Seguridad en la nube: motivos para añadir la defensa en tiempo de ejecución a su estrategia y formas de hacerlo

Hace tiempo que algunas tecnologías nativas en la nube, como los contenedores y las funciones sin servidor, dejaron de ser una novedad. Con sus características actuales, llevan ya entre nosotros la mayor parte de la última década. Docker se remonta a 2013, por ejemplo, mientras que las funciones sin servidor de AWS Lambda aparecieron en 2014.

Lo que sí está cambiando muy rápidamente es la velocidad a la que las tecnologías nativas en la nube se abren paso en los entornos de producción. Según un informe publicado en marzo de 2020, por ejemplo, el 29 por ciento de las organizaciones ejecutaban más de la mitad de sus aplicaciones de producción dentro de contenedores, lo que supone un incremento de aproximadamente el 31 por ciento con respecto a los seis meses anteriores. Gartner prevé que de aquí a 2023 el 70 por ciento de las organizaciones ejecutarán al menos tres aplicaciones en contenedores. Y un informe de Forrester concluyó que ampliar el uso de los contenedores y otras tecnologías nativas en la nube es una de las principales prioridades de más de uno de cada cuatro directores de tecnología.

Esta rápida adopción de las tecnologías nativas en la nube se traduce en que las herramientas y los procesos de DevSecOps están cobrando protagonismo en el ciclo de desarrollo. A su vez, los equipos están añadiendo nuevas capas de seguridad para ayudar a proteger las cargas de trabajo nativas en la nube a lo largo de todas las fases de la cadena de CI/CD.

De entre estas capas de seguridad adicionales, destaca la seguridad en tiempo de ejecución. La seguridad en tiempo de ejecución, que automatiza la protección de las aplicaciones ágiles y dinámicas —como las que se ejecutan en los contenedores—, responde como ninguna otra metodología de seguridad a las necesidades particulares de los entornos nativos en la nube en lo que concierne a la seguridad y el cumplimiento normativo, a la vez que permite a los equipos aplicar todos los procesos de DevSecOps a las cargas de trabajo nativas en la nube.

¿Qué es la seguridad en tiempo de ejecución?

La seguridad en tiempo de ejecución se refiere a la supervisión y validación de toda la actividad que se desarrolla en los contenedores, hosts y funciones sin servidor.

Este tipo de seguridad se vale del control de aplicaciones y de las listas de permitidos para establecer unos valores de referencia que permitan detectar comportamientos anómalos en todos y cada uno de los hosts, contenedores, funciones sin servidor y demás objetos que habitan en un entorno nativo en la nube. Después, mediante la observación en tiempo real de los sistemas de archivos, los procesos y la actividad en la red, las herramientas de seguridad en tiempo de ejecución identifican la actividad sospechosa o anómala y alertan a los equipos pertinentes.

La supervisión de la seguridad en tiempo real no es un concepto nuevo, como ya se sabe. Las plataformas de los sistemas de información de seguridad y gestión de eventos (SIEM, por sus siglas en inglés) llevan años supervisando los entornos de aplicaciones en busca de anomalías.

Sin embargo, a diferencia de aquellas, la seguridad en tiempo de ejecución nativa en la nube se aplica a entornos muy dinámicos en los que no existen valores de referencia en el sentido tradicional. Cuando se están iniciando y terminando instancias de los contenedores y las funciones sin servidor todo el rato y los equilibradores de carga redirigen el tráfico constantemente de una instancia a otra, las fuentes de datos convencionales —como los logs y el tráfico de la red— dejan de ser útiles para detectar anomalías que podrían apuntar a una brecha de seguridad. La seguridad en tiempo de ejecución va más allá al interpretar cómo varían las tendencias en el comportamiento a lo largo del tiempo para establecer unos valores de referencia dinámicos. A partir de ahí, las herramientas de seguridad en tiempo de ejecución detectan cambios en los procesos internos de los contenedores, la actividad de los sistemas de archivos, etc., que se desvían de la norma, incluso en entornos que cambian de tamaño rápidamente.

Dicho de otro modo, la defensa en tiempo de ejecución es un conjunto de funciones que proporcionan protección tanto predictiva como basada en amenazas para entornos que cambian a gran velocidad.

Motivos para adoptar la seguridad en tiempo de ejecución

La seguridad en tiempo de ejecución permite detectar las anomalías que se producen en entornos dinámicos, lo que, en entornos nativos en la nube, ofrece bastantes ventajas con respecto a las herramientas de supervisión tradicionales.

Detección de amenazas en entornos dinámicos

La primera ventaja (y la más importante) es que la seguridad en tiempo de ejecución es la única manera de proteger las aplicaciones nativas en la nube a gran escala. Como ya hemos apuntado, establecer unos valores de referencia que permitan diferenciar el comportamiento «normal» del comportamiento anómalo para después identificar las desviaciones del primero en entornos dinámicos y distribuidos es todo un reto, sobre todo cuando esos entornos contienen cientos de contenedores y funciones sin servidor y docenas de microservicios.

La seguridad en tiempo de ejecución emplea la inteligencia artificial y el aprendizaje automático para automatizar el proceso de modelado de la actividad «saludable» y detectar las desviaciones de aquella, incluso en entornos complejos en los que a los propios ingenieros les resultaría muy difícil identificar la actividad normal a mano.

Brechas de bajo impacto, o mejor todavía: cero brechas

La seguridad en tiempo de ejecución ayuda a reforzar los entornos frente a las vulnerabilidades. Las defensas en tiempo de ejecución, que proporcionan control sobre los sistemas de archivos, los procesos y la actividad en la red de todos los contenedores y las funciones sin servidor, amortiguan el daño que podría provocar una posible brecha de seguridad en su entorno.

Por si no fuera suficiente, las herramientas de defensa en tiempo de ejecución modelan automáticamente el comportamiento seguro para las aplicaciones y aplican reglas que previenen el desarrollo de actividad peligrosa en el contenedor o el host. Protegen de distintas situaciones, como la posibilidad de que un contenedor atacado ejecute procesos que propaguen la brecha a otros contenedores o el host, por ejemplo.

Capacidad de respuesta a incidentes

Los datos recopilados por las herramientas de seguridad en tiempo de ejecución también son importantes a la hora de responder a incidentes, ya que recopilan y almacenan datos de auditoría de las aplicaciones nativas en la nube para proporcionar a los equipos la información que necesitan para entender qué falló para que se produjera un incidente dado, aunque el entorno nativo en la nube original investigado ya no exista como tal.

Los retos de implementar la seguridad en tiempo de ejecución

La seguridad en tiempo de ejecución es un concepto complejo e implementarla de forma eficiente y eficaz no está exento de dificultades. Los retos de los que hablaremos a continuación se pueden superar, pero requieren herramientas de seguridad en tiempo de ejecución diseñadas para entornos modernos de gran complejidad.

Unos entornos que cambian constantemente

Como decíamos, en los entornos nativos en la nube (cuyas configuraciones y escala no paran de cambiar), no resulta sencillo establecer unos valores de referencia coherentes que permitan discriminar la actividad normal de la anómala. Hay que tener en cuenta un gran número de variables, como el modo en que cambian los patrones de tráfico a distintas horas del día y según el día de la semana, y cómo reaccionan las herramientas de orquestación de contenedores a los cambios en la demanda de las aplicaciones y los fallos en los pods.

Diversidad de tecnologías

Los entornos nativos en la nube están formados por distintos tipos de tecnologías: contenedores, funciones sin servidor, máquinas virtuales, servicios en la nube... Las herramientas de seguridad en tiempo de ejecución deben ser capaces de interpretar las características arquitectónicas y los patrones conductuales de cada uno de estos componentes para poder modelar y aplicar un comportamiento seguro.

Riesgo de alertas inexactas

Enviar alertas es fácil. Lo difícil es asegurarse de que todas las alertas sean de interés, de que las reglas de las alertas no queden obsoletas conforme cambian los entornos y de que las configuraciones de alertas manuales que antes proporcionaban alarmas valiosas no resulten en falsos positivos o falsos negativos.

Qué puede esperar de la seguridad en tiempo de ejecución

Una solución de seguridad en tiempo de ejecución bien implementada debe ofrecer varias funciones clave:

Modelado automático del comportamiento de las aplicaciones

Las herramientas de seguridad en tiempo de ejecución deben ser capaces de entender automáticamente si el comportamiento de una aplicación es seguro o no. Una organización con docenas de servicios que gestionar alojados en cientos de contenedores, funciones sin servidor y máquinas virtuales no tiene tiempo de configurar modelos de comportamiento a mano, ni tan siquiera de recopilar los datos del comportamiento de esta forma. Necesita herramientas que lo hagan automáticamente.

Control del comportamiento de las aplicaciones

Además de modelar el comportamiento seguro, las defensas en tiempo de ejecución deben ser capaces de definir automáticamente qué comportamiento está permitido y cuál no en cada contenedor, función sin servidor o cualquier otro objeto del entorno. Por ejemplo, han de ser capaces de definir otro contenedor como un contenedor con el que pueden comunicarse o a qué volúmenes de almacenamiento de datos pueden acceder. Aplicar estas reglas es fundamental para garantizar que, de producirse una brecha, sus consecuencias sean limitadas.

Envío de alertas útiles

Aunque las herramientas de seguridad en tiempo de ejecución pueden implementar algunas defensas automáticamente, también deben avisar a los equipos cuando les toque intervenir. Para ello, deben vigilar los recursos de la infraestructura nativa en la nube —como los procesos, las conexiones de red o las lecturas y escrituras del sistema de archivos— y alertar de los cambios sospechosos que se produzcan nada más detectarlos.

También deben ser capaces de decidir si enviar o no una alerta en función de unas reglas de alerta dinámicas. Las reglas de alerta estáticas no sirven para frenar las amenazas que se ciernen sobre los recursos nativos en la nube, pues una actividad que puede apuntar a una amenaza de seguridad en un momento dado puede ser benigna en otro.

Integración con otras soluciones de seguridad

La seguridad en tiempo de ejecución tan solo representa una de las capas de defensa que no pueden faltar en las soluciones de seguridad de una organización. Igual de importantes son las herramientas automatizadas de protección de los datos, control de accesos y auditorías, escáneres de imágenes de contenedor, etc.

Las soluciones de seguridad en tiempo de ejecución más completas, además de integrase con otras herramientas de seguridad para proporcionar información pormenorizada y el contexto de los incidentes, son capaces de entender cómo afecta una amenaza en una capa de la solución tecnológica (como el entorno en tiempo de ejecución) a otra capa (como los datos en reposo).

Aproveche al máximo la seguridad en tiempo de ejecución

Las herramientas de seguridad en tiempo de ejecución ofrecen multitud de funciones y el valor que extraiga de ellas dependerá, en buena parte, de la estrategia de defensa en tiempo de ejecución que elija. Para aprovechar al máximo las soluciones de seguridad en tiempo de ejecución, busque los siguientes resultados.

Cobertura exhaustiva

Supervisar únicamente una parte de su entorno, o centrarse en los servicios o la infraestructura claves, no es suficiente para garantizar la detección de todas las amenazas de seguridad. Para obtener los mejores resultados, aplique la seguridad en tiempo de ejecución a todas las capas de su entorno y utilícela para proteger tanto las cargas de trabajo de desarrollo y pruebas como las de producción.

Detección de incidentes en tiempo real

Aunque la seguridad en tiempo de ejecución sea capaz de mitigar el impacto de una brecha una vez ocurrida, lo ideal sería que la solución que elija le permita encontrar y corregir las amenazas en tiempo real antes de que tengan la oportunidad de ser más dañinas.

Cada recurso es único

Cada host, instancia de contenedor, función sin servidor, etc., de su entorno nativo en la nube tiene una configuración y un comportamiento únicos. Por lo tanto, lo ideal sería modelar cada uno de ellos por separado. No dé por sentado que todos los contenedores se comportarán igual, por mucho que estén basados en una imagen de contenedor común, por ejemplo. Hacerlo conduce a un enfoque poco representativo que limita la visibilidad de los incidentes de seguridad.

Seguridad en tiempo de ejecución con Prisma® Cloud

Cuando se da el paso a la tecnología nativa en la nube, la seguridad en tiempo de ejecución se convierte en una parte fundamental de la estrategia de seguridad. Sin unas defensas en tiempo de ejecución que protejan su inversión, no podrá sacar el debido provecho a soluciones como los contenedores, funciones sin servidor y servicios en la nube.

Prisma Cloud, una completa plataforma de seguridad nativa en la nube, ofrece soluciones de seguridad en tiempo de ejecución, así como otros mecanismos de defensa —como protección de datos, gestión del control de accesos y gestión de la estrategia de seguridad en la nube— que las organizaciones necesitan para proteger sus entornos nativos en la nube, con independencia de lo complejos que sean esos entornos y de lo rápido que escalen. Para obtener más información, solicite una demostración.

paloalto NETWORKS

Oval Tower, De Entrée 99 - 197
1101HE Ámsterdam
Países Bajos

Tel.: +31 20 888 1883

www.paloaltonetworks.es