Akamai

WHITE PAPER

Protección de las cargas de trabajo en entornos híbridos y multinube

Protección de las cargas de trabajo en entornos híbridos y multinube

En la búsqueda de innovación, ventajas competitivas y la máxima eficiencia, las empresas han migrado a un modelo de infraestructura de nube basado en DevOps. Esto ha hecho que aumente la velocidad y agilidad de TI empresarial de formas nunca antes vistas. Muchas organizaciones siguen adoptando la infraestructura de nube pública y nuevos enfoques de implementación, como contenedores y tecnologías sin servidor. Al adoptar este nuevo modelo, la última tecnología de cloud computing está acelerando drásticamente el ritmo de cambio. Estas prácticas permiten que las cargas de trabajo, aplicaciones e incluso entornos se puedan automatizar, escalar automáticamente, migrar y mucho más. Las ventajas competitivas resultantes son enormes.

Al mismo tiempo, algunos servicios y sistemas heredados, como la infraestructura del centro de datos tradicional, siguen utilizándose. Es posible que las empresas estén en proceso de eliminarlos o modernizarlos, pero los sistemas siguen existiendo de forma inherente porque contienen aplicaciones y flujos de trabajo críticos para la empresa.

Además, las técnicas de seguridad tradicionales no han podido seguir el ritmo de los cambios, lo que plantea la cuestión de cómo pueden protegerse las cargas de trabajo de nube en estos nuevos entornos de nube híbrida y multinube. Más allá de la velocidad, la seguridad perimetral ya no es eficaz cuando la gran mayoría del tráfico se produce dentro de la nube o en el centro de datos (de este a oeste), en lugar de venir del exterior (de norte a sur). Esta transformación también obliga a los ejecutivos de TI a replantearse su estrategia de seguridad.

> Las técnicas de seguridad tradicionales no son eficaces en entornos híbridos ni multinube.

De hecho, ningún modelo de ciberseguridad tradicional se creó teniendo en mente la infraestructura como servicio (IaaS). La nube pública necesita nuevas estrategias basadas en sus propios desafíos únicos.

La seguridad empresarial debe evolucionar para adaptarse al nuevo entorno empresarial. Las organizaciones ya han realizado cambios drásticos para satisfacer los requisitos empresariales y la metodología de trabajo Agile. La seguridad se ha dejado atrás a pesar de la enorme inversión que se ha hecho.

La realidad es que gastar dinero en soluciones que se desarrollaron sin la nube en mente es un error. No ayudan a detectar y prevenir las filtraciones actuales o futuras. Entonces, ¿cómo puede utilizar los servicios de nube pública y disfrutar de las ventajas de la velocidad y la agilidad sin poner en peligro la protección de los datos críticos?

El centro de datos moderno en la nube híbrida

La composición del centro de datos moderno, el aumento del nivel de detalle de las cargas de trabajo y la velocidad de desarrollo están cambiando rápidamente. Un centro de datos híbrido moderno típico se compone de cargas de trabajo que se ejecutan tanto en el entorno local como en la nube pública o la IaaS, con el uso de varios proveedores y utilizando la plataforma como servicio (PaaS), ya sea en el entorno local o en la nube. La cantidad de cargas de trabajo que se ejecutan en la nube pública sigue creciendo. Al mismo tiempo, los centros de datos locales no van a desaparecer por ahora. Aquí tenemos un ejemplo: una encuesta reciente a ejecutivos del área de tecnología demostró que, en lo que respecta a los entornos de TI modernos, alrededor del 59 % tiene "algunos en la nube, pero la mayoría en el entorno local", y el 34 % tiene "principalmente en la nube, pero otros en el entorno local". Solo el 7 % lo tiene "todo en la nube", pero se prevé que ese número aumente drásticamente.[1]

Como podemos ver, las empresas están adoptando cada vez más las prácticas de DevOps y mejorando su agilidad. La implementación de los servicios nativos en la nube y la tecnología sin servidor es cada vez más fácil. Al utilizar una combinación de contenedores, máquinas virtuales y cargas de trabajo sin servidor en la nube, puede ganar en rentabilidad y capacidad de transformación desde un punto de vista estratégico.

La seguridad debe encajar en este paradigma de nube híbrida. Las empresas deben abordar la seguridad en todas las etapas del proceso de DevOps, desde las pruebas, la creación y la planificación hasta la supervisión, el funcionamiento, la implementación y el lanzamiento de nuevas funciones. La migración a la nube no puede ser un obstáculo que impida el éxito.

Las cargas de trabajo distribuidas no están bien protegidas, lo que limita el uso de nuevas tecnologías de nube

Hoy en día, muchas empresas tienen que proteger las cargas de trabajo que están distribuidas en el entorno local, centros de coubicación y distintas plataformas de nube pública e IaaS. Así, tienen dificultades para proteger estas cargas de trabajo con los modelos de seguridad de red locales tradicionales.

Las cosas se complican aún más cuando intenta implementar nuevas herramientas y técnicas basadas en la nube para proteger las nuevas tecnologías de nube. Los niveles de complejidad se multiplican a medida que las empresas intentan aplicar diferentes controles de seguridad en diferentes entornos e introducen riesgos al implementar estos controles sin una visibilidad adecuada.

En otras palabras, la nube, cuyo objetivo es hacer que las empresas sean más dinámicas, ágiles, rápidas e innovadoras, está poniendo en riesgo a muchas organizaciones. Debido a la falta de herramientas de seguridad relevantes centradas en la nube, las empresas tienen una capacidad limitada para adoptar esta nueva tecnología sin generar puntos ciegos y más desafíos.

Aquí es donde entra en juego la protección adaptable de las cargas de trabajo.

El cambio a la IaaS genera la necesidad de una protección adaptable de las cargas de trabajo

La mejor forma de proteger las cargas de trabajo detalladas con ciclos de vida cortos es mediante la aplicación dinámica de protección tan pronto como se procesan. La aplicación de las políticas de seguridad es mucho más sencilla en las soluciones centradas en las cargas de trabajo en comparación con su aplicación en los modelos de seguridad de red tradicionales en lo que respecta a la infraestructura de nube pública.

Las plataformas de protección de cargas de trabajo en la nube admiten soluciones de seguridad independientes de la plataforma y centradas en las cargas de trabajo

Dado que una política sigue la carga de trabajo, independientemente de la infraestructura subyacente, el modelo se puede aplicar a todas las cargas de trabajo en todo el entorno del centro de datos ubicado en la nube híbrida. El resultado es un enfoque coherente e independiente de la plataforma para los controles de seguridad.

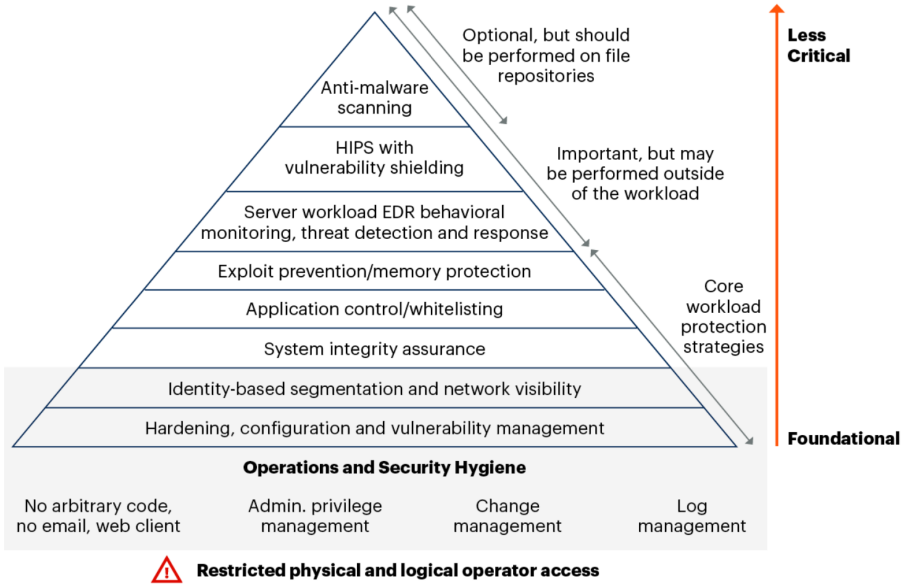
Aunque existen herramientas de seguridad nativas en la nube, las plataformas de protección adaptable de las cargas de trabajo en la nube (CWPP) proporcionan un control más completo y detallado en los niveles de proceso, usuario y nombre de dominio completamente calificado. También funcionan en varios proveedores de nube y en el entorno local, lo que proporciona una protección más sólida y completa para máquinas virtuales, contenedores y cargas de trabajo sin servidor.

Estrategias básicas de protección de cargas de trabajo procesables: asignación de controles según las directrices de Gartner sobre protección de cargas de trabajo en la nube

Unas de las directrices más seguidas para la protección de las cargas de trabajo en la nube han sido redactadas por expertos del sector de Gartner. Según Gartner, existe una clara jerarquía de controles a la hora de proteger las cargas de trabajo en la nube.

La siguiente pirámide pasa de controles básicos a menos críticos, mostrando las estrategias que Gartner considera fundamentales, así como las que son importantes, pero opcionales. Lo ideal es que estos pasos se incluyan en cada carga de trabajo para garantizar que la seguridad esté integrada en cada acción en la nube.

Jerarquía basada en el riesgo de los controles de protección de las cargas de trabajo[2]



Las directrices de protección de cargas de trabajo en la nube de Gartner proporcionan una jerarquía clara de controles de seguridad para las empresas

A continuación, se ofrece una explicación ampliada de las estrategias principales que satisface nuestra solución para ayudarle a comprender cómo puede incorporar estas estrategias a su programa de protección del centro de datos en entornos híbridos o multinube:

- **Refuerzo, configuración y gestión de vulnerabilidades**
  Según Gartner, la estrategia de protección de cargas de trabajo más básica consiste en configurar los sistemas y los ajustes de forma adecuada para reducir el riesgo. Las herramientas de gestión de vulnerabilidades llevan la eliminación manual de vectores de ataque mucho más allá y automatizan este proceso. Después podrá encontrar y resolver problemas de software que podrían abrir la puerta de par en par a las actividades maliciosas.

- **Segmentación basada en identidades y visibilidad de la red**
  Gartner destaca la segmentación y la visibilidad de la red como estrategias básicas para la protección de la nube. La mayoría de las organizaciones utilizan firewalls locales de nueva generación, pero muchas aceptan una solución menos segura cuando se trasladan a la nube.

  Los equipos de seguridad entienden que los firewalls de nueva generación no son suficientes para la protección en la nube, pero no saben cómo lograr una visualización o un control heterogéneos en un entorno de centro de datos híbrido y dinámico. Dediquemos un momento a repasar cómo se puede hacer bien.

  En primer lugar, establezca la visibilidad. Una visibilidad rápida reduce el tiempo de amortización, ya que todos los usuarios están en sintonía de forma inmediata y automática.

  Las herramientas nativas de nube pueden proporcionar mapas de instantáneas o registros textuales, pero suelen ser densos, incompletos o insuficientes. La mejor solución debería detectar automáticamente todas las aplicaciones, el tráfico y las dependencias que hay en la red. De esta forma, podrá ver de un vistazo todo su ecosistema de TI, incluso si su empresa está distribuida de forma híbrida.

  Su solución también debe incluir un contexto sólido, con una imagen clara de lo que realmente está sucediendo en el centro de datos. Para cualquier empresa que desee gestionar las operaciones de seguridad y las consultas a escala, todos los flujos deben disponer de este contexto, además de la capacidad de desglosar los procesos individuales y las comunicaciones del servidor. Esto permite el tipo de toma de decisiones basada en datos que refuerza la creación de políticas.

  Después de establecer la visibilidad y el contexto, cree reglas de segmentación que se ajusten a las prácticas recomendadas para su negocio. Por ejemplo, puede que desee separar los entornos de producción y desarrollo o aislar los datos de los clientes por razones de cumplimiento. También puede desarrollar políticas de microsegmentación más detalladas para proporcionar una seguridad y un control exhaustivos que se adapten a su contexto empresarial específico.

- **Control de aplicaciones/listas de autorización**
  Cuando su equipo de seguridad pueda establecer políticas y tener la seguridad de que se ejecutarán en todas partes, la transición a la nube será más sencilla y segura en cada etapa.

  Confiar únicamente en puertos/IP no le proporcionará el nivel de visibilidad que necesita para una protección completa de las cargas de trabajo en la nube. El control estricto del tráfico entre los componentes de las aplicaciones es una parte fundamental de una solución de microsegmentación sólida. Las mejores tecnologías tienen visibilidad y control detallados hasta el nivel de proceso de aplicación, usuario y nombre de dominio completamente calificado, utilizando detalles como valores hash, suma de comprobación, ruta completa, resoluciones y autenticaciones del almacén de identidades.

  Algunas características adicionales que pueden aumentar el control de aplicaciones incluyen las siguientes:

  - Microsegmentación capaz de limitar el movimiento lateral en la nube, incluso dentro del mismo clúster de aplicaciones
  - Un enfoque de vista unificada, que se traduce en una seguridad mejorada
  - Posibilidad de crear modelos de lista de autorización y lista de denegación para bloquear aplicaciones o tráfico no autorizados y garantizar que las conexiones importantes funcionen sin obstáculos

- **Prevención de explotaciones/protección de la memoria**
  La última estrategia de protección de los servidores en la guía de Gartner para la CWPP es la prevención de explotaciones. Busque una herramienta de seguridad de microsegmentación que proporcione detección y respuesta a filtraciones. De esta forma, podrá sustituir las herramientas redundantes y reducir la complejidad en su centro de datos.

  Además, como se ha mencionado anteriormente, la visibilidad y la asignación son fundamentales. Una vez que tenga un mapa completo de toda su red, será fácil ver las vulnerabilidades no corregidas o las comunicaciones maliciosas que actúan fuera de la norma. Cuando su empresa haya establecido la referencia para el tráfico legítimo, el movimiento no autorizado destacará.

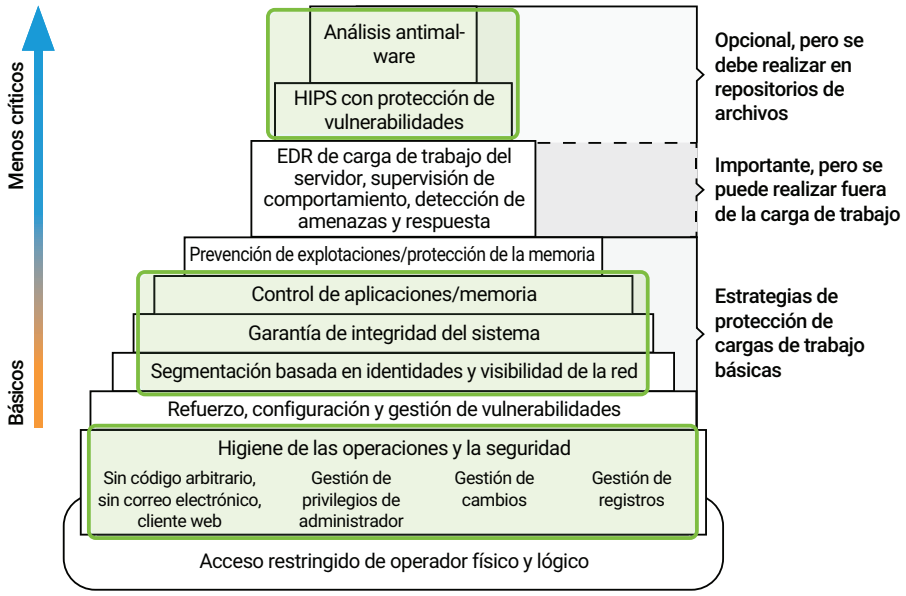
Otras estrategias de protección importantes

Las estrategias de servidor básicas mencionadas anteriormente son fundamentales para la seguridad en la nube. Al mismo tiempo, Gartner identifica otras estrategias que pueden fortalecer su entorno híbrido o multinube, como la detección y respuesta en los terminales (EDR) para las cargas de trabajo del servidor, la supervisión del comportamiento y la detección y respuesta a amenazas (TDR).

La EDR, la supervisión del comportamiento y la TDR son partes importantes de la detección de filtraciones y la respuesta a incidentes. Para cubrir estos aspectos de la seguridad, busque una solución que incluya análisis de reputación. Esto le permitirá identificar más información sobre un ataque y le proporcionará funciones dinámicas de engaño avanzadas a fin de engañar a los atacantes para que revelen sus métodos. De esta forma, puede reforzar su política y su procedimiento de seguridad de cara al futuro.

Puede que se necesiten datos de visibilidad para establecer información sobre un evento pasado. Los mejores proveedores almacenan sus datos durante meses, lo que permite a los usuarios centrarse en aplicaciones, procesos y periodos de tiempo específicos. Los equipos de seguridad también pueden utilizar estos datos para llevar a cabo una investigación forense y mejorar la respuesta a incidentes.

Guardicore Segmentation de Akamai: Protección de cargas de trabajo en la nube híbrida según la jerarquía de CWPP



Las áreas resaltadas muestran dónde cumple nuestra solución los requisitos de CWPP

Guardicore Segmentation aborda las brechas inherentes a las herramientas de seguridad en la nube nativas, cumpliendo muchos de los principios fundamentales establecidos en la CWPP. Además, la solución promueve de forma inteligente una mayor visibilidad, la creación de políticas y su aplicación en centros de datos híbridos y multinube.

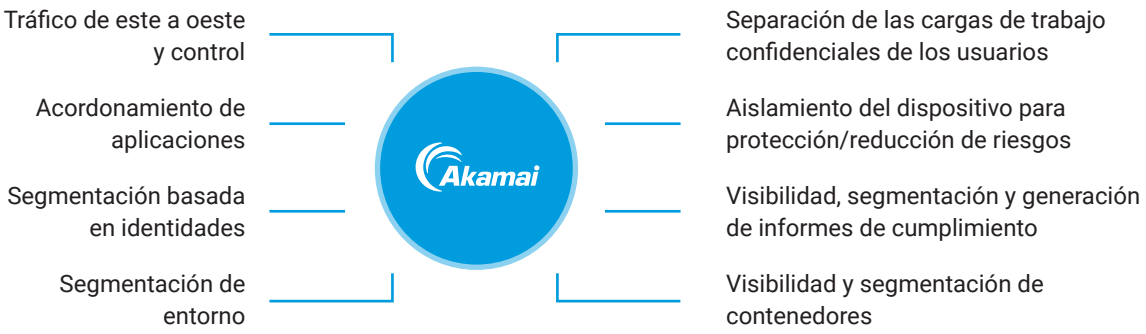
Nuestra solución proporciona visibilidad detallada: una vista unificada que ofrece una panorámica de todo el centro de datos. Al visualizar su centro de datos híbrido en su conjunto, puede comprender a fondo las dependencias de las aplicaciones y el efecto que cualquier política tendrá en su red. Esto tiene una gran influencia en la migración a la nube, ya que permite que los clientes accedan a la nube de forma mucho más rápida que con las herramientas de visualización nativas.

Esta visibilidad detallada le permite:

- Crear una lista de tareas pendientes para las redes en la nube
- Detectar rápidamente las aplicaciones en cualquier infraestructura y las dependencias de las aplicaciones, una función crítica para una migración correcta
- Comprender los costes operativos y de infraestructura con antelación
- Obtener información sobre la creación de las mejores políticas para reducir el riesgo en las fases de planificación de la migración
- Aprovechar la ruta más corta, sencilla y segura hacia la consecución de sus objetivos empresariales para la nube

> La visibilidad detallada y basada en el contexto de Guardicore Segmentation de Akamai le permite comprender sus entornos de forma rápida y exhaustiva

Nuestra visibilidad completa también incluye contexto para cada comunicación y flujo, lo que le permite reducir los errores y la complejidad general. Puede agrupar y filtrar la información para ayudar a cualquier parte interesada a leer el mapa, proporcionándole fácilmente la información exacta que necesita. Esta vista basada en el contexto reduce la necesidad de utilizar proveedores externos y creadores de políticas, ya que permite comprender rápidamente sus entornos para que pueda crear, perfeccionar o modificar las políticas aplicables.



Ejemplos de casos de uso de Guardicore Segmentation de Akamai

Entre otras características críticas que ofrece nuestra solución se incluyen las siguientes:

- Políticas en el nivel de proceso y servicio que permiten una seguridad más sencilla y sólida cuando se trata de protocolos dinámicos como FTP o Spark
- Políticas de microsegmentación basadas en identidades, que aplican las conexiones en función del usuario que crea la conexión
- Políticas basadas en nombres de dominio completamente calificados que le permiten llegar a recursos de escalabilidad automática cuyas direcciones IP son dinámicas
- El uso de etiquetas de nube pública existentes como etiquetas, lo que simplifica la visualización de su centro de datos híbrido o multinube
- Creación automática de políticas a partir del tráfico observado, para que pueda obtener orientación rápida y experta al iniciar su proceso de microsegmentación

Nuestra solución es independiente de la plataforma y de la infraestructura, lo que permite gestionar la visibilidad y el cumplimiento de las políticas en toda la infraestructura

Reducir la complejidad es el objetivo final cuando se busca proteger un centro de datos híbrido. En respuesta a esta necesidad, Guardicore Segmentation de Akamai no depende de la plataforma ni de la infraestructura, lo que le proporciona una vista de toda la aplicación y la política que sigue la carga de trabajo, independientemente de dónde se encuentre. Cada regla se aplica a todas las cargas de trabajo, desde vCenter y nubes públicas (AWS, Azure, GCP) hasta servidores bare metal y contenedores.

La reducción de la complejidad no solo da como resultado una estrategia de seguridad más sólida, sino que también reduce la carga de trabajo de los equipos de TI y seguridad. Con los grupos de seguridad basados en la nube, necesita expertos en nube nativa para cada proveedor. Por el contrario, con una solución de seguridad que gestiona la visibilidad y el cumplimiento de las políticas en toda la infraestructura, solo necesita usuarios certificados para una única tecnología.

Una plataforma de protección de cargas de trabajo en la nube preparada para el futuro

Uno de los pilares de la metodología Agile y DevOps es la capacidad de fallar y pasar rápida y fácilmente al "próximo gran reto". Lamentablemente, y algo irónicamente también, la migración de sus cargas de trabajo entre distintos proveedores de nube puede ralentizarle enormemente. También puede ser difícil mantener la seguridad.

Necesita poder mantener sus opciones abiertas. Si desea migrar a una infraestructura multinube, o incluso migrar cargas de trabajo a un nuevo proveedor de nube, estas migraciones no deberían tener un efecto negativo en la seguridad, ni tampoco deberían impedirle dar el paso.

Guardicore Segmentation de Akamai le permite mantener la flexibilidad y avanzar al ritmo de la empresa, migrando sus cargas de trabajo con las políticas de seguridad intactas. No obstaculiza el proceso de DevOps ni la agilidad, ni requiere procesos de reconfiguración en cada etapa. En su lugar, proporciona los conceptos básicos de una plataforma de protección de cargas de trabajo en la nube de confianza para que pueda mantener protegido su centro de datos híbrido o multinube.

Guardicore Segmentation de Akamai permite una migración segura a la nube y entre nubes, y proporciona una visibilidad con contexto sin precedentes. Con nuestra solución, puede aplicar políticas hasta en el nivel de usuario y proceso, y seguir sus cargas de trabajo dondequiera que vayan.

Ahora puede convertir la seguridad en una característica de cada etapa del proceso de DevOps, lo que fomenta la agilidad y el respaldo a su empresa. Su organización podrá adoptar capacidades de nube de vanguardia sin renunciar a la seguridad.

Obtenga más información sobre cómo proteger los entornos de nube con la microsegmentación líder del sector. Visite akamai.com/guardicore hoy mismo.

1 2022. Foundry (formerly IDG) Cloud Computing Study (Estudio de cloud computing de Foundry [anteriormente IDG]).

2 Market Guide for Cloud Workload Protection Platforms (Guía del mercado para las plataformas de protección en la nube); escrita por los analistas de Gartner Neil MacDonald y Tom Crow; publicada el 14 de abril 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 en 05/23.