Guía de seguridad para plataformas cloud

Tabla de contenido

3 Replantear la seguridad para las aplicaciones basadas en la nube
4 Verificar la identidad y gestionar el acceso a las plataformas en la nube
6 Redefinir el aislamiento y la protección de red
7 Proteger los datos con cifrado y gestión de claves
9 Automatizar la seguridad para DevOps
11 Crear un sistema de seguridad inmune mediante la monitorización inteligente
12 Seguridad que fomenta el éxito de la empresa

Mensajes clave

1 En teoría, un proveedor cloud debe poder integrar en su plataforma el sistema de gestión de identidades de la compañía – y, en cualquier caso, proporcionar una solución de gestión de identidades fiable por si su uso es necesario.

2 Uno de los pasos para establecer confianza es verificar que una plataforma en la nube ofrece cortafuegos, grupos de seguridad y opciones bien integradas de microsegmentación basada en cargas de trabajo y hosts de cálculo de confianza.

3 Debe esperar que los proveedores cloud ofrezcan soluciones BYOK que permitan a su organización gestionar claves exclusivamente, en todo el almacenamiento de datos y los servicios.

4 La mejor práctica de seguridad para contenedores es la de explorar en ellos la posible existencia de vulnerabilidades antes del despliegue y mientras se ejecutan.

5 La seguridad de la plataforma en la nube debe controlar de forma eficaz el acceso, operar al nivel de las cargas de trabajo, realizar un seguimiento de la actividad en detalle e integrarse en los sistemas locales.

Replantear la seguridad para las aplicaciones basadas en la nube

A medida que más organizaciones se mueven hacia un modelo nativo cloud para el desarrollo de apps y la gestión de cargas de trabajo, las plataformas de cloud computing limitan rápidamente la eficacia del modelo de seguridad tradicional basado en perímetros. Aunque siga siendo necesaria, la seguridad perimetral es en sí misma insuficiente. Puesto que los datos y aplicaciones de la nube están fuera de los límites de la empresa, deben protegerse de nuevas formas.

Las organizaciones que transitan hacia un modelo nativo cloud o piensan realizar despliegues de aplicaciones de cloud híbrida deben complementar la seguridad de red tradicional basada en perímetros con tecnologías que protejan cargas de trabajo basadas en la nube. Las empresas deben poder tener confianza en cómo un proveedor de servicios cloud asegura su stack desde la infraestructura. Establecer confianza en la seguridad de plataforma se ha convertido en un factor fundamental en la selección de proveedores.

Factores de la seguridad de la nube

La protección de datos y el cumplimiento normativo se encuentran entre los principales factores de la seguridad en la nube – y también son inhibidores de la adopción a cloud. La respuesta a estas preocupaciones se extiende a todos los aspectos del desarrollo y las operaciones. Con las aplicaciones nativas cloud los datos pueden estar dispersos entre almacenes de objetos, servicios de datos y nubes, lo cual crea múltiples frentes para ataques potenciales. Y los ataques no solo proceden de grupos sofisticados y fuentes externas; según una reciente encuesta, el 53 % de los encuestados confirmaron ataques internos en los 12 meses anteriores.[1]

Cinco elementos básicos de la seguridad en la nube

Cuando las organizaciones resuelven las necesidades especiales que plantea el uso de plataformas cloud, necesitan y esperan que los proveedores se conviertan en socios tecnológicos de confianza. De hecho, una organización debe evaluar a los proveedores cloud en función de estos cinco aspectos de la seguridad y su relación con los requisitos específicos propios de la organización:

1. **Gestión de identidad y acceso:** Autenticación y controles de acceso e identidad
2. **Seguridad de red:** Protección, aislamiento y segmentación
3. **Protección de datos:** Cifrado de datos y gestión de claves
4. **Seguridad de aplicación y DevSecOps:** Incluidas las pruebas de seguridad y la seguridad de los contenedores
5. **Visibilidad e inteligencia:** Monitorización y análisis de registros, flujos y eventos para encontrar patrones

Verificar la identidad y gestionar el acceso en las plataformas cloud

Cualquier interacción con una plataforma cloud se inicia con la verificación de la identidad, la determinación de quién o qué está realizando la interacción – un administrador, un usuario o un servicio. En la economía de las API, los servicios se encargan de su propia identidad, por lo que la capacidad para efectuar una llamada API de forma precisa y segura a un servicio basado en esta identidad es esencial para ejecutar satisfactoriamente aplicaciones nativas de nube.

Debe buscar proveedores que ofrezcan una forma consistente de autenticar una identidad para el acceso a las APIs y las llamadas de servicio. También necesita un modo de identificar y autenticar usuarios finales que accedan a aplicaciones alojadas en la nube. Por ejemplo, IBM Cloud utiliza App ID como medio para que los desarrolladores integren la autenticación en sus aplicaciones móviles y web.

Una autenticación fuerte impide que los usuarios no autorizados puedan acceder a los sistemas en la nube. Ya que la gestión de identidad y acceso (IAM) de la plataforma es tan fundamental, las organizaciones que tengan un sistema existente deben esperar que los proveedores cloud integren el sistema de gestión de identidades de sus compañías. Este soporte suele proporcionarse mediante la tecnología de federación de identidades que vincula el ID de una persona y sus atributos entre múltiples sistemas.

¿Por qué autenticar las llamadas de servicio?

En arquitecturas basadas en microservicios, las APIs permiten a las aplicaciones comunicarse y compartir datos. Cuando se ejecuta una aplicación, utiliza APIs para llamar a servicios y poder llevar a cabo varias operaciones. Por ejemplo, la aplicación podría llamar a un servicio de almacén de objetos para pedir datos. Como parte del cumplimiento de la petición, el servicio del almacén de objetos en sí podría llamar, a su vez, a un servicio de gestión de claves para obtener las claves de cifrado necesarias para descifrar los datos. Y como parte de la entrega de su experiencia de usuario, una app podría utilizar APIs para acceder a información de identidad del usuario, publicar contenido entre aplicaciones (como, por ejemplo, publicar contenido desde una app en Twitter) y determinar la ubicación de un usuario para servir información específica de la ubicación. **Todos estos puntos de integración plantean retos de seguridad.**

Los proveedores cloud deben tener una forma consistente de autenticar la identidad de un usuario o servicio que necesita acceder a una API o a un servicio. Evidentemente, como parte de la autenticación, todas las sesiones y transacciones que soliciten acceso deben ser registradas a efectos de auditoría. **Las APIs y los servicios muy probablemente contienen propiedad intelectual valiosa; no querrá que nadie más los utilicen.**

Pida a los proveedores potenciales que demuestre que su arquitectura y sistemas IAM cubren todas las bases. En IBM Cloud, por ejemplo, la gestión de identidad y acceso se basa en varias funcionalidades (Figura 1):

Identidad

- Cada usuario tiene un identificador exclusivo
- Los servicios y aplicaciones se identifican por medio de sus IDs de servicio
- Los recursos se identifican y se direccionan mediante el nombre de recurso cloud (CRN)
- Los usuarios y servicios se autentican y se les emiten tokens con sus identidades

Gestión de acceso

- Cuando los usuarios y servicios intentan acceder a recursos, un sistema IAM determina si dicho acceso y acciones se permiten o se deniegan.
- Los servicios definen acciones, recursos y roles
- Los administradores definen políticas que asignan roles y permisos a varios recursos
- La protección se extiende hasta las APIs, funciones de nube y recursos de back-end alojados en la nube

Cuando evalúe la seguridad de un proveedor cloud, debe buscar las listas de control de accesos junto con los nombres de recursos comunes que le permiten limitar usuarios no solo a ciertos recursos, sino también a ciertas operaciones en dichos recursos. Estas capacidades permiten asegurarse de que los datos están protegidos de accesos no autorizados tanto internos como externos.

La extensión del proveedor de identidad empresarial propio (Enterprise IdP) hasta la nube es particularmente útil cuando se desarrolla una aplicación nativa de nube sobre una aplicación empresarial existente que utiliza el Enterprise IdP. Los usuarios pueden iniciar sesión de forma transparente en las aplicaciones tanto nativas de nube como subyacentes, sin tener que utilizar varios sistemas o IDs. La reducción de la complejidad es siempre un objetivo valioso.

Mensaje clave

En teoría, un proveedor cloud debe poder integrar en su plataforma el sistema de gestión de identidades de la compañía – y, en cualquier caso, proporcionar una solución de gestión de identidades fiable por si su uso es necesario.

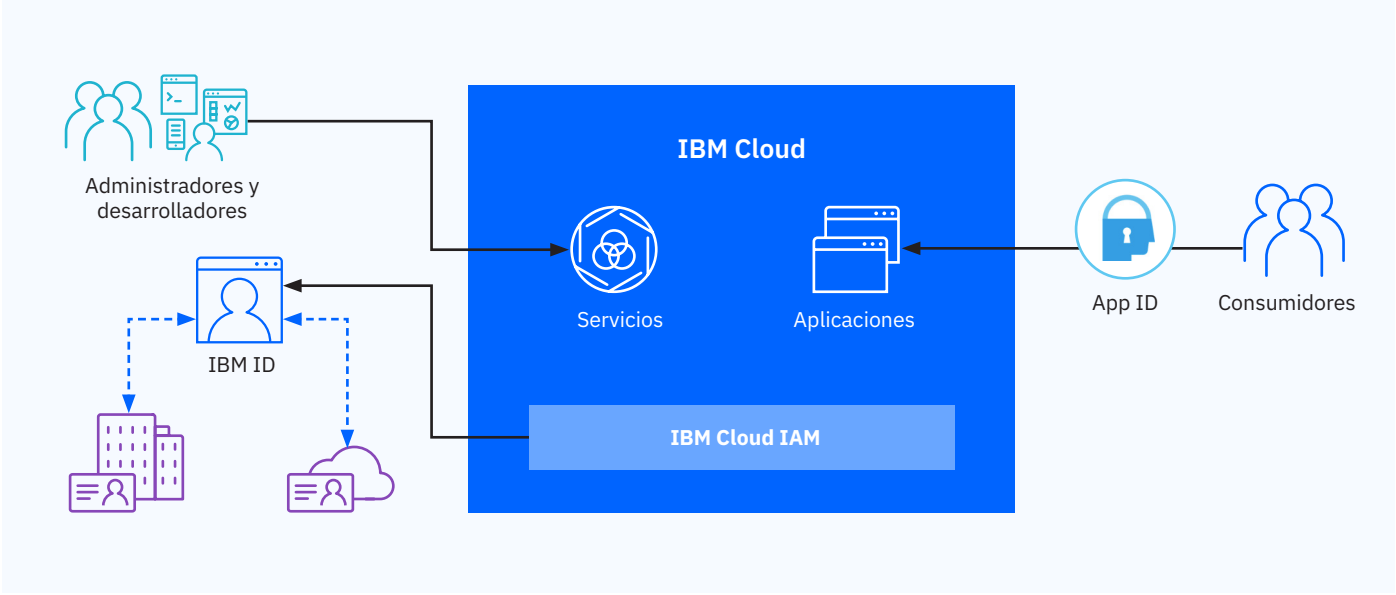


Figura 1. Separación de los elementos de clúster gestionados por el proveedor y gestionados por el cliente.

Redefinir el aislamiento y la protección de red

Muchos proveedores utilizar la segmentación de red para limitar el acceso a dispositivos y servidores de la misma red. Adicionalmente, los proveedores crean redes aisladas virtuales encima de la infraestructura física y limitan automáticamente usuarios o servicios en una red aislada específica. Estas y otras tecnologías básicas de seguridad de red son esenciales para generar confianza en una plataforma en la nube.

Los proveedores de nube ofrecen tecnologías de protección – desde cortafuegos de aplicaciones web hasta redes privadas virtuales y mitigación de denegación de servicio – como servicios para la seguridad de red definida por software y utilizan un modelo de tarifas según uso. Considere las siguientes tecnologías como la seguridad de red crucial en la era del cloud computing.

Grupos de seguridad y cortafuegos

Los clientes de cloud utilizan con frecuencia cortafuegos de red para la protección del perímetro (nube privada virtual / acceso de red a nivel de subred) y crean grupos de seguridad de red para el acceso a nivel de instancia. Los grupos de seguridad son una buena primera línea de defensa para asignar accesos a recursos de la nube. Puede utilizar estos grupos para añadir seguridad de red a nivel de instancia de forma fácil, para gestionar el tráfico entrante y saliente en redes tanto públicas como privadas.

Muchos clientes requieren control perimetral para proteger la red y subredes perimetrales, y los cortafuegos virtuales son una forma fácilmente desplegable para satisfacer esta necesidad. Los cortafuegos se han diseñado para impedir que el tráfico no deseado llegue a los servidores y para reducir la superficie de ataque. Debe esperar que los proveedores de nube ofrezcan cortafuegos tanto virtuales como de hardware que le permitan configurar reglas basadas en permisos para toda la red o sus subredes.

Las redes privadas virtuales (VPN), por supuesto, proporcionan conexiones seguras entre la nube y los recursos locales. Son necesarias si se ejecuta un entorno de nube híbrida.

Microsegmentación

El desarrollo de aplicaciones nativas cloud como un conjunto de servicios pequeños proporciona la ventaja de poder aislarlos por medio de segmentos de red. Debe buscar una plataforma en la nube que implemente microsegmentación mediante la automatización de la configuración de red y aprovisionamiento de red. **Las aplicaciones contenerizadas que se crean en el modelo de microservicios se están convirtiendo rápidamente en la norma para dar soporte al aislamiento de cargas de trabajo a escala.**

Mensaje clave

Uno de los pasos para establecer confianza es verificar que una plataforma en la nube ofrece cortafuegos, grupos de seguridad y opciones bien integradas de microsegmentación basada en cargas de trabajo y hosts de cálculo de confianza.

Proteger los datos con cifrado y gestión de claves

La protección fiable de datos es un elemento básico de seguridad de cualquier empresa digital – especialmente aquellas que pertenecen a sectores muy regulados, tales como los servicios financieros y la sanidad.

Los datos asociados a las aplicaciones nativas de nube pueden estar dispersos entre almacenes de objetos, servicios de datos y nubes. Las aplicaciones tradicionales pueden tener su propia base de datos, su propia máquina virtual (VM) y datos confidenciales almacenados en archivos. En estos casos, el cifrado de los datos confidenciales tanto en reposo como en movimiento es crítico.

Las empresas tienen toda la razón de preocuparse por los operadores de cloud u otros usuarios no autorizados que acceden a sus datos sin su conocimiento, y de esperar una completa visibilidad del acceso a los datos. **El control del acceso a los datos con cifrado y también el control del acceso a las claves de cifrado se están convirtiendo en las protecciones esperadas.** Como resultado, un modelo "bring-your-own-keys" (BYOK), o de uso de claves propias, ya se ha convertido en un requisito de seguridad en la nube. Le permite gestionar claves de cifrado en un lugar centralizado, proporciona la certeza de que las claves raíz nunca salen de los límites del sistema de gestión de claves y le permite auditar todas las actividades del ciclo de vida de la gestión de claves (Figura 2).

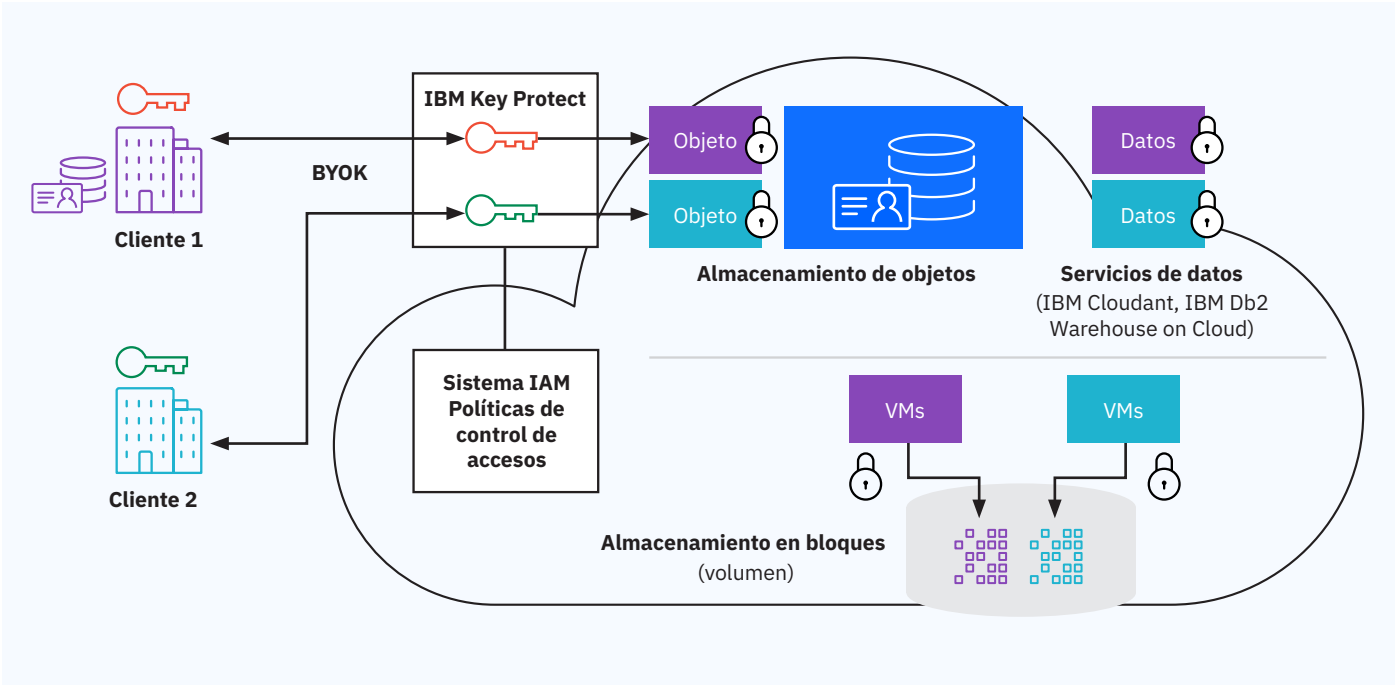
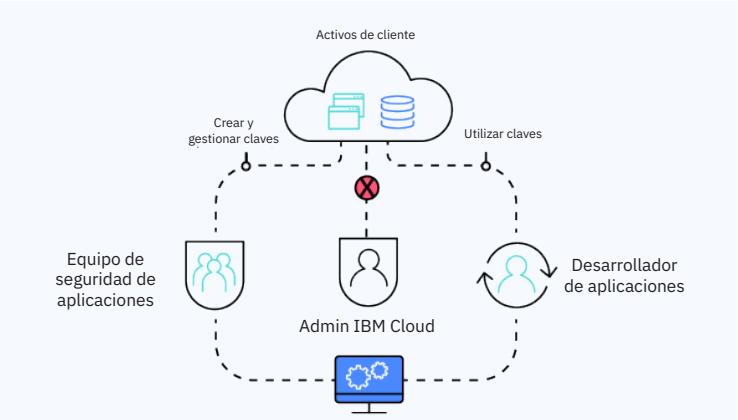


Figura 2. Arquitectura de una solución BYOK.

"Keep your own key" (KYOK)

Para implementar una seguridad de datos que sea 100 % en la nube pública, IBM ofrece en exclusiva una solución que le permite ser el único custodiador de su clave de cifrado. Como el único servicio del mercado basado en hardware certificado por FIPS 140-2 Nivel 4, IBM Cloud Hyper Protect Crypto Services proporciona una gestión de claves y un módulo de seguridad de hardware en la nube (HSM).



Hosts de cálculo de confianza

Todo se reduce al hardware: nadie quiere desplegar datos y aplicaciones valiosas en un host no fiable. Los proveedores de plataformas en la nube que ofrecen hardware con protocolos “medir-verificar-lanzar le ofrecen hosts muy seguros para aplicaciones desplegadas en el sistema de orquestación de contenedores.

Intel Trusted Execution Technology (Intel TXT) y Trusted Platform Module (TPM) son ejemplos de tecnologías a nivel de host que generan confianza en las plataformas de nube. Intel TXT se defiende de los ataques basados en software dirigidos a robar información confidencial mediante la corrupción del sistema o del código BIOS, o mediante la modificación de la configuración de la plataforma. Intel TPM es un dispositivo de seguridad basada en hardware que ayuda a proteger el proceso de arranque del sistema asegurándose de que está libre de manipulaciones indebidas antes de ceder el control del sistema al sistema operativo.

Protección de datos en reposo y en tránsito

El cifrado incorporado con BYOK le permite mantener el control de los datos, estén basados en la nube o sean locales. Es una forma excelente de controlar el acceso a los datos en despliegues de aplicaciones nativas cloud. En este enfoque, el sistema de gestión de claves del cliente genera una clave local y la pasa al servicio de gestión de claves del proveedor. Este enfoque engloba el cifrado de datos en reposo en diferentes tipos de almacenamiento: de bloques, objetos y servicios de datos.

Para los datos en tránsito, la comunicación y transferencia seguras tiene lugar a través de la seguridad de la capa de transporte / Capa de sockets seguros (TLS/SSL). El cifrado TLS/SSL también le permite demostrar el cumplimiento normativo, seguridad y gobierno sin necesidad de un control administrativo del sistema criptográfico o infraestructura. La capacidad para gestionar certificados SSL es un requisito para la confianza en una plataforma cloud.

Satisfacer las necesidades de auditoría y cumplimiento

Proporcionar sus propias claves de cifrado y conservarlas en la nube – sin que el proveedor de servicios pueda acceder a ellas – le ofrece la visibilidad y el control de la información necesarios para las auditorías de cumplimiento CISO.

Mensaje clave

Debe esperar que los proveedores de nube ofrezcan soluciones BYOK que permitan a su organización gestionar claves , en todo el almacenamiento de datos y los servicios.

Automatizar la seguridad para DevOps

Cuando los equipos de DevOps desarrollan servicios nativos cloud y trabajan con tecnologías de contenedores, necesitan poder integrar comprobaciones de seguridad en un pipeline cada vez más automatizado. Dado que sitios como Docker Hub promocionan el intercambio abierto, los desarrolladores pueden ahorrar fácilmente tiempo de preparación de imágenes simplemente descargando lo que necesitan. Pero esta flexibilidad va acompañada de la necesidad de inspeccionar todas las imágenes de contenedor colocadas en un registro, antes de poder ser desplegadas.

Un sistema de exploración automatizado ayuda a asegurar la confianza al buscar vulnerabilidades potenciales en las imágenes antes de empezar a ejecutarlas. Pregunte a los proveedores de plataformas si permiten la creación de políticas (tales como “no desplegar imágenes que tengan vulnerabilidades” o “avisarme antes de desplegar estas imágenes en producción”) como parte de la seguridad del pipeline de DevOps.

IBM Cloud Container Service, por ejemplo, ofrece un sistema Asesor de vulnerabilidades (VA) que ofrece exploraciones de contenedores tanto estáticos como activos. El VA inspecciona todas las capas de cada imagen del registro privado de los clientes de nube para detectar vulnerabilidades o malware antes del despliegue de imágenes. Ya que una simple exploración de imágenes del registro puede no detectar problemas tales como la deriva desde la imagen estática hasta los contenedores desplegados, el VA también explora los contenedores en ejecución. También ofrece recomendaciones en forma de niveles de alertas.

Mensaje clave

La mejor práctica de seguridad para contenedores es la de explorar en ellos la posible existencia de vulnerabilidades antes del despliegue y mientras se ejecutan.

Otras funciones del VA que ayudan a automatizar la seguridad en el pipeline de DevOps son las siguientes:

- **Configuración de la violación de políticas:** Con el VA, los administradores pueden definir políticas de despliegue de imágenes basadas en tres tipos de situaciones de anomalía de imagen: paquetes instalados con vulnerabilidades conocidas; inicios de sesión remotos habilitados; e inicios de sesión remotos habilitados con usuarios que tienen contraseñas fáciles de adivinar.
- **Mejores prácticas:** El VA comprueba 26 reglas basadas en ISO 27000, que incluyen valores como la antigüedad mínima de contraseña y la longitud mínima de contraseña.
- **Detección de configuraciones incorrectas de seguridad:** El VA señala los problemas de configuración incorrecta, proporciona una descripción de la misma y recomienda acciones para remediarlos.
- **Integración con IBM X-Force:** El VA extrae inteligencia de seguridad de fuentes de terceros y utiliza criterios tales como ventores de ataque, complejidad y disponibilidad de una solución conocida para valorar cada vulnerabilidad. El sistema de valoración (crítico, alto, moderado o bajo) ayuda a los administradores a conocer rápidamente la gravedad de las vulnerabilidades y priorizar su corrección.

En el caso de la corrección, el VA no interrumpe las imágenes en ejecución para la aplicación de parches. Al contrario, IBM corrige la imagen “dorada” del registro y despliega una nueva imagen en el contenedor. Este enfoque permite tener la certeza de que todas las instanciaciones futuras de dicha imagen contendrán el mismo arreglo. Las VMs se pueden seguir gestionando de forma tradicional, utilizando un servicio de seguridad de endpoint para parchear VMs y corregir vulnerabilidades de seguridad Linux.

Se habla Kubernetes

Si su equipo de DevOps trabaja con el software de orquestación de contenedores Kubernetes, asegúrese de que pueda seguir utilizando sus herramientas preferidas. Asimismo, evalúe la facilidad con la que una plataforma aprovisiona nuevas imágenes y gestiona los clústeres Kubernetes existentes.

Pregunte si un proveedor de plataformas cloud admite Calico e Istio en su sistema Kubernetes. Calico e Istio son dos componentes importantes de Kubernetes que ayudan en la seguridad de aplicaciones y cargas de trabajo. Calico ayuda a simplificar la gestión de direcciones IP asignadas a las cargas de trabajo de un nodo de cálculo y programa las listas de control de accesos de cada nodo de cálculo para que aplique políticas de seguridad. Por medio de definiciones de políticas configuradas y aplicadas mediante etiquetas de configuración, Istio proporciona un control basado en certificados de la comunicación entre microservicios de un pod o clúster de Kubernetes.

Crear un sistema de seguridad inmune mediante la monitorización inteligente

Cuando se mueven a la nube, muchas veces a los CISOs les preocupa una baja visibilidad y una pérdida del control. Puesto que toda la nube de la organización puede caer si se suprime una clave concreta o un cambio de configuración corta accidentalmente una conexión con los recursos locales o con el centro de operaciones de seguridad (SOC) de una empresa, ¿por qué los ingenieros de operaciones no deben esperar tener plena visibilidad de las cargas de trabajo basadas en nube, APIs, microservicios – todo?

Rastro de accesos y registros de auditoría

Todos los accesos de usuario y administrativos, ya sean del proveedor de nube o de su organización, deben registrarse automáticamente. Un rastreador de actividades de nube incorporado puede crear un rastro de todos los accesos a la plataforma y los servicios, incluidas las APIs, y accesos web y móvil. Su organización debe poder consumir estos registros e integrarlos en el SOC de la empresa.

Inteligencia de seguridad empresarial

Asegúrese de que dispone de la opción de integrar todos los registros y eventos en el sistema de información de seguridad local y de gestión de eventos (SIEM) (Figura 3). Algunos proveedores de servicios cloud también ofrecen la monitorización de la seguridad con gestión e informes de incidencias, análisis en tiempo real de alertas de seguridad y una vista integrada entre despliegues híbridos.

IBM QRadar, por ejemplo, es una completa solución SIEM que ofrece un conjunto de soluciones de inteligencia de seguridad que puede crecer según las necesidades de la organización. Sus capacidades de machine learning se entrenan con patrones de amenazas de modo que crean un sistema inmune de seguridad predictiva.

Seguridad gestionada con experiencia

Si la organización no dispone de una experiencia significativa en seguridad, debe explorar proveedores que puedan gestionarle la seguridad. Algunos proveedores pueden monitorizar las incidencias de seguridad, aplicar inteligencia de amenazas de varios sectores y correlacionar esta información para poder actuar. Pregunte si también pueden ofrecer un cuadro de mandos único que integre servicios de seguridad gestionados e internos.

Mensaje clave

La seguridad de la plataforma cloud debe controlar de forma eficaz el acceso, operar al nivel de las cargas de trabajo, realizar un seguimiento de la actividad en detalle e integrarse en los sistemas locales.

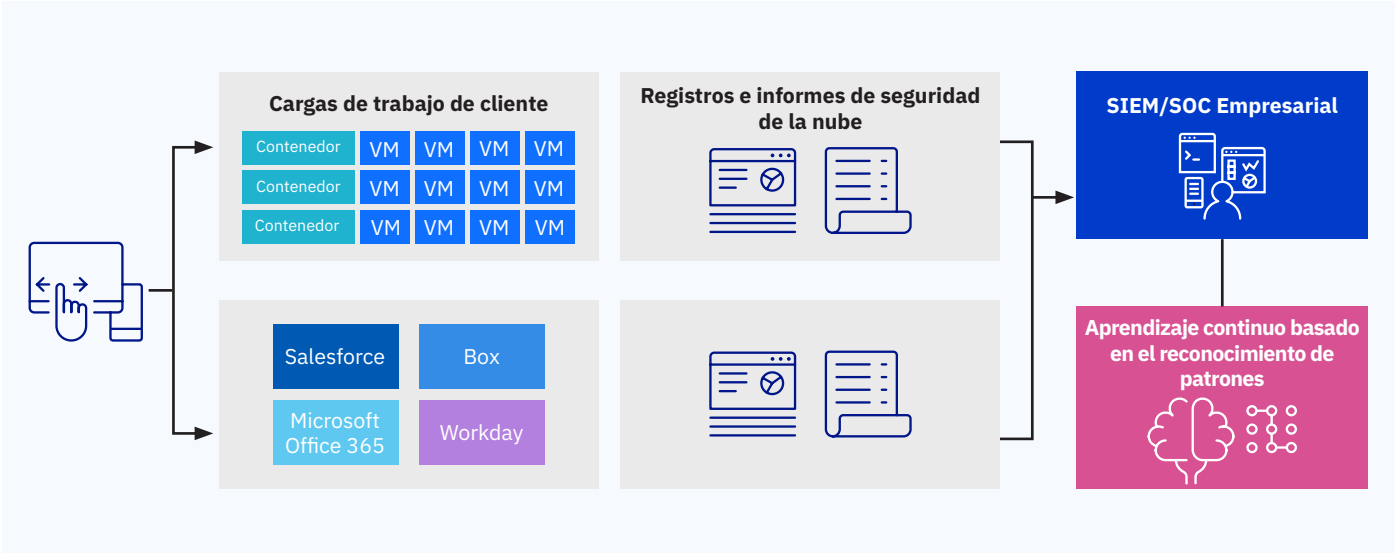


Figura 3. Integración de visibilidad de la nube en un SIEM/SOC empresarial.

Seguridad que fomenta el éxito de la empresa

Para la tecnología cloud, que cada vez es una parte más grande e importante de las operaciones de una empresa digital, es importante buscar un proveedor que ofrezca el conjunto adecuado de capacidades y controles para proteger sus datos, aplicaciones y la infraestructura de nube de la que dependen las aplicaciones presenciales. Debe esperar que la solución de seguridad de la plataforma cubra las cinco áreas de atención más importantes de la seguridad de la nube: identidad y acceso; seguridad de red; protección de datos; seguridad de aplicación; y visibilidad e inteligencia. El objetivo es preocuparse menos por la tecnología y centrarse más en la actividad principal.

Una nube bien protegida proporciona ventajas significativas de negocio y TI, como las siguientes:

- **Menor tiempo de generación de valor:** Dado que la seguridad ya está instalada y configurada, los equipos pueden aprovisionar recursos fácilmente y crear prototipos de experiencias de usuario rápidamente, evaluar resultados e iterar si es necesario.
- **Menor gasto de capital:** El uso de servicios de seguridad en la nube puede eliminar muchos costes iniciales, incluidos los del servidores, licencias de software y dispositivos.
- **Menor carga administrativa:** Al establecer y mantener la confianza en la plataforma de nube, el proveedor con las soluciones de seguridad adecuadas asume la mayor carga administrativa, reduciendo los costes en la creación de informes y mantenimiento de recursos.

Lea Gartner Peer Insights para ver por qué IBM Cloud:

Ha recibido las puntuaciones más altas en integración empresarial (4,6 de 5 estrellas)

Y logra la puntuación global más alta de los proveedores de nube más importantes (4,7 de 5 estrellas)

...basado en **90 análisis realizados en los últimos 12 meses, en fecha de 1 de junio de 2020.**

https://www.gartner.com/reviews/market/public-cloud-iaas/vendor/ibm/product/ibm-cloud

Los análisis de Gartner Peer Insights constituyen las opiniones subjetivas de usuarios finales en base a sus experiencias y no representan las opiniones de Gartner o sus filiales.

Más información

Si desea obtener más información de las cinco áreas clave de la seguridad de nube, así como de tecnologías relacionadas y servicios de IBM, visite: **ibm.com**/cloud/security

Esté conectado

IBM Cloud Blog

Síganos

@IBMcloud
Facebook

Contacte con nosotros

LinkedIn
YouTube

IBM España, S.A
Tel.: +34-91-397-6611
Santa Hortensia, 26-28
28002 Madrid
Spain

La página de inicio de IBM se encuentra en:
ibm.com

[1] Informe Insider Threat 2018t, publicado en noviembre de 2017, http://crowdresearchpartners.com/portfolio/insider-threat-report