SOPHOS

Proteger la nube pública: 7 prácticas recomendadas

Monográficos de Sophos Junio de 2019

Contenido

Proteger la nube pública: 7 prácticas recomendadas

Cuando se trata de proteger aplicaciones en la nube pública, ¿qué es para usted tener éxito?

Tal vez sea sobrevivir al año sin salir en las noticias por una filtración de datos. O ser capaz de comprender la huella de infraestructura en la nube de su empresa para poder protegerla con precisión. Quizás quiera asegurarse de que las auditorías de cumplimiento se llevan a cabo sin problemas. O mejorar la colaboración en correcciones de seguridad y cumplimiento con equipos de desarrollo y cumplimiento independientes.

Al margen de lo que quiera hacer, esta guía le puede ayudarle. Explica los siete pasos más importantes para proteger la nube pública y ofrece orientación práctica que puede seguir cualquier empresa. Incluye los resultados de la investigación de amenazas de SophosLabs sobre la frecuencia con la que los ciberdelincuentes atacan las instancias basadas en la nube. Esta guía también analiza cómo Sophos Cloud Optix permite a las empresas hacer frente a sus retos de seguridad y visibilidad.

Crear nuevas instancias en Amazon Web Services (AWS), Microsoft Azure o Google Cloud Platform (GCP) es sencillo. Lo difícil para los equipos de operaciones, seguridad, desarrollo y cumplimiento es llevar un registro de los datos, las cargas de trabajo y los cambios de arquitectura en esos entornos para mantener la seguridad en todos los frentes.

Si bien los proveedores de la nube pública se encargan de la seguridad de la nube (los centros de datos físicos y la separación de los entornos y los datos de los clientes), la responsabilidad de proteger las cargas de trabajo y los datos que coloca en la nube recae rotundamente sobre usted. Del mismo modo que necesita proteger los datos almacenados en sus redes locales, también necesita proteger su entorno en la nube. Los malentendidos en torno a esta distribución de la propiedad son muy frecuentes y las brechas de seguridad resultantes han hecho que las cargas de trabajo basadas en la nube sean el nuevo tesoro que codiciar para los habilidosos hackers de hoy en día.

Los retos más difíciles de la seguridad en la nube

Dada la simplicidad y la rentabilidad de la nube pública, no es de extrañar que cada vez más empresas recurran a Amazon Web Services, Microsoft Azure y Google Cloud Platform. Puede crear una nueva instancia en cuestión de minutos, ampliar o reducir los recursos cuando lo necesite, pagando solo por lo que utiliza, y evitar la inversión de hardware inicial.

Aunque la nube pública resuelve muchos de los retos tradicionales de recursos de TI, introduce nuevos quebraderos de cabeza. El secreto de una ciberseguridad efectiva en la nube es mejorar su posición general en materia de seguridad: asegurarse de que su arquitectura es segura y está configurada correctamente y de que tiene la visibilidad necesaria de su arquitectura y, lo que es más importante, de quién accede a ella.

Aunque todo esto parece sencillo, nada más lejos de la realidad.

El rápido crecimiento del uso de la nube ha dado lugar a una distribución fraccionada de los datos, con cargas de trabajo repartidas en distintas instancias y, para algunas empresas, en distintas plataformas. Una empresa típica ya ejecuta aplicaciones en dos nubes públicas y al mismo tiempo experimenta con otras 1,8 nubes públicas [1]. Este enfoque multinube aumenta el desafío de la visibilidad para los equipos de TI que necesitan saltar de una plataforma a otra para obtener una imagen completa de sus entornos basados en la nube.

La falta de visibilidad de las cargas de trabajo que se basan en la nube conlleva riesgos tanto de seguridad como de cumplimiento:

Mayor exposición

El aumento de la agilidad y la aceleración del plazo de comercialización de productos y servicios son importantes factores de motivación para que una empresa se traslade a la nube pública. Hacer esto suele requerir la agilidad y capacidad de respuesta de un enfoque de DevOps. Para muchos, este nuevo enfoque al desarrollo y lanzamiento de productos implica que varios desarrolladores trabajen en múltiples plataformas y a menudo en diferentes zonas horarias.

Hacer un seguimiento de las cargas de trabajo no suponía un problema cuando los ciclos de desarrollo duraban meses o incluso años, pero eso ya es historia. Ahora es necesario seguir el ritmo que implican múltiples lanzamientos, a veces en un mismo día. Es casi imposible realizar un seguimiento de los vertiginosos cambios de arquitectura, las actualizaciones de configuración y la configuración de los grupos de seguridad las 24 horas del día. Todo esto se traduce en una mayor exposición a las ciberamenazas, en que las vulnerabilidades pueden explotarse rápidamente.

Amenazas a los datos, la propiedad intelectual y los servicios

Así como las empresas disfrutan de las ventajas de la automatización que ofrece la nube pública, también lo hacen los ciberdelincuentes. Los atacantes de hoy en día escudriñan cada vez más los entornos en la nube y aprovechan las API en la nube nativas de los proveedores para automatizar las implementaciones en nuevas instancias, infiltrarse en bases de datos abiertas, cambiar configuraciones de seguridad y bloquear a los usuarios legítimos.

Para cuantificar el problema, recientemente SophosLabs creó entornos en 10 de los centros de datos AWS más populares del mundo. La investigación reveló que:

- En el transcurso de dos horas, los 10 centros de datos experimentaron intentos de inicio de sesión[2].
- Cada dispositivo registró un promedio de 13 intentos de inicio de sesión por minuto, es decir, alrededor de 757 por hora.

Estos sorprendentes resultados ponen de manifiesto la frecuencia con la que los ciberdelincuentes se dirigen a las instancias basadas en la nube, utilizando técnicas sofisticadas y automatizadas. El desafío para los equipos de seguridad consiste en identificar y proteger vulnerabilidades potenciales antes que los atacantes e identificar comportamientos inusuales (maliciosos) en tiempo real para detener un ataque al instante.

Mantenimiento de los estándares de cumplimiento

Independientemente de la ubicación de su infraestructura y sus datos, debe demostrar que cumple con las normativas pertinentes, incluidas las normas CIS, HIPPA, RGPD y PCI, o corre el riesgo de incumplimiento normativo.

El reto en la nube es que los entornos cambian día a día, hora a hora e incluso minuto a minuto. Si bien las comprobaciones de cumplimiento semanales o mensuales pueden haber funcionado para las redes locales, no son suficientes en la nube pública. La necesidad de un análisis continuo del cumplimiento de normativas puede suponer un despilfarro de recursos para los equipos que gestionan entornos en la nube de forma manual o con herramientas nativas. Y lo que es más, una vez que se identifica un problema de cumplimiento, la naturaleza fragmentada de los equipos de seguridad, desarrollo, operaciones y cumplimiento de la mayoría de empresas significa que a menudo es difícil abordar la situación a tiempo.

7 pasos para proteger la nube pública

Paso 1: Conozca sus responsabilidades

Esto parece evidente, pero la seguridad en la nube se gestiona de manera un tanto distinta. Los proveedores de la nube pública como Amazon Web Services, Microsoft Azure y Google Cloud Platform utilizan un modelo de responsabilidad compartida, lo que significa que ellos garantizan la seguridad de la nube, mientras que usted es responsable de todo lo que coloca en ella.

Aspectos como la protección física en el centro de datos y la separación virtual de los datos y los entornos de los clientes están bajo la responsabilidad de los proveedores de la nube pública.

Es posible que obtenga algunas reglas básicas de tipo firewall para controlar el acceso a su entorno. Pero si no las configura correctamente (por ejemplo, si deja los puertos abiertos a todo el mundo), eso es problema suyo. Así que debe conocer sus responsabilidades de seguridad.

La figura 1 ofrece una visión general de estas responsabilidades compartidas o, si lo prefiere, puede ver este vídeo.

Modelo de seguridad de responsabilidad compartida	Local	Nube pública	¿Por qué?
Usuarios	■	■	Imponga la autenticación, defina las restricciones de acceso y realice un seguimiento del uso de las credenciales.
Datos	■	■	Detener pérdidas de datos y definir e imponer quién puede acceder a qué datos, al tiempo que se satisfacen los estándares de cumplimiento
Aplicaciones	■	■	Evitar que las aplicaciones se vean comprometidas por medio de políticas, parches y seguridad.
Controles de redes	■	◪	Realizar un seguimiento y aplicar los permisos de acceso a la red.
Infraestructura del host	■	◪	Administrar y proteger los sistemas operativos, las soluciones de almacenamiento y los sistemas relacionados para evitar errores no corregidos y aumentos de privilegios.
Seguridad física	■	■	Limitar el acceso físico a los sistemas y diseñar la redundancia para evitar puntos únicos de error.

■ Cliente ■ Proveedor de la plataforma

Fig 1. Resumen de Sophos del modelo de responsabilidad compartida. Para conocer la versión específica de cada proveedor de la nube, vaya a es.sophos.com/public-cloud.

Paso 2: Planifique su estrategia previendo el uso de múltiples nubes

La multinube ya no es una estrategia deseable, sino imprescindible. Hay muchas razones por las que puede querer utilizar múltiples nubes, como la disponibilidad, la mayor agilidad o la funcionalidad. Al planificar su estrategia de seguridad, parta del supuesto de que utilizará múltiples nubes; si no ahora, en algún momento en el futuro. De esta manera, podrá preparar su enfoque para el futuro.

Piense en cómo gestionará la seguridad, la supervisión y el cumplimiento en múltiples proveedores en la nube, en sistemas y consolas diferentes. Cuanto más fácil sea la experiencia de gestión, más fácil será reducir los tiempos de respuesta ante incidentes, aumentar la detección de amenazas y reducir los quebraderos de cabeza que suponen las auditorías de cumplimiento. Por no hablar de que ayuda a conservar a los miembros valiosos del equipo.

Busque soluciones sin agentes que le permitan supervisar varios entornos de proveedores en la nube desde una única consola SaaS, lo que reduce la cantidad de tiempo, personas y herramientas necesaria para gestionar la seguridad en cuentas y regiones en múltiples nubes.

Paso 3: Véalo todo

Si no lo puede ver, no lo puede proteger. Por eso, uno de los mayores obstáculos para conseguir una posición correcta en materia de seguridad es lograr una visibilidad precisa de su infraestructura.

Utilice herramientas que proporcionen una visualización en tiempo real de la topología de red y el flujo de tráfico, con un desglose completo del inventario que incluya hosts, redes, cuentas de usuario, servicios de almacenamiento, contenedores y funciones sin servidor.

Para mejorar la visibilidad, busque herramientas capaces de identificar posibles vulnerabilidades dentro de su arquitectura, de modo que pueda evitar una posible brecha. Las posibles áreas de riesgo incluyen:

- Bases de datos con puertos abiertos a la Internet pública que podrían permitir el acceso de atacantes.
- Servicios públicos Amazon Simple Storage Service (Amazon S3).
- Comportamientos de inicio de sesión de usuarios sospechosos y llamadas a la API, como múltiples inicios de sesión en la misma cuenta al mismo tiempo o un usuario que inicia sesión desde distintas partes del mundo el mismo día.

Paso 4: Integre el cumplimiento en los procesos diarios

El traslado de cargas de trabajo a la nube presenta el reto de ajustarse a las normativas de cumplimiento en una red más distribuida, lo que a menudo implica versiones de desarrollo periódicas. Para garantizar el cumplimiento, debe crear informes de inventario y diagramas de red precisos de su presencia en la nube y asegurarse de que los requisitos de su lista de comprobación de cumplimiento se satisfacen en un entorno dinámico.

A la hora de cumplir con los plazos de auditoría, a menudo las empresas recurren a la solución a corto plazo de desviar recursos de proyectos empresariales rentables. Sin embargo, este método no es sostenible a largo plazo y, como las instantáneas diarias se vuelven obsoletas rápidamente, no ofrece la monitorización continua del cumplimiento que requieren estándares como ISO 27001, HIPAA y RGPD.

Busque soluciones que le permitan incrementar sus niveles de cumplimiento sin necesidad de contratar a más personal, proporcionando instantáneas en tiempo real de la topología de red y detectando automáticamente los cambios realizados en sus entornos en la nube en tiempo real. También es recomendable la opción de personalizar la política para satisfacer las necesidades específicas de su sector o mercado vertical.

Por supuesto, la presentación de informes es solo un aspecto del cumplimiento. También es necesario abordar los fallos de cumplimiento. El desafío es que, a menudo, es difícil conseguir que las personas adecuadas en operaciones, desarrollo y cumplimiento trabajen juntas debido a la falta de canales de colaboración eficaces.

Para que el proceso de solucionar los problemas de cumplimiento se desarrolle eficazmente, busque soluciones que se integren con sus soluciones de emisión de incidencias existentes y que incluyan información de alertas que se pueda utilizar para crear, asignar y realizar un seguimiento de los problemas hasta su resolución, lo que garantiza que las tareas importantes nunca se pierdan, incluso durante un lanzamiento.

Paso 5: Automatice sus controles de seguridad

La capacidad de automatizar procesos es uno de los placeres de DevOps. Pero, del mismo modo que sus equipos disfrutan automatizando la implementación de scripts y plantillas de infraestructura, ahorrando así horas de desarrollo, también debe considerar qué controles de seguridad puede automatizar.

En el marco de colaboración de DevOps, la seguridad es una responsabilidad compartida, integrada de extremo a extremo. Esta actitud llevó a acuñar el término "DevSecOps", que enfatiza la necesidad de construir cimientos de seguridad sólidos en las iniciativas de DevOps.

La necesidad de automatizar la seguridad es evidente a medida que los ciberdelincuentes se aprovechan cada vez más de la automatización en sus ataques, por ejemplo, al utilizar credenciales de usuario robadas para automatizar el aprovisionamiento de instancias para actividades como el criptojacking, cambiar la configuración de cuentas o revocar usuarios legítimos para evitar la detección. De hecho, ahora es habitual la búsqueda de vulnerabilidades en las contraseñas, la configuración de grupos de seguridad y el código en los entornos en la nube.

Las dos razones principales por las que los ataques a los entornos en la nube pública tienen éxito son que la configuración de la arquitectura no es segura y que la respuesta a las amenazas no ha seguido el ritmo de los atacantes. La automatización de los controles de seguridad es clave para abordar estos problemas.

Para garantizar la seguridad de sus entornos en la nube pública, busque una solución que pueda:

- **Reparar automáticamente las vulnerabilidades y los recursos de acceso de los usuarios**, con acceso desde cualquier origen en cualquier puerto.
- **Identificar llamadas a la API y eventos de inicio de sesión en la consola sospechosos** que sugieran que un atacante está utilizando credenciales de usuario compartidas o robadas.
- **Informar de anomalías en el tráfico de salida** para alertar a su empresa sobre actividades como el criptojacking o la exfiltración de datos.
- **Revelar cargas de trabajo de aplicaciones ocultas** a partir del comportamiento de la instancia del equipo host para destacar puntos de exposición ocultos (p. ej., bases de datos).

Paso 6: Proteja TODOS sus entornos (incluidos los de desarrollo y CC)

Aunque las filtraciones de datos de la nube pública que aparecen en las noticias suelen ser las que afectan al entorno de producción en la nube de una empresa (el que utilizan sus clientes), es igual de probable que los delincuentes ataquen su potencia informática (en sus entornos de desarrollo y control de calidad) para realizar actividades como el criptojacking.

Necesita una solución que pueda proteger todos sus entornos (producción, desarrollo y CC) de forma reactiva y proactiva. La solución debe poder procesar sus registros de actividad (por ejemplo, registros de flujo de VPC y registros de CloudTrail) para identificar problemas que ya hayan ocurrido, como cuando hay un puerto abierto en el firewall. Al mismo tiempo, la solución tiene que poder escanear de forma proactiva las plantillas de infraestructura como código (IaC) de sus repositorios como GitHub e integrarse con sus herramientas de canalización de CI/CD como Jenkins. Así se garantiza que las vulnerabilidades introducidas en el código se detectan mucho antes de que se despliegue en los servidores, evitando así titulares desagradables.

Paso 7: Aplique sus conocimientos de seguridad local

Esto puede parecer extraño en una guía de la nube pública, pero la seguridad local es el resultado de décadas de experiencia y de investigación. A la hora de proteger sus servidores basados en la nube contra la infección y la pérdida de datos, piense en lo que ya hace para su infraestructura tradicional y adáptelo a la nube:

- Firewall next-gen: para empezar, evite que las amenazas accedan a sus servidores basados en la nube mediante la instalación de un firewall de aplicaciones web (WAF) en su puerta de enlace en la nube. Trate también de incluir IPS (para ayudar con el cumplimiento) y control de contenido saliente para proteger sus servidores y VDI.
- Protección para servidores: implemente una protección de ciberseguridad eficaz en sus servidores basados en la nube, de la misma forma que lo haría con sus servidores físicos.
- Protección para endpoints: aunque su red puede estar en la nube, sus portátiles y otros dispositivos permanecen en tierra firme, y todo lo que se necesita es un correo electrónico de phishing o spyware para robar las credenciales de usuario de las cuentas en la nube. Asegúrese de mantener actualizada la protección para endpoints y el correo electrónico en sus dispositivos para impedir el acceso no autorizado a las cuentas en la nube.

Presentamos Sophos Cloud Optix:

Véalo todo; protéjalo todo

La visibilidad es la base sobre la que se construyen todas las políticas y actividades de seguridad de la nube pública. Sophos Cloud Optix simplifica la supervisión de varios entornos de proveedores en la nube pública, incluidas las cuentas de Amazon Web Services (AWS), las suscripciones a Microsoft Azure, los proyectos de Google Cloud Platform (GCP), los clústeres de Kubernetes y los repositorios de código de desarrollo. Esta visibilidad superior, dispuesta con controles y alertas de políticas de cumplimiento y de DevSecOps, permite a los equipos tomar el control y desarrollar su estrategia de seguridad en la nube con confianza.

Cloud Optix, un servicio sin agentes basado en SaaS que se integra con las API nativas de los proveedores de la nube pública, crea automáticamente una imagen completa de la arquitectura, incluyendo un inventario completo y una visualización de la topología de red en tiempo real que abarca hosts, redes, cuentas de usuario, servicios de almacenamiento, contenedores y funciones sin servidores.

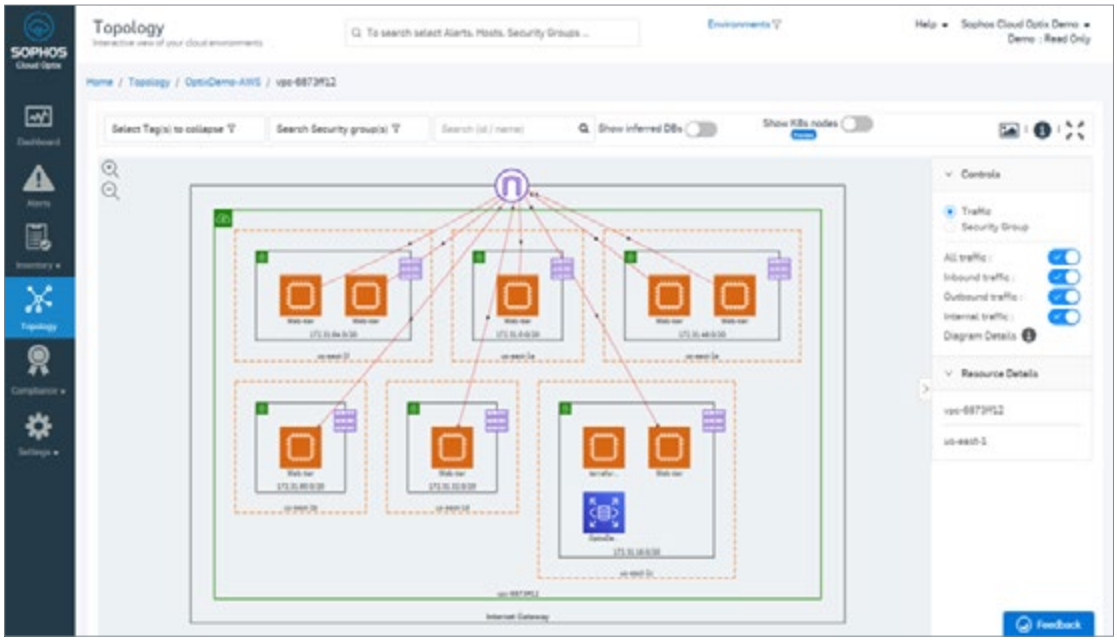

Fig 2. Visualización de la topología de red de Sophos Cloud Optix que muestra el tráfico de entrada, de salida e interno en un entorno AWS.

Más que simples comprobaciones de configuración

Cloud Optix se sirve de la inteligencia artificial del Machine Learning para comprobar si hay anomalías y vulnerabilidades de seguridad en su plataforma. Supervisa el tráfico de red, las configuraciones de recursos, los eventos de inicio de sesión de usuarios y llamadas a la API, el estado de cumplimiento, los repositorios de infraestructura como código (IaaC), etc., además de establecer defensas para corregir automáticamente cambios accidentales o maliciosos en la configuración de la red.

Todo ello mientras las alertas contextuales identifican la causa raíz de los problemas de seguridad y cumplimiento, lo que le permite centrarse en las áreas más críticas que necesitan actualizaciones de seguridad, con una descripción del problema, los pasos de remediación y los recursos afectados.

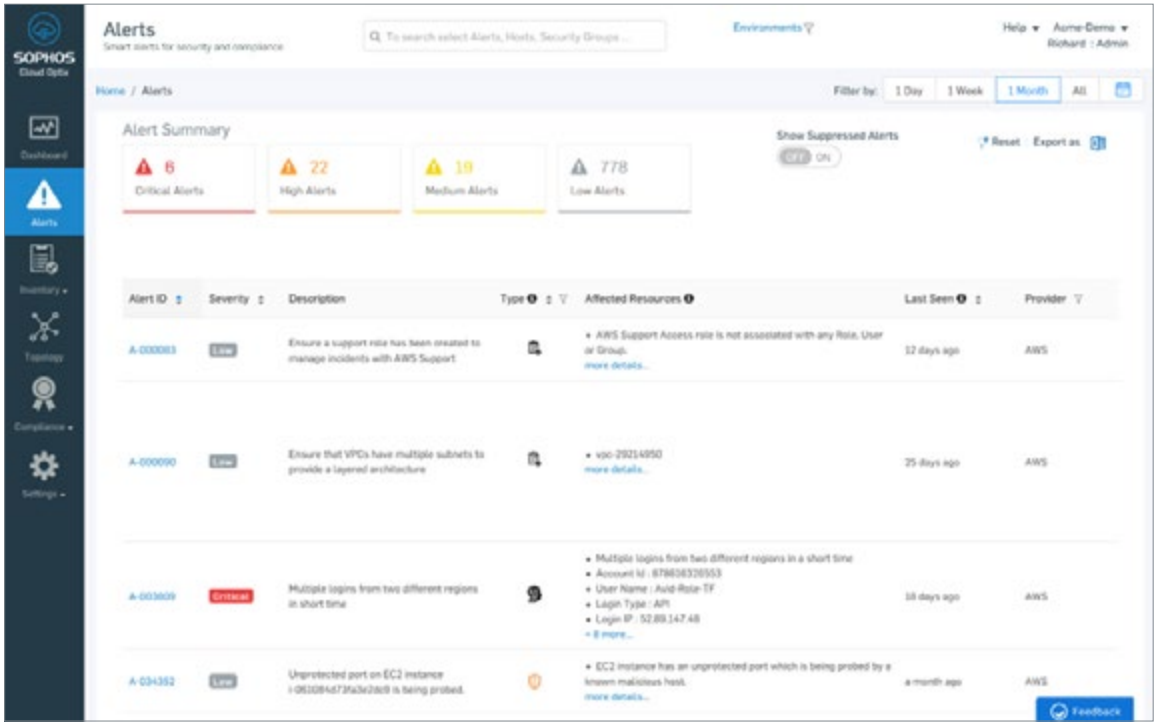

Fig 3. Resumen de alertas de Sophos Cloud Optix que muestra alertas críticas de varios inicios de sesión de cuentas de diferentes regiones al mismo tiempo.

Monitorización y respuesta a su manera

Cloud Optix proporciona una API REST e integración con Splunk, PagerDuty y Amazon GuardDuty para ofrecer información de alertas en tiempo real allá donde la necesite. Gracias a las integraciones incorporadas con Jira y ServiceNow, la información de alertas puede incluso utilizarse para crear incidencias de las que puede realizarse un seguimiento hasta su resolución, lo que garantiza que las tareas importantes nunca se pierdan, incluso durante un lanzamiento.

Al presentarse con paneles de control directos en informes bajo demanda, ahorrará horas o incluso días de esfuerzo a la hora de gestionar su posición en materia de seguridad en la nube, lo que le ayudará a cumplir con los siete pasos más importantes para proteger la nube pública.

Más información

Sophos Cloud Optix es la solución ideal para las empresas que utilizan la nube pública o que se van a trasladar a ella. Al combinar la potencia de la IA y la automatización, proporciona a su empresa la visibilidad continua necesaria para detectar, responder y prevenir vulnerabilidades de seguridad y cumplimiento que podrían dejarle expuesto.

Para obtener más información acerca de Sophos Cloud Optix e iniciar una prueba de 30 días en sus propios entornos en la nube sin compromiso alguno, o bien o empezar una demostración online inmediata, visite es.sophos.com/cloud-optix.

Conclusión

Pasarse de las cargas de trabajo tradicionales a las cargas de trabajo en la nube ofrece enormes oportunidades a empresas de todos los tamaños. Sin embargo, la protección de la nube pública es imprescindible si desea proteger su infraestructura y su empresa de los ciberataques. Si sigue los siete pasos de esta guía, puede maximizar la seguridad de sus nubes públicas, a la vez que simplifica la administración y la generación de informes de cumplimiento.

Modelo de responsabilidad compartida: Cómo puede ayudar Sophos

	Local	Nube pública	¿Por qué?	Contribución de Sophos
Usuarios	■	■	Imponer la autenticación, definir las restricciones de acceso y realizar un seguimiento del uso de las credenciales.	XG Firewall y Sophos UTM imponen la autenticación de entrada/salida con SSO y 2FA y proporcionan informes de acceso detallados. Sophos Cloud Optix realiza un seguimiento del uso compartido o no autorizado de las credenciales de las cuentas.
Datos	■	■	Detener la pérdida de datos; definir e imponer quién puede acceder a qué datos al tiempo que se satisfacen los estándares de cumplimiento.	Sophos Cloud Optix ofrece automatización del cumplimiento de normativas, control y supervisión de la seguridad en la nube, mientras que Sophos Safeguard, DLP y Sophos Mobile ayudan a proteger los datos y a determinar los permisos de acceso.
Aplicaciones	■	■	Evitar que las aplicaciones se vean comprometidas por medio de políticas, parches y seguridad.	La función IPS de XG Firewall y Sophos UTM y las funciones HIPS y Lockdown de Sophos Server Protection protegen contra los ataques de aplicaciones y la exposición involuntaria de aplicaciones.
Control de redes	■	◪	Realizar un seguimiento y aplicar los permisos de acceso a la red.	La interfaz fácil de usar de XG Firewall y Sophos UTM, la inspección detallada de paquetes y la Seguridad Sincronizada (solo XG) ayudan a proteger y administrar el acceso a la red y a hacer cumplir los privilegios de la red.
Infraestructura del host	■	◪	Administrar y proteger los sistemas operativos, las soluciones de almacenamiento y los sistemas relacionados para evitar errores no corregidos y aumentos de privilegios.	Sophos Intercept X protege contra las amenazas de día cero mediante el análisis de técnicas de explotación. La función Lockdown de Sophos Server Protection aplica restricciones en tiempo de ejecución y Sophos XG Sandstorm detiene la proliferación de código desconocido.
Seguridad física	■	■	Limitar el acceso físico a los sistemas y diseñar la redundancia para evitar puntos únicos de error.	Tanto XG Firewall como Sophos UTM disponen de opciones de implementación de alta disponibilidad tanto para dispositivos físicos como para plataformas en la nube.

■ Cliente ■ Proveedor de la plataforma

Fig 4. Cómo ayuda Sophos con el modelo de responsabilidad compartida de la nube pública

"Sophos Cloud Optix pone al alcance de nuestro equipo una visibilidad inteligente y en tiempo real de nuestros entornos AWS y del estado de cumplimiento de la configuración que necesitamos. Esto permite un nivel de monitorización y alertas que antes era imposible en una sola vista. Contar con Sophos Cloud Optix nos da una visión integral de la actividad de la infraestructura y nos permite centrarnos en las protecciones completas".

Ryan Stinson
Director de ingeniería de seguridad
HubSpot Inc.

1 RightScale 2019 State of the Cloud Report de Flexera

2 Fuente de datos del ataque automatizado: Exposed: Cyberattacks on Cloud Honeypots, Matt Boddy, Sophos, abril de 2019

Pruebe Sophos Cloud Optix

es.sophos.com/cloud-optix

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

© Copyright 2019. Sophos Ltd. Todos los derechos reservados.
Constituida en Inglaterra y Gales bajo el número de registro 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido
Sophos es la marca registrada de Sophos Ltd. Todos los demás productos y empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.

19-06-19 WP-ES (RP)

SOPHOS