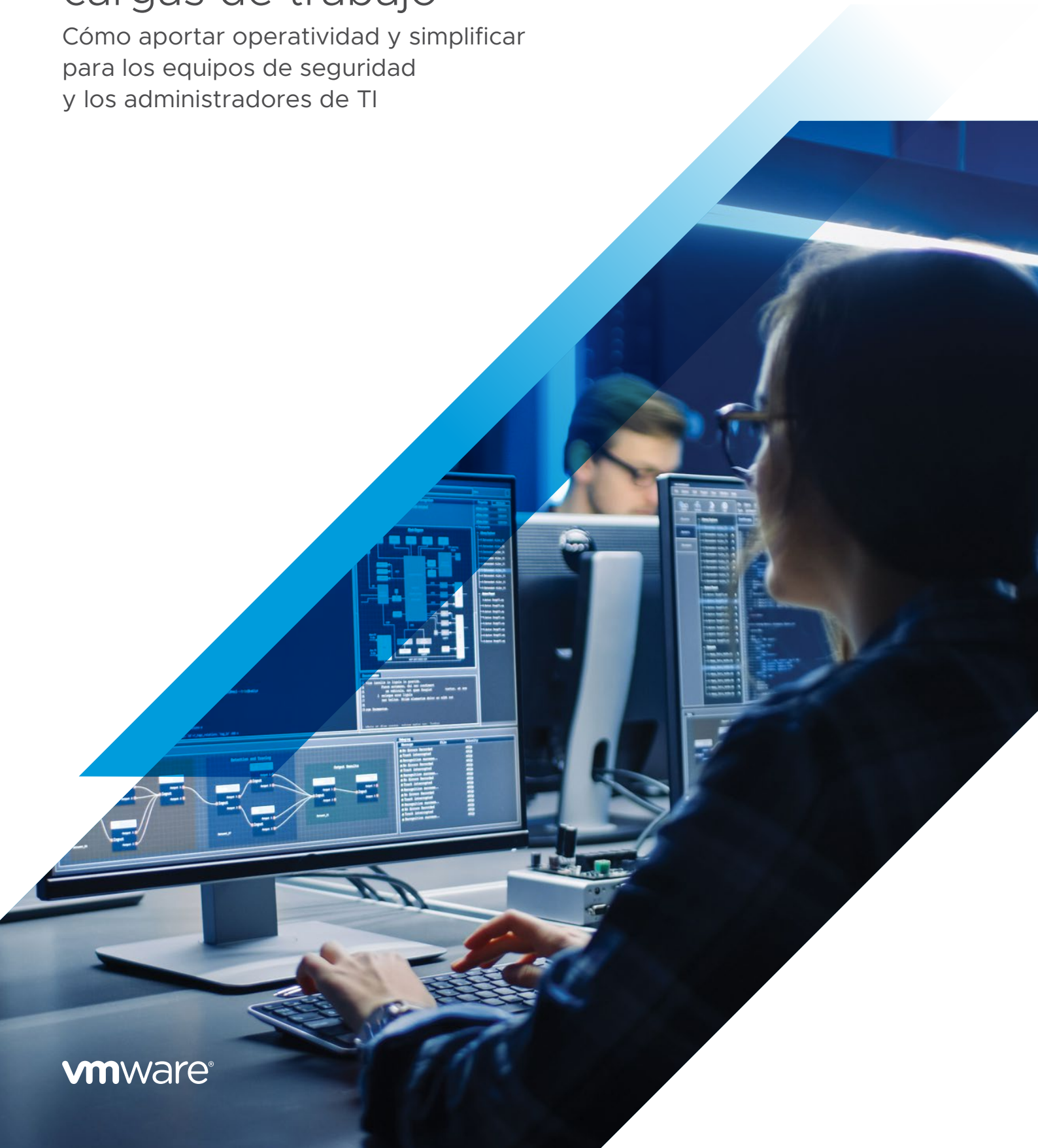
Compartir la carga de proteger las cargas de trabajo

Cómo aportar operatividad y simplificar para los equipos de seguridad y los administradores de TI



vmware®

Índice

Introducción

Los equipos de seguridad necesitan la ayuda de los equipos de operaciones de TI para proteger las cargas de trabajo

Tanto los administradores de TI como los equipos de seguridad contribuyen a mantener los sistemas a salvo, no obstante, de forma relativamente aislada. Sin embargo, la transición a los entornos de nube para las aplicaciones y las cargas de trabajo está forzando un cambio en la manera en la que se ejecutan estas funciones.

Los equipos de seguridad de una organización suelen estar compuestos por grupos de políticas y auditoría, así como por equipos dedicados a perseguir amenazas y dar respuesta a incidentes. La carga diaria de la seguridad y conformidad recae en el personal de operaciones de TI y en recursos que no están necesariamente orientados a la seguridad. De hecho, según un informe de Forrester Consulting Spotlight, solo el 33 % de las organizaciones tienen hoy en día un equipo unificado de TI y seguridad, pero el 47 % cree que la unificación será lo normal dentro de tres a cinco años.[1] Es el mejor momento para implementar un nuevo enfoque que facilite la cohesión entre estos equipos.

Este documento técnico abarca los elementos clave que permiten a los equipos de seguridad y de TI reducir proactivamente la superficie de ataque y reforzar los activos. Adoptar estas estrategias reducirá la brecha entre estos equipos, simplificará las operaciones y repartirá la carga de proteger las cargas de trabajo.

ESTRATEGIA CLAVE	DESCRIPCIÓN
Minimizar la sobrecarga de agentes	Eliminar la necesidad de instalar agentes en las cargas de trabajo reduce la proliferación de agentes de seguridad, minimiza las instalaciones y los reinicios, y reduce los costes generales operativos. Esto simplifica al departamento de TI la distribución de la seguridad como servicio.
Compartir la visibilidad de las vulnerabilidades	Una visión unificada de los datos de seguridad garantiza la comunicación clara y la comprensión de las vulnerabilidades detectadas.
Automatizar la priorización de riesgos	Para minimizar la fatiga por alertas y el exceso de trabajo de los recursos, ambos equipos necesitan saber en qué tienen que centrarse para lograr la mayor repercusión en las defensas. Es fundamental disponer de un sistema centrado en el contexto que pueda priorizar las vulnerabilidades automáticamente y sin prejuicios.
Optimizar los procesos de las cargas de trabajo	Gracias a la visibilidad compartida y la priorización de riesgos, los equipos de seguridad y de TI disfrutan de una experiencia fluida al automatizar y poner en marcha una seguridad coherente como parte de la ciberintegridad.

TABLA 1: Cuatro estrategias clave para reducir la superficie de ataque y reforzar los activos.

1. Forrester Consulting, por encargo de VMware. «Security As A Team Sport: A Spotlight On The Growing Role Of IT In Security Tasks». Mayo de 2020.

El desafío

Las cargas de trabajo se han convertido en una vulnerabilidad que fomenta la búsqueda de culpables

Las cargas de trabajo se distribuyen cada vez más a medida que nuestros entornos adquieren tamaño y complejidad. Muchas aplicaciones basadas en la nube son esenciales, pero son vulnerables a los riesgos si cualquier parte de la carga de trabajo (aplicación, datos o sistema operativo) funciona mal. Naturalmente, apagar un servidor corporativo cuando se produce un incidente no es la solución. La seguridad y las operaciones de TI son secundarias a la productividad del negocio. Esto significa que proteger y supervisar cada parte de la carga de trabajo es ahora una parte adicional, y fundamental, de la seguridad de su empresa.

¿Quién es responsable de proteger las cargas de trabajo?
Cuando las cargas de trabajo residían en servidores de rack estáticos en centros de datos locales, era fácil asignar la responsabilidad de mantenerlas seguras. Actualmente, las cargas de trabajo pueden residir en servidores físicos, servidores virtuales, en la nube pública o incluso en entornos sin servidores. Además, las cargas de trabajo se pueden mover por todos estos entornos, lo que dificulta su seguimiento y gestión. Tanto equipos de seguridad, administradores de TI, administradores de nube, administradores de VMware vCenter®, ingenieros de fiabilidad de sitios (SRE), equipos de DevOps y desarrolladores pueden participar en el ciclo de vida de las cargas de trabajo. En algunos casos pueden influir en las cargas de trabajo y alcanzar objetivos comunes, pero en otros sus objetivos pueden ser incluso contrarios.

Los administradores de TI pueden proteger eficientemente las cargas de trabajo. Sin embargo, no disponen de visibilidad de la mayoría de las vulnerabilidades de las cargas de trabajo y, desde luego, no tienen la información contextual para priorizar el impacto de las vulnerabilidades. Teniendo en cuenta que los administradores de TI no suelen tener control del entorno de nube, las funciones y responsabilidades se vuelven imprecisas. Los equipos de seguridad pueden tener parte de la información necesaria para identificar las vulnerabilidades, pero es posible que no cuenten con una priorización de riesgos clara o con la información contextual que necesitarían para gestionar la corrección con eficacia.

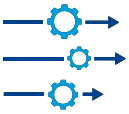
En otras palabras, es probable que nadie esté gestionando suficientemente la protección de las cargas de trabajo.

¿Es posible compartir la responsabilidad?
La conclusión es que tanto los equipos de seguridad como los administradores de TI deben participar en la protección de las cargas de trabajo. Pero para evitar perder el tiempo buscando culpables, estos equipos deben unificarse con los procesos, la información y las herramientas específicas de las cargas de trabajo.

Si disponen de una comprensión y una metodología compartida para automatizar la detección y priorización de las correcciones de vulnerabilidades, a los administradores de TI les resultará mucho más fácil compartir la responsabilidad de reforzar y reducir las superficies de ataque. De hecho, es posible aportar operatividad a la protección de las cargas de trabajo para eliminar la tensión y la búsqueda de culpables entre estos dos equipos fundamentales. Para hacerlo realidad, solo se necesitan cuatro pasos clave.

DATOS CLAVE PARA COMPARTIR ENTRE LOS EQUIPOS DE SEGURIDAD Y LOS ADMINISTRADORES DE TI

- Indicadores de riesgo (IOC)
- Tácticas, técnicas y procedimientos (TTP)
- Visibilidad de los ataques bloqueados y detectados
- Eventos comunes que se producen en el sistema
- Evaluación de más de 2000 estados de configuración de cargas de trabajo
- Inventario de cargas de trabajo y su estado de protección
- Información contextual sobre las vulnerabilidad sin necesidad de análisis, con puntuaciones de riesgo y enlaces a la base de datos federal de vulnerabilidades de EE. UU.
- Seguimiento y tendencias de la ciberintegridad a lo largo del tiempo



Cuatro pasos para simplificar y aportar operatividad a la protección de las cargas de trabajo

Paso 1: Minimizar la sobrecarga de agentes

La proliferación de agentes de seguridad añadidos causa muchos problemas, tanto a los administradores de TI como a los equipos de seguridad. Los desafíos más comunes son:

- Fuentes dispares de información de seguridad que desembocan en mala comunicación
- Aumento de la carga de mantenimiento y mayor probabilidad de errores
- Costes añadidos de almacenamiento de los datos recopilados

Para eliminar estos problemas, consolide las pilas de TI y de seguridad sustituyendo las múltiples soluciones puntuales por un enfoque de seguridad global, capaz de recopilar datos en los entornos locales y de nube.

Elija un único agente integrado

La solución óptima es utilizar un único agente en la capa de virtualización que esté integrado en su infraestructura actual. Esto permitirá registrar los eventos necesarios para disponer de una visibilidad plena en todos los entornos. Contar con un único agente hace que la supervisión de la seguridad prácticamente no necesite implementar software adicional.

Grandes ventajas de un solo agente

La consolidación de las soluciones de seguridad en un solo agente, es decir, una única y completa fuente de datos, ofrece grandes ventajas para mejorar la protección de las cargas de trabajo:

- Facilita al departamento de TI aportar operatividad a la gestión de agentes.
- Permite integrar el flujo de trabajo e intercambiar datos entre equipos.
- Proporciona información centrada en el contexto, de forma que los resultados sean más procesables.
- Elimina los análisis puntuales para detectar vulnerabilidades, lo que mejora el rendimiento y acorta el tiempo de respuesta a los ataques.
- Reduce los costes de almacenamiento y las tareas de mantenimiento.

Paso 2: Compartir la visibilidad de las vulnerabilidades

El grupo responsable de aplicar parches rara vez es el mismo que analiza el efecto de las vulnerabilidades en la seguridad. Los datos de los análisis clásicos se desincronizan rápidamente y los sistemas de tiques son lentos, algo que da lugar a diversas interpretaciones de las correcciones necesarias.

Los administradores de TI consumen fuentes de datos distintas a las que consume el equipo de seguridad, pero se espera que contribuyan a procesos de seguridad más amplios. Esto lleva a la existencia de distintas expectativas y a que la integridad sea deficiente.

Una visión unificada de los datos de seguridad garantiza la claridad en la comunicación y la comprensión de las vulnerabilidades detectadas y de su nivel de riesgo asociado.

Una visión unificada reduce los riesgos de forma eficaz

La consolidación en un solo agente (paso 1) produce datos de seguridad que los administradores de TI y los equipos de seguridad pueden compartir fácilmente. Lo ideal sería que esta información se presentase dentro de las herramientas que estos equipos utilizan a diario, como las herramientas de virtualización (por ejemplo, VMware vSphere® y vCenter).

Disponer de los mismos datos y resultados de evaluación en todos los equipos mejora la comunicación y la colaboración. Lo más importante es tener siempre a mano los datos de vulnerabilidad actualizados, en lugar de efectuar análisis puntuales. Esto garantiza que los equipos siempre estén coordinados. Un inventario compartido de las vulnerabilidades de las cargas de trabajo, priorizadas por riesgo, garantizará que los recursos se dediquen a resolver los problemas más críticos.

Paso 3: Automatizar la priorización de riesgos

Utilizar un único agente y tener una visibilidad compartida de los datos de seguridad son grandes pasos para avanzar en la gestión de la protección de las cargas de trabajo. Sin embargo, el acceso a las vulnerabilidades conocidas por sí solo no significa que haya una visión compartida sobre dónde concentrar los recursos.

El siguiente paso lógico es establecer una manera estandarizada de evaluar los riesgos. Piense, por ejemplo, en una solución de seguridad que gestione automáticamente la evaluación y priorización de riesgos.

Datos priorizados por riesgo en las herramientas actuales para obtener resultados procesables

Una evaluación de riesgos basada únicamente en la normativa Common Vulnerability Scoring System no es suficiente. La información contextual extraída a partir de conjuntos de datos personalizados sobre amenazas (incluyendo listas publicadas de vulnerabilidades e inteligencia para la detección de amenazas, así como más de 7000 millones de vulnerabilidades gestionadas) brindan a las organizaciones la capacidad de aplicar modelos predictivos para pronosticar nuevas vulnerabilidades y priorizar las actividades de corrección en función del nivel de gravedad.

Lo ideal sería que los administradores de TI tuvieran una visión de las vulnerabilidades más comunes y de las de alto riesgo en su consola de vCenter. De este modo, se incorpora fácilmente el refuerzo de las cargas de trabajo a las actividades de integridad diarias.

Además, los administradores de TI necesitan información de auditoría del estado actual del sistema para poder colaborar con los equipos de seguridad en la corrección de las amenazas. Naturalmente, disponer de una visión compartida de esta información permitirá a estos equipos colaborar para aplicar parches conforme a la prioridad o tomar medidas alternativas, como apagar los sistemas vulnerables.

Una visión compartida de las amenazas y vulnerabilidades actuales, con los riesgos asociados, permite establecer prioridades claras y centrar los esfuerzos. Lo que se traduce en una solución más rápida de las amenazas existentes y una mejor protección contra futuros ataques.

Paso 4: Optimizar los procesos de las cargas de trabajo

Históricamente, los análisis para detectar vulnerabilidades han sido una actividad mensual o trimestral. Pero estos ejercicios puntuales no son suficientes. Debido a la continua expansión de las cargas de trabajo en entornos multinube, estos análisis no proporcionan una información tan amplia u oportuna como se necesita para mitigar los riesgos de seguridad críticos.

Una vez establecidas la visibilidad compartida y la priorización de riesgos, el siguiente paso para los equipos de seguridad y de TI es lograr que la protección de las cargas de trabajo sea una parte habitual de la ciberintegridad.

Aportar operatividad a la protección de las cargas de trabajo

Aportar operatividad a la protección de las cargas de trabajo requiere que los administradores de TI reduzcan continuamente las superficies de ataque como parte de las prácticas estándar de ciberintegridad. Los administradores de TI necesitan acceder a evaluaciones de miles de estados de configuración en sus cargas de trabajo, así como a la información y orientación para corregir las vulnerabilidades identificadas.

Los equipos de gestión de TI deben tener acceso a una visión compartida de las tendencias de ciberintegridad a lo largo del tiempo. Esto fomentará las discusiones de equipo en torno a la gestión de las vulnerabilidades, y permitirá medir el rendimiento. Los responsables de TI deben utilizar esta información para asegurarse de que se siguen las prioridades, así como de que los recursos se asignan adecuadamente para reforzar continuamente las cargas de trabajo.

¿Qué está por venir?

Coordinar los equipos de TI para proteger las cargas de trabajo reduce los ataques

Los equipos de seguridad y los administradores de TI pueden colaborar para mejorar la protección de las cargas de trabajo. Además, con las funciones de seguridad adecuadas, esta colaboración puede ser sencilla y fácil de incorporar en las operaciones diarias. Para aprovechar esta oportunidad, asegúrese de que estos equipos:

- Utilizan una solución integrada con un único agente.
- Tienen una visión unificada de los datos de seguridad integrada en sus herramientas de trabajo actuales.
- Tienen el contexto necesario y supervisan continuamente las vulnerabilidades con priorización de riesgos automatizada.
- Cuentan con el apoyo de sus superiores para garantizar que el refuerzo de las cargas de trabajo forma parte de las operaciones.

Tres claves para mejorar la protección de las cargas de trabajo

1. Reunir a los administradores de TI y a los responsables de seguridad para hablar sobre la oportunidad de colaborar a fin de reducir los ataques.
2. Identificar las deficiencias actuales en la recopilación de datos y la visibilidad, a fin de priorizar mejor las vulnerabilidades y reforzar las cargas de trabajo.
3. Estudiar soluciones que permitan a los administradores de TI y a los equipos de seguridad compartir la visibilidad y el contexto necesarios para tener éxito.

Abordar la protección de las cargas de trabajo resulta muy rentable

- Cobertura y visibilidad en todas las cargas de trabajo
- Simplificación de la pila de seguridad de TI
- Capacidad para responder más rápido a los problemas gracias a la detección temprana
- Activos mejor reforzados
- Mejor prevención contra software y procesos indeseados, y programas maliciosos
- Eliminación completa de programas no maliciosos
- Implementación de una seguridad preparada para el futuro (entornos y cargas de trabajo modernos)

Más información

Consulte esta ficha para descubrir cómo VMware Carbon Black Cloud™ capacita a los equipos de TI y de seguridad para que mejoren juntos la protección de las cargas de trabajo.

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