Protección para cargas de trabajo de la nube

Cómo proteger cargas de trabajo en nubes híbridas

vmware®

Índice

Resumen ejecutivo

La nube híbrida es el eje central de la transformación digital. Actualmente, más del 90 % de las empresas afirman que utilizan una estrategia de nubes múltiples, en la que la mayoría combina el uso de nubes públicas y privadas.[1] Lo bueno es que este enfoque ofrece la flexibilidad y escalabilidad necesarias para una rápida innovación. La desventaja es que suele sumarle mayor complejidad y riesgo, lo que convierte la seguridad en un componente fundamental de las nubes públicas y privadas.

Mientras los equipos empresariales implementan y administran cargas de trabajo críticas en entornos de nubes múltiples, es fundamental tener visibilidad de la posición de seguridad de las cargas de trabajo y poder controlar la superficie de ataque para proteger los datos y mantener las operaciones.

Muchos de los equipos de la empresa, como operaciones de TI y operaciones de seguridad (SecOps), son partes interesadas clave en el rendimiento, la disponibilidad y la seguridad de las cargas de trabajo de la nube. Otro factor de éxito fundamental es mantener a los miembros de los equipos alineados, en lugar de fragmentados.

Este caso de uso del producto aborda los desafíos clave que los equipos empresariales detectaron a la hora de proteger las cargas de trabajo de la nube y cómo superarlos mediante el enfoque de seguridad intrínseca de VMware, que incluye VMware Carbon Black Cloud™, VMware vSphere® y VMware NSX®. Este informe también incluye un análisis sobre cómo la nube nos obliga a resignificar el riesgo de una manera que acerque a las partes interesadas de los distintos equipos, en lugar de mantenerlas del otro lado de la brecha digital. También se proporciona una lista de verificación de evaluación de la plataforma de protección de cargas de trabajo de la nube con el fin de ayudar a las organizaciones a analizar los requisitos clave a la hora de considerar las soluciones.

Desafíos de seguridad con nubes privadas, públicas e híbridas

Se requiere un gran esfuerzo para implementar y administrar cargas de trabajo y aplicaciones en nubes públicas, privadas e híbridas. Lo que alguna vez consideramos la TI tradicional ahora es un trabajo conjunto. Los equipos de operaciones de TI, DevOps y SecOps ahora colaboran para suministrar y proteger aplicaciones y servicios desde la nube.

1. Flexera. “Flexera 2020 State of the Cloud Report.” Abril de 2020.

Tal como se muestra en la Tabla 1, si se falla en la coordinación de equipos y la planificación de los aspectos exclusivos de las cargas de trabajo de la nube, los riesgos pueden incrementarse.

	OPERACIONES DE NUBE HÍBRIDA	DESAFÍOS DE SEGURIDAD	OPERACIONES DE TI TRADICIONALES	DEFICIENCIAS DE 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 incrementan el riesgo.	Monolíticas y aisladas	• El antivirus (AV) tradicional no está diseñado para un contexto de cargas de trabajo de la nube. • El monitoreo centrado en el centro de datos carece de la comprensión básica del comportamiento normal de la red.
Modelo operacional	Propiedad y administración distribuidas	• El equipo de operaciones de TI es responsable de la posición, administración y disponibilidad de las cargas de trabajo, pero no tiene visibilidad de las vulnerabilidades internas. • Los silos de tecnología y procesos contribuyen a errores de configuración, configuraciones inseguras y otros errores humanos.	Centralizadas	• La incorporación de productos de seguridad puntuales requiere la instalación de otros agentes, lo que ralentiza el rendimiento del sistema y complica las operaciones. • La falta de una visibilidad unificada en las cargas de trabajo, y de todas las cargas de trabajo y nubes, complica la coordinación entre los equipos.
Escalabilidad	Altamente dinámicas y automáticas	• La falta de control de cambios ocasiona errores de configuración, como almacenamiento de datos no seguro, exceso de permisos, ajustes predeterminados de configuración y credenciales, e inhabilitación de controles de seguridad. • La imposibilidad de estandarizar las políticas de seguridad de las cargas de trabajo en nubes públicas y privadas incrementa el riesgo.	Estáticas y manuales	• El análisis tradicional no está diseñado para detectar errores de configuración comunes de la nube, que es la causa principal de infracciones de datos basadas en la nube.[2] • La implementación de soluciones de seguridad puntuales para cada entorno de nube diferente complica la administración de la gobernanza y de las políticas a gran escala.

TABLA 1: Los desafíos de seguridad de las cargas de trabajo de la nube híbrida se originan en la imposibilidad de reconocer las diferencias clave entre la computación de nube y la TI tradicional.

2. Cloud Security Alliance. "Top Threats to Cloud Computing: Egregious Eleven Deep Dive" (Principales amenazas para la computación de nube: análisis de once amenazas atroces). Septiembre de 2020.

Los equipos de operaciones de TI, DevOps y SecOps comparten la responsabilidad de mantener la seguridad y disponibilidad de las cargas de trabajo críticas de la nube.

Tres pasos para redefinir el riesgo

La mejor manera de aprovechar al máximo la transformación digital es aceptar el cambio de paradigma que esta representa. Los modelos antiguos de administración de riesgos ya no sirven cuando el cambio es una constante y hay demasiadas personas trabajando en lo mismo.

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

1. Aumentar la visibilidad para identificar los riesgos desconocidos o no detectados en las cargas de trabajo
2. Acelerar la recuperación de riesgos incorporando adaptabilidad en las cargas de trabajo de la nube
3. Simplificar la seguridad para unificar la mitigación de riesgos en cargas de trabajo, terminales y contenedores

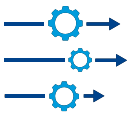
Paso uno: Aumentar la visibilidad para identificar los riesgos desconocidos o no detectados en las cargas de trabajo

- **Por qué es un desafío:** no se pueden administrar los riesgos que se desconocen. Desafortunadamente, la mayoría de los administradores de máquinas virtuales (virtual machine, VM) no están al tanto de la potencial vulnerabilidad a los ataques de las aplicaciones y cargas de trabajo que se ejecutan en sus VM. Mientras que un atacante solo necesita identificar y explotar una sola vulnerabilidad para obtener acceso no autorizado, los encargados de la protección deben conocer todas las formas de explotarla para cerrar esos accesos. Además, una vez que se identifican las vulnerabilidades, la obtención del consenso entre los equipos de operaciones de TI y SecOps sobre cuáles son las vulnerabilidades de mayor prioridad para corregir, por qué y cuándo hacerlo no siempre es una tarea sencilla.
- **Ejemplo:** Joe es ingeniero de confiabilidad del sitio (site reliability engineer, SRE) en una importante empresa de servicios de salud. Es responsable de administrar la infraestructura de nube privada, que incluye servidores, cargas de trabajo y aplicaciones que procesan datos de salud confidenciales. Joe sabe que necesita identificar y mitigar cualquier vulnerabilidad que pudiera afectar el cumplimiento o exponer datos de pacientes. Dicho eso, el rendimiento y la disponibilidad del servicio y el tiempo de servicio del sistema son las principales prioridades para Joe y los demás SRE de su equipo. Después de todo, la atención de los pacientes es fundamental.

  Actualmente, Joe espera que Sarah, una analista de seguridad, le avise cuando un análisis programado detecte una vulnerabilidad grave que deba mitigarse. Por lo general, les cuesta ponerse de acuerdo y decidir cuál es el mejor plan de acción, ya que cada uno usa un conjunto de herramientas diferente. Sin un sistema de registro común, es difícil llegar a un consenso sobre estas cuestiones críticas: cuáles son las vulnerabilidades de mayor prioridad, si son suficientes estos controles compensatorios, cuál es el objetivo de los atacantes, cómo proceden, etc.
- **Qué se necesita: Detección de riesgos entre dominios** para descubrir todos los riesgos de las cargas de trabajo de la nube, desde todos los ángulos y vectores de ataque, y emplear un sistema de registro común para administrarlos. Si no es posible implementar un parche debido al riesgo de tiempo fuera de servicio, obtenga el consenso sobre un control compensatorio, o bien configure una lista de observación para detectar cuándo la vulnerabilidad está en la mira.

Paso dos: Acelerar la recuperación de riesgos incorporando adaptabilidad en las cargas de trabajo de la nube

- **Por qué es un desafío:** para la mayoría de las empresas, las infracciones de datos ya no son una cuestión hipotética, sino de tiempo. Durante una infracción, es fundamental conocer la extensión o el radio de alcance de la exposición a fin de evitar ataques similares en el futuro. Además, esa información es esencial para lograr una recuperación rápida y total. Se trata de un desafío de prioridades contrapuestas. Para los equipos de DevOps y operaciones de TI, la prioridad es restaurar los servicios cuanto antes, incluso si eso implica la destrucción de la evidencia forense o los artefactos que el equipo de SecOps necesita a fin de identificar e investigar el origen y alcance total del ataque.
- **Ejemplo:** la recuperación de un ataque de ransomware en un entorno de nube puede ser costosa, complicada y ardua. Estos ataques pueden migrar de las cargas de trabajo a los servidores que las alojan, y a los terminales que usan los empleados para acceder a estas cargas de trabajo. El objetivo es reducir la superficie de ataque del ransomware mediante la neutralización de las primeras etapas del ataque, como la ejecución del código en la carga de trabajo, antes de implementar por completo el conjunto de herramientas o de establecer las conexiones de comando y control (C2) para extraer o cifrar los datos secuestrados.



- **Qué se necesita: Adaptabilidad al riesgo:** restaurar los servicios rápidamente en la nube después de una infracción o ataque de malware, y conservar los datos necesarios para realizar investigaciones forenses es posible siempre que se cuente con la plataforma de seguridad de cargas de trabajo adecuada. De hecho, cerrar esta brecha es un aspecto fundamental para incorporar adaptabilidad al riesgo en las cargas de trabajo de la nube. La administración de la seguridad de las cargas de trabajo y los terminales desde una misma plataforma les permite a los equipos identificar los riesgos en todos estos puntos de control y aplicar una estrategia de recuperación más adaptable.

Paso tres: Simplificar la seguridad para unificar la mitigación de riesgos en cargas de trabajo, terminales y contenedores

- **Por qué es un desafío:** la administración de riesgos en cargas de trabajo de la nube con soluciones puntuales tradicionales supone procesos anticuados que incrementan los costos operacionales generales y agravan el riesgo. Cualquier estrategia uniforme de mitigación de riesgos queda fuera de juego cuando se usan diferentes herramientas de seguridad basadas en el proveedor de nube pública, sistema operativo host o tipo de nube (pública frente a privada). Después de todo, cuando no hay una única fuente fiable en materia de seguridad, los equipos no pueden llegar a un consenso sobre cómo evitar ataques de malware, encontrar y corregir errores de configuración, o contener amenazas en constante evolución.
- **Ejemplo:** para optimizar la adaptabilidad operacional, algunos equipos de operaciones de TI deciden usar varios proveedores de nube, o combinar el uso de infraestructura de nube pública y privada. Sin una política de seguridad verdaderamente independiente que pueda trascender estos entornos, los equipos quedan a merced de controles dispares o se ven limitados a un único proveedor de servicios de nube o arquitectura de nube (pública o privada).
- **Qué se necesita: Seguridad unificada** a fin de implementar una seguridad unificada diseñada para la nube y aplicada de manera uniforme, independientemente de dónde se encuentre la carga de trabajo (nube pública frente a privada). El uso de una sola administración del ciclo de vida en diferentes nubes, cargas de trabajo y contenedores garantiza una políticas de seguridad y una estrategia de mitigación de riesgos uniformes y generalizadas. Por ejemplo, el empleo de una sola plataforma para administración de vulnerabilidades, auditorías y correcciones, y detección y respuesta en terminales (endpoint detection and response, EDR) simplifica la seguridad de las cargas de trabajo y permite la colaboración entre los equipos de operaciones de TI, SecOps y DevOps.

Seguridad intrínseca de las cargas de trabajo de la nube

Tal como muestra este informe, el uso de distintas tecnologías para administrar las cargas de trabajo de la nube agrava los riesgos y, sencillamente, no es escalable. Al mismo tiempo, es fundamental permitir que cada equipo, desde operaciones de TI hasta DevOps y SecOps, use la consola que prefiera. Esto no quiere decir que la migración a la nube requiere la adopción de un proceso completamente nuevo, o una nueva interfaz de usuario o consola de administración. Después de todo, estos equipos ya tienen demasiado con qué lidiar.

Con el enfoque de seguridad intrínseca de VMware, se implementan un monitoreo profundo y un análisis del comportamiento en cada punto de control (nube, carga de trabajo, terminal, red e identidad) que luego se unifican para lograr un contexto completo. De la misma forma que una videocámara registra los movimientos en cada punto de control, la seguridad intrínseca permite reconocer el contexto de manera integral. Dado que no es necesario recomponer manualmente la telemetría desde distintos puntos de control, los equipos pueden rastrear las amenazas rápidamente desde el punto de entrada y en cada paso intermedio.

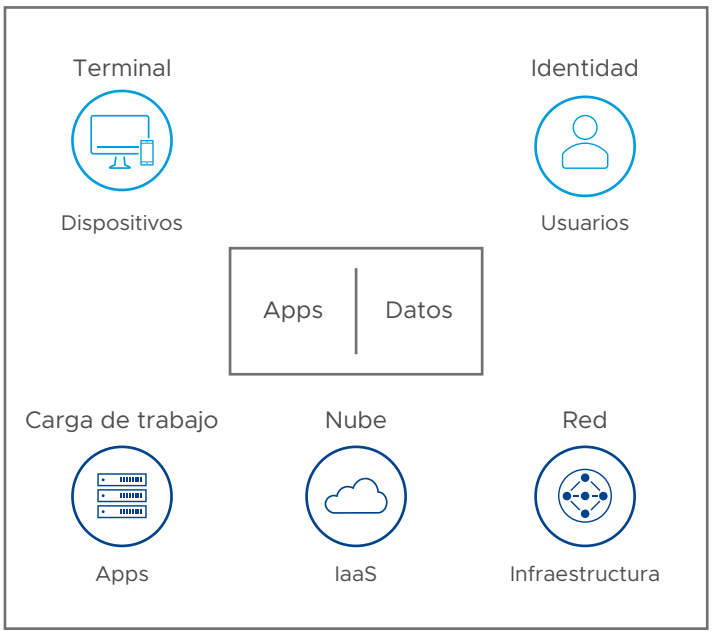


FIGURA 1: Los cinco puntos de control de la seguridad intrínseca.

Protección escalable para cargas de trabajo de la nube

VMware Carbon Black Cloud proporciona toda la funcionalidad de protección escalable para las cargas de trabajo de la nube y se integra de forma nativa con vSphere y NSX. Gracias a esta estrecha integración, los administradores de vSphere y NSX pueden acceder a toda la información relevante sobre amenazas en el contexto de los respectivos dominios y en la misma consola optimizada para sus propios roles.

Además de ofrecer reconocimiento contextual completo en todas las nubes, cargas de trabajo, terminales, redes e identidades, VMware Carbon Black Cloud proporciona el sistema de registro común necesario para que los equipos de operaciones de TI, DevOps y SecOps puedan prevenir, detectar y neutralizar las amenazas que impactan en sus aplicaciones y cargas de trabajo críticas.

Estos son los componentes básicos de la seguridad intrínseca:

- 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 de la nube que es nativa de la nube y que combina el fortalecimiento inteligente de sistemas y la prevención de comportamientos que resultan necesarios para mantener alejadas las amenazas emergentes, a través de una única consola de administración del ciclo de vida fácil de usar.

VMware vSphere

vSphere es la plataforma de virtualización de procesamiento líder del sector; fue rediseñada con *Kubernetes* nativo para permitir a los clientes modernizar las cargas de trabajo que se ejecutan en vSphere.

VMware NSX Advanced Threat Prevention™

VMware NSX Service-defined Firewall™ utiliza tecnología de aprendizaje automático y ofrece análisis del tráfico de red, prevención y detección de intrusiones, y análisis de malware avanzado con funciones integrales de detección y respuesta en redes.

Protección de VMware para cargas de trabajo de la nube: cómo funciona

El enfoque de seguridad intrínseca de VMware permite a las empresas proteger las cargas de trabajo de la nube mediante el uso de la infraestructura actual para identificar proactivamente riesgos, evitar ataques y exposiciones, y detectar y responder rápidamente a amenazas nuevas y emergentes.

El proceso de tres pasos funciona de la siguiente manera, con el respaldo de controles de seguridad esenciales.

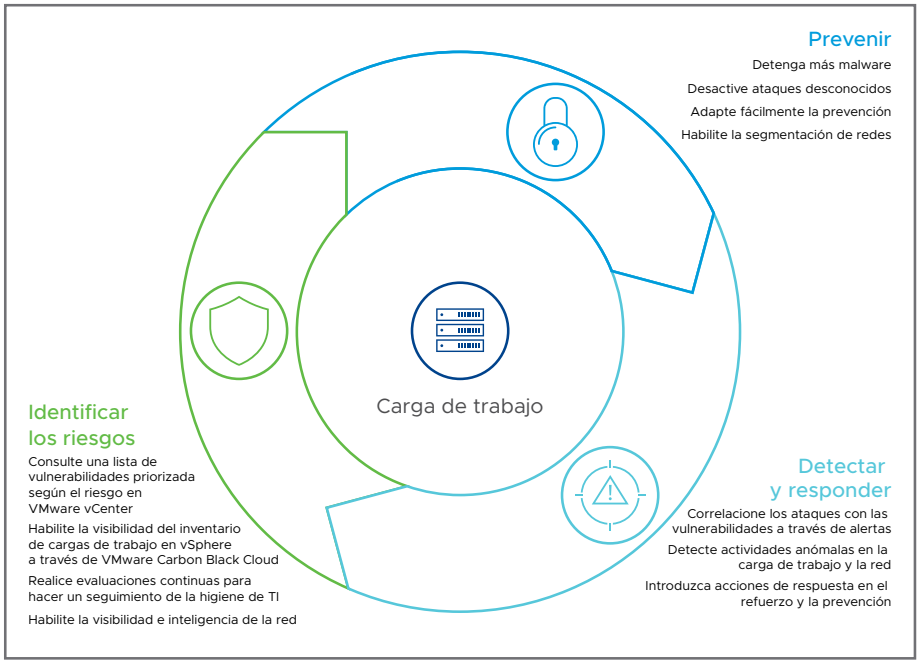


FIGURA 2: La seguridad intrínseca de cargas de trabajo de la nube brinda protección integral de cargas de trabajo de vSphere.

Paso uno: Identificar los riesgos

- **Verificación de integridad de estado inicial:** VMware Carbon Black Cloud realiza una verificación de integridad del estado inicial para validar que el sistema en el que se va a instalar la carga de trabajo no tenga problemas, cumpla con los requisitos y sea el adecuado para el tipo de carga de trabajo. También recopila y analiza los niveles de parches del sistema operativo, evalua vulnerabilidades y errores de configuración, y determina si es necesario un mayor fortalecimiento.
- **Visibilidad continua del estado del sistema:** VMware Carbon Black Cloud identifica desvíos en la configuración, la presencia de aplicaciones desconocidas o no autorizadas, vulnerabilidades y cualquier otra actividad dinámica que amplíe la superficie de ataque del entorno. Estas son algunas de las tareas que lleva a cabo:
  - Monitorear cualquier cambio que señale actividad maliciosa (p. ej., puesta a cero de contraseñas o cambios en la configuración de BitLocker)
  - Realizar auditorías y correcciones para consultar 1.500 artefactos de cada carga de trabajo y terminal en nubes públicas y privadas
  - Permitir que los administradores ejecuten consultas SQL personalizadas en busca de actividades o comportamientos maliciosos específicos
- **Visibilidad continua de vulnerabilidades y actividad de la red:** VMware Carbon Black Cloud permite a los administradores de vSphere ver las vulnerabilidades de las cargas de trabajo priorizadas según el riesgo en VMware vCenter® y realizar periódicamente evaluaciones de vulnerabilidades sin análisis en todas las cargas de trabajo. NSX ofrece un firewall distribuido integrado para que los equipos de operaciones de TI puedan monitorear la comunicación de las cargas de trabajo en nubes públicas y privadas, determinar cuáles son las cargas de trabajo que integran una aplicación y definir cómo segmentar las cargas de trabajo no relacionadas.

Paso dos: Prevenir el escalamiento de los riesgos

- **Prevenir exploits en la carga de trabajo:** VMware Carbon Black Cloud ofrece un antivirus de próxima generación (next generation antivirus, NGAV) para brindar protección más allá de indicadores puntuales de malware, ransomware, día cero, variantes rápidas, archivos sospechosos y procesos potencialmente no deseados (Potentially Unwanted Process, PUP) específicos de las cargas de trabajo en nubes públicas y privadas. La plataforma de VMware combina señuelos de ransomware, análisis dinámico y aprendizaje automático para ofrecer análisis continuos que permitan impedir la ejecución de archivos sospechosos.
- **Prevenir ataques sin malware:** además de bloquear los ataques de malware, VMware Carbon Black Cloud brinda protección contra los ataques persistentes más recientes mediante tácticas de malware sin archivos, basadas en la memoria y "Living off the Land" (LotL). Estos ataques utilizan software existente, aplicaciones de listas seguras (p. ej., PowerShell) y protocolos autorizados para realizar actividades maliciosas. A diferencia de los enfoques convencionales que se basan en amenazas conocidas, la plataforma de VMware puede identificar nuevas variantes y exploits de día cero comprendiendo comportamientos relacionados.
- **Prevenir ataques basados en la red:** NSX Service-defined Firewall protege las cargas de trabajo mediante la mitigación del desplazamiento lateral y el bloqueo de exploits entrantes en aplicaciones y servicios vulnerables. Con este nivel de visibilidad, es posible comprender cómo se desplazan por la red los ataques LotL, identificar indicadores de compromiso (indicator of compromise, IOC) y bloquear esas conexiones de red para aislar las cargas de trabajo de los atacantes.
- **Personalizar la prevención:** cada entorno tiene distintas limitaciones operacionales que suelen ser contrapuestas. VMware ofrece a nuestros clientes la posibilidad de equilibrar los riesgos operacionales y de seguridad con granularidad precisa. El motor de políticas de VMware le permite elegir cómo mitigar las amenazas según el tipo específico de carga de trabajo, su función, su criticidad y la adyacencia a otras cargas de trabajo fundamentales. Por ejemplo, para aislar una carga de trabajo fundamental, un administrador de sistemas o servidores puede impedir que PowerShell desguace la memoria de otro proceso o invoque una aplicación poco confiable.

Paso tres: Detectar y responder a riesgos constantes

- **Saber cuándo y dónde iniciar una investigación (enfocarse):** utilice la detección de amenazas automatizada y lista para usar de VMware mediante la inteligencia de detección de amenazas actualizada de VMware Threat Analysis Unit™ a fin de identificar los sistemas afectados y aislarlos para su reparación. Las API de VMware le permiten integrar sus propias fuentes y listas de vigilancia de terceros, y completar la información compartida sobre amenazas de la sólida comunidad de intercambio de VMware.
- **Ver el período y alcance completos del ataque (obtener perspectiva):** la plataforma de VMware permite a los investigadores rebobinar la cinta para comprender cómo se desplegó un ataque, qué sistemas se vieron afectados y cómo este avanzó en el tiempo. Dado que VMware captura todos los datos (p. ej., actividad detallada de los procesos, interacción entre procesos, relaciones entre procesos primarios y secundarios, etc.), la creación a posteriori de una línea de tiempo sin puntos ciegos brinda a los equipos forenses y de respuesta a incidentes los recursos para descubrir la verdad.
- **Flujo de trabajo rápido desde la detección hasta la prevención:** en tres simples pasos, VMware Carbon Black Cloud le permite convertir la detección de amenazas en una política de prevención estandarizada en todas las cargas de trabajo. En primer lugar, aplique políticas automatizadas en función de detecciones previas y personalizadas para sus cargas de trabajo. Segundo, prevea de forma instantánea las repercusiones de la política de prevención antes de implementarla. Tercero, implemente con solo un clic la política actualizada en todas las cargas de trabajo de cualquier entorno.

Para proteger las cargas de trabajo de la nube contra una amplia variedad de amenazas, es necesario adoptar un enfoque de múltiples frentes, con visibilidad detallada, y a la vez unificada, de todos los aspectos del entorno de procesamiento. Los equipos de operaciones de TI, DevOps y SecOps deben trabajar conjuntamente para compartir la responsabilidad de la protección de las cargas de trabajo críticas en la nube. Las empresas que intentan usar enfoques tradicionales para proteger las nubes híbridas enfrentan muchos desafíos, como falta de visibilidad de la forma en la que se conectan las cargas de trabajo, procesos fragmentados y errores de configuración. Tal como vimos en este informe, el aumento de la visibilidad, la aceleración de la recuperación y la simplificación de la seguridad son tres estrategias clave que los equipos empresariales deben implementar para mitigar los riesgos.

VMware está posicionada de forma única para proteger cargas de trabajo en nubes híbridas. Más específicamente, las soluciones de VMware permiten a los equipos identificar con precisión los riesgos emergentes para las cargas de trabajo, evitar que estos riesgos escalen y contener rápidamente los ataques sin interrumpir las operaciones. Mientras otros productos de seguridad de terminales y cargas de trabajo solo recopilan un conjunto de datos relacionado con actores maliciosos conocidos, VMware Carbon Black Cloud recopila permanentemente datos integrales de cargas de trabajo, terminales y redes, y analiza los patrones de comportamiento de los atacantes para detener proactivamente los ataques antes del impacto. Este mayor nivel de visibilidad operacional simplifica la seguridad y acelera la recuperación del sistema.

Si bien hay muchos proveedores de protección de cargas de trabajo de la nube en el mercado, no todas las soluciones son iguales. Las empresas deben tener en cuenta requisitos clave, como la arquitectura de diseño, los modelos operacionales y la escalabilidad, y hacerse las preguntas adecuadas para determinar en qué medida una plataforma se adapta a sus necesidades. Use la lista de verificación de la Tabla 2 a fin de evaluar las plataformas de protección de cargas de trabajo de la nube. Tiene 100 puntos disponibles para asignar a cada pregunta clave en función de su organización. El total de la columna Valor ponderado debe sumar 100. Si completa esta lista de verificación, tendrá una mejor idea de las consideraciones y prioridades clave.

Lista de verificación de evaluación de la plataforma de protección de cargas de trabajo de la nube

	REQUISITO CLAVE	PREGUNTAS CLAVE	VALOR PONDERADO
Arquitectura de diseño	Describa de qué manera la plataforma de protección de cargas de trabajo de la nube visualiza las comunicaciones y conexiones entre las cargas de trabajo.	¿Puede consolidar los datos de telemetría de todas las 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 alguno de estos elementos?	
		¿Puede reconocer un comportamiento normal en una carga de trabajo o entre cargas de trabajo?	
		¿Qué modelos de comportamiento implementa para detectar ataques de malware y sin malware (sin archivos) en las cargas de trabajo y entre ellas?	
Modelo operacional	Describa de qué manera la plataforma de protección de cargas de trabajo de la nube permite la alineación y coordinación sin inconvenientes entre los equipos de operaciones de TI, DevOps y SecOps para reducir los riesgos, simplificar el cumplimiento y mejorar la adaptabilidad.	¿Cuántos agentes deben instalarse en cada carga de trabajo, contenedor y sistema operativo?	
		¿Pueden aprovechar los equipos de operaciones de TI, DevOps y SecOps el mismo conjunto de datos para monitorear y responder a incidentes?	
		¿Qué marcos de gobernanza admite su plataforma (p. ej., NIST 800-53)?	
		¿Cómo sería un flujo de trabajo típico entre los equipos de operaciones de TI, DevOps y SecOps una vez que se identifica una amenaza, una vulnerabilidad o un error de configuración?	
Escalabilidad	Describa de qué manera la plataforma de protección de cargas de trabajo de la nube respalda los programas de control de cambios seguros y rápidos para mejorar la estandarización de las políticas de seguridad y reducir el riesgo de errores de configuración y otros errores humanos según las necesidades.	¿Cuál es el consumo de CPU promedio de cada agente de protección de cargas de trabajo de la nube?	
		¿Puede consolidar varias capacidades de seguridad, como EDR, NGAV y administración de vulnerabilidades, en un solo agente y consola de administración?	
		¿Puede la plataforma de protección de cargas de trabajo de la nube aplicar una política de seguridad uniforme y estandarizada en entornos de nube híbrida, pública y privada, y generar los informes correspondientes?	
		¿Cómo realiza análisis habituales de vulnerabilidades sin afectar la disponibilidad ni el rendimiento?	

TABLA 2: Lista de verificación de evaluación de protección de cargas de trabajo de la nube.

VMware, Inc. 3401 Hillview Avenue, Palo Alto, CA 94304, USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com/latam