Akamai

WHITE PAPER

Cumplimiento de la promesa de los contenedores

Simplificación y aceleración de la segmentación para aplicaciones y activos esenciales

Introducción

La contenedorización ha surgido rápidamente como la solución preferida para la implementación de aplicaciones en entornos híbridos y de nube, y la proliferación de contenedores sigue acelerándose. 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.[1] Según un estudio de Forrester para Capital One, el **86 % de los responsables de TI encuestados han dado prioridad a un uso más amplio de contenedores para más aplicaciones**.[2]

> 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

Todo esto, por supuesto, ejerce una presión adicional sobre los responsables de proteger los entornos de TI para adaptarse al ritmo de implementación de contenedores, especialmente en un modelo de DevOps que prioriza la adopción y la expansión rápidas. Aunque han surgido diferentes soluciones especializadas en seguridad de contenedores, estas entidades específicas de la plataforma y solo para contenedores acaban añadiendo complejidad y sobrecarga de gestión sin considerar el centro de datos empresarial en su conjunto, lo que dificulta la labor de los equipos de seguridad. Lo que se necesita es una solución de seguridad única y completa que funcione de forma coherente en todas las aplicaciones y tecnologías que se ejecutan en entornos locales, de nube e híbridos, incluidos los contenedores.

Sin embargo, antes de profundizar en las soluciones, echemos un vistazo rápido al fenómeno de los contenedores, las fuerzas que lo impulsan y las implicaciones desde una perspectiva de seguridad.

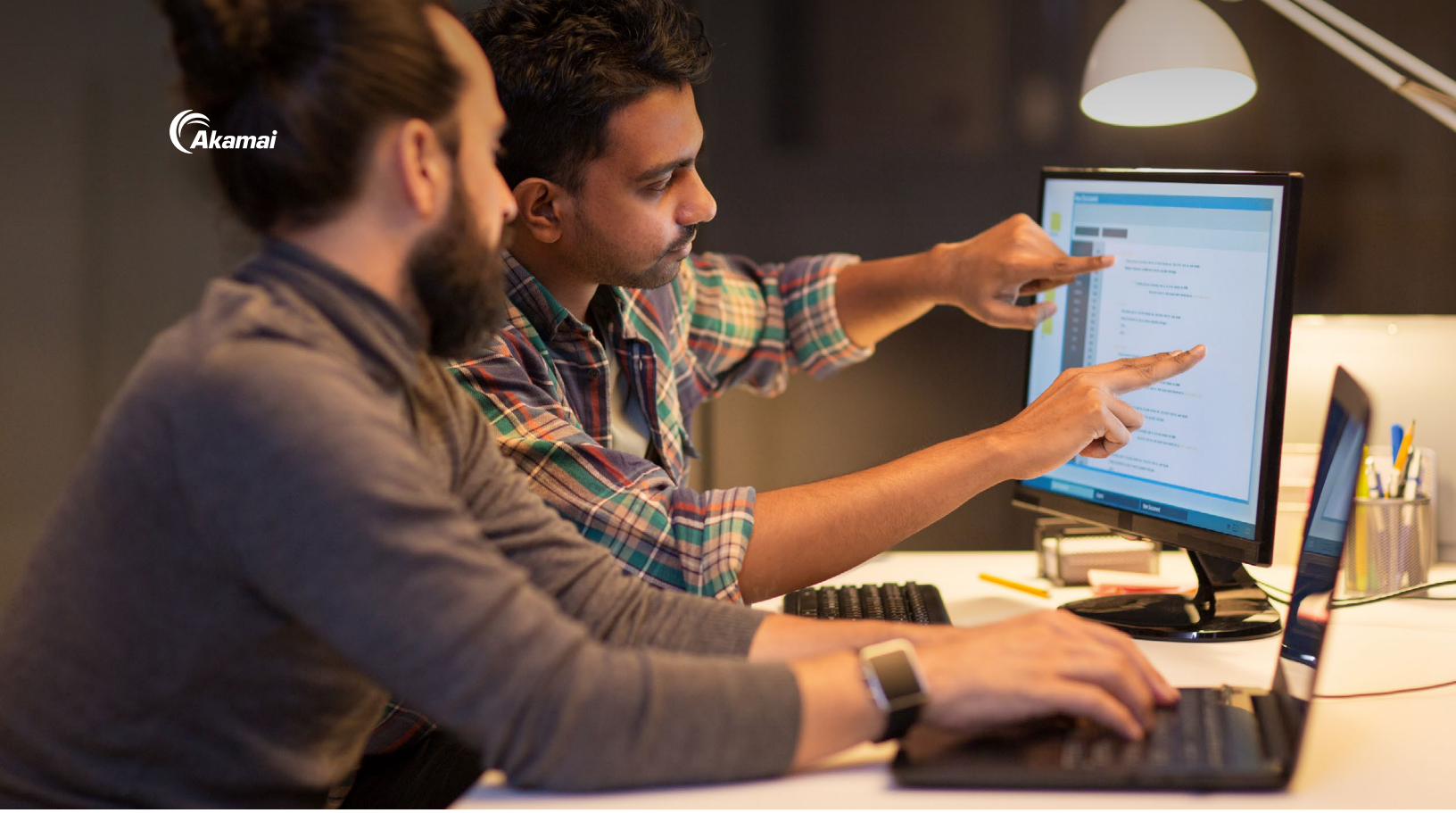
Hay mucha presión: Las exigencias empresariales impulsan la adopción

La tendencia hacia la adopción de contenedores y su crecimiento previsto pueden atribuirse a las exigencias impuestas a los departamentos de TI de las empresas. Las empresas modernas esperan poder avanzar con rapidez y agilidad en respuesta a las amenazas competitivas y las oportunidades de mercado. Necesitan soluciones que respalden la innovación y aceleren el tiempo de comercialización. Siempre buscan una mejora continua de la eficiencia. En un mundo cada vez más interconectado, quieren facilitar la realización de negocios de forma digital, con proveedores, socios comerciales y, especialmente, con sus clientes.

Estas son algunas de las razones principales por las que el departamento de TI de las empresas está migrando a la nube o, más concretamente, a modelos híbridos en las instalaciones y en la nube. También son los principales impulsores de la tendencia de DevOps, que busca acelerar la implementación de aplicaciones críticas eliminando los puntos de fricción desde las ideas hasta la puesta en práctica, aprovechando la automatización y la escalabilidad automática para llevar las aplicaciones a fase de producción más rápidamente.

> "Las organizaciones a menudo subestiman el esfuerzo necesario para operar contenedores en la fase de producción".
>
> Gartner

Todo esto ayuda a explicar por qué los departamentos de TI han adoptado la contenedorización. En comparación con las máquinas virtuales, los contenedores son mucho más fáciles y rápidos de lanzar, lo que posibilita una distribución oportuna sin prácticamente latencia y permite a los equipos centrarse en "poner en marcha servicios, no servidores". Una ventaja clave de los contenedores es la portabilidad para los entornos de centros de datos dinámicos de hoy en día, puesto que facilitan la migración de aplicaciones entre las instalaciones locales y las instancias multinube. Esta ventaja se hace aún más evidente mediante la orquestación de contenedores a través de Kubernetes, o "K8s", que permite a los equipos implementar y gestionar mayores volúmenes de aplicaciones contenedorizadas según sus necesidades en los distintos entornos. La orquestación se considera cada vez más una práctica recomendada en la implementación y gestión de contenedores.



En resumen, los contenedores permiten al departamento de TI responder mejor a las exigencias empresariales de velocidad, automatización, flexibilidad y disponibilidad, y hacerlo con un coste total de propiedad menor en comparación con otras tecnologías. Sin embargo, las iniciativas de implementación no carecen de inconvenientes. "Las organizaciones a menudo subestiman el esfuerzo necesario para operar contenedores en la fase de producción", afirma un informe de Gartner de 2019 sobre las prácticas recomendadas en materia de contenedorización.[3] A pesar del popular atractivo de la contenedorización, la tecnología sigue siendo relativamente incipiente y las prácticas recomendadas para una implementación segura no se han delimitado completamente. Según el informe de seguridad State of Kubernetes 2022 de Red Hat, "la seguridad es [todavía] una de las mayores preocupaciones con respecto a la adopción de contenedores, y los problemas de seguridad siguen causando retrasos en la implementación de aplicaciones en la fase de producción".[4] Está claro que las empresas no pueden aprovechar todas las ventajas potenciales de los contenedores sin una estrategia de implementación que incluya necesariamente la ciberseguridad.

Según el informe de seguridad State of Kubernetes 2022 de Red Hat, "**la seguridad es [todavía] una de las mayores preocupaciones con respecto a la adopción de contenedores**, y los problemas de seguridad siguen causando retrasos en la implementación de aplicaciones en la fase de producción"

¿Qué supone eso para el equipo de seguridad?

"La seguridad no puede plantearse a posteriori", afirma Gartner en su informe de prácticas recomendadas. "Debe integrarse en el proceso de DevOps". Sin embargo, con demasiada frecuencia, no es así. En el afán por implementar la contenedorización, los equipos de seguridad a veces pueden sentir que están en la cima de un "triángulo imposible", una ilusión óptica habitualmente llamada "triángulo imposible de Penrose" (también conocida en Akamai como el triángulo imposible de Klein y Howard).

> Las soluciones de seguridad heredadas no se adaptan a la empresa moderna. Las soluciones de seguridad deben ser rápidas, adaptables, dinámicas y encajar perfectamente en un enfoque de "DevSecOps".

Del mismo modo que el punto superior del triángulo parece estar más lejos que sus otros dos vértices, la seguridad parece estar rezagada respecto a las exigencias empresariales y a las iniciativas de TI para satisfacerlas. Pero, al igual que el triángulo es una ilusión óptica, las soluciones de seguridad están más cerca de lo que parecen. Los equipos simplemente tienen que superar las soluciones engorrosas y heredadas en las que han confiado en el pasado y buscar soluciones que se adapten a la forma en que la TI empresarial funciona hoy en día y se integren perfectamente en un enfoque de "DevSecOps". Esto implica una solución rápida, adaptable y dinámica, que en sí misma emplea el enfoque de la guía de DevOps. Lo más importante es que sea una solución independiente de los sistemas operativos y la plataforma subyacentes para simplificar la implementación y la gestión.

Triángulo imposible de Klein y Howard

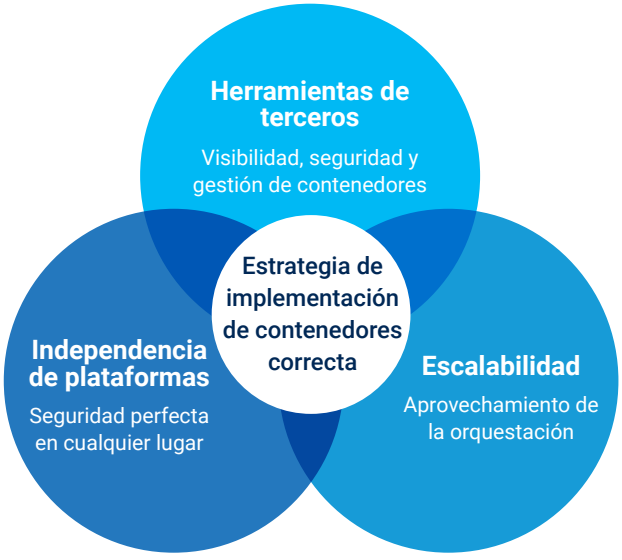
Por qué lo "nativo" no es suficiente

En los albores de la virtualización y la migración a la nube, las empresas a menudo creían que los controles nativos de la nube eran suficientes para visualizar, gestionar y proteger sus cargas de trabajo. Solo tras muchas pruebas y errores, los responsables de TI se dieron cuenta de que necesitaban un modelo de gestión superpuesto que incorporara soluciones de terceros que ofrecieran seguridad más allá de los controles nativos.

Como han observado Gartner y Forrester Research, una estrategia de implementación de contenedores exitosa se basa en el "trío de contenedores":

- Ejecutar contenedores de forma portátil e independiente de la plataforma, que se puedan implementar sin problemas en cualquier lugar en varias arquitecturas locales y de nube
- Aprovechar la orquestación para ejecutar y gestionar contenedores a escala
- Utilizar herramientas de terceros para la gestión de contenedores, la visibilidad y la seguridad

A diferencia de las iniciativas anteriores de virtualización y nube, el sector de los contenedores ha reconocido desde sus inicios que los sistemas de gestión nativos de la nube, y los controles de seguridad en concreto, son inadecuados para una estrategia de contenedores eficaz. En el estudio de Gartner sobre soluciones de gestión de contenedores, **el 65 % de los encuestados afirmó que tenía la intención de aprovechar las herramientas de gestión de terceros para visualizar, gestionar y proteger las cargas de trabajo contenedorizadas**.[5] Sin embargo, estas herramientas de terceros deben funcionar sin problemas tanto en las instancias locales como en la nube, y adoptar un enfoque detallado para evitar los inconvenientes de los engorrosos métodos mixtos utilizados en el pasado, como los grupos de seguridad, las VLAN y los firewalls, que ofrecen visibilidad cero y una granularidad insignificante.



Facilite la adopción de contenedores con Guardicore Segmentation de Akamai

Guardicore Segmentation de Akamai se ha diseñado para hacer frente a los desafíos de las infraestructuras de centros de datos híbridos y dinámicos de hoy en día. Proporcionamos visibilidad completa de todas las aplicaciones y cargas de trabajo que se ejecutan en los diferentes entornos, y posibilitamos una segmentación detallada y fácil de implementar definida por software mediante la creación, implementación y aplicación rápidas de políticas de seguridad en torno a aplicaciones individuales o agrupadas de forma lógica.

Una apreciación importante: Guardicore Segmentation de Akamai no es un producto específico de contenedores. En su lugar, la seguridad de los contenedores es una función clave de la plataforma, que funciona de forma coherente en entornos mixtos que también pueden incluir servidores bare metal, máquinas virtuales, cargas de trabajo sin servidor y dispositivos remotos. En consecuencia, proporcionamos a las organizaciones una solución única e integral para proteger todos los activos de centro de datos y nube, independientemente de dónde residan o cómo se implementen, lo que elimina la necesidad de gestionar varias soluciones puntuales. Además, como nuestra solución está desvinculada de las plataformas y los sistemas operativos subyacentes, las políticas de seguridad siguen las aplicaciones y las cargas de trabajo a medida que se mueven entre los entornos locales y de nube, lo que mejora el factor de portabilidad que hace que los contenedores resulten atractivos para la implementación de aplicaciones en infraestructuras de nube híbrida.

> La seguridad de contenedores es una función clave de la plataforma Guardicore Segmentation de Akamai, que funciona sistemáticamente en entornos de centros de datos dinámicos y heterogéneos

Con respecto a los contenedores, Guardicore Segmentation de Akamai coloca agentes en nodos de host de contenedores, lo que permite ver todo el clúster de contenedores, incluidos los flujos de comunicación de módulo a módulo y de módulo a máquina virtual. Esto posibilita una implementación y aplicación de políticas de seguridad muy detalladas por proceso, usuario y nombre de dominio completo (FQDN). En un escenario de orquestación, admitimos la orquestación K8s y ofrecemos visibilidad de los metadatos de Kubernetes y OpenShift para obtener un contexto superior. Un modelo de etiquetado flexible permite a los operadores expresar políticas mediante terminología de K8s nativa. Para la aplicación de K8s, utilizamos la interfaz de red de contenedores (CNI) nativa, un método no intrusivo para aplicar políticas en K8s 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. También adaptamos las cargas de trabajo y las tasas de cambio a K8s. Puesto que nuestra solución también funciona con todas las demás cargas de trabajo empresariales de forma similar, sirve como una solución única para visualizar, gestionar y proteger los activos de toda la empresa.

De particular importancia en un entorno de DevOps, las políticas de seguridad que cree se integrarán de forma eficaz en los procesos de integración e implementación continua (CI/CD), lo que ayuda a garantizar que la seguridad no se plantee a posteriori, sino que esté totalmente integrada en el modelo de entrega.

Conclusión

Los contenedores son una parte cada vez más integral de muchos entornos empresariales. Pueden aumentar la eficiencia del uso de los recursos, agilizar los procesos y permitir una mayor portabilidad y escalabilidad. Al mismo tiempo, la seguridad integrada que proporcionan no es suficiente, especialmente para las empresas que utilizan un entorno híbrido.

Cuando busque una solución de seguridad que crezca con su empresa, asegúrese de elegir una herramienta independiente de la plataforma que le proporcione información detallada sobre sus procesos de principio a fin, sin importar dónde se produzcan. Guardicore Segmentation de Akamai hace eso y mucho más, ofreciendo la gama de funciones y capacidades que las empresas modernas necesitan para estar preparadas para el presente y el futuro.

Con Guardicore Segmentation, su equipo de seguridad puede lograr una protección sistemática en entornos de centros de datos dinámicos y heterogéneos. Al hacerlo, puede ayudar a los equipos de TI a cumplir la promesa de la contenedorización, logrando el desarrollo y la implantación rápidos, rentables y seguros de aplicaciones esenciales para las exigencias de su empresa.

Simplifique la seguridad en todo su entorno. Obtenga más información sobre nuestra potente solución de seguridad unificada para contenedores y mucho más: akamai.com/guardicore.

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

2 "Cloud Container Adoption In The Enterprise", Forrester, junio de 2020.

3 "Best Practices for Running Containers and Kubernetes in Production", Gartner, 25 de febrero de 2019.

4 "State of Kubernetes Security Report", Red Hat, mayo de 2022.

5 "Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024", 25 de junio de 2020.

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. Para obtener más información acerca de las soluciones de seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado el 23 de mayo.