñadas para los casos de uso más comunes. La aplicación de políticas se desvincula completamente de la infraestructura subyacente, de modo que las políticas de seguridad se pueden crear o modificar sin cambios de red complejos ni tiempo de inactividad. Además, las políticas se aplican a la carga de trabajo sin importar dónde resida, en centros de datos locales o entornos de nube pública. Nuestras capacidades de segmentación se complementan con un sofisticado conjunto de capacidades de defensa ante amenazas y detección de vulneraciones, además de Akamai Hunt, nuestro servicio administrado de búsqueda de amenazas.



# Protección integral a escala

## Cualquier entorno

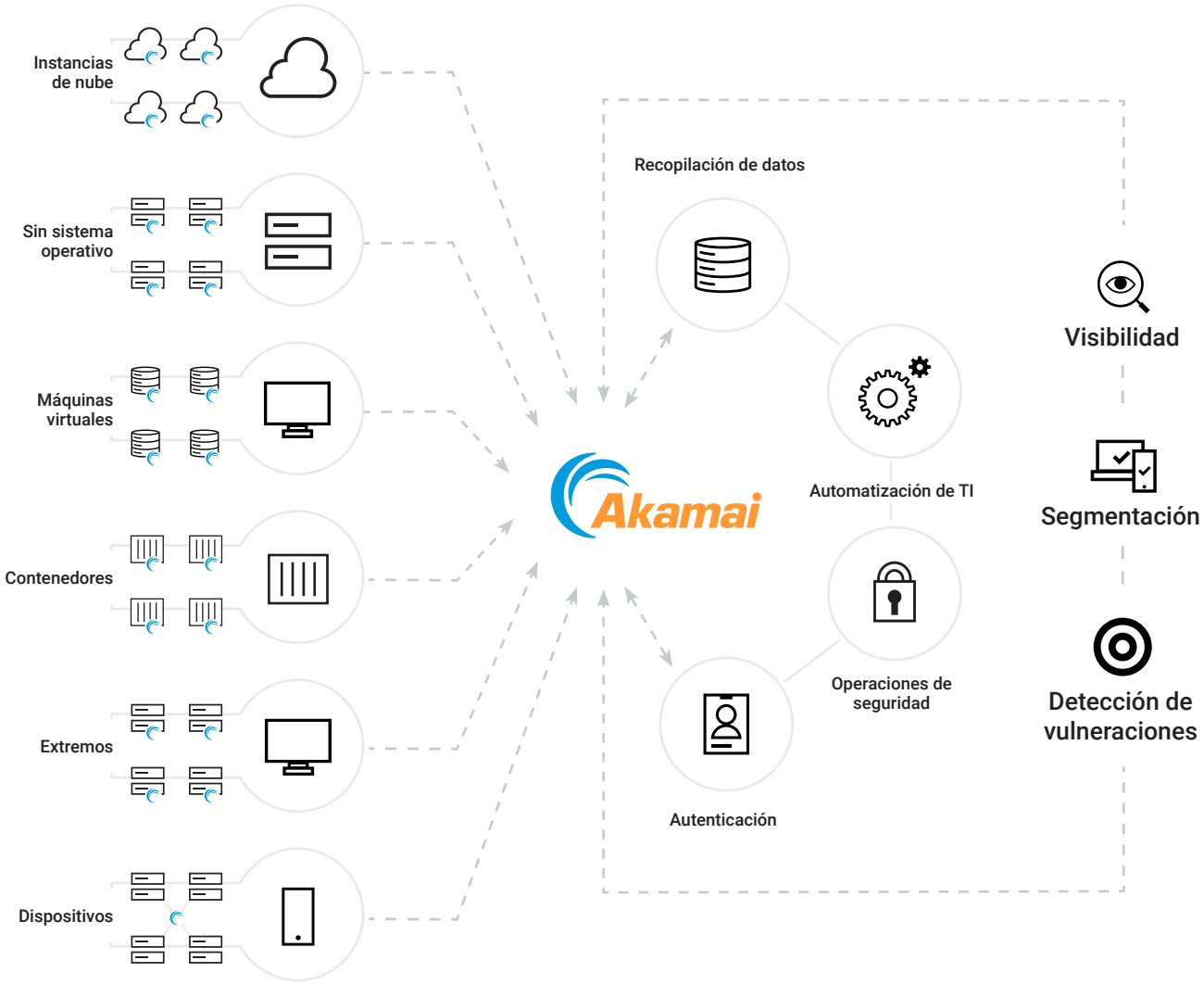
Proteja las cargas de trabajo en entornos de TI complejos con una combinación de cargas de trabajo locales, máquinas virtuales, sistemas heredados, contenedores y organización, instancias de nube pública/privada e IoT/TO.

## Seguridad simplificada

Simplifique la administración de la seguridad con una plataforma que proporciona visualización de la red, segmentación, defensa contra amenazas, capacidades de detección de vulneraciones y aplicación de políticas guiadas para iniciativas de Zero Trust.

## Escalabilidad y rendimiento empresarial

Comience con una protección focalizada de sus activos digitales más importantes y escale para proteger toda su empresa sin complejidad, cambios en la infraestructura ni cuellos de botella en el rendimiento.



## Plataformas y tecnologías compatibles

- Akamai Guardicore Segmentation está diseñado para integrarse en su infraestructura existente.
- Nuestra compatibilidad con sistemas operativos se expande continuamente con las necesidades de nuestros clientes.
- Revise la página de nuestros socios de tecnología para obtener una lista completa de nuestras integraciones.

## Sistemas operativos

Linux


Apple

Microsoft


Unix


## Proveedores de nube pública


## Hipervisores


## Organización de hipervisión


## Puertas de enlace de seguridad


## Organización de contenedores y motores


## Navegadores para consola web

## Requisitos mínimos del sistema y de memoria

**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 bien para solicitar una demostración personalizada del producto, visite akamai.com/guardicore.

 | Soporte | | Publicado en julio de 2023