IBM **Cloud**

Una guía para asegurar las plataformas de la nube

Tabla de contenido

IBM

Conclusiones claves

1 Idealmente, un proveedor de servicios de la nube debería poder integrar su sistema de gestión de identidad en la plataforma de ellos –y de cualquier modo, proveer una solución de gestión de identidad digna de confianza para que usted la usa según sea necesario.

2 Como parte de establecer la confianza, verifique si una plataforma para la nube ofrece cortafuegos bien integrados, grupos de seguridad, y opciones para la micro-segmentación basada en la carga de trabajo y en ‘hosts’ de computación confiables.

3 Es de esperar que los proveedores de la nube ofrezcan soluciones BYOK que le permitan a su organización gestionar exclusivamente las claves en todos los almacenamientos y servicios de datos.

4 La mejor práctica de seguridad para los contenedores es escanearlos para descubrir vulnerabilidades tanto antes de la implementación como durante su funcionamiento.

5 La seguridad de plataformas en la nube debe ser efectiva para controlar el acceso, operar al nivel de las cargas de trabajo, hacer el seguimiento de la actividad en detalle e integrarse con los sistemas ya instalados.

Repensar la seguridad para las aplicaciones basadas en la nube

A medida que más organizaciones adoptan un modelo nativo en la nube para desarrollar aplicaciones y gestionar cargas de trabajo, las plataformas de computación en la nube está limitando rápidamente la efectividad del tradicional modelo de seguridad basado en el perímetro. Si bien todavía es necesaria, la seguridad perimetral es insuficiente por sí misma. Como los datos y las aplicaciones en la nube están fuera de los antiguos límites empresariales, deben ser protegidos de nuevas maneras.

Las organizaciones que encararon la transición a un modelo nativo en la nube o planean implementaciones de aplicaciones de nube híbrida, deben suplementar la seguridad de red tradicional basada en el perímetro con tecnologías que protejan las cargas de trabajo basadas en la nube. Las empresas deben tener confianza en la manera en que un proveedor de servicios en la nube asegura toda su instalación, desde la infraestructura hacia arriba. El establecimiento de la confianza en la seguridad de la plataforma se ha convertido en un factor fundamental para elegir a un proveedor.

Impulsores de la seguridad en la nube

La protección de los datos y el cumplimiento regulatorio están entre los principales impulsores de la seguridad en la nube –y también resultan inhibidores de la adopción de la nube. Abordar estas preocupaciones se extiende a todos los aspectos de desarrollo y operaciones. Con las aplicaciones nativas de la nube, los datos pueden extenderse a lo largo de tiendas de objetos, servicios de datos y nubes, que crean múltiples frentes para potenciales ataques. Y los ataques ya no provienen solamente de sofisticados delincuentes cibernéticos y fuentes externas; según una encuesta reciente, el 53 por ciento de los entrevistados confirmaron ataques internos en los 12 meses previos.[1]

Cinco principios fundamentales de la seguridad en la nube

A medida que las organizaciones abordan las necesidades especializadas de seguridad que requiere el uso de plataformas en la nube, necesitan y esperan que sus proveedores se conviertan en confiables socios tecnológicos. En realidad, una organización debería evaluar a los proveedores de servicios para la nube basándose en estos cinco aspectos de la seguridad en la medida en que se relacionan con los propios requisitos específicos de la organización.

1. **Gestión de identidades y accesos:** Controles de autentificación, identidad y acceso
2. **Seguridad de la red:** Protección, aislamiento y segmentación
3. **Protección de datos:** Cifrado de datos y gestión de claves
4. **Seguridad de aplicaciones y DevSecOps:** Incluye pruebas de seguridad y seguridad de contenedores
5. **Visibilidad e inteligencia:** Monitorizado y análisis de registros, flujos y sucesos para detectar patrones

Verificar la identidad y gestionar el acceso sobre una plataforma de la nube

Cualquier interacción con una plataforma en la nube comienza con la verificación de identidad, para establecer quién o qué está haciendo la interacción –un administrador, un usuario o incluso un servicio. En la economía de las API, los servicios toman su propia identidad, así que la capacidad de hacer que, de manera exacta y segura, una API llame a un servicio con base en esta identidad, es esencial para ejecutar con éxito las aplicaciones nativas de la nube.

Busque proveedores que ofrezcan una manera sistemática de autentificar una identidad para el acceso a API y llamadas de servicio. También necesita una manera de identificar y autentificar a los usuarios finales que acceden a aplicaciones alojadas en la nube. Como ejemplo, IBM® Cloud usa App ID como una manera de que los desarrolladores integren la autentificación en sus aplicaciones móviles y de la red.

Una autentificación sólida impide que los usuarios no autorizados tengan acceso a los sistemas en la nube. Como la gestión de identidad y acceso (IAM) en la plataforma es tan fundamental, las organizaciones que tienen un sistema existente deberían esperar que los proveedores de servicios en la nube integren los sistemas de gestión de identidad de sus compañías. Esto es a menudo soportado a través de una tecnología de federación de identidad que vincula la ID y los atributos de una persona en múltiples sistemas.

¿Por qué autentificar las llamadas de servicio?

En las arquitecturas basadas en microservicios, las API habilitan aplicaciones para comunicar y compartir datos. Cuando una aplicación es ejecutada, la misma usa las API para convocar los servicios necesarios para completar distintas operaciones. Por ejemplo, su aplicación podría convocar a un servicio de tienda de objetos para obtener datos. Como parte de satisfacer el pedido, el mismo servicio de tienda de objetos podría entonces llamar a un servicio de gestión de claves para obtener las claves cifradas necesarias para descifrar los datos. Y como parte de la entrega de su experiencia de usuario, una aplicación podría usar las API para acceder a la información sobre la identidad del usuario, publicar contenido entre una aplicación y otra (tal como publicar contenido de una aplicación en Twitter), y determinar la ubicación de un usuario para brindar inrformación específica de la ubicación. **Todos estos puntos de integración plantean retos de seguridad.**

Los proveedores de servicios en la nube deberían tener un método sistemático de autentificar la identidad de un usuario o un servicio que necesita acceder a una API o a un servicio. Desde luego, como parte de la autentificación, todas las sesiones y transacciones de pedido de acceso deberían registrarse para los propósitos de auditoría. **Es muy probable que las API y los servicios contengan valiosa propiedad intelectual; usted no querrá que puedan ser usados por cualquiera.**

Pida a los posibles proveedores de servicios en la nube que demuestren que su arquitectura y sistemas IAM cubren todos los aspectos anteriores. In IBM Cloud, por ejemplo, la gestión de identidad y acceso se basa en varias características clave (Figura 1):

Identidad

- Cada usuario tiene un identificador único
- Los servicios y las aplicaciones se identifican por sus identificaciones (ID) de servicio
- Los recursos se identifican y se direccionan por el nombre del recurso en la nube (CRN)
- Los usuarios y servicios son autentificados y se les emiten 'tokens' con sus identidades

Gestión de accesos

- Cuando los usuarios y los servicios intentan tener acceso a los recursos, un sistema IAM determina si el acceso o las acciones se permiten o se niegan
- Los servicios definen acciones, recursos y roles
- Los administradores definen las políticas que asignan a los usuarios los roles y permisos para varios recursos
- La protección se extiende a las API, funciones de la nube y recursos indirectos (back-end) alojados en la nube

Cuando evalúe la seguridad de un proveedor de servicios en la nube, busque las listas de control de acceso junto con nombres de recursos comunes que le habiliten a usted la posibilidad de limitar el acceso de los usuarios no solo a ciertos recursos, sino también a ciertas operaciones en esos recursos. Estas capacidades contribuyen a asegurar que su información estará protegida contra acceso no autorizado externo e interno.

La extensión de su propio Proveedor de Identidad Empresarial (Enterprise IdP) a la nube es particularmente útil cuando usted construye una aplicación nativa de la nube sobre una aplicación empresarial existente que usa el Enterprise IdP. Sus usuarios podrán así iniciar sesión sin problemas tanto en la aplicación nativa de la nube como en la subyacente, sin tener que usar múltiples sistemas o ID. Reducir la complejidad siempre es una meta que vale la pena alcanzar.

Conclusión clave

Idealmente, un proveedor de servicios de la nube debería poder integrar su sistema de gestión de identidad en la plataforma de ellos – y de cualquier modo, proveer una solución de gestión de identidad digna de confianza para que usted la use según sea necesario.

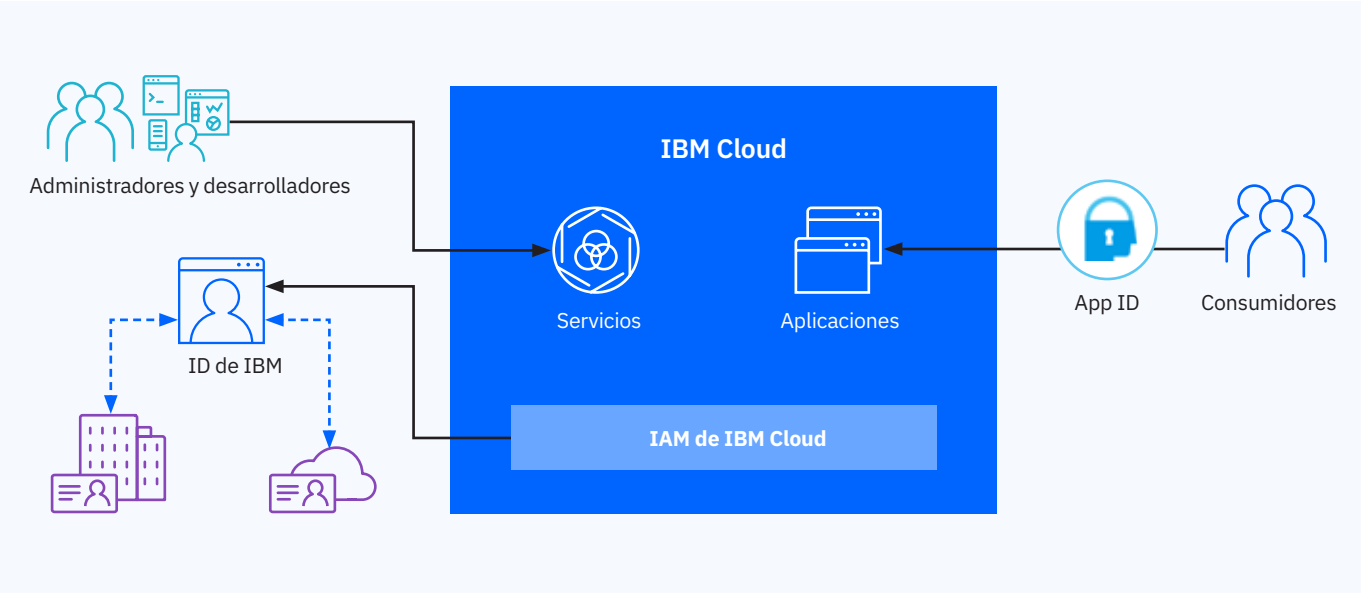

Figura 1. Separación de elementos de clúster gestionados por el proveedor y por el cliente.

Redefinir el aislamiento y la protección de las redes

Muchos proveedores de servicios en la nube usan la segmentación de redes para limitar el acceso a dispositivos y servidores en la misma red. Además, los proveedores crean redes virtuales aisladas sobre la infraestructura física y limitan automáticamente a los usuarios o servicios a una red aislada específica. Esta y otras tecnologías básicas de seguridad de redes son apuestas mínimas para establecer confianza en una plataforma de la nube.

Los proveedores de servicios en la nube ofrecen tecnologías de protección –desde cortafuegos de aplicaciones en la red hasta redes virtuales privadas y mitigación de denegación de servicio– como servicios para seguridad en la red definida por software y cargos por uso. Considere las tecnologías siguientes como seguridad crucial de red en la era de la computación en la nube.

Grupos de seguridad y cortafuegos

Los clientes de la nube a menudo insertan cortafuegos de red para la protección perimetral (acceso a nube privada virtual/nivel sub-red de red) y crean grupos de seguridad de red para acceso a nivel de instancia. Los grupos de seguridad son una buena primera línea de defensa para asignar acceso a los recursos en la nube. Estos grupos se pueden usar para agregar fácilmente seguridad de red a nivel de instancia con el fin de gestionar tráfico entrante o saliente tanto en redes públicas como privadas.

Muchos clientes requieren el control perimetral para asegurar la red y subredes perimetrales, y los cortafuegos virtuales son un elemento fácil de implementar para satisfacer esta necesidad. Los cortafuegos se diseñan para evitar que el tráfico no deseado llegue a los servidores y para reducir la superficie de ataque. Usted debería esperar que los proveedores de servicios en la nube le ofrezcan cortafuegos tanto virtuales como de hardware que le permitan configurar reglas basadas en permisos para toda la red o para las subredes.

Desde luego, las VPN, proporcionan conexiones seguras desde la nube hasta sus recursos instalados en su sede. Son obligatorios si está manejando un entorno de nube híbrida.

Micro-segmentación

El desarrollo de aplicaciones nativas en la nube como un conjunto de pequeños servicios, le permite disponer de la ventaja de seguridad de poder aislarlos mediante la segmentación de la red. Debe buscar una plataforma en la nube que implemente la micro-segmentación a través de la automatización de la configuración de redes y el aprovisionamiento de redes. **Las aplicaciones incluidas en contenedores basadas en el modelo de microservicios se están convirtiendo en una norma para soportar el creciente aislamiento de cargas de trabajo.**

Conclusión clave

Como parte de establecer la confianza, verifique si una plataforma para la nube ofrece cortafuegos bien integrados, grupos de seguridad, y opciones para la micro-segmentación basada en la carga de trabajo y en ‘hosts’ de computación confiables.

Proteger los datos con el cifrado y la gestión de claves.

La protección confiable de la información es un fundamento básico para cualquier empresa digital – especialmente las pertenecientes a sectores altamente regulados tales como los servicios financieros y el cuidado de la salud.

La información asociada con aplicaciones nativas de la nube puede diseminarse a través de tiendas de objetos, servicios de datos y nubes. Las aplicaciones tradicionales pueden tener su propia base de datos, su propia VM e información sensible ubicadas en archivos. En estos casos, se hace crítico el cifrado de la información sensible tanto en reposo como en movimiento.

Las empresas hacen bien en preocuparse por el hecho de que los operadores de la nube u otros usuarios no autorizados tengan acceso a su información sin su conocimiento, y también en esperar disponer de completa visibilidad sobre el acceso a la información. **El control del acceso a la información mediante el cifrado y también el control del acceso a las claves de cifrado, se están convirtiendo en salvaguardas esperadas.** El resultado es que el modelo 'traiga sus propias claves' (BYOK) es ahora un requisito de seguridad en la nube. Le permitirá a usted gestionar las claves de cifrado en un lugar central, la asegurará que las claves raíces nunca dejarán los límites del sistema de gestión de claves y le permitirá auditar todas las actividades del ciclo vital de gestión de claves (Figura 2).

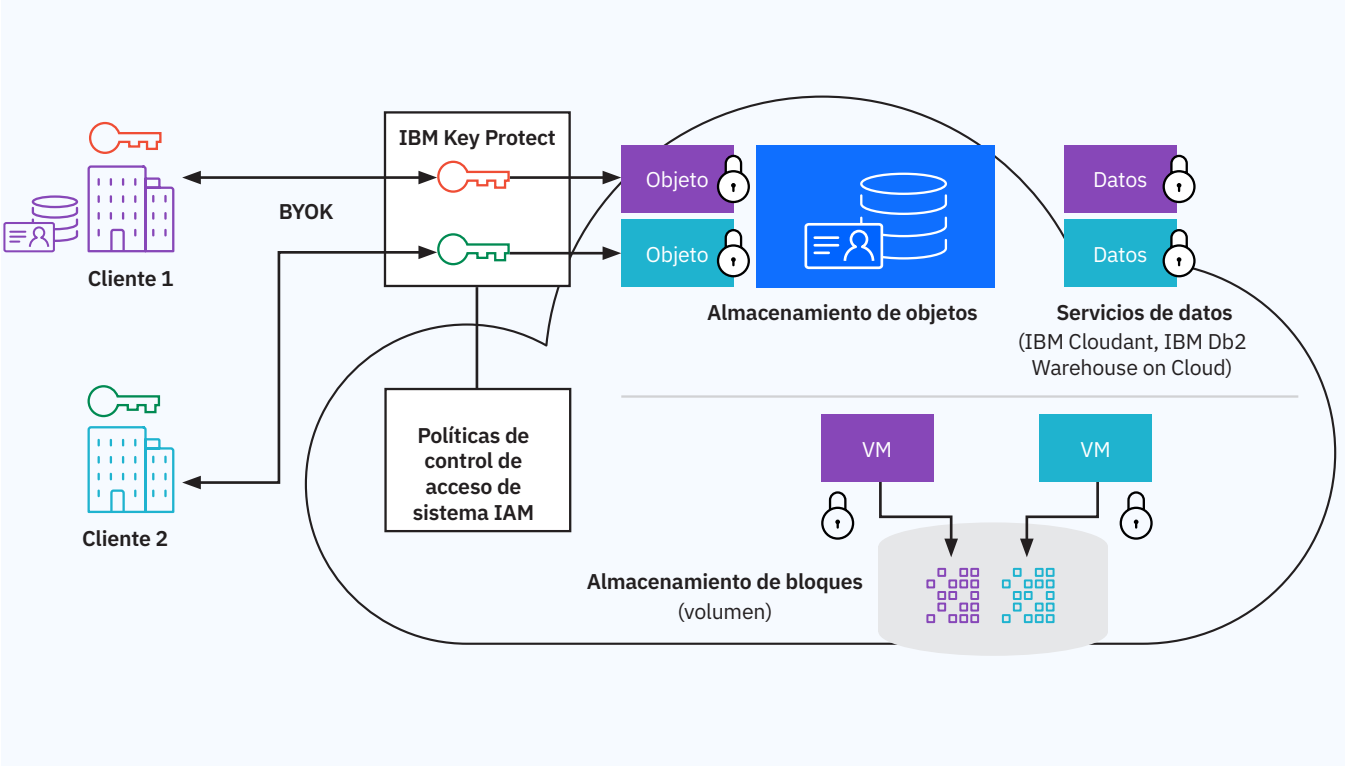

Figura 2. Arquitectura de una solución BYOK.

“Hosts” (alojamientos) de computación confiables

Se reduce al hardware: nadie desea implementar información y aplicaciones valiosas en un “host” no confiable. Los proveedores de plataformas en la nube que ofrecen hardware con protocolos medir-verificar-lanzar, le proporcionarán “hosts” seguros para aplicaciones implementadas dentro del 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 habilitan la confianza en las plataformas de la nube. Intel TXT defiende contra ataques basados en software, como los dirigidos a robar información sensible corrompiendo el código del sistema o del BIOS, o los que tratan de modificar la configuración de la plataforma. Intel TPM es un dispositivo de seguridad basado en hardware que ayuda a proteger el proceso de arranque del sistema al asegurar que está libre de alteraciones antes de liberar el control del sistema al sistema operativo.

Protección de datos en reposo y en tránsito

El cifrado incorporado con BYOK le permitirá mantener el control de sus datos, ya sea que estén basados en su sede o en la nube. Es una manera excelente de controlar el acceso a los datos en implementaciones de aplicaciones nativas de la nube. Con este enfoque, el sistema de gestión de claves del cliente genera una clave en la sede y la pasa al servicio de gestión de claves del proveedor. Este enfoque abarque el cifrado de datos en reposo en todos los tipos de almacenamiento, tales como de bloques, de objetos y servicios de datos.

Para los datos en tránsito, la comunicación y transferencia seguras se realizan mediante Transport Layer Security/Secure Sockets Layer (TLS/SSL). El cifrado TLS/SSL también le permitirá a usted demostrar el cumplimiento, la seguridad y la gobernanza sin requerir el control administrativo del sistema de cifrado o la infraestructura. La capacidad de gestionar certificados SSL es un requisito necesario para confiar en una plataforma para la nube.

Satisfacer las necesidades de auditoría y cumplimiento

La provisión de sus propias claves de cifrado y su almacenamiento en la nube –sin acceso del proveedor del servicio– le da a usted la visibilidad y el control de la información requeridos para las auditorías de cumplimiento de CISO.

Conclusión clave

Es de esperar que los proveedores de la nube ofrezcan soluciones BYOK que le permitan a su organización gestionar exclusivamente las claves en todos los almacenamientos y servicios de datos.

Automatizar la seguridad para DevOps (Operaciones de desarrollo)

A medida que los equipos de DevOps construyen servicios nativos de la nube y trabajan con tecnologías de contenedores, necesitan una manera de integrar las comprobaciones de seguridad dentro de un flujo de procesos cada vez más automatizado. Ya que los sitios como Docker Hub promueven el intercambio abierto, los desarrolladores pueden ahorrar el tiempo que insume la preparación de imágenes, simplemente descargando lo que necesitan. Pero esa flexibilidad requiere inspeccionar rutinariamente todas las imágenes del contenedor ubicadas en un registro antes de que sean implementadas.

Un sistema de escaneado automático ayuda a garantizar la confianza al buscar posibles vulnerabilidades en sus imágenes antes de que comience a ejecutarlas. Consulte a los proveedores de plataformas si le permitirán a su organización crear políticas (tales como “no implementar imágenes que tengan vulnerabilidades” o “advertirme antes de implementar estas imágenes en producción”) como parte de la seguridad del flujo de procesos de DevOps.

Por ejemplo, IBM Cloud Container Service, ofrece un sistema denominado Vulnerability Advisor (VS), que provee escaneado de contenedores estáticos y vivos. VA inspecciona cada capa de cada imagen en un registro privado del cliente de la nube para detectar vulnerabilidades o ‘malware’ antes de implementar una imagen. Como el simple escaneo de imágenes en un registro pueden pasar por alto problemas tales como la deriva de la imagen estática a los contenedores implementados, VA también escanea los contenedores que se ejecutan para detectar anomalías. También proporciona recomendaciones en forma de alertas de distintos niveles.

Conclusión clave

La mejor práctica de seguridad para los contenedores es escanearlos para descubrir vulnerabilidades tanto antes de la implementación como durante su funcionamiento.

Otras características de VA que ayudan a automatizar la seguridad en el flujo de proceso de DevOps son:

- **Configuración contra violación de políticas:** Con VA, los administradores pueden establecer políticas para la implementación de imágenes basadas en tres tipos de situaciones de fallas de imagen: paquetes instalados con vulnerabilidades conocidas; habilitación de inicios de sesión a distancia; y habilitación de inicios de sesión a distancia con algunos usuarios que tengan contraseñas fáciles de adivinar.
- **Las mejores prácticas:** VA verifica corrientemente 26 reglas basadas en ISO 27000, incluso configuraciones tales como edad mínima de la contraseña y longitud mínima de la contraseña.
- **Detección de configuración errónea de seguridad:** VA alerta cada problema de configuración errónea, proporciona una descripción del mismo y recomienda un curso de acción para solucionarlo.
- **Integración con IBM X-Force®:** VA toma inteligencia de seguridad de cinco fuentes de terceros y usa criterios tales como vector de ataque, complejidad y disponibilidad de una solución conocida para clasificar cada vulnerabilidad. El sistema de clasificación (crítica, alta, moderada o baja) ayuda a los administradores a entender rápidamente la severidad de las vulnerabilidades y a priorizar la solución.

Cuando se procede a la solución, VA no interrumpe las imágenes que se ejecutan para aplicar un parche. En cambio, IBM soluciona la imagen "dorada" en el registro e implementa una nueva imagen en el contenedor. Este enfoque ayuda a asegurar que todas las instanciaciones futuras de esa imagen tendrán aplicada la solución. Las VM también se pueden manejar de la manera tradicional, recurriendo a un servicio de seguridad de punto final para aplicar un parche a las VM y solucionar las vulnerabilidad de seguridad de Linux.

Aquí se habla "Kubernetes"

Si sus equipos de DevOps trabajan con el popular software "Kubernetes" de orquestación de contenedores, asegúrese de que puedan continuar usando sus herramientas preferidas. Además, evalúe la facilidad con la que una plataforma aprovisiona nuevos clústeres de "Kubernetes" y gestiona los existentes.

Pregunte si un proveedor de plataforma en la nube admite Calico e Istio con su sistema de "Kubernetes". Calico e Istio son dos componentes importantes de "Kubernetes" que contribuyen a la seguridad de las aplicaciones y cargas de trabajo. Calico ayuda a simplificar la gestión de las direcciones de IP asignadas a las cargas de trabajo en un nodo de computación y programa las listas de control de accesos en cada nodo de computación para imponer las políticas de seguridad. Mediante el establecimiento de definiciones de políticas y su imposición a través de etiquetas de configuración, Istio proporciona el control de la comunicación, basado en certificados, entre los microservicios dentro de un "pod" o clúster de Kubernetes.

Crear un sistema de seguridad inmune a través del monitoreo inteligente

Cuando se concreta la transición a la nube, los CISO a menudo se preocupan por la baja visibilidad y la pérdida de control. Como toda la nube de la organización puede colapsar si una clave en particular es eliminada o un cambio de configuración corta inadvertidamente una conexión con los recursos instalados en la sede o con un centro de operaciones de seguridad de la empresa (SOC), ¿por qué razón los ingenieros de operaciones no deberían esperar disponer de plena visibilidad de las cargas de trabajo basadas en la nube, API, microservicios –y de todo?

Rastros de acceso y registros de auditorías

Todos los accesos administrativos y de usuarios, ya sean del proveedor de la nube o de su organización, deberían registrarse automáticamente. Un seguidor de actividad en la nube incorporado puede crear un rastro de todos los accesos a la plataforma y los servicios, incluyendo los accesos a API, red y móviles. Su organización debería poder consumir estos registros e integrarlos en el SOC de su empresa.

Inteligencia de seguridad empresarial

Asegúrese de que tiene la opción de integrar todos los registros y eventos en el sistema de información de seguridad y gestión de eventos (SIEM) de su sede (Figura 3). Algunos proveedores de servicios en la nube también ofrecen monitoreo de seguridad con gestión e informes de incidentes, análisis en tiempo real de alertas de seguridad y una visión integrada sobre todas las implementaciones híbridas.

Por ejemplo, IBM QRadar®, es una solución SIEM total que ofrece un conjunto de soluciones de inteligencia de seguridad que pueden crecer al ritmo de las necesidades de una organización. Sus capacidades de aprendizaje en la máquina se entrenan sobre patrones de amenazas de una manera que construye un sistema inmune de seguridad predictivo.

Seguridad gestionada con idoneidad

Si su organización no tiene una significativa idoneidad sobre seguridad, busque a proveedores que puedan gestionar la seguridad para usted. Algunos proveedores pueden monitorizar sus incidentes de seguridad, aplicar inteligencia de amenazas de una variedad de sectores y correlacionar esta información para tomar medidas. Pregúnteles si también pueden entregar un único panel de vidrio que integre servicios de seguridad en la sede y gestionados.

Conclusión clave

La seguridad de plataformas en la nube debe ser efectiva para controlar el acceso, operar al nivel de las cargas de trabajo, hacer el seguimiento de la actividad en detalle e integrarse con los sistemas ya instalados.

Figura 3. Integrar la visibilidad de la nube en un SIEM/SOC de empresa.

Seguridad que promueve el éxito de las empresas

Como la tecnología de la nube se está convirtiendo en una parte más grande y más importante de la operación de una empresa digital, realmente vale la pena buscar un proveedor de servicios en la nube que ofrezca el conjunto adecuado de capacidades y controles para proteger su información, aplicaciones y la infraestructura de la nube de la cual dependen las aplicaciones de cara al cliente. La solución de seguridad de la plataforma debería cubrir las cinco áreas clave de enfoque de seguridad en la nube: identidad y acceso, seguridad de la red, protección de datos, seguridad de aplicaciones y visibilidad e inteligencia. La meta es preocuparse menos por la tecnología y enfocarse más en su negocio esencial.

Una nube bien protegida brinda significativas ventajas comerciales y de TI, como:

- **Menor tiempo hasta llegar a la rentabilidad:** Como la seguridad ya está instalada y configurada, los equipos pueden aprovisionar recursos fácilmente y hacer prototipos rápidamente de las experiencias de los usuarios, evaluar resultados y replicar según sea necesario.
- **Menor inversión de capital:** El uso de servicios de seguridad en la nube puede eliminar muchos costos iniciales, entre los que se incluyen servidores, licencias de software y aplicaciones.
- **Menor carga administrativa:** Al establecer y mantener exitosamente la confianza en la plataforma de la nube, el proveedor con las prestaciones correctas de seguridad asume la mayor carga de administración, reduciendo los costes de su empresa relacionados con informes y mantenimiento de recursos.

Para obtener más información

Para más información sobre las cinco áreas clave de la seguridad en la nube y las tecnologías y servicios IBM relacionados, visite: ibm.com/cloud/security

Permanezca conectado.

Blog de IBM Cloud

Síganos en

@IBMcloud
Facebook

Póngase en contacto

LinkedIn
YouTube

IBM Corporation
1 New Orchard Road
Armonk,
NY 10504-1722

Creado en los Estados Unidos de América en enero de 2018

[1] Informe sobre amenazas internas 2018, publicado en noviembre de 2017, http://crowdresearchpartners.com/portfolio/insider-threat-report