Introducción a la seguridad de los contenedores

COMPRENSIÓN DE LOS CONCEPTOS BÁSICOS DE LA PROTECCIÓN DE CONTENEDORES

PRISMA
BY PALO ALTO NETWORKS

MediaOps

A estas alturas, resulta evidente para los equipos de ciberseguridad de todo el mundo que el legendario genio de los contenedores ha salido de la lámpara. Los desarrolladores han adoptado con entusiasmo el uso de contenedores porque consiguen que la creación e implementación de las denominadas «aplicaciones nativas en la nube» sea más fácil que nunca. Los contenedores no solo eliminan gran parte de la fricción asociada generalmente a la migración del código de la aplicación desde la fase de prueba a la fase de producción, sino que el código de la aplicación empaquetado en contenedores se puede ejecutar además en cualquier parte. Todas las dependencias asociadas a cualquier aplicación se incluyen en la aplicación distribuida en contenedores. Esta distribución se traduce en una gran portabilidad en máquinas virtuales o servidores dedicados que se ejecutan en un centro de datos local o en una nube pública.

Gracias a ese nivel de flexibilidad, los desarrolladores consiguen una mejora de la productividad demasiado importante como para ignorarla. No obstante, como ocurre con la aparición de cualquier arquitectura de TI nueva, sigue siendo necesario proteger las aplicaciones nativas en la nube. Los entornos basados en contenedores traen consigo una serie de problemas que afectan a imágenes, contenedores, hosts, tiempos de ejecución, registros y plataformas de organización que hay que proteger.

.

El reto al que se enfrentan las organizaciones es, en primer lugar, comprender el modo en que las distintas capas de un entorno informático nativo en la nube interactúan entre sí y, después, encontrar las herramientas adecuadas para crear un conjunto reiterativo de procesos para proteger cada capa. Entre los problemas en materia de ciberseguridad específicos de los contenedores se incluyen los siguientes:

IMÁGENES: las vulnerabilidades pueden afectar a las imágenes de los contenedores del mismo modo que a cualquier otro fragmento de código. La creación de una lista de materiales, la identificación de cualquier elemento secreto incrustado y la clasificación de todas las capas de una imagen siguen siendo tareas fundamentales en materia de ciberseguridad que hay que abordar. Las cosas se complican debido a la gran cantidad de contenedores que se ejecutan en un entorno de aplicaciones y la frecuencia con la que estos se actualizan. Gracias a la mayor adopción de las prácticas de DevOps, ahora es habitual que las organizaciones actualicen una aplicación basada en contenedores varias veces a la semana. Cada actualización de lo que puede convertirse rápidamente en miles de contenedores que se ejecutan en un entorno de TI constituye una oportunidad para que las vulnerabilidades penetren en ese entorno.

REGISTROS DE CONTENEDORES: el registro de un contenedor supone un medio cómodo y centralizado de almacenar y distribuir imágenes de aplicaciones. En la actualidad, las organizaciones pueden tener fácilmente decenas de miles de imágenes almacenadas en sus registros. Puesto que el registro es fundamental para el funcionamiento de su entorno basado en contenedores, su protección resulta vital. Un registro es imprescindible para ordenar el posible caos de un contenedor, pero también puede proporcionar a los ciberdelincuentes una vía que puede poner en riesgo la seguridad de todo el entorno. La supervisión constante de los registros para detectar cualquier cambio en el estado de vulnerabilidad es un requisito de seguridad fundamental que debe incluir el bloqueo del servidor que aloja el registro.

TIEMPOS DE EJECUCIÓN DEL CONTENEDOR: el tiempo de ejecución del contenedor es una de las partes más difíciles de proteger de una pila de contenedores. Esto se debe a que las herramientas de seguridad tradicionales no estaban diseñadas para supervisar contenedores en ejecución. Generalmente, las herramientas heredadas no pueden ver dentro de los contenedores, y mucho menos establecer una referencia sobre el aspecto que debe tener un entorno basado en contenedores. Los problemas relacionados con la seguridad del tiempo de ejecución de los contenedores obligan a los equipos de ciberseguridad a centrarse en las cuestiones de seguridad de las aplicaciones a las que los cortafuegos heredados no hacen frente

ORGANIZACIÓN DE CONTENEDORES: el control de acceso a las plataformas de organización de contenedores, como Kubernetes, para evitar riesgos procedentes de cuentas con demasiados privilegios, ataques a través de la red y movimiento lateral no deseado, se debe llevar a cabo mediante técnicas de listas blancas de un modo muy parecido a la gestión del acceso a entornos de TI heredados. La diferencia en una plataforma de organización de contenedores radica en la necesidad de proteger también las comunicaciones entre «pods» en un clúster de Kubernetes compartido por varias aplicaciones.

SISTEMAS OPERATIVOS HOST: el sistema operativo donde se aloja su entorno de contenedores es quizá el aspecto más importante, y con frecuencia más olvidado, de la protección de un entorno de contenedores. Cualquier riesgo que corra el entorno del host proporciona a los ciberdelincuentes acceso a todo el entorno de las aplicaciones. Cada host debe aplicar su propio conjunto de controles de acceso de seguridad; además, se debe supervisar constantemente para detectar nuevas vulnerabilidades que puedan haberse descubierto desde que se implementó el host por primera vez.

VENTAJAS DE LOS CONTENEDORES EN MATERIA DE CIBERSEGURIDAD

Debido a los retos que conlleva la protección de aplicaciones distribuidas en contenedores, resulta comprensible que muchos profesionales de la ciberseguridad sean un poco reacios a la implantación de contenedores en un entorno de producción. Si bien existen algunas ventajas claras en cuanto a la productividad de los desarrolladores, ahora es cuando la mayoría de las organizaciones están empezando a comprender las herramientas y procesos que tendrán que adoptarse para proteger las aplicaciones en contenedores. No obstante, aunque pueda parecer un reto de enormes proporciones, los contenedores ofrecen una ventaja inestimable para la ciberseguridad que los equipos de ciberseguridad no valoran inicialmente tanto como deberían. Como los contenedores terminan siendo extraídos y sustituidos con mucha frecuencia, los procesos asociados a la solución de vulnerabilidades se simplifican enormemente. En lugar de tener que esperar meses, en ocasiones, para la aplicación de un parche en una aplicación monolítica, la nueva funcionalidad se integra en un entorno de aplicaciones mediante la extracción y sustitución de contenedores. Ese proceso está limitado a un subconjunto de la aplicación, conocido como microservicio, y generalmente puede llevarse a cabo en unos minutos como parte del proceso de gestión de ciclo de vida de la aplicación habilitado por una plataforma de integración/implementación continua (CI/CD, por sus siglas en inglés) como Jenkins. Dicha capacidad se traduce en una reducción drástica del tiempo en que una aplicación se ejecutará con vulnerabilidades conocidas en un entorno de producción.

Podría decirse que esa capacidad es la que ha dado lugar a la aparición de los mejores procesos de DevSecOps, a través de los cuales los desarrolladores están asumiendo ahora una mayor responsabilidad en la aplicación de controles de ciberseguridad. Esos controles todavía debe definirlos el equipo de ciberseguridad y después validar su aplicación. No obstante, puesto que los desarrolladores ahora son los responsables de aplicar esos controles, el número de aplicaciones que pueden superar una auditoría de ciberseguridad aumenta paulatinamente a medida que los procesos de DevSecOps adoptados ganan en madurez.

PRISMA BY PALO ALTO NETWORKS | MediaOps

HERRAMIENTAS PARA LA SEGURIDAD DE LOS CONTENEDORES

ISolo en el último año, las herramientas en las que pueden confiar las organizaciones para proteger los contenedores han mejorado tanto en lo que se refiere a capacidades como a su sofisticación. Independientemente del grado de madurez en materia de DevSecOps que se haya conseguido, las herramientas de seguridad de los contenedores son ahora más accesibles que nunca. Entre las herramientas de ciberseguridad para contenedores que cualquier organización deberá adoptar y dominar se encuentran las siguientes:

SUPERVISIÓN DE CONTENEDORES: indispensable para poder aplicar y mantener la seguridad de los contenedores, las herramientas de supervisión de contenedores son necesarias para realizar el seguimiento de las unidades de computación que se encuentran entre las más efímeras y elementales jamás concebidas. Debido a que los desarrolladores extraen y sustituyen contenedores constantemente, las herramientas de supervisión que permiten que los equipos de operaciones de TI y ciberseguridad apliquen marcadores de series temporales a los contenedores resultan de vital importancia al tratar de determinar con exactitud qué ha ocurrido en un entorno de contenedores.

HERRAMIENTAS DE ANÁLISIS DE CONTENEDORES: los contenedores se deben analizar constantemente en busca de vulnerabilidades tanto antes de su implementación en un entorno de producción como después de su sustitución. Resulta demasiado fácil que los desarrolladores incluyan por error una biblioteca con vulnerabilidades conocidas en un contenedor. No hay que olvidar que se descubren vulnerabilidades nuevas casi a diario, lo que implica que la imagen de un contenedor que hoy parece totalmente segura podría terminar siendo mañana la vía de distribución de todo tipo de malware.

CORTAFUEGOS DE CONTENEDORES: el cortafuegos de un contenedor inspecciona y protege todo el tráfico de entrada y salida de los contenedores, así como el tráfico hacia redes externas y aplicaciones heredadas y procedente de ellas. La mayoría de los cortafuegos se ejecutan como «sidecares» que les permiten gestionar un amplio espectro del tráfico que entra y sale de los microservicios compuestos por muchos contenedores.

POLICY ENGINES: las herramientas de ciberseguridad modernas permiten que los equipos de ciberseguridad definan políticas que, básicamente, autoricen qué y quiénes tienen acceso a un microservicio determinado. Las organizaciones necesitan un marco para definir, en primer lugar, esas políticas y luego velar por que se mantengan sistemáticamente en un entorno de aplicaciones en contenedores muy distribuido.

DEFENSA DE LA SUPERFICIE DE ATAQUE HÍBRIDA

Ahora que los contenedores simplifican la portabilidad de las aplicaciones en contenedores entre distintas plataformas, las organizaciones también necesitarán poder aplicar en primer lugar políticas de ciberseguridad y, después, solucionar cualquier problema que surja en las distintas plataformas. En la actualidad, la mayoría de los contenedores se implementan inicialmente por encima de las máquinas virtuales tradicionales para garantizar que haya una capa de aislamiento entre la carga de trabajo de las aplicaciones que comparten la misma plataforma.

Sin embargo, se está empezando a dar un caso de uso en el que las organizaciones no quieren implementar una máquina virtual debido a la sobrecarga adicional generada, que puede afectar negativamente al rendimiento de las aplicaciones. En esos casos, los desarrolladores preferirán implementar sus contenedores en servidores dedicados o encima de una nueva clase de máquinas virtuales más ligeras. Esto ocurre sobre todo en entornos que dependen de unidades de procesamiento de gráficos (GPU, por sus siglas en inglés) que no se prestan a técnicas de virtualización tradicionales que no sean los contenedores. En otros casos, el no querer tener que pagar una cuota por las licencias de software comercial para máquinas virtuales es otro motivo por el que una organización podría optar por implementar contenedores en un servidor dedicado.

Sea cual sea el motivo, lo único con lo que pueden contar los equipos de ciberseguridad es que las aplicaciones en contenedores tendrán sus propios manifiestos de forma local o en diversos entornos informáticos de la nube pública. Cada entorno estará compuesto por varios tipos de máquinas virtuales y físicas que ejecutarán contenedores que, a su vez, tendrán que estar protegidos a través de un marco común.

Para complicarlo todo aún más, los marcos de informática sin servidor creados con contenedores representan otra superficie de ataque que habrá que proteger. Los marcos de informática sin servidor, basados en una arquitectura orientada a eventos, permiten que los desarrolladores invoquen un proceso secundario desde sus aplicaciones bajo demanda. Esa capacidad suprime la necesidad de incluir código en una aplicación para ejecutar una función que solo se requiere de forma ocasional. Cuanto menos código haya en una aplicación, más fácil es protegerla. Sin embargo, los equipos de seguridad no deberían pasar por alto la necesidad de proteger el marco de la informática sin servidor.

LA GRAN PARADOJA DE LA CIBERSEGURIDAD

Ya existen millones de empleos en el campo de la ciberseguridad que van a quedar vacantes. Como la cantidad de código de aplicaciones que hay que proteger sigue aumentando de forma exponencial gracias, principalmente, al auge de los contenedores, la única forma de seguir el ritmo que tendrán los equipos de ciberseguridad y los desarrolladores de aplicaciones será recurrir más a la automatización.

Aunque hubiera profesionales de la ciberseguridad suficientes para cubrir todas esas vacantes, para la mayoría de las organizaciones seguiría siendo un reto el retener toda esa experiencia y conocimiento en ciberseguridad. La única forma de reducir con eficacia el impacto de la rotación de personal en los equipos de ciberseguridad es automatizar la mayor cantidad de procesos manuales existentes posibles. Este enfoque no solo simplifica el mantenimiento de las políticas de ciberseguridad a escala, sino que también permite que el personal de ciberseguridad dedique más tiempo a tareas como la detección de malware antes de que se active.

De ahora en adelante, ya no se trata de si las tareas de ciberseguridad se van a automatizar, sino de hasta qué punto van a hacerlo.

ARGUMENTOS PARA LA UNIFICACIÓN

A medida que la computación nativa en la nube —en todas sus formas— habilitada por contenedores se hace cada vez más omnipresente, existe una necesidad clara de disponer de un marco de ciberseguridad que pueda aplicarse a los contenedores y a los marcos de computación sin servidor asociados. Ese argumento, no obstante, no se limita a aplicaciones de computación nativa en la nube. Este tipo de aplicaciones no van a suprimir todo el código de aplicaciones monolíticas implementado en las empresas en un futuro próximo. Organizaciones de todos los tamaños ejecutarán una combinación de aplicaciones heredadas y nativas en la nube hasta el final la próxima década. El próximo gran reto en materia de ciberseguridad consistirá en encontrar una forma de elaborar y mantener políticas de ciberseguridad en ambos entornos utilizando el mismo marco de gestión.

Conseguir ese objetivo es la razón principal que movió, a principios de este año, a Palo Alto Networks a adquirir Twistlock, proveedor de una plataforma de seguridad para contenedores, y PureSec, proveedor de un marco para proteger marcos de informática sin servidor. Palo Alto Networks ya ha invertido millones de dólares en el desarrollo de un marco Prisma para automatizar la gestión de la ciberseguridad dentro de entornos de aplicaciones monolíticas heredadas. Ahora Prisma se está ampliando para añadir compatibilidad con aplicaciones de computación nativa en la nube basadas en contenedores y en marcos de informática sin servidor.

De hecho, Prisma está a punto de convertirse en la plataforma de gestión del ciclo de vida de la ciberseguridad más completa que haya habido jamás.

CONCLUSIÓN

Como siempre, es el mejor y el peor momento para la ciberseguridad. En muchos aspectos, mantener la ciberseguridad nunca ha sido tan difícil, ya que los entornos de TI han pasado a ser más heterogéneos que nunca. Al mismo tiempo, sin embargo, el ritmo al que se innova en materia de ciberseguridad nunca ha sido tan rápido.

Probablemente, la decisión más importante en cuanto a ciberseguridad que tome cualquier organización en los próximos meses sea decidir qué proveedor dispone de las herramientas y el conocimiento necesarios para proteger no solo sus entornos existentes, sino también para proteger los entornos de aplicaciones emergentes, ya que los desarrolladores siguen adoptando plataformas innovadoras con independencia de las reservas que pueda plantear inicialmente el resto de la organización en materia de ciberseguridad.

Para obtener más información sobre cómo proteger esos entornos, visite *www.paloaltonetworks.es/cloud-security*.


PRISMA™
BY PALO ALTO NETWORKS