INFORME SOBRE LA SOLUCIÓN DE AKAMAI

Visualice y proteja Kubernetes con Akamai Guardicore Segmentation

Kubernetes (K8s) sigue siendo una de las tecnologías más ampliamente adoptadas para implementar y gestionar aplicaciones en centros de datos nativos de la nube, ya que ofrece unos niveles de velocidad y flexibilidad que nunca antes habían sido posibles. Según Gartner, el 90 % de las organizaciones internacionales ejecutarán aplicaciones basadas en contenedores en fase de producción en 2026, lo que supone un aumento respecto al 40 % de 2021. Además, en 2026, el 20 % de las aplicaciones empresariales se ejecutarán en contenedores, en comparación con el 10 % de 2020.[1] La creciente popularidad de esta plataforma no solo ha atraído a usuarios, sino también a atacantes, lo que ha obligado a los equipos de seguridad a afrontar retos para los que no estaban preparados inicialmente.

Nueva tecnología, nuevos retos de seguridad

Un clúster K8s proporciona un ecosistema completo que incluye servicios DNS, balanceo de carga, conexiones de red, escalabilidad automática y cualquier otra capacidad necesaria para ejecutar aplicaciones. Por ello, no es de extrañar que K8s se esté adoptando de forma tan generalizada, pues permite a las empresas innovar con rapidez y reducir sus costes. Sin embargo, los mismos atributos que constituyen el atractivo de K8s también hacen que sea más difícil de proteger.

Se trata de una red intrínsecamente plana, lo que implica que todos los módulos pueden comunicarse entre sí dentro del clúster. Desde la primera vulneración, los atacantes pueden desplazarse lateralmente y acceder a todos los centros de datos conectados. Se trata de un proceso de ataque muy común en el ransomware, pero esta estrategia se puede aprovechar fácilmente en otro vector de ataque.

Según el informe de seguridad State of Kubernetes 2022 de Red Hat, donde se encuestó a más de 300 profesionales de DevOps, ingeniería y seguridad, el 93 % de los participantes sufrieron al menos un incidente de seguridad en sus entornos K8s en los últimos 12 meses, lo que en ocasiones supuso pérdidas de ingresos o clientes.

¿La solución? Microsegmentación

El propio concepto de implementación de aplicaciones en K8s es diferente y requiere métodos de seguridad distintos. Los equipos de seguridad no pueden simplemente migrar una solución de seguridad existente y esperar que funcione con esta nueva tecnología. La protección de los clústeres K8s se debe realizar de forma nativa de K8s.

Por este motivo, Akamai ofrece una solución de segmentación basada en software que cuenta con un servicio de asistencia dedicado a proteger clústeres K8s. La solución se comporta de forma similar con otras cargas de trabajo del entorno en particular, incluidos los sistemas heredados, las nubes, las cargas de trabajo locales y los contenedores. Como resultado, es posible visualizar, proteger y gestionar activos para toda la empresa desde un único panel.

Ventajas

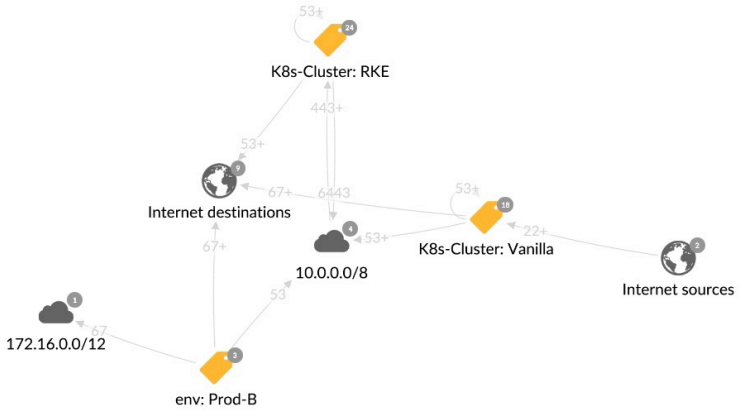
- Visualización, aplicación y supervisión de clústeres K8s a través del mismo panel y los mismos procesos que se emplean para cualquier otro activo
- Protección sencilla contra ataques avanzados que explotan las vulnerabilidades de K8s
- Visualización en tiempo real y con perspectiva histórica de todas las conexiones entre módulos, servicios y hosts o espacios de nombres
- Plantillas predefinidas para acordonar clústeres K8s fácilmente
- Gestión unificada de políticas y consolas para cargas de trabajo locales, en la nube, de terminales y de K8s
- Recepción de datos operativos sobre los clústeres implementados, incluido el número de agentes que los supervisan y el estado de la orquestación de Kubernetes

Akamai

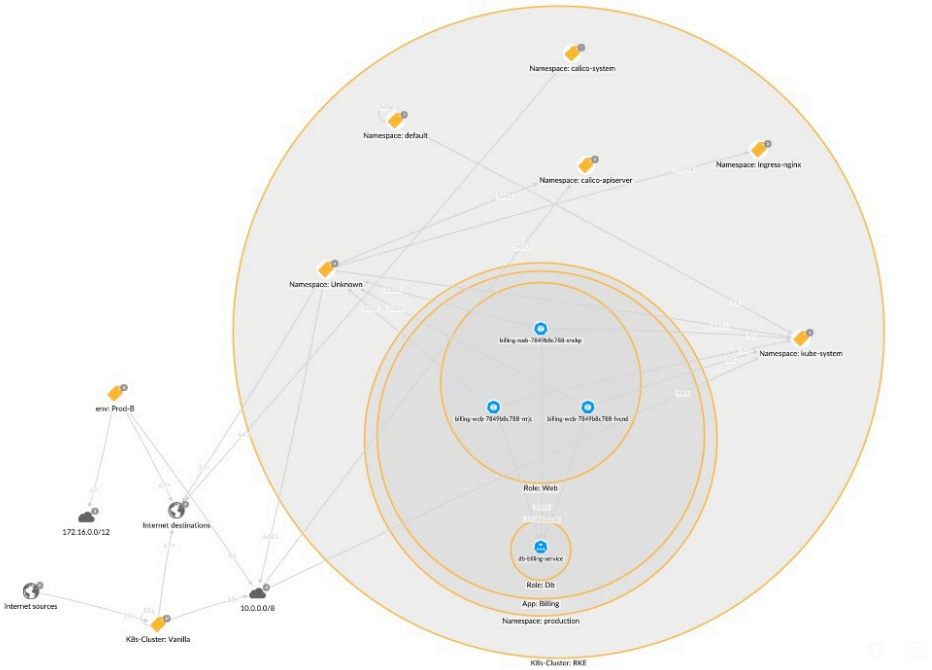
Funciones clave para segmentar los clústeres de Kubernetes

Visibilidad. Akamai Guardicore Segmentation permite conocer lo que se ejecuta en su entorno K8s y confirmar que el tráfico se dirige solamente a donde debe ir, algo fundamental para la creación de políticas eficaces.

- **Mapas de interdependencias**: Akamai proporciona un mapa para visualizar las comunicaciones internas y entre centros de datos para todo tipo de tecnologías, como máquinas virtuales, K8s, contenedores Docker, etc. Gracias a estos mapas, es posible visualizar y detectar cualquier conexión sospechosa entre módulos, servicios, hosts o espacios de nombres.
- **Etiquetas**: Los mapas reflejan con precisión la forma en que se implementan las aplicaciones en el clúster, gracias a la utilización de varias capas de etiquetas. Esta visualización describe la jerarquía de K8s tal y como la planificaron los administradores de la aplicación. Este nivel de detalle ayuda a los usuarios de Akamai a comprender exactamente lo que se implementa en el clúster, así como las relaciones de red entre las aplicaciones implementadas y el resto de la infraestructura.



Clústeres representados en el mapa de Reveal. Al hacer doble clic en un clúster, se muestran los espacios de nombres y sus interconexiones dentro del clúster.



Mapa de Reveal que muestra información de módulo

> El 93 % de los participantes sufrieron al menos un incidente de seguridad en sus entornos K8s en los últimos 12 meses, lo que en ocasiones supuso pérdidas de ingresos o clientes.

Aplicación. Para minimizar la superficie de ataque de los clústeres K8s, se necesita una política de segmentación estricta. Una solución de segmentación debe atenerse a dos criterios principales. Debe ser no intrusiva, carecer de limitaciones de escala y rendimiento, y proporcionar una forma flexible de acordonar todos los niveles de objetos K8s, incluidos los espacios de nombres, los controladores y las etiquetas K8s.

Akamai aprovecha la interfaz de red de contenedores (CNI) de Kubernetes nativa. CNI consta de un complemento de política de seguridad de red que se diseñó originalmente para aplicar segmentación de red en K8s. Se trata de un método no intrusivo sin limitaciones de escala. Las plantillas dedicadas permiten a los usuarios acordonar las aplicaciones de Kubernetes vitales para la actividad empresarial, ya sea un espacio de nombres, una aplicación o cualquier otro objeto.

Ring Fence a K8s Application by whitelisting inbound and outbound flows for an application on K8s cluster K8s-Cluster within Namespace

Plantilla de acordonamiento de aplicaciones de Kubernetes

Supervisión avanzada. Mediante un sistema avanzado de registro y supervisión, se ajusta un registro de red dedicado a la red K8s y muestra los servicios de destino, las direcciones IP de los nodos, los puertos de origen y destino, y los procesos para cada evento. De esta manera, es posible investigar de forma sencilla la actividad anómala en la red y exportar los datos a una aplicación de terceros, como un sistema de gestión de eventos e información de seguridad (SIEM).

Resumen

Kubernetes se ha convertido en una parte integral de muchos entornos empresariales. Se trata de un enfoque novedoso que mejora la eficiencia en el uso de los recursos y proporciona procesos de desarrollo más racionalizados, así como unos mayores niveles de portabilidad y escalabilidad. No obstante, esta estrategia diferente de desarrollo de aplicaciones requiere también un nuevo planteamiento de la seguridad.

Akamai Guardicore Segmentation proporciona una solución integral que permite ver los flujos de comunicación en diferentes tipos de implementaciones (bare metal, máquinas virtuales, K8s, etc.) desde un único mapa. Con un enfoque nativo de K8s no intrusivo y escalable en cuanto respecta a la visibilidad, la supervisión y la aplicación, la solución alivia la carga de trabajo de los equipos de seguridad y desarrollo, lo que permite a su empresa innovar rápidamente sin sacrificar la seguridad.

Según el informe de seguridad State of Kubernetes 2022 de Red Hat, la seguridad es una de las mayores preocupaciones asociadas a la adopción de K8s, y los problemas de seguridad siguen provocando retrasos en la implementación de aplicaciones en la fase de producción.

Para obtener más información, visite akamai.com o póngase en contacto con su equipo de ventas de Akamai.

1. Gartner, The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem, Arun Chandrasekaran, Wataru Katsurashima, 18 de agosto de 2021.