IBM **Cloud**

Proteger la plataforma de contenedores

Construir una cadena de confianza

IBM

El desafío DevOps: Innovar de forma segura con velocidad

Para apoyar los objetivos de negocios en los mercados altamente competitivos, los ejecutivos de desarrollo de aplicaciones y sus equipos deben entregar experiencias del cliente de alta calidad a través de dispositivos a un ritmo acelerado. Como resultado, los equipos de DevOps cada vez en mayor medida usan plataformas de la nube basadas en contenedores con métodos de colaboración ágil y una cadena de herramientas para maximizar la automatización en el proceso de crear e iterar aplicaciones nativas de la nube como microservicios independientes pero interoperables.

Aunque establecer y mantener una seguridad excelente puede crear tensión al trasladarse a un escenario de DevOps basado en la nube, definitivamente, no se puede ignorar la seguridad. La mayoría de las plataformas de la nube usan Docker para contenedores, por ejemplo, y los contenedores se ejecutan en un kernel Linux compartido, heredando así sus desafíos de seguridad. El software de contenedores no autorizado y no detectado, descargado desde un intercambio comunitario, que obtiene un escalamiento privilegiado en el kernel Linux de un host podría comenzar a exfiltrar datos o extenderse para causar daños mediante ataques por denegación de servicio (DoS). Los contenedores también pueden interferir con otros contenedores porque todos comparten acceso a recursos como canales, bibliotecas y binarios.

Dado el aumento de la adopción del modelo “Trae tu propio dispositivo” (BYOD), muchas organizaciones también han perdido el control de los puntos de conexión corporativos, con lo que se ha debilitado el perímetro de la empresa tradicional. Ahora la seguridad debe ir donde va la carga de trabajo mientras esta se desplaza a través del centro de datos y la nube.

Aunque la cadena de ataques —intrusión, bloqueo, expansión, recopilación, exfiltración— sigue siendo la misma, el ingenio de los atacantes es ilimitado. Los titulares frecuentes sobre filtraciones catastróficas reflejan que el panorama general sobre seguridad sigue cambiando:

- Los atacantes han comprendido que el cibercrimen compensa, lo que ha originado un aumento en las amenazas avanzadas persistentes y en otro malware de rápida mutación.
- Las naciones estados se han vuelto más sofisticadas en sus capacidades para la guerra informática. En muchas naciones estados, los atacantes han utilizado recursos estatales para desarrollar herramientas sofisticadas que usan clandestinamente para ganar mucho más dinero que con sus trabajos regulares.

Los desafíos fundamentales para proteger una plataforma en la nube, por cierto, pueden quitar el sueño a un director de seguridad. El objetivo de un CISO (Director de Seguridad Informática) es definir el marco de seguridad y requisitos de la organización para minimizar el riesgo y satisfacer el cumplimiento de las regulaciones. Las implementaciones deben ser auditables.

Estos requisitos pueden producir conflictos entre el CISO y el ejecutivo de AppDev, el cual necesita una solución de seguridad que proporcione automatización siempre que sea posible y que se integre de manera flexible a las canalizaciones y los procesos de DevOps (si es que no puede ser completamente invisible).

¿Cómo una plataforma en la nube puede satisfacer de manera eficiente y eficaz las importantes y antagónicas necesidades de los principales interesados?

Crear una cadena de confianza

La solución es crear una cadena de confianza liberada por hardware que verifique la integridad de cada componente correspondiente en la plataforma de la nube. **Una verdadera cadena de confianza comenzaría en el firmware del chip del host y se desarrollaría a través del sistema de orquestación y motor del contenedor, protegiendo así todas las cargas de trabajo y datos críticos durante el ciclo de vida de una aplicación.** El resultado sería un sistema de contenedores confiable y altamente automatizado.

El hardware es la base ideal porque se basa en silicio, por lo cual es difícil que los hackers lo alteren. La cadena de confianza se debe partir de esta base usando el modelo de seguridad de medir y verificar, en el cual cada componente mide, verifica e inicia el siguiente nivel. Este proceso se extendería al motor del contenedor, creando un límite de confianza, con mediciones almacenadas en un Módulo de Plataforma Confiable (TPM) en el host. Un software de certificación en un servidor diferente verificaría las mediciones actuales con respecto a valores correctos conocidos. El orquestador de contenedores se comunicaría con el servidor de certificación para verificar la integridad de hosts de trabajador y cualquier imagen de contenedor implementada en estos.

Conclusión principal

Asegúrese de que la plataforma de la nube admita un límite de confianza administrado por política, lo que es vital para automatizar la seguridad.

La Figura 1 representa una cadena de confianza, basada en el hardware, que estaría involucrada al agregar un nuevo trabajador a un clúster Kubernetes. Los números de la ilustración corresponden a los pasos 1 al 6 aquí descritos. Tenga presente que para verificar una medición en el host de arranque se requiere una comparación con un elemento conocido almacenado en un servidor de atestación separado.

1. En el host de trabajador, el hardware de TPM autentica el firmware del sistema, midiendo y verificando el BIOS, incluidas las ROM opcionales. Luego este inicia el BIOS.
2. El BIOS mide, verifica e inicia el sistema operativo (SO).
3. El SO mide, verifica e inicia el tiempo de ejecución del contenedor Docker, los complementos Docker y todos los componentes clave que forman parte de una base informática de confianza (TCB).
4. Con un complemento Cloud Integrity Technology (CIT), el Kubernetes maestro verifica el host de trabajador a través del servidor de certificación. La certificación también podría incluir verificar información de ubicación geográfica/límite para el clúster Kubernetes, como bloquear el uso de un trabajador cuya ubicación geográfica no es adecuada.
5. El Kubernetes maestro configura el host atestado válidamente como parte del clúster existente, que incluye asignarle contenedores.
6. El motor Docker en el host de trabajador, comunicándose a través de una conexión cifrada con el servidor de certificación, verificaría la integridad de las imágenes del contenedor y las comprobaría según una política de seguridad.

Dado que depende de políticas de seguridad, la plataforma completa de contenedores automáticamente solo ejecuta hosts y contenedores en estados correctos conocidos.

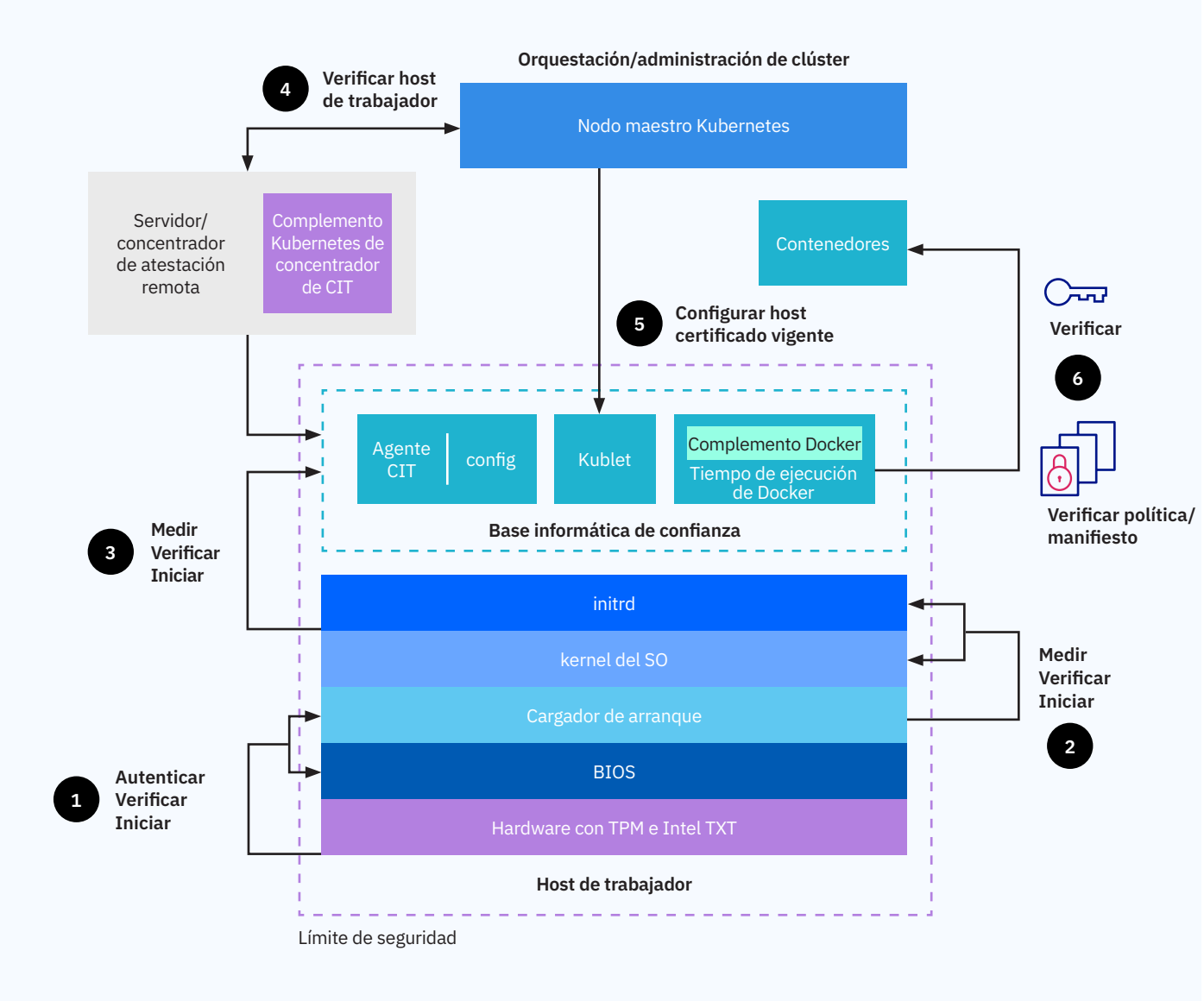


Figura 1. Arquitectura de referencia que habilita una cadena de confianza para contenedores que emplea el modelo de seguridad de medir y verificar como el cimiento que se extiende al nivel de orquestación Kubernetes. Ver página 3 para obtener descripciones completas de los seis pasos.

Habilitar contenedores confiables

Los sistemas de contenedores como Docker tienen metodologías incorporadas para crear micro perímetros en torno a elementos separados del sistema que ayudan a proteger la comunicación entre ellos.

Para evaluar si las aplicaciones en contenedores estarán lo suficientemente protegidas, consulte al proveedor de la plataforma de la nube acerca de estos aspectos sobre su implementación Docker:

¿Se mantienen las imágenes de software en un registro privado? Las plataformas de la nube basadas en Docker Registry V2 pueden asignar a cada organización un registro de imágenes privadas protegido en el cual las imágenes se almacenan y comparten solo entre usuarios y grupos específicos. Agregar imágenes al registro privado comprende autorizar a los usuarios para que crean o copien imágenes locales o importen una imagen directamente de un repositorio público como Docker Hub.

¿La implementación Docker permite el cifrado de sus imágenes?
El cifrado protege contra la manipulación de las imágenes del registro.

¿Los daemons de Docker que se ejecutan en los hosts informáticos se configuran sin acceso directo del usuario? ¿Solo los configura el proveedor de servicio?
La pregunta a ambas interrogantes debería ser sí. El acceso directo al host por parte de otros clientes podría comprometer la seguridad de sus contenedores.

¿Todos los sockets de daemon de Docker están protegidos con certificados de seguridad de la capa de transporte (TLS)?
TLS combina las ventajas de la criptografía de clave pública, validación externa de terceros y cifrado por sesión.

¿Se admite cualquier contenedor Docker privilegiado?
Al no permitir contenedores privilegiados, se garantiza que contenedores de clientes de otros proveedores de servicio no tengan acceso a discos duros del host informático que podrían contener sus datos y aplicaciones.

Cambiar del límite de confianza del nodo a la nube confiable

Dado que el nodo informático se convierte en el centro al establecer la cadena de confianza, y debido a que cada nodo tiene su propio límite de confianza, todos los miembros de un pod y clúster Kubernetes comienzan protegiendo la carga general antes de que ocurra cualquier cálculo y transferencia de datos.

Exija que los proveedores de la nube describan y demuestren sus tecnologías de confianza. Por ejemplo, Intel Trusted Execution Technology (Intel TXT), cualquier TPM que cumpla con las especificaciones 1.2 o 2.0, e Intel CIT son tecnologías establecidas que un proveedor podría usar para construir una nube de confianza.

- **Intel TXT,** defiende contra ataques basados en software destinados a robar información sensible corrompiendo el sistema o código BIOS o modificando la configuración de la plataforma.
- **TPM** es un dispositivo de seguridad basado en hardware que almacena las mediciones usadas en el proceso de seguridad de medir y verificar. Permite garantizar que el sistema está libre de manipulaciones antes de liberar el control del sistema al siguiente nivel de software.
- **Intel CIT** se basa en la raíz de confianza para proporcionar información de certificación basada en políticas, de modo que las cargas de trabajo se ejecuten en hardware verificado con cumplimiento en entornos de la nube pública y privada.

La certificación remota es un paso importante en el proceso de confianza que se extiende más allá del límite de confianza de host hasta el nivel de orquestación de contenedores. Un orquestador como Kubernetes deber ser capaz de verificar la integridad de un nodo informático antes de implementarle contenedores.

Para proporcionar atestación remota, los proveedores de la nube pueden usar tecnologías CIT, que agregan un paso adicional de verificación cada vez que se asigne un nodo informático de nube al entorno de contenedores. Intel CIT, por ejemplo, funciona en conjunto con Intel TXT para ayudar a garantizar que el nodo siga estando libre de manipulaciones y siga siendo confiable antes de que se acepte en un clúster de contenedores. Intel CIT también proporciona una extensión que hace que a un equipo de DevOps le resulte fácil habilitar políticas de seguridad para cargas de trabajo sin requerir que el desarrollador de aplicaciones lidie con las políticas.

Conclusión principal

Para extender el límite de confianza a nivel de nodo se requiere una solución de cifrado comprobada.

Proteger la seguridad mediante la separación de recursos

El orquestador Kubernetes también ayuda a proteger un clúster al permitir la separación de los recursos administrados por el proveedor de servicio de los elementos privados de la cuenta de una organización (Figura 2):

- El nodo maestro dedicado Kubernetes y el registro de imágenes privadas con acceso de imágenes controlado pueden ejecutarse en la red administrada.
- Los nodos de trabajador Kubernetes, con pods de carga de trabajo en contenedores, se pueden implementar en la cuenta de infraestructura de la organización en redes dedicadas controladas por la organización y no por el proveedor.

Este enfoque entrega a los equipos de DevOps un alto nivel de control y proporciona el aislamiento que desean los CISO. La comunicación entre el nodo maestro y el nodo de trabajador se realizaría a través de una conexión de red cifrada, en la cual Kubernetes proporciona el cifrado y las claves; un controlador de entrada autogeneraría certificados TLS para obtener acceso a los pods Kubernetes. Al usar controles de acceso basado en roles de Kubernetes, las organizaciones pueden establecer restricciones detalladas sobre los recursos dentro de los clústeres.

Automatización basada en políticas

Kubernetes permite que los equipos de DevOps dividan las funciones del sistema en elementos atómicos muy pequeños, cada uno de los cuales se puede ligar a la arquitectura de confianza base para ayudar a garantizar que cada elemento permita el acceso y la comunicación según la política. A medida que los equipos extienden arquitecturas complejas de microservicios, la automatización basada en políticas puede controlar el acceso y enrutamiento, con lo que se facilita la expansión y contracción de la escala de cada aplicación y sus componentes.

Calico e Istio son dos importantes componentes del ecosistema Kubernetes que ayudan con la seguridad de la carga de trabajo y las aplicaciones. Calico simplifica la administración de las direcciones IP asignadas a las cargas de trabajo en un nodo informático y programa listas de control de acceso en cada nodo informático para hacer cumplir las políticas de seguridad. Mediante definiciones de política establecidas y aplicadas a través de etiquetas, Istio proporciona control de comunicación basado en certificados entre los microservicios dentro de un pod o clúster Kubernetes.

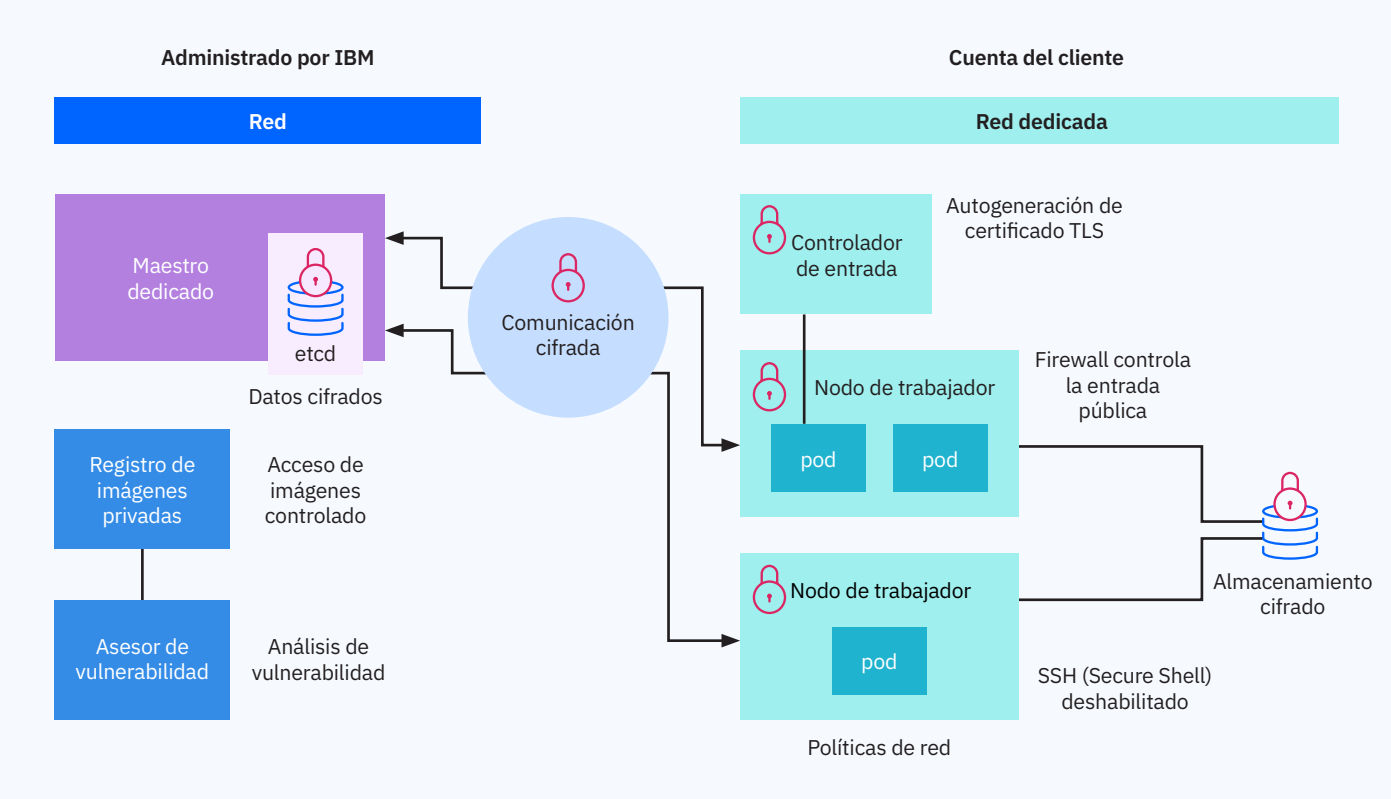


Figura 2. Separación de elementos de clúster administrados por el proveedor y por el cliente.

Extender las ventajas de una cadena de confianza

Una cadena de confianza completamente implementada con certificación remota y cifrado ligado a políticas de seguridad habilita estas importantes capacidades para administrar contenedores, aplicaciones y cargas de trabajo:

- **Transparencia y escalabilidad:** Gracias a la automatización posible a través de la cadena de confianza, los equipos de DevOps son libres para trabajar a una velocidad sin obstáculos. Solo necesitan gestionar las políticas de seguridad con respecto a las cuales el sistema de contenedores de confianza evalúa sus mediciones. Con la configuración adecuada establecida, la orquestación escala recursos de aplicaciones de manera relativamente automática basándose en tráfico en tiempo real.
- **Verificación de políticas de carga de trabajo geográfica:** La orquestación inteligente de contenedores limita el movimiento solo a ubicaciones aprobadas.
- **Garantía de integridad de contenedores:** Cuando los contenedores se mueven, estos se verifican para asegurar que no se haya producido ninguna manipulación durante el proceso. Se verifica que el contenedor movido sea el mismo que el contenedor creado originalmente.
- **Seguridad para datos sensibles:** Los contenedores cifrados solo se pueden descifrar en servidores aprobados en ubicaciones específicas.
- **Información y controles de cumplimiento simplificados:** Una pista de auditoría de metadatos proporciona visibilidad y evidencia auditable de que las cargas de trabajo de contenedores críticas se ejecutan en servidores de confianza.

Conclusión principal

Cuando su equipo evalúe las plataformas de la nube, solicite a los proveedores que expliquen cómo se establece y se mantiene la confianza para la huella de tecnología que alojará las aplicaciones. Esta es la base de la cual depende el negocio de su organización para atraer clientes y mantener datos importantes.

Caso ilustrativo: Aliviar las inquietudes con respecto a GDPR (Reglamento General de Protección de Datos)

Supongamos que tiene clientes en Europa y le preocupan las responsabilidades potencialmente significativas que surgirán cuando el Reglamento General de Protección de Datos (GDPR) de la Unión Europea entre en vigor. Dado que las exigencias de soberanía y otras regulaciones implican que ciertos tipos de datos no pueden dejar el país en el cual se originaron, usted necesita:

- Garantía sólida de que cuando desee su carga de trabajo en una ubicación específica, esta no pueda dirigirse y no se dirigirá a ningún otro lugar.
- Claves de cifrado para su carga de trabajo administradas de tal forma que los datos no se puedan descifrar en ningún lugar excepto donde usted coloque la carga de trabajo.

Una vez que haya establecido la cadena de trabajo liberada por hardware, puede vincular todos los elementos críticos para el mantenimiento de la integridad, la administración de sus claves y la garantía de la ubicación de sus cargas de trabajo. Y puede impulsar esta confianza mediante políticas, escalando la seguridad junto con las implementaciones de las aplicaciones.

Análisis de contenedores estáticos y vivos

Comenzar con los contenedores Docker es fácil: Los desarrolladores pueden extraer cualquier imagen de contenedor públicamente disponible en Docker Hub, por ejemplo, evitando o reduciendo significativamente el tiempo necesario para preparar las partes de una pila de imágenes. El problema es no saber a ciencia cierta qué hay en esa imagen antes de implementarla. Por lo tanto, una práctica necesaria es analizar cada imagen antes de liberarla a la canalización de DevOps adecuada. Las plataformas en la nube deben proporcionar una manera eficiente de hacer esto.

IBM® Cloud Container Service, por ejemplo, ofrece un sistema Vulnerability Advisor (VA) para proporcionar análisis de contenedores estático y vivo (Figura 3). VA inspecciona cada capa de cada imagen en el registro privado de un cliente de la nube para ayudar a detectar vulnerabilidades o malware antes de la implementación de la imagen. Sin embargo, dado que el simple análisis de imágenes de registro puede omitir problemas, como la desviación de la imagen estática hacia los contenedores implementados, VA también analiza los contenedores en ejecución para detectar anomalías. Además, proporciona recomendaciones en forma de alertas en niveles.

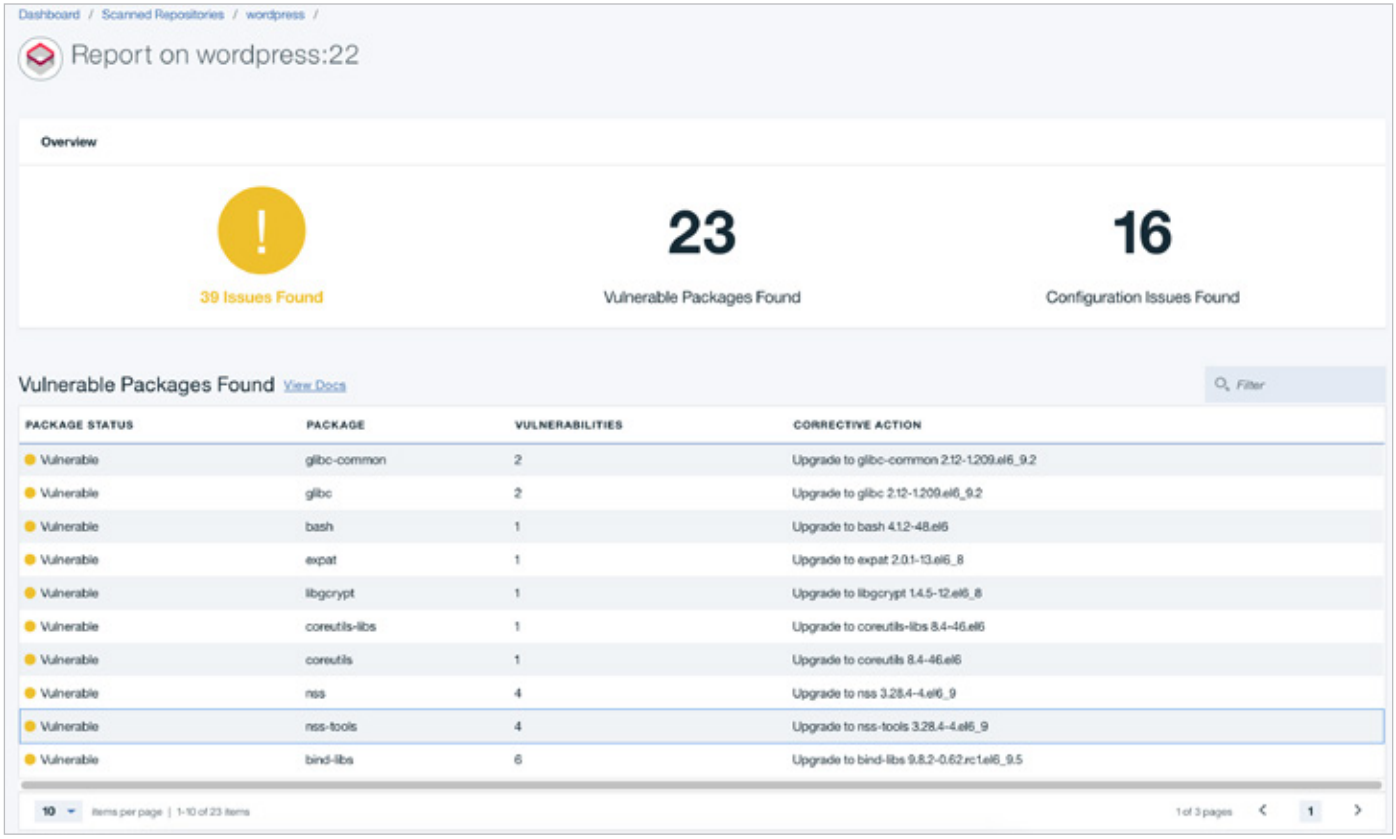


Figura 3. VA se integra a X-Force para calificar vulnerabilidades basándose en el vector de ataque, complejidad y disponibilidad de una corrección conocida.

Tecnologías de aislamiento en la nube

Implícita en las tecnologías basadas en chip, la implementación de una cadena de confianza requiere la capacidad de implementarse en hosts dedicados que admitan acceso VPN. Todos los contenedores se deben ejecutar como procesos independientes y aislados en un host informático y deben tener acceso restringido a sus recursos.

Con el uso de kernels de host informático optimizados, un proveedor de la nube debería poder limitar automáticamente el número total de subprocesos y procesos que se ejecutan en cualquier host informático. Esta optimización lo favorece al garantizar que el host no se encuentra sobrecargado, lo cual podría afectar el rendimiento de su aplicación.

Un proveedor de servicio también debería monitorear permanentemente los hosts informáticos para controlar y remediar "fork bombs" y otros ataques de DoS a nivel de proceso. Los controles de seguridad que controlan el acceso a las carpetas, archivos, dominios de redes y permisos para crear y cambiar datos deben comenzar en el nivel kernel de Linux.

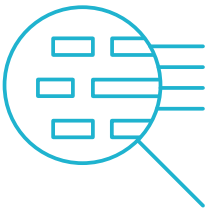
Visibilidad de la seguridad de la nube

Los ingenieros de operaciones suelen examinar sus recursos locales y, de manera justificada, esperan la misma información sobre sus cargas de trabajo en contenedores basadas en la nube. Para proporcionar esta visibilidad, los proveedores de la nube deben registrar automáticamente todo acceso administrativo y de usuario, ya sea por parte de la organización o del proveedor. Un rastreador de actividad en la nube incorporado puede crear una pista de todos los accesos a la plataforma y servicios, otorgando acceso a las organizaciones de clientes a registros pertinentes.

Asegúrese de tener la opción de integrar todos los registros y eventos en su centro de operaciones de seguridad local (SOC) y en el sistema de información de seguridad y de administración de eventos (SIEM). Algunos proveedores de servicio en la nube ofrecen servicios adicionales, como monitoreo de seguridad con información y administración de incidentes, análisis de alertas de seguridad en tiempo real y una visualización integrada a través de las implementaciones híbridas.

IBM QRadar®, por ejemplo, es una solución SIEM integrada que proporciona un conjunto de capacidades de inteligencia de seguridad que puede crecer con las necesidades de una organización. Contiene capacidades de aprendizaje automático que se entrenan en patrones de amenaza de manera que desarrolla un sistema inmunológico de seguridad inteligente.

Explorar asesor de vulnerabilidad



Entre las características del IBM Vulnerability Advisor, se incluyen las siguientes:

- **Configuración de violación de política:** Gracias a VA, los administradores pueden establecer políticas de implementación de imágenes basándose en tres tipos de situaciones de errores de imágenes: paquetes instalados con vulnerabilidades conocidas, inicios de sesión remotos habilitados e inicios de sesión remotos habilitados con algunos usuarios que han adivinado fácilmente las palabras clave.
- **Mejores prácticas:** Actualmente, VA verifica 26 reglas basándose en ISO 27000. Las comprobaciones incluyen configuración como antigüedad mínima de palabra clave, longitud mínima de palabra clave y habilitación de inicios de sesión remotos.
- **Detección de configuración incorrecta de seguridad:** VA marca cada problema de configuración incorrecta proporcionando una descripción de este y recomendando un curso de acción para remediarlo.
- **Integración con IBM X-Force®:** VA incorpora inteligencia de seguridad de cinco fuentes de terceros y usa criterios como vector de ataque, complejidad y disponibilidad de una corrección conocida para calificar cada vulnerabilidad. El sistema de calificación (crítico, alto, moderado o bajo) ayuda a los administradores a comprender rápidamente la seriedad de las vulnerabilidades y a priorizar su corrección.

Seguridad integral en servicio de las necesidades de negocios.

La tecnología de contenedores sirve a los equipos de desarrollo de aplicaciones al racionalizar y agilizar la velocidad de su trabajo de colaboración en entornos en la nube. Pero para entregar estas ventajas, una plataforma en la nube también debe satisfacer los requisitos de seguridad del CISO sin introducir fricción indebida. Por lo tanto, para cumplir con los objetivos de negocios, los equipos de DevOps necesitan implementar políticas de CISO mediante seguridad automatizada.

Una cadena de confianza liberada por hardware es una base eficaz para este objetivo. Debe incluir tecnologías para garantizar contenedores de confianza y aplicar políticas de seguridad que controlen la implementación de los contenedores. La arquitectura de la cadena de confianza está diseñada para satisfacer la necesidad urgente de seguridad e innovación rápida:

- Los ejecutivos de seguridad pueden formular políticas de seguridad que se apliquen automáticamente a cada contenedor que se cree o mueva.
- Cada paso de la secuencia está automatizado, lo cual permite que los equipos de DevOps desarrollen e implementen las aplicaciones rápidamente sin detenerse para agregar componentes de seguridad.

Esta arquitectura protege los datos y las aplicaciones desde el nivel de hardware hasta la capa de orquestación de contenedores de las plataformas de la nube, ayudando a las organizaciones a observar los regímenes de cumplimiento, como el GDPR de la UE, el Programa de administración federal de riesgos y autorizaciones de Estados Unidos (FedRAMP) y la Ley de Transferibilidad y Responsabilidad de Seguro Médico de Estados Unidos (HIPAA). Las organizaciones definen exactamente las políticas requeridas para su sector y garantizan los elementos de seguridad.

El punto de vista de IBM

Innovar en la cadena de confianza es un enfoque clave para IBM y sus asociados. IBM e Intel tienen una duradera asociación dedicada a desarrollar soluciones de la cadena de seguridad y ahora están aplicando sus conocimientos especializados en los productos basados en contenedores. El objetivo: Ayudar a las organizaciones a implementar contenedores de manera segura pero ágil que permita la flexibilidad del desarrollo y las arquitecturas de microservicios de vanguardia que exigen y merecen los innovadores de hoy.

IBM Cloud dota a los equipos de herramientas de código abierto fácilmente disponibles para automatizar la implementación y la administración. Además, si los clientes desean implementar cargas de trabajo en múltiples nubes, la plataforma en nube debe permitirles usar las mismas herramientas de manera uniforme a través de su entorno de múltiples nubes. El futuro de la seguridad de contenedores es abierto, ágil, automatizado cada vez que es posible, y fuertemente defensivo con inteligencia.

El futuro de la seguridad de contenedores es abierto, ágil, automatizado cada vez que es posible, y fuertemente defensivo con inteligencia.

Más información

Para obtener más información acerca de cómo desarrollar una cadena de confianza para la seguridad de los contenedores, visite ibm.com/cloud/container-service

¿Se interesa en seguridad y DevOps? Únase a nuestro canal Slack e intercambie impresiones con los desarrolladores del equipo de productos de IBM Cloud Container Service.

Manténgase conectado

IBM Cloud Container Service
IBM Cloud Blog

Síganos

@IBMcloud
Facebook

Conéctese con nosotros

LinkedIn
YouTube

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

Producido en Estados Unidos de América, febrero de 2018