Guía sobre las herramientas de gestión de la estrategia de seguridad en la nube

paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

Contenido

PRISMA BY PALO ALTO NETWORKS

Para proteger bien un entorno en la nube, se necesita una visibilidad completa de todos los recursos alojados en él, así como de su correspondiente estrategia de seguridad y cumplimiento normativo. Si solo se utiliza una nube, bastará con combinar las herramientas de supervisión y auditoría del proveedor de nube con soluciones de terceros que subsanen posibles carencias (p. ej., la falta de funciones de detección de amenazas). En arquitecturas de varias nubes, por el contrario, mantener una estrategia sólida de seguridad es muchísimo más complicado.

Por un lado, en los entornos de varias nubes cuesta más tener una perspectiva centralizada y aplicar de manera coherente las políticas y las reglas de cumplimiento normativo. Por otro, las amenazas que afectan a las arquitecturas distribuidas de varias capas son muy complejas, lo que dificulta su detección y hace que las vulnerabilidades tarden más en resolverse.

Solucionar estos problemas está en su mano, y hacerlo es vital para aprovechar con seguridad las ventajas que ofrece una arquitectura de varias nubes. En esta guía se abordan los factores que dificultan la gestión de la estrategia de seguridad en la nube (CSPM, por sus siglas en inglés) en entornos compuestos por más de una nube. Una vez identificados estos retos, se explica cómo superarlos con herramientas y estrategias para CSPM que ofrezcan una visibilidad centralizada de todas las nubes del entorno, ayuden a controlar si cumplen la normativa, detecten las amenazas que las acechan, protejan sus datos y automaticen ciertas tareas relacionadas con ellas.

Factores que dificultan la gestión de la estrategia de seguridad en varias nubes

Los métodos de gestión de la estrategia de seguridad en una sola nube no pueden trasladarse sin más a arquitecturas de varias nubes, cuyas necesidades son distintas. Veamos cuáles son las principales diferencias entre ambos tipos de entorno en lo que respecta a la seguridad.

Heterogeneidad y dispersión de los datos

En los entornos de varias nubes, los datos están dispersos por todas ellas. Tal vez se utilice una nube más barata para guardar grandes volúmenes de datos y otra distinta (y más cara) solo para aquellos datos a los que haga falta acceder más rápido. En otros casos, los datos se reparten por regiones, para almacenarlos en nubes más próximas a quienes vayan a usarlos.

Cuando los datos no están en un mismo sitio, es más difícil protegerlos y evitar infecciones de malware. Habrá que asegurarse de que, en cada nube de cada almacén de datos, haya reglas que controlen la gestión de identidades y accesos (IAM, por sus siglas en inglés). Además, todos los depósitos deben tener la configuración adecuada, que será la establecida por el proveedor de servicios en la nube al que pertenezcan.

Aplicaciones repartidas por distintas nubes

Las aplicaciones y las herramientas con las que se entregan también suelen estar dispersas por entornos de varias nubes. A veces se opta por duplicar instancias de la misma aplicación en distintas nubes, de modo que, si una falla, las otras sigan estando disponibles. O puede que una cadena de herramientas de desarrollo alojada en una nube se implemente desde otra.

En este contexto, la gestión de la estrategia de seguridad en la nube solo será eficaz si permite asegurarse de que todos los servicios y recursos que componen la aplicación son seguros. No basta con supervisar por separado cada instancia de una aplicación que se ejecute en varias nubes; lo importante es saber si la seguridad de una instancia podría afectar a las demás. Por ejemplo, si se produce una brecha en un entorno en la nube, ¿podría acabar afectando a otro debido a la interacción entre unas instancias y otras? Estos riesgos disminuyen si la configuración de las aplicaciones se supervisa constantemente para que no llegue a desviarse de lo estipulado en las políticas.

Dada la dificultad de implementar aplicaciones en varias nubes, hay algo aún más importante: lograr que la seguridad esté integrada en el ciclo de desarrollo de las aplicaciones, en lugar de ser un mero añadido. Una vez que la aplicación llega a la fase de producción, las vulnerabilidades tardan más en resolverse, sobre todo si el código vulnerable se implementa en varios entornos. Si los controles de seguridad se integran en el ciclo de desarrollo de las aplicaciones, será menos probable que surja la necesidad de responder a un problema o corregirlo cuando la aplicación ya esté en fase de producción.

Variedad de amenazas y vulnerabilidades

Hoy en día, el abanico de amenazas al que nos enfrentamos es amplísimo: operaciones de *cryptojacking* llevadas a cabo por personal interno a través de las API, intentos de exfiltración de datos, imágenes de contenedor con malware, aplicaciones con vulnerabilidades que pueden desencadenar ataques por inyección de código SQL... Es imposible combatir todo esto con un solo mecanismo de detección de amenazas. Si se utilizan de manera aislada, ni los análisis de malware ni las auditorías de configuraciones bastan para proteger los entornos. Lo que hay que hacer es recopilar inteligencia sobre amenazas procedente de distintas fuentes, analizarla y ver a qué amenazas conocidas se asemejan los resultados. Si, además, se complementan las políticas basadas en reglas con otras basadas en el aprendizaje automático, será posible detectar también las amenazas desconocidas.

Multitud de usuarios y permisos

Para los equipos de seguridad, la gestión de identidades y accesos ni siquiera resulta fácil en los entornos de una sola nube. Aunque haya una sola nube que administrar, no es fácil aplicar el acceso según el criterio del mínimo privilegio cuando los usuarios tienen asociadas infinidad de políticas, como las gestionadas por ellos mismos o por los proveedores de servicios en la nube (CSP, por sus siglas en inglés), o bien las vinculadas a otros grupos, funciones, recursos o listas de control de acceso.

En los entornos de varias nubes, la dificultad es aún mayor, ya que cada CSP define de manera distinta los permisos y derechos de acceso de los usuarios. Para cada nube, hay que supervisar un conjunto de configuraciones de IAM distinto y correlacionar las funciones y permisos de los usuarios con los requisitos aplicables a cada uno de ellos. No vale con auditar las mismas credenciales para los mismos usuarios en todas las nubes.

Ampliación de la superficie de ataque

Cuantas más nubes tenga un entorno, mayor será la complejidad que lo rodea y a más cuentas, servicios o políticas de control de acceso estará asociado. Todo esto amplía la superficie de ataque y puede convertir cualquier descuido (un recurso mal configurado, un permiso demasiado laxo o una vulnerabilidad del código) en una rendija por la que infiltrarse.

A ello se suma la falta de una visibilidad y un control centralizados, que dificulta aún más la detección de amenazas y vulnerabilidades. Si las herramientas de un solo CSP no permiten supervisar y auditar todas las configuraciones de todos los servicios, será más difícil evitar los tipos de errores de configuración con más riesgo de provocar una brecha.

Cómo gestionar con eficacia la estrategia de seguridad en varias nubes: 4 características principales

Para superar las dificultades mencionadas y mejorar la seguridad en varias nubes, las herramientas y estrategias de CSPM elegidas deberán reunir cuatro características principales.

Optimización de la visibilidad, la gobernanza y el cumplimiento normativo

Una buena estrategia de gestión de la seguridad en varias nubes se basa en supervisar y auditar constantemente todos los recursos de los CSP. Cada vez que se modifique una configuración o se implemente un nuevo servicio o una nueva carga de trabajo, las herramientas deberán detectar el cambio, analizarlo y comprobar si se ajusta a los requisitos y a las prácticas recomendadas en materia de seguridad.

Si algo se sale de lo esperado, las propias herramientas tendrán que alertar al equipo e indicarle qué hacer. También deben servir para hacer correcciones sencillas (p. ej., actualizar una dirección IP mal escrita o añadir una instrucción a una política de IAM), de modo que algunos problemas se solucionen automáticamente sin que los equipos de seguridad lleguen a intervenir.

Para que se generen menos alertas en tiempo de ejecución, también conviene evitar que las configuraciones no seguras lleguen a los entornos de producción. Esto se consigue utilizando herramientas de CSPM que analicen las plantillas de infraestructura como código (IaC, por sus siglas en inglés), comprueben si presentan errores de configuración y apliquen políticas tanto en tiempo de ejecución como a lo largo del ciclo de vida del desarrollo de software.

Detección de amenazas exhaustiva

Los entornos de varias nubes están expuestos a amenazas complejas cuyos riesgos no son fáciles de entender. Para valorarlos bien, es importante que las herramientas de gestión de la estrategia de seguridad en la nube recopilen inteligencia sobre amenazas de diversas fuentes (p. ej., configuraciones de IaC, imágenes de contenedor o imágenes de máquinas virtuales que se ejecuten en la nube) que muchos equipos ya analizan para detectar vulnerabilidades.

Una organización que quiera un sistema de detección de amenazas más completo y que aporte información más precisa no podrá limitarse a analizar estos componentes; necesitará también inteligencia sobre amenazas de alta fidelidad con la que identificar las amenazas más recientes y valorar su gravedad. Asimismo, es importante poder detectar anomalías en la red y correlacionarlas con otros tipos de datos relativos a las amenazas, pues toda esta información contextual permite valorar mejor los riesgos. Y, de la misma manera, habrá que cotejar los datos obtenidos mediante técnicas de análisis del comportamiento de entidades y usuarios (UEBA, por sus siglas en inglés).

Un sistema de detección de amenazas moderno debe permitir analizar, correlacionar y contextualizar datos procedentes de diversas fuentes, no solo para facilitar la identificación de amenazas en entornos complejos y de varias capas, sino también para que los equipos de seguridad puedan priorizar los riesgos y solucionar los problemas con rapidez. Contar con un sistema de detección de amenazas completo es la única forma de asociar una anomalía en la red a una imagen de contenedor no segura o de averiguar qué cuenta es el origen de una brecha, por poner unos ejemplos. Cuanto menos tarde el equipo de seguridad en entender las amenazas, más se reducirá el tiempo medio necesario para resolverlas.

Protección de datos integrada

Para proteger los datos almacenados en la nube —sean del tipo que sean y contengan o no información de identificación personal—, conviene utilizar diversos métodos que, combinados, nos permitan hacernos una idea exacta del estado en que se encuentran los datos. En primer lugar, tendremos que supervisar la configuración de todos los depósitos pertenecientes a los servicios de almacenamiento utilizados. Así, desaparecerá el riesgo de que las aplicaciones y los usuarios no autorizados accedan a los datos. Al mismo tiempo, habrá que auditar el contenido de los depósitos para determinar si contienen información de identificación personal (PII, por sus siglas en inglés) sujeta a normativas o requisitos especiales.

También es importante comprobar si los datos en reposo contienen malware, un aspecto de la protección de los datos en la nube al que no suele prestarse la debida atención. No basta con analizar solamente los depósitos donde se guardan los datos; también habrá que comprobar si hay indicios de malware en las bases de datos, los sistemas de archivos de las máquinas virtuales, los volúmenes de almacenamiento de los contenedores e incluso los sistemas de archivos de contenedores creados con carácter temporal.

Por último, dado que en la nube no siempre es fácil lograr el justo equilibrio entre la disponibilidad y la protección de los datos, es recomendable que las herramientas de CSPM elegidas permitan calcular el riesgo de una posible brecha y ayuden a limitar su efecto. Quizás se pregunte si los datos que tiene en la nube exigen un control de acceso más o menos estricto, según su grado de confidencialidad, y si utilizar políticas de acceso menos detalladas simplificaría la gestión. Una herramienta que calcule los riesgos a los que se expone le ayudará a entender qué le conviene más.

Corrección de alertas automática

Puesto que los entornos de varias nubes son grandes y complejos por definición, los procesos y controles de seguridad descritos anteriormente no pueden implementarse sin ayuda de herramientas que supervisen y corrijan los riesgos de forma automática.

Esto no quiere decir que la gestión de la estrategia de seguridad en varias nubes deba automatizarse por completo. Cuando las herramientas de CSPM no basten para responder a incidentes de seguridad o riesgos complejos, siempre será necesaria una intervención manual. Sin embargo, las tareas rutinarias de supervisión de la seguridad, auditoría y corrección de problemas sí deberían ser automáticas, de forma que el personal pueda dedicarse a asuntos más importantes.

Carencias de las herramientas que ofrecen los proveedores de nube

Los proveedores de servicios en la nube ofrecen diversas herramientas que ayudan a combatir algunos de los problemas expuestos en esta guía. Existen servicios de protección de datos —como Amazon Macie® y el servicio Cloud DLP de Google— que, por ejemplo, permiten averiguar si los datos almacenados en depósitos o bases de datos presentan vulnerabilidades, y otras herramientas, como Amazon CloudWatch y Azure® Monitor de Microsoft, supervisan el entorno y generan alertas cuando detectan eventos sospechosos. Las herramientas de supervisión de los CSP son útiles y tal vez le interese añadirlas a su arsenal de gestión de la estrategia de seguridad en la nube, pero presentan dos grandes limitaciones:

1. **No están diseñadas para ofrecer una gestión completa e integral de la estrategia de seguridad en la nube**. Aunque permitan auditar algunos archivos de configuración y comprobar si determinados almacenes de datos contienen ciertos tipos de información de identificación personal, no analizan constantemente las imágenes de contenedor, no sirven para detectar anomalías en las redes ni corrigen las amenazas automáticamente.
2. **Las herramientas de cada proveedor funcionan solo en sus nubes**. Dicho de otro modo, las herramientas de Google solo funcionan con Google Cloud; las de Amazon, solo con Amazon Web Services; las de Microsoft, solo con Azure; y así sucesivamente.

En entornos de varias nubes, no es fácil ni eficiente utilizar un sinfín de herramientas dispares de proveedores distintos, ya que será imposible correlacionar los datos entre todas ellas y detectar amenazas teniendo en cuenta todas las fuentes de datos disponibles en los entornos de varias nubes.

Conclusión

Para gestionar la estrategia de seguridad en varias nubes se necesita, pues, una plataforma de seguridad exhaustiva que busque continuamente posibles errores de configuración, vulnerabilidades y amenazas, con métodos de supervisión muy precisos que emitan alertas cuando corresponda.

Gracias a sus funciones de automatización y a la visibilidad centralizada que ofrece, Prisma® Cloud de Palo Alto Networks permite proteger con eficacia todas las nubes de un entorno. Toda la información que obtiene —procedente de los logs de flujo, configuración y auditoría almacenados en las diversas nubes que se ejecutan— se muestra a los equipos de seguridad mediante una vista centralizada, perfecta para supervisar la estrategia de seguridad y cumplimiento normativo de todo el entorno.

El sistema de detección de amenazas de Prisma Cloud, que tiene en la cuenta la actividad anómala y sus efectos, ayuda al equipo de seguridad a ser consciente de la gravedad de cada riesgo y a tomar las medidas oportunas. Con Prisma Cloud, ya no perderá tiempo decidiendo a qué amenazas conviene responder primero ni tratando de averiguar la causa principal de los incidentes de seguridad complejos.

Además, las funciones de corrección automatizada le ahorrarán trabajo, pues permiten resolver con rapidez muchos tipos de errores de configuración relacionados con la seguridad y comprobar automáticamente si se han corregido en un panel central.

Con Prisma Cloud, es más fácil gestionar la estrategia de seguridad aplicable a entornos complejos de varias nubes. Para informarse de cómo podemos ayudar a su equipo, vea una demostración o concierte una reunión con un experto de Palo Alto Networks.

paloalto NETWORKS

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

Tel.: +31 20 888 1883

www.paloaltonetworks.es