Responsabilidad compartida de la seguridad de las cargas de trabajo

Cómo pueden poner en práctica y simplificar esto los equipos de seguridad y los administradores de TI

vmware®

Índice

Introducción

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

Tanto los administradores de TI como los equipos de seguridad cumplen sus funciones para proteger los sistemas, pero relativamente aislados unos de otros. Sin embargo, la transición a los entornos de nube para aplicaciones y cargas de trabajo impone un cambio en la manera en la que se desempeñan estos roles.

Los equipos de seguridad de una organización suelen estar compuestos por grupos de auditoría y políticas, así como por equipos de persecución de amenazas y respuesta a incidentes. La responsabilidad diaria de la seguridad y el cumplimiento recae en el personal y los recursos de las operaciones de TI, que no están necesariamente orientados a la seguridad. De hecho, de acuerdo con un informe destacado de Forrester Consulting, solo el 33 por ciento de las organizaciones cuentan actualmente con TI y seguridad en un mismo equipo unificado, pero el 47 por ciento cree que la unificación será la norma en tres a cinco años.[1] Este es el momento perfecto para un nuevo enfoque que facilite la cohesión entre estos equipos.

En este caso de uso del producto, se describen los principios clave para permitir que tanto los equipos de seguridad como los de TI reduzcan la superficie de ataque y fortalezcan los recursos de manera proactiva. La adopción de estos principios tenderá un puente entre los equipos, simplificará las operaciones y permitirá compartir la responsabilidad de las cargas de trabajo.

PRINCIPIO CLAVE	DESCRIPCIÓN
Minimizar los costos generales de los agentes	La eliminación de la necesidad de instalar agentes en las cargas de trabajo reduce la proliferación de agentes de seguridad, minimiza la instalación y los reinicios, y reduce los costos operacionales generales. Esto simplifica el suministro de seguridad como servicio para TI.
Compartir la visibilidad de las vulnerabilidades	Una visión unificada de los datos de seguridad garantiza una comunicación y un entendimiento claros en relación con las vulnerabilidades detectadas.
Automatizar la priorización de los riesgos	Para minimizar la fatiga por alertas y la sobrecarga de los recursos, ambos equipos necesitan saber en qué enfocarse a fin de lograr el mayor impacto en las defensas. Es fundamental contar con un sistema centrado en el contexto que pueda priorizar automáticamente las vulnerabilidades de manera imparcial.
Optimizar los procesos de las cargas de trabajo	Gracias a la visibilidad compartida y la priorización de los riesgos, los equipos de seguridad y de TI disfrutan de una experiencia sin inconvenientes mediante la automatización y la puesta en práctica de una seguridad coherente como parte de la higiene de TI.

TABLA 1: Cuatro principios clave para reducir la superficie de ataque y fortalecer los recursos.

1. Forrester Consulting, encargado por 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 convirtieron en una vulnerabilidad para la que se buscan responsables

La ampliación continua y el aumento de la complejidad de nuestros entornos hacen que las cargas de trabajo se distribuyan cada vez más. Muchas aplicaciones basadas en la nube son fundamentales para el negocio, pero quedan vulnerables si alguna parte de la carga de trabajo (aplicación, datos o sistema operativo) presenta fallas. Ciertamente, la solución no es apagar un servidor corporativo cuando ocurre un incidente. Las operaciones de TI y seguridad son secundarias para la productividad del negocio. Esto significa que la protección y el monitoreo de cada parte de la carga de trabajo ahora es un elemento adicional, y fundamental, de la protección de su negocio.

¿Quién es el responsable de proteger las cargas de trabajo?
Cuando las cargas de trabajo residían en los servidores de racks estáticos de los centros de datos en las instalaciones, era fácil asignar la responsabilidad de protegerlas. Hoy en día, las cargas de trabajo pueden existir en servidores físicos, en servidores virtuales, en la nube pública o, incluso, sin servidores. Además, las cargas de trabajo se pueden mover a través de todos estos entornos, lo que dificulta el seguimiento y la administración. Los equipos de seguridad, los administradores de TI, los administradores de nube, los administradores de VMware vCenter®, los ingenieros de confiabilidad del sitio (site reliability engineer, SRE), los equipos de DevOps y los desarrolladores, todos pueden formar parte del ciclo de vida de la carga de trabajo. Algunas veces, pueden tener un impacto en las cargas de trabajo de formas que alcanzan objetivos comunes, pero otras, sus objetivos pueden contrarrestarse.

Los administradores de TI son capaces de proteger de forma eficiente las cargas de trabajo. Sin embargo, desconocen la mayoría de las vulnerabilidades de las cargas de trabajo y, definitivamente, no tienen el contexto para priorizar el impacto. Además, debido a que los administradores de TI, por lo general, no tienen el control del entorno de nube, los roles y las responsabilidades se desdibujan por completo. Los equipos de seguridad pueden contar con una parte de la información necesaria para identificar las vulnerabilidades, pero quizá no dispongan de una priorización clara del riesgo o el contexto para administrar su neutralización de manera eficaz.

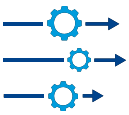
En otras palabras, parece que nadie administra la seguridad de las cargas de trabajo en su totalidad.

¿La responsabilidad puede compartirse?
Lo más importante es que tanto los equipos de seguridad como los administradores de TI deben desempeñar un rol en la seguridad de las cargas de trabajo. Sin embargo, para evitar la búsqueda de responsables, estos equipos deben unificar los procesos, la información y las herramientas específicos de las cargas de trabajo.

Con una metodología y un entendimiento compartidos para automatizar el descubrimiento y la priorización de las correcciones de vulnerabilidades, es mucho más fácil para los administradores de TI compartir la responsabilidad de fortalecer y reducir las superficies de ataque. De hecho, la seguridad de las cargas de trabajo puede ponerse en práctica para eliminar la tensión y la búsqueda de responsables entre estos dos equipos fundamentales. Para hacerlo realidad, solo se necesitan implementar cuatro pasos clave.

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

- Indicadores de compromiso (indicator of compromise, IOC)
- Tácticas, técnicas y procedimientos (TTP)
- Visibilidad de ataques bloqueados y detectados
- Eventos normales que ocurren en el sistema
- Evaluación de más de 2.000 estados de configuración de cargas de trabajo
- Inventario de las cargas de trabajo y sus estados de protección
- Contexto de vulnerabilidades sin escaneo con puntuaciones de riesgo y enlaces a la base de datos nacional de vulnerabilidades
- Seguimiento y tendencias de la higiene de TI a lo largo del tiempo



Cuatro pasos para poner en práctica y simplificar la seguridad de las cargas de trabajo

Paso 1: Minimizar los costos generales de los agentes

La proliferación de agentes de seguridad acoplados causa muchos problemas tanto para los administradores de TI como para los equipos de seguridad. Los desafíos más comunes son los siguientes:

- Fuentes de información de seguridad dispares que generan problemas de comunicación
- Aumento de la carga de mantenimiento y mayor probabilidad de errores
- Mayores costos de almacenamiento para los datos recopilados

Para eliminar estos problemas, consolide las pilas de TI y seguridad mediante el reemplazo de múltiples soluciones puntuales con un enfoque integral de la seguridad, uno que pueda recopilar datos en las instalaciones y en los entornos de nube.

Elija un único agente incorporado

La solución óptima es que utilice un único agente en la capa de virtualización integrada en la infraestructura existente. Esto permitirá el registro de los eventos necesarios para la visibilidad completa en todos los entornos. El uso de un único agente brinda un monitoreo de la seguridad tan cercano a una superficie cero como es posible.

Las grandes ventajas de utilizar un agente

La consolidación de las soluciones de seguridad en un agente, una fuente de datos única e integral, ofrece grandes ventajas para mejorar la seguridad de las cargas de trabajo:

- Simplifica la puesta en práctica de la administración del agente para TI
- Permite la integración del flujo de trabajo y el intercambio de datos entre los equipos
- Brinda información centrada en el contexto que facilita el procesamiento de los resultados
- Elimina los escaneos de vulnerabilidades en un momento determinado, lo que mejora el rendimiento y acelera el tiempo de respuesta a los ataques
- Reduce los costos de almacenamiento y los esfuerzos de mantenimiento

Paso 2: Compartir la visibilidad de las vulnerabilidades

El grupo responsable de la aplicación de parches raramente es el mismo que analiza el impacto de seguridad de las vulnerabilidades. Los datos de escaneo clásicos pierden rápidamente sincronismo y los sistemas de vales son lentos, lo que da lugar a distintas interpretaciones de las correcciones necesarias.

Los administradores de TI consumen fuentes de datos distintas de las que utilizan los equipos de seguridad, pero se espera que contribuyan a procesos de seguridad más grandes. Esto genera expectativas incompatibles y resultados de higiene deficientes.

Una visión unificada de los datos de seguridad garantiza una comunicación clara y un entendimiento de las vulnerabilidades detectadas y su nivel de riesgo asociado.

Una visión unificada reduce los riesgos de manera eficaz

La consolidación en un solo agente del Paso 1 produce datos de seguridad que pueden intercambiarse fácilmente entre los administradores de TI y los equipos de seguridad. Lo ideal sería que esta información se presentara en las herramientas que esos equipos usan diariamente, como las herramientas de virtualización (por ejemplo, VMware vSphere® y vCenter).

El uso de los mismos datos y resultados de evaluación entre los equipos mejora la comunicación y la colaboración. La clave más importante es tener siempre a mano los datos sobre la vulnerabilidad actual, más que un escaneo de un momento determinado. Esto garantizará que los equipos estén siempre de acuerdo. Un inventario compartido de las vulnerabilidades de las cargas de trabajo priorizadas por riesgo garantizará que los recursos sean dirigidos a resolver los problemas más importantes.

Paso 3: Automatizar la priorización de los riesgos

El uso de un único agente y la visibilidad compartida de los datos de seguridad son pasos importantes para administrar la seguridad de las cargas de trabajo. Sin embargo, el mero acceso a las vulnerabilidades conocidas no significa que haya un entendimiento compartido sobre dónde enfocar los recursos.

El siguiente paso lógico es tener una forma estandarizada de acceder al riesgo. Considere una solución de seguridad que gestiona automáticamente la evaluación y priorización de los riesgos.

Datos que priorizan los riesgos en las herramientas actuales para obtener resultados viables

Una evaluación de riesgos basada únicamente en el sistema de puntuación de vulnerabilidad común no es suficiente. Los datos contextuales seleccionados de conjuntos de datos de amenazas personalizados, incluidas las fuentes de inteligencia de detección de amenazas y ataques y más de 7.000 millones de vulnerabilidades administradas, les brindarán a las organizaciones la capacidad de aplicar un modelado predictivo para prever nuevas vulnerabilidades y priorizar las actividades de neutralización basadas en el nivel de importancia.

Lo ideal sería que los administradores de TI pudieran ver las vulnerabilidades de mayor riesgo y los ataques más comunes en la consola de vCenter. Esto incorporará fácilmente el fortalecimiento de las cargas de trabajo en las actividades diarias de higiene.

Además, los administradores de TI necesitan información de auditoría del estado actual del sistema para poder colaborar con los equipos de seguridad en la neutralización de amenazas. Una visión compartida de esta información habilitará de forma natural a estos equipos para trabajar juntos en la aplicación de parches según la prioridad, o en la adopción de medidas alternativas, como el apagado de los sistemas vulnerables.

Una visión compartida de las amenazas y vulnerabilidades actuales con los riesgos asociados permite priorizar y enfocar claramente las iniciativas, lo que lleva a una resolución más rápida de las amenazas existentes y una mejor protección de los ataques futuros.

Paso 4: Optimizar los procesos de las cargas de trabajo

Históricamente, los análisis de vulnerabilidades se consideran una actividad mensual o trimestral. Pero estos ejercicios realizados en un momento determinado no son suficientes. Con la continua expansión de las cargas de trabajo en los entornos de nubes múltiples, estos escaneos no proporcionan una información tan amplia ni tan oportuna como se necesita para mitigar los riesgos de seguridad importantes.

Con la visibilidad compartida y la priorización de los riesgos, el paso siguiente, tanto para los equipos de seguridad como de TI, es lograr que la seguridad de las cargas de trabajo sea una parte regular de la higiene de TI.

Puesta en práctica de la seguridad de las cargas de trabajo

La puesta en práctica de la seguridad de las cargas de trabajo requiere que los administradores de TI reduzcan continuamente las superficies de ataque como parte de las prácticas estándar de higiene de TI. Los administradores de TI necesitan acceder a las evaluaciones de miles de estados de configuración en sus cargas de trabajo, así como a la información y dirección para neutralizar las vulnerabilidades descubiertas.

La administración de TI debe tener acceso a una vista compartida de las tendencias de higiene de TI a lo largo del tiempo. Esto fomentará las conversaciones del equipo relacionadas con la administración de las vulnerabilidades y la medición del desempeño. Los administradores de TI deben utilizar esta información a fin de garantizar el seguimiento de las prioridades y la asignación adecuada de los recursos para un fortalecimiento continuo de las cargas de trabajo.

¿Cuál es el siguiente paso?

La alineación de TI con la seguridad de las cargas de trabajo disminuye los ataques

Los equipos de seguridad y los administradores de TI pueden trabajar juntos para mejorar la seguridad de las cargas de trabajo. Además, con las capacidades de seguridad correctas, esta colaboración puede lograrse sin inconvenientes e implementarse fácilmente en la práctica diaria. Para capitalizar esta oportunidad, asegúrese de que estos equipos compartan las siguientes características:

- Utilicen una solución incorporada con un único agente
- Tengan una visión unificada de los datos de seguridad integrados en las herramientas de trabajo actuales
- Dispongan del contexto necesario y el monitoreo continuo de las vulnerabilidades con una priorización automática de los riesgos
- Cuenten con el soporte de liderazgo para garantizar la puesta en práctica del fortalecimiento de la carga de trabajo

Tres claves para mejorar la seguridad de las cargas de trabajo

1. Reúna a los administradores de TI y los líderes de seguridad para evaluar la posibilidad de que trabajen juntos en la reducción de ataques.
2. Identifique las deficiencias actuales en la recopilación y visibilidad de los datos para mejorar la priorización de las vulnerabilidades y fortalecer las cargas de trabajo.
3. Busque soluciones que les brinden a los administradores de TI y los equipos de seguridad la visibilidad y el contexto compartidos necesarios para lograr el éxito.

El abordaje de la seguridad de las cargas de trabajo genera mayores dividendos

- Cobertura y visibilidad en todas las cargas de trabajo
- Simplificación de la pila de seguridad de TI
- La capacidad de responder más rápido a los problemas con la detección temprana
- Recursos más fortalecidos
- Mejor prevención de malware, y de software y procesos no deseados
- Eliminación completa de ataques sin software malicioso
- Activación de la seguridad para el futuro: cargas de trabajo y entornos modernos

Más información

Lea esta hoja de datos para descubrir cómo VMware Carbon Black Cloud™ impulsa a TI y la seguridad a mejorar juntas 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/latam