DOCUMENTO TÉCNICO, MAYO DE 2020

Protección de cargas de trabajo de nube

Cómo proteger las cargas de trabajo en las nubes híbridas

vmware®

Índice

Resumen ejecutivo

La nube híbrida es el eje de la transformación digital. Actualmente, más del noventa por ciento de las empresas afirman utilizar una estrategia multinube y, además, la mayoría combina el uso de nubes públicas y privadas.[1] La parte positiva es que este enfoque ofrece la flexibilidad y escalabilidad necesarias para apoyar la rápida innovación. El inconveniente es que a menudo añade una mayor complejidad y riesgo, lo que hace que la seguridad sea un componente esencial en las nubes privadas y públicas.

A medida que los equipos de la empresa distribuyen y gestionan cargas de trabajo esenciales en entornos multinube, la visibilidad de la situación de seguridad de las cargas de trabajo y el control de la superficie de ataque son fundamentales para proteger los datos y mantener las operaciones.

Muchos equipos distintos de la empresa, incluidos los de operaciones de TI y operaciones de seguridad, son partes interesadas clave en el rendimiento, la disponibilidad y la seguridad de las cargas de trabajo de nube. Mantener a los miembros del equipo coordinados en lugar de fragmentados también es un factor esencial para el éxito.

Este documento técnico trata los principales desafíos que los equipos empresariales han encontrado a la hora de proteger las cargas de trabajo de nube, y cómo superarlos con el enfoque de seguridad intrínseca de VMware usando VMware Carbon Black Cloud™, VMware vSphere® y VMware NSX®. Este documento también incluye un análisis sobre cómo la nube obliga a crear una nueva forma de pensar en el riesgo, que pueda reunir a las partes interesadas de distintos equipos en lugar de mantener la brecha digital. También se proporciona una lista de comprobación para evaluar plataformas de protección de cargas de trabajo de nube, a fin de ayudar a las organizaciones a estudiar los requisitos clave al contemplar posibles soluciones.

Desafíos de seguridad en las nubes privadas, públicas e híbridas

Distribuir y gestionar cargas de trabajo y aplicaciones en entornos de nube privada, pública e híbrida es un trabajo en equipo. Lo que antes considerábamos el departamento de TI tradicional, ahora ha sido sustituido por un colectivo de grupos. Los departamentos de operaciones de TI, DevOps y de operaciones de seguridad deben colaborar para distribuir y proteger las aplicaciones y los servicios de nube.

1. Flexera: «State of the Cloud Report», abril de 2020.

Tal y como se muestra en la tabla 1, no desarrollar la coordinación entre equipos ni planificar los aspectos únicos de las cargas de trabajo de nube puede aumentar los riesgos.

	OPERACIONES DE NUBE HÍBRIDA	DESAFÍOS DE SEGURIDAD	OPERACIONES TRADICIONALES DE TI	CARENCIAS EN LA SEGURIDAD DE TI TRADICIONAL
Arquitectura de diseño	Servicios interconectados	• No hay visibilidad de cómo se comunican y conectan las cargas de trabajo. • Las redes planas y no segmentadas aumentan el riesgo.	Monolíticas y aisladas	• Los antivirus tradicionales no están diseñados para funcionar en el contexto de las cargas de trabajo de nube. • La supervisión centrada en el centro de datos carece de un valor de referencia del comportamiento normal de la red.
Modelo operativo	Propiedad y gestión distribuidas	• El departamento de operaciones de TI se encarga de la situación, gestión y disponibilidad de las cargas de trabajo, pero no puede ver las vulnerabilidades de estas. • Los silos tecnológicos y de procesos contribuyen a que se produzcan configuraciones erróneas e inseguras, y otros errores humanos.	Centralizadas	• La incorporación de productos de seguridad para fines específicos exige la instalación de agentes adicionales, lo que ralentiza el rendimiento del sistema y complica las operaciones. • La falta de visibilidad unificada dentro de las cargas de trabajo, y entre cargas de trabajo y nubes, complica la coordinación entre equipos.
Escalabilidad	Muy dinámicas, automáticas	• La falta de control de los cambios produce configuraciones erróneas, como el almacenamiento de datos sin protección, el exceso de permisos, las credenciales y los ajustes de configuración predeterminados y la desactivación de los controles de seguridad. • La incapacidad para estandarizar las políticas de seguridad de cargas de trabajo en nubes privadas y públicas aumenta el riesgo.	Estáticas, manuales	• El análisis tradicional no está diseñado para detectar las configuraciones erróneas más habituales de la nube (la principal causa de las vulneraciones de datos basadas en la nube).[2] • Implementar soluciones de seguridad puntuales para cada entorno de nube distinto dificulta gestionar el control y las políticas según las necesidades.

TABLA 1: Los desafíos de seguridad de las cargas de trabajo de nube híbrida surgen al no reconocer las diferencias esenciales entre la informática de nube y la tradicional.

2. Cloud Security Alliance. «Top Threats to Cloud Computing: Egregious Eleven Deep Dive». Septiembre de 2020.

Los equipos de operaciones de TI, DevOps y de operaciones de seguridad tienen la responsabilidad compartida de mantener la seguridad y la disponibilidad de las cargas de trabajo esenciales en la nube.

Tres pasos para redefinir el riesgo

La mejor manera de sacar el máximo partido a la transformación digital es aceptar el cambio de paradigma que representa. Los viejos modelos de gestión de riesgos ya no sirven cuando el cambio es constante y hay muchos gallos en el gallinero.

Para proteger las cargas de trabajo de nube, los equipos empresariales necesitan:

1. Mejorar la visibilidad: identificar los riesgos desconocidos o no detectados en las cargas de trabajo.
2. Acelerar la recuperación: mejorar la velocidad de la recuperación ante riesgos integrando la flexibilidad en las cargas de trabajo de nube.
3. Simplificar la seguridad: unificar la mitigación de riesgos en las cargas de trabajo, los terminales y los contenedores.

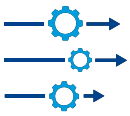
Paso 1: Mejorar la visibilidad: identifique los riesgos desconocidos o no detectados en las cargas de trabajo

- **Por qué es un desafío:** es imposible gestionar los riesgos si no sabe que existen. Lamentablemente, la mayoría de los administradores de máquinas virtuales carecen de visibilidad sobre las posibles vulnerabilidades de las aplicaciones y cargas de trabajo que se ejecutan en sus máquinas virtuales. Mientras que un atacante solo necesita identificar y aprovechar una única vulnerabilidad para obtener un acceso no autorizado, quienes las protegen deben conocer todas las formas en las que se pueden vulnerar para poder cerrar esas posibles vías de acceso. Además, una vez que se identifican las vulnerabilidades, no siempre es sencillo lograr que los departamentos de operaciones de TI y de operaciones de seguridad se pongan de acuerdo respecto a qué vulnerabilidad hay que corregir primero, cuándo y por qué.
- **Ejemplo:** Joe es ingeniero de fiabilidad de sitios (SRE) en una gran empresa de servicios sanitarios. Es responsable de la gestión de su infraestructura de nube privada, que incluye servidores, cargas de trabajo y aplicaciones que tratan información confidencial sobre la atención sanitaria. Joe sabe que tiene que identificar y mitigar cualquier vulnerabilidad que pueda afectar la conformidad o exponer los datos de los pacientes. No obstante, el rendimiento, la disponibilidad y el tiempo de actividad del servicio son las principales prioridades para Joe y los demás SRE de su equipo. Al fin y al cabo, la atención al paciente es una misión esencial.

  Actualmente, Joe espera que Sarah, analista de seguridad, le informe cuando un análisis programado detecte una vulnerabilidad de alta gravedad que requiera mitigación. A menudo no están de acuerdo al respecto de cuál es la mejor forma de actuar, porque cada uno utiliza un conjunto de herramientas diferente. Sin un sistema de registro común, llegar a un consenso sobre estas cuestiones esenciales sigue siendo complicado: qué vulnerabilidades tienen la máxima prioridad, si estos controles compensatorios son suficientes, cuál es el objetivo de los atacantes y cómo pretenden alcanzarlo, etc.
- **Se necesita identificación de riesgos entre dominios:** detecte todos los riesgos de la carga de trabajo de nube, desde todos los ángulos y vectores de ataque, y utilice un sistema de registro común para gestionarlos. Si no es posible aplicar un parche debido al riesgo de tiempo de inactividad, alcance una decisión consensuada sobre un control compensatorio o establezca una lista de vigilancia para detectar cuándo se produce un ataque orientado a la vulnerabilidad.

Paso 2: Acelerar la recuperación: mejore la velocidad de la recuperación ante riesgos integrando la flexibilidad en las cargas de trabajo de nube

- **Por qué es un desafío:** para la mayoría de las empresas, la cuestión ya no es si se va a producir una vulneración de datos, sino cuándo. Durante una vulneración, conocer el alcance o «la onda expansiva» de la exposición es fundamental para prevenir ataques similares en el futuro. Además, estos conocimientos son fundamentales para una recuperación rápida y completa. El desafío es una cuestión de prioridades que compiten entre sí. La prioridad de los equipos de DevOps y de operaciones de TI es restablecer los servicios lo antes posible, aunque eso signifique destruir las pruebas forenses y los elementos que el equipo de operaciones de seguridad necesita para identificar e investigar el origen y el alcance real del ataque.
- **Ejemplo:** recuperarse de un ataque de un programa de secuestro dentro del entorno de nube puede ser caro, complicado y laborioso. Estos ataques pueden migrar desde las cargas de trabajo hasta los servidores que las alojan, y hasta los terminales utilizados por los empleados para acceder a estas cargas de trabajo. El objetivo es reducir la superficie de ataque del programa de secuestro frenando sus primeras etapas (es decir, la ejecución del código dentro de la propia carga de trabajo) y, además, hacerlo antes de que el conjunto de herramientas esté completamente implementado o de que se establezcan las conexiones de mando y control (C2) a fin de robar o cifrar los datos para pedir un rescate.



- **Se necesita flexibilidad ante el riesgo:** restablecer los servicios rápidamente después de una vulneración o del ataque de un programa malicioso, y conservar los datos necesarios para realizar investigaciones forenses es posible en la nube, siempre que se cuente con la plataforma de seguridad de cargas de trabajo adecuada. De hecho, salvar esta brecha es un aspecto clave de integrar la flexibilidad ante el riesgo en sus cargas de trabajo de nube. Gestionar la seguridad de las cargas de trabajo y de los terminales desde la misma plataforma permite a los equipos identificar los riesgos en estos puntos de control y seguir una estrategia de recuperación más flexible.

Paso 3: Simplificar la seguridad: unifique la mitigación de riesgos en las cargas de trabajo, los terminales y los contenedores

- **Por qué es un desafío:** gestionar los riesgos en las cargas de trabajo de nube con soluciones puntuales tradicionales produce procesos compartimentados, que añaden costes de funcionamiento y agravan el riesgo. El uso de diferentes herramientas de seguridad basadas en el proveedor de nube pública, el sistema operativo del host o el tipo de nube (privada o pública), hace impracticable una estrategia coherente de mitigación de riesgos. Al fin y al cabo, cuando no hay una única fuente fiable en materia de seguridad, los equipos no se pueden poner de acuerdo al respecto de cómo prevenir los ataques de programas maliciosos, encontrar y arreglar las configuraciones erróneas, o contener las amenazas de rápida evolución.
- **Ejemplo:** para optimizar la flexibilidad operativa, algunos equipos de operaciones de TI optan por utilizar varios proveedores de nube o combinar el uso de infraestructuras de nube privada y pública. A falta de una política de seguridad verdaderamente independiente que pueda trascender estos entornos, los equipos se quedan con una amalgama de controles o con un único proveedor de servicios de nube o arquitectura de nube (privada o pública).
- **Se necesita seguridad unificada:** el objetivo es implementar una seguridad unificada diseñada para la nube y aplicada de manera uniforme, independientemente de dónde se encuentre la carga de trabajo (nube pública o privada). Aplicar una única gestión del ciclo de vida en todas las nubes, cargas de trabajo y contenedores hace posible disponer tanto de políticas de seguridad como de estrategias de mitigación de riesgos coherentes y amplias. Por ejemplo, utilizar una única plataforma para la gestión de vulnerabilidades, la auditoría y la corrección, y la detección y respuesta en los terminales (EDR) simplifica la seguridad de las cargas de trabajo y permite la colaboración entre los equipos de operaciones de TI, de operaciones de seguridad y DevOps.

Seguridad intrínseca para cargas de trabajo de nube

Tal y como se muestra en este documento, el uso de tecnologías dispares para gestionar las cargas de trabajo de nube complica el riesgo y no es escalable. Al mismo tiempo, es fundamental permitir que todos los equipos, desde el de operaciones de TI hasta el de DevOps, pasando por el de operaciones de seguridad, utilicen la consola de su elección. Esto no quiere decir que migrar a la nube requiera la adopción de un proceso completamente nuevo, una nueva interfaz de usuario o una nueva consola de gestión. Al fin y al cabo, estos equipos ya tienen bastante trabajo.

Con el enfoque de seguridad intrínseca de VMware, la supervisión profunda y el análisis del comportamiento se implementan en cada punto de control: nube, carga de trabajo, terminal, red e identidad, y posteriormente se unifican para obtener información contextual completa. Al igual que una cámara de vídeo que graba cada movimiento en los puntos de control, la seguridad intrínseca permite obtener información contextual completa. Dado que no es necesario unir manualmente la telemetría de puntos de control dispares, los equipos pueden rastrear rápidamente las amenazas desde el punto de entrada y en cada paso intermedio.

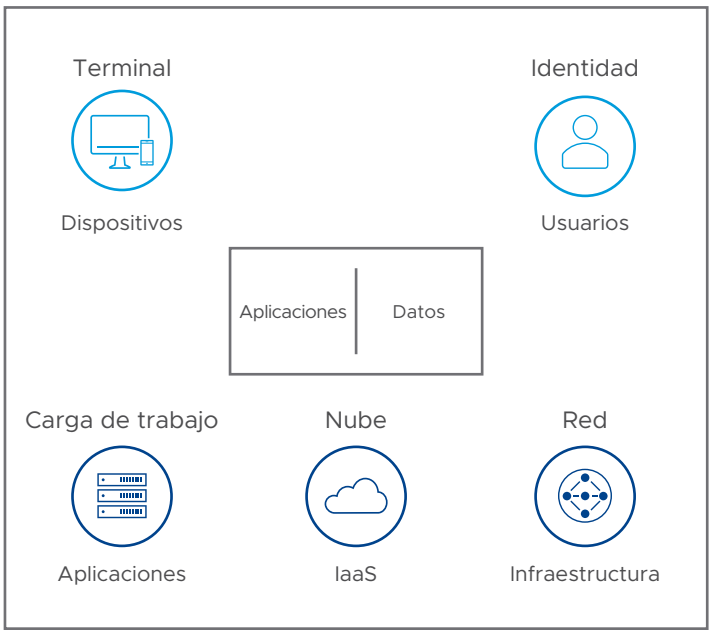


FIGURA 1: Los cinco puntos de control de la seguridad intrínseca.

Protección escalable de las cargas de trabajo de nube

VMware Carbon Black Cloud proporciona toda la funcionalidad para la protección escalable de las cargas de trabajo de nube, y se integra de manera nativa con vSphere y NSX. Gracias a esta estrecha integración, los administradores de vSphere y NSX pueden acceder a todos los datos relevantes sobre amenazas en el contexto de sus respectivos dominios y dentro de la misma consola, optimizada para sus perfiles particulares.

Además de proporcionar un conocimiento contextual completo en los entornos de nube, las cargas de trabajo, los terminales, las redes y las identidades, y de las relaciones entre ellos, VMware Carbon Black Cloud proporciona el sistema común de registro para que los equipos de operaciones de TI, DevOps y de operaciones de seguridad puedan prevenir, detectar y corregir las amenazas que afectan a las aplicaciones y cargas de trabajo esenciales.

Los componentes fundamentales de la seguridad intrínseca son:

- VMware Carbon Black Cloud
- VMware vSphere
- VMware NSX

VMware Carbon Black Cloud

VMware Carbon Black Cloud es una plataforma de protección de cargas de trabajo nativa de nube que combina el refuerzo inteligente de la seguridad del sistema y la prevención según el comportamiento que permiten mantener a raya las amenazas emergentes mediante una única solución de gestión del ciclo de vida y una consola fácil de usar.

VMware vSphere

vSphere es la plataforma de virtualización de recursos informáticos líder, que hemos rediseñado con *Kubernetes* nativo para que los clientes puedan modernizar las cargas de trabajo que ejecutan en vSphere.

VMware NSX Advanced Threat Prevention™

Con tecnología de aprendizaje automático, VMware NSX Service-defined Firewall™ ofrece análisis de tráfico de red, detección y prevención de intrusiones, y análisis avanzado de programas maliciosos, junto con funciones integrales de detección y respuesta de red.

Protección de VMware de las cargas de trabajo de nube: funcionamiento

El enfoque de seguridad intrínseca de VMware permite a las empresas proteger las cargas de trabajo de nube utilizando la infraestructura existente para identificar proactivamente los riesgos, prevenir los ataques y las vulnerabilidades, y detectar y responder rápidamente a las amenazas nuevas y emergentes.

El proceso de tres pasos, que cuenta con el apoyo de controles de seguridad esenciales, funciona de la siguiente manera:

FIGURA 2: La seguridad intrínseca para cargas de trabajo de nube proporciona una protección completa para las cargas de trabajo de vSphere.

Paso 1: Identificar el riesgo

- **Comprobación inicial de integridad del estado:** VMware Carbon Black Cloud lleva a cabo una comprobación inicial de la integridad del estado para validar que el sistema en el que se está instalando la carga de trabajo esté limpio, y sea compatible y adecuado para el tipo de carga de trabajo en cuestión. También recopila y analiza los niveles de parches del sistema operativo, evalúa las vulnerabilidades y los errores de configuración, y determina si es necesario un refuerzo adicional.
- **Visibilidad continua del estado del sistema:** VMware Carbon Black Cloud identifica las discrepancias de configuración, la presencia de aplicaciones desconocidas o no autorizadas, las vulnerabilidades y otras actividades dinámicas que aumentan la superficie de ataque del entorno. Por ejemplo:
  - Supervisa cualquier cambio que indique una actividad maliciosa (por ejemplo, borrado de contraseñas, cambios en la configuración de BitLocker).
  - Audita y corrige para consultar 1500 elementos de cada carga de trabajo y terminal en nubes privadas y públicas.
  - Permite que los administradores puedan ejecutar consultas SQL personalizadas para buscar comportamientos o actividades maliciosos específicos.
- **Visibilidad continua de las vulnerabilidades y la actividad de la red:** VMware Carbon Black Cloud permite a los administradores de vSphere ver en VMware vCenter® las vulnerabilidades de las cargas de trabajo priorizadas según su riesgo, así como llevar a cabo evaluaciones de las vulnerabilidades periódicamente sin analizar las cargas de trabajo. NSX ofrece un cortafuegos distribuido integrado que permite a los equipos de operaciones de TI supervisar la comunicación de las cargas de trabajo en las nubes privadas y públicas, determinar qué cargas de trabajo forman parte de una aplicación y establecer cómo pueden segmentar las cargas de trabajo no relacionadas.

Paso 2: Evitar que se agraven los riesgos

- **Evite los ataques en las cargas de trabajo:** VMware Carbon Black Cloud ofrece un antivirus de nueva generación (NGAV) para una protección que trasciende los indicadores puntuales de programas maliciosos, programas de secuestro, ataques de día cero, variantes rápidas, archivos sospechosos y procesos potencialmente no deseados (PUP) específicos de las cargas de trabajo en las nubes privadas y públicas. La plataforma de VMware combina señuelos para los programas de secuestro, análisis dinámicos y aprendizaje automático para proporcionar un análisis continuo que impide la ejecución de archivos sospechosos.
- **Evite los ataques sin programas maliciosos:** además de bloquear los ataques de programas maliciosos, VMware Carbon Black Cloud protege de los últimos ataques persistentes que utilizan tácticas de programas maliciosos sin archivos, basadas en la memoria y basadas en programas que ya están instalados. Estos ataques perniciosos utilizan el software existente y las aplicaciones permitidas (por ejemplo, PowerShell), así como los protocolos autorizados, para llevar a cabo actividades maliciosas. A diferencia de los enfoques heredados que se basan en las amenazas conocidas, la plataforma de VMware puede identificar nuevas variantes y ataques de día cero al reunir la información sobre los comportamientos relacionados.
- **Evite los ataques basados en la red:** NSX Service-defined Firewall protege las cargas de trabajo mediante la mitigación del desplazamiento lateral y el bloqueo de los ataques entrantes de aplicaciones y servicios vulnerables. Con este nivel de visibilidad, puede comprender cómo se mueven por la red los ataques que aprovechan programas ya instalados, identificar los indicadores de riesgo (IOC) y bloquear estas conexiones de red para aislar las cargas de trabajo de los atacantes.
- **Personalice la prevención:** cada entorno tiene limitaciones operativas diferentes y a menudo contrapuestas. VMware ofrece a nuestros clientes la posibilidad de equilibrar la seguridad y los riesgos operativos con una granularidad precisa. Con el motor de políticas de VMware, usted tiene la posibilidad de elegir cómo mitigar las amenazas según el tipo específico de carga de trabajo, su función, gravedad y adyacencia a otras cargas de trabajo esenciales. Por ejemplo, para aislar una carga de trabajo esencial, un administrador de sistemas puede impedir que PowerShell extraiga la memoria de otro proceso o invoque una aplicación no fiable.

Paso 3: Detectar y responder a los riesgos actuales

- **Sepa cuándo y dónde se debe iniciar una investigación (observación de cerca):** utilice la prestación prediseñada de detección automática de amenazas de VMware, disponible mediante la función actualizada de inteligencia para la detección de amenazas de VMware Threat Analysis Unit™, para localizar los sistemas afectados y aislarlos para su reparación. Las API de VMware le permiten integrar fuentes de información y listas de seguimiento de terceros, y completar la información compartida y colaborativa sobre las amenazas desde la robusta plataforma de VMware, User Exchange.
- **Conozca todo el alcance y la duración del ataque (observación de lejos):** la plataforma de VMware permite a los investigadores rebobinar la cinta para comprender cómo se desarrolló un ataque, qué sistemas se vieron afectados y cómo progresó el ataque a lo largo del tiempo. Gracias a que VMware captura todos los datos (por ejemplo, la actividad detallada de los procesos, las interacciones entre ellos, las relaciones entre los principales y los secundarios, etc.), elaborar un cronograma detallado sin puntos ciegos, mucho después de los hechos, permite a los equipos forenses y de respuesta a incidentes descubrir la verdad.
- **Flujo de trabajo rápido de detección para la prevención:** en tres sencillos pasos, VMware Carbon Black Cloud le permite convertir la detección de amenazas en una política de prevención estandarizada aplicable a todas sus cargas de trabajo. En primer lugar, aplique políticas automatizadas basadas en detecciones anteriores personalizadas para sus cargas de trabajo. En segundo lugar, previsualice al instante los efectos descendentes de la política de prevención antes de aplicarla. En tercer lugar, con un solo clic, aplique la política actualizada a todas las cargas de trabajo en cualquier entorno.

Proteger las cargas de trabajo de nube ante una amplia variedad de amenazas requiere un enfoque múltiple, con visibilidad granular pero unificada de todos los aspectos del entorno informático. Los departamentos de operaciones de TI, DevOps y de operaciones de seguridad deben trabajar en armonía, ya que tienen la responsabilidad compartida de proteger las cargas de trabajo de nube esenciales. Las empresas que intentan utilizar los enfoques tradicionales para proteger las nubes híbridas se enfrentan a muchos desafíos, como la falta de visibilidad sobre cómo se conectan las cargas de trabajo, los procesos fragmentados y los errores de configuración. Como se comenta en este documento, aumentar la visibilidad, acelerar la recuperación y simplificar la seguridad son tres estrategias clave que los equipos empresariales deben poner en marcha para mitigar los riesgos.

VMware se encuentra en una posición privilegiada para proteger las cargas de trabajo en las nubes híbridas. En concreto, las soluciones de VMware permiten a los equipos identificar con precisión los riesgos emergentes para las cargas de trabajo, evitar que estos riesgos se agraven y contener rápidamente los ataques sin interrumpir las operaciones. Mientras que otros productos de seguridad para terminales y cargas de trabajo solo recopilan un conjunto de datos relacionados con atacantes conocidos, VMware Carbon Black Cloud recopila continuamente todos los datos sobre las cargas de trabajo, los terminales y la red, y analiza los patrones de comportamiento de los atacantes para detener proactivamente los ataques antes de que repercutan en su entorno. Esta mayor visibilidad operativa simplifica la seguridad y acelera la recuperación del sistema.

Aunque en el mercado hay muchos proveedores de protección de cargas de trabajo de nube, no todas las soluciones son iguales. Las empresas deben tener en cuenta los requisitos fundamentales, como la arquitectura de diseño, los modelos operativos y la escalabilidad, y plantear las preguntas adecuadas para determinar si la plataforma se ajusta a sus necesidades. Utilice la lista de comprobación de la tabla 2 cuando se plantee adquirir una plataforma de protección de cargas de trabajo de nube. Cuenta con un total de cien puntos, que debe asignar a cada pregunta fundamental sobre su organización. El valor total de la columna de valores ponderados debe ser igual a cien. Completar esta lista de comprobación le permitirá hacerse una mejor idea de sus prioridades y consideraciones básicas.

Lista de comprobación para evaluar plataformas de protección de cargas de trabajo de nube

	REQUISITO FUNDAMENTAL	PREGUNTAS PRINCIPALES	VALOR PONDERADO
Arquitectura de diseño	Describa cómo la plataforma de protección de cargas de trabajo de nube visualiza las comunicaciones y conexiones entre las cargas de trabajo.	¿Puede consolidar los datos de telemetría de nubes, cargas de trabajo, redes y terminales?	
		¿Es compatible con todas las aplicaciones, independientemente del sistema operativo, la configuración y la nube, o depende de alguna de ellas?	
		¿Puede reconocer qué constituye un comportamiento normal en las cargas de trabajo y entre ellas?	
		¿Qué modelos de comportamiento implementa para detectar ataques de programas maliciosos y de otro tipo de programas (sin archivos) en las cargas de trabajo y entre ellas?	
Modelo operativo	Describa cómo la plataforma de protección de cargas de trabajo de nube respalda la colaboración y coordinación fluidas entre equipos de operaciones de TI, DevOps y de operaciones de seguridad para reducir el riesgo, simplificar la conformidad y aumentar la flexibilidad.	¿Cuántos agentes hay que instalar en cada carga de trabajo, contenedor y sistema operativo?	
		¿Pueden los equipos de operaciones de TI, DevOps y de operaciones de seguridad utilizar el mismo conjunto de datos para supervisar y responder a los incidentes?	
		¿Qué marcos de control admite su plataforma (por ejemplo, NIST 800-53)?	
		¿Cómo funcionaría un flujo de trabajo normal entre los equipos de operaciones de TI, DevOps y de operaciones de seguridad una vez que se ha identificado una amenaza, una vulnerabilidad o una configuración errónea?	
Escalabilidad	Describa cómo la plataforma de protección de cargas de trabajo de nube respalda el uso de programas de control de cambios seguros y rápidos para aumentar la estandarización de las políticas de seguridad y reducir el riesgo de configuraciones erróneas, y otros errores humanos, según las necesidades.	¿Cuál es el consumo medio de CPU de cada agente de protección de las cargas de trabajo de nube?	
		¿Puede consolidar múltiples funciones de seguridad, como EDR, NGAV y gestión de vulnerabilidades, en un único agente y consola de gestión?	
		¿Puede la plataforma de protección de las cargas de trabajo de nube aplicar una política de seguridad estandarizada y coherente en los entornos de nube privada, pública e híbrida y presentar informes al respecto?	
		¿Cómo lleva a cabo el análisis periódico de vulnerabilidades sin afectar a la disponibilidad ni al rendimiento?	

TABLA 2: Lista de comprobación para evaluar la protección de cargas de trabajo de nube.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.es