Guardicore Segmentation de Akamai

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 modelos de implementación de aplicaciones y 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.

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

CASOS DE USO

- **Prevención del ransomware**
- **Migración segura a la nube**
- **Implantación del modelo Zero Trust**
- **Protección de los trabajadores remotos**
- **Aceleración del cumplimiento**
- **Protección de los terminales**
- **Delimitación de aplicaciones esenciales**
- **Sustitución de firewall internos**

CARACTERÍSTICAS PRINCIPALES DE LA SOLUCIÓN

Segmentación exhaustiva basada en IA

Implemente políticas en 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 a 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

Añada contexto enriquecido con una jerarquía de etiquetado personalizable e integración con herramientas de orquestación y bases de datos de gestión de la configuración

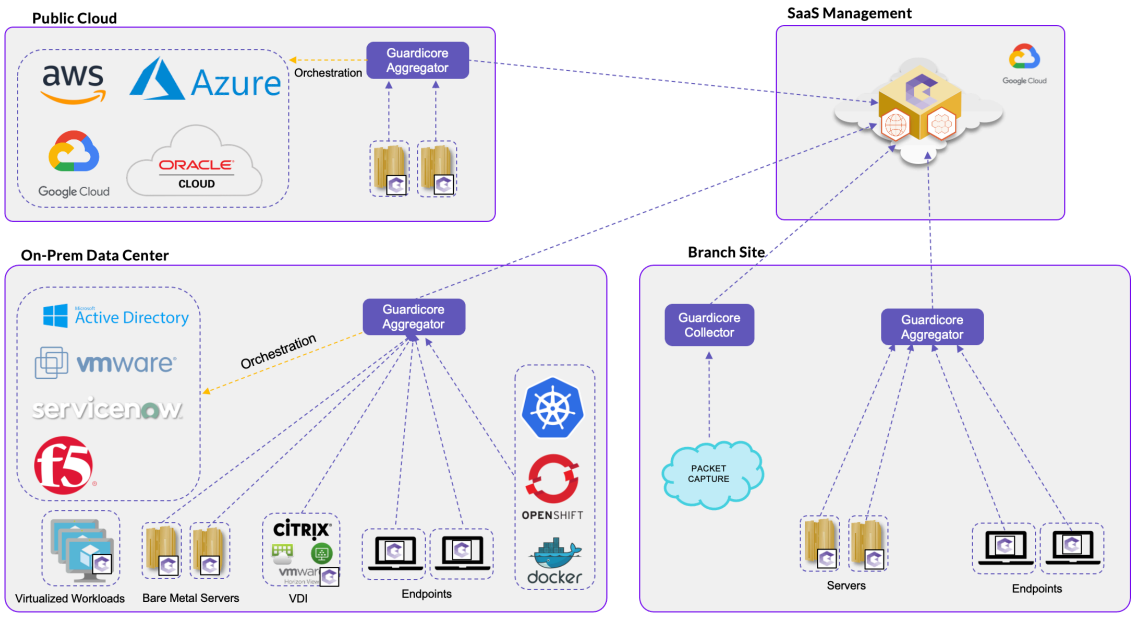
Múltiples métodos de protección

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

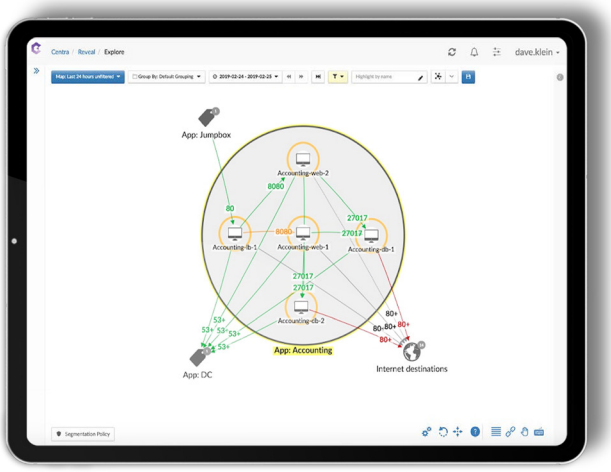
Funcionamiento

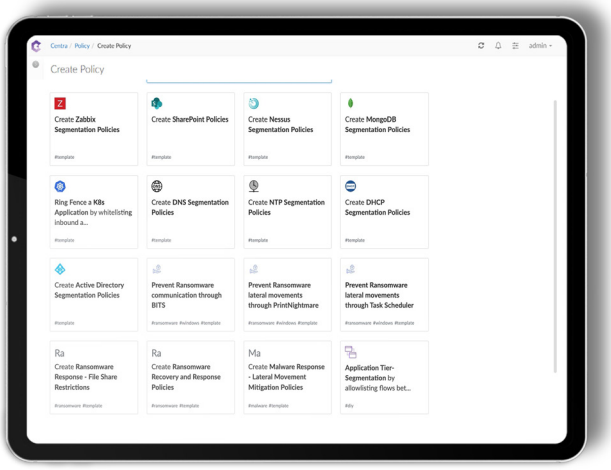
Guardicore Segmentation de Akamai recopila información detallada sobre la infraestructura de TI de una organización mediante una combinación de sensores basados en agentes, recopiladores de datos basados en red, registros de flujo de nubes privadas virtuales de proveedores de nube e integraciones que 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 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 servicios de búsqueda de amenazas proporcionados por Akamai Threat Labs.

PROTECCIÓN INTEGRAL A ESCALA

Cualquier entorno

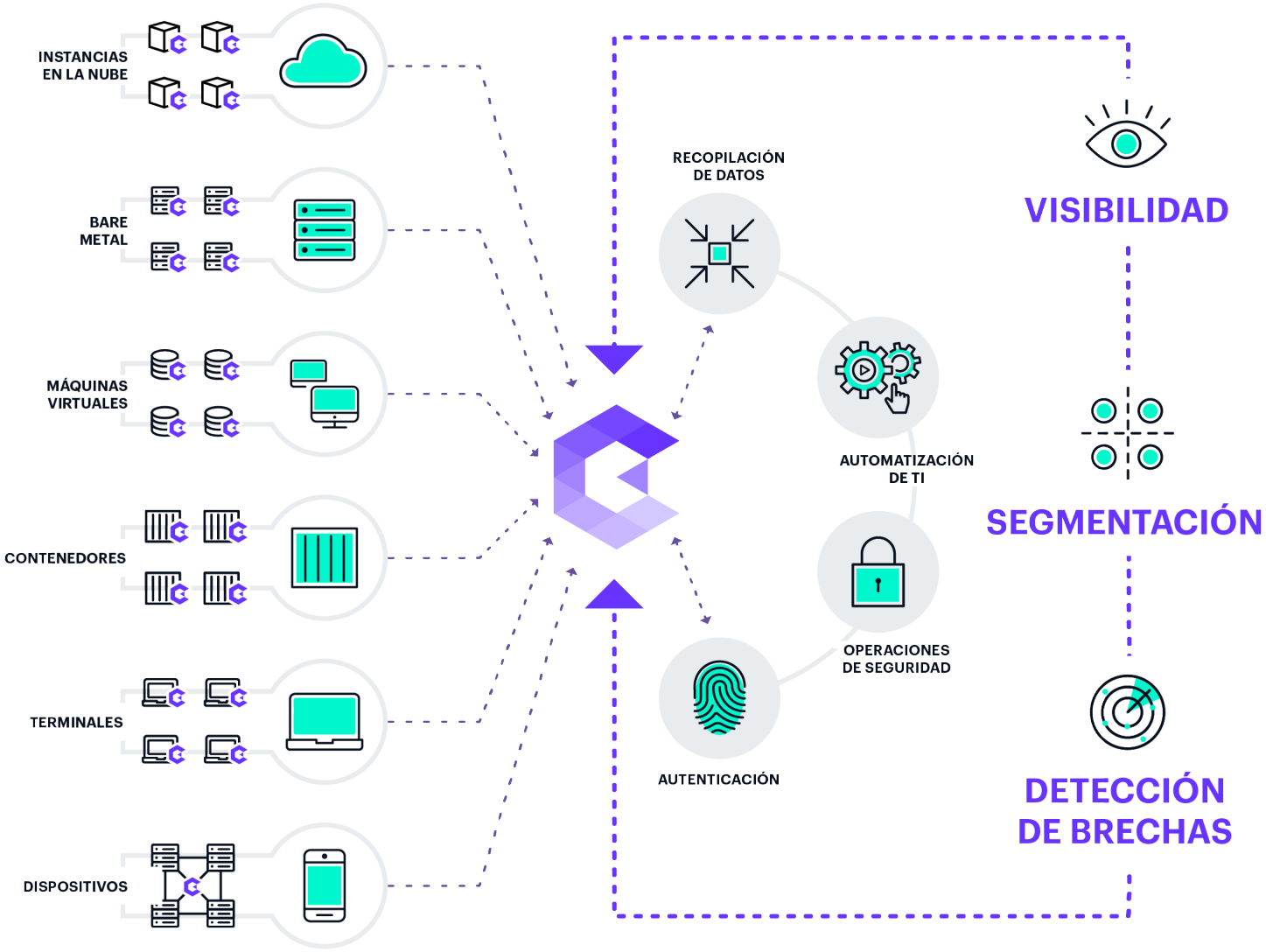
Proteja las cargas de trabajo en entornos de TI complejos con una combinación de cargas de trabajo locales, máquinas virtuales, sistemas heredados, contenedores y orquestación, instancias de nube pública/privada, e IoT/OT

Simplificar la seguridad

Simplifique la gestión de la seguridad con una plataforma que proporciona visualización de red, segmentación, defensa contra amenazas, 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



Nuestra solución integral combina las capacidades clave necesarias para lograr un pleno marco Zero Trust en su entorno de TI.

Plataformas y tecnologías compatibles

- Diseño que permite la integración con su ***infraestructura*** existente
- La compatibilidad con los diferentes sistemas operativos se amplía continuamente para adaptarse a las exigencias de nuestros clientes
- Haga clic aquí para obtener una lista completa de nuestras integraciones y partners de tecnología

SISTEMAS OPERATIVOS

Linux

SUSE, CentOS, Red Hat, debian, aws, aws 2, ORACLE LINUX, ubuntu

Apple

Microsoft

Windows Server, Windows

UNIX

AIX, ORACLE SOLARIS, FreeBSD, hp UX

PROVEEDORES DE NUBE PÚBLICA

aws, Microsoft Azure, ORACLE, Google Cloud

HIPERVISORES

KVM, CITRIX XenServer, VMware ESXi, vSphere Hypervisor, NUTANIX, AHV, Hyper-V

ORQUESTACIÓN DE HIPERVISORES

vCenter Server, vSphere, NSX, apachecloudstack open source cloud computing, openstack., MIRANTIS, nuagenetworks From Nokia

PUERTAS DE ENLACE DE SEGURIDAD

CISCO, paloalto NETWORKS, CHECK POINT

ORQUESTACIÓN DE CONTENEDORES Y MOTORES

docker, kubernetes, Red Hat OpenShift

NAVEGADORES PARA CONSOLA WEB

REQUISITOS MÍNIMOS DE MEMORIA Y SISTEMA

Servidor de gestión
32 GB DE RAM, 8 CPU VIRTUALES y 530 GB

Agregador
4 GB DE RAM, 4 CPU VIRTUALES y 30 GB

Servidor de engaño
32 GB DE RAM, 8 CPU VIRTUALES y 100 GB

Recopilador ESC
2 GB DE RAM, 2 CPU VIRTUALES y 30 GB

PROTOCOLOS DE EXPORTACIÓN CON INTERCAMBIO DE INFORMACIÓN

STIX, Syslog, SMTP, CEF y API OPEN basadas en REST

Protección en cualquier entorno complejo.
Guardicore.com