Aumente la seguridad de la nube híbrida

Proteja su empresa teniendo en cuenta los aspectos principales de la seguridad de la nube

/Ábrase a las posibilidades

Red Hat

Escrito por Lucy Huh Kerner, directora de Promoción y Estrategia Global de Seguridad, Red Hat

Contenido

Capítulo 1

Implemente una nube híbrida centrada en la seguridad

La adopción de la nube y su popularidad continúan creciendo. Actualmente, el 65 % de las empresas afirma utilizar mucho este entorno y el 72 % cuenta con una estrategia de nube híbrida[1].

Esta es una arquitectura de TI que incorpora cierto grado de portabilidad, organización y gestión de las cargas de trabajo en dos o más entornos conectados, pero separados, que incluyen los de servidor dedicado (bare metal) y los virtualizados, además de las nubes privadas y públicas. Con ella puede ejecutar cargas de trabajo en cualquier entorno conectado, trasladando los recursos de uno a otro y utilizándolos de forma indistinta.

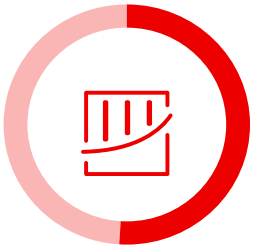
Las empresas adoptan los entornos de nube híbrida para poder:

- Conectar la infraestructura, las plataformas, las aplicaciones y las herramientas de distintos proveedores
- Aumentar la eficiencia y la capacidad de ajuste
- Reducir los costos
- Aumentar la agilidad
- Optimizar el alojamiento de los datos

[1] Flexera, "2023 State of the Cloud Report", marzo de 2023.

La seguridad es una de las preocupaciones principales para las empresas, independientemente de la parte del proceso de adopción de la nube híbrida en la que se encuentren. El 79 % de ellas informan que este aspecto es un desafío[1]. Los puntos vulnerables del entorno mencionado suelen generarse por la falta de supervisión y control de los recursos. Son ejemplos de esto, entre otras causas, el uso no autorizado de la nube pública, la falta de monitoreo de los recursos, el manejo inadecuado de los cambios, la mala gestión de la configuración, los controles de acceso poco efectivos y los errores humanos. Los usuarios no autorizados se aprovechan de estas fallas para obtener acceso a los datos confidenciales y los recursos internos, lo cual puede llegar a ser costoso.

El costo total en promedio de las filtraciones de datos llegó a un nuevo pico de USD **4,45 millones** en 2023, de los cuales el **29,2 %** corresponde a la pérdida del cliente[2].



51 %

de las empresas afirma que planea aumentar las inversiones en seguridad a raíz de una filtración de datos[2].

[1] Flexera, "2023 State of the Cloud Report", marzo de 2023.
[2] IBM Security, "Cost of a Data Breach Report 2023", 2023.

En 2023, no solo aumentó el costo promedio por cada registro asociado con una filtración de datos, sino también el tiempo requerido para evitarlas[2]. Al adaptar los métodos para tener en cuenta las diferencias entre las arquitecturas de las instalaciones y de la nube, puede implementar una nube híbrida centrada en la seguridad y superar estos desafíos crecientes. En este ebook, se mencionan los enfoques nuevos y los aspectos relacionados con la seguridad del entorno mencionado.

277 días

es el tiempo en promedio que se necesita para identificar y controlar una filtración de datos en 2023[2].

USD 1,02 millones

es la suma que se puede ahorrar si se identifica y controla una filtración en un plazo de menos de 200 días[2].

[2] IBM Security, "Cost of a Data Breach Report 2023", 2023.

Capítulo 2

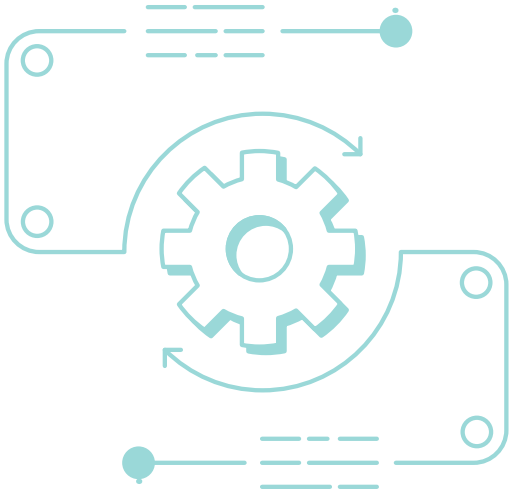
La seguridad es un proceso, no un producto

Para que la seguridad sea eficaz, se necesita un enfoque integral que combine el personal, los procesos y la tecnología. No basta con implementar productos y herramientas centrados en la seguridad para proteger la infraestructura, la nube o la empresa. También se deben tener en cuenta las estrategias y los procesos de protección para aprovechar al máximo las funciones de los productos y disminuir los riesgos.

Estos planes de acción se pueden adaptar con el tiempo a medida que evolucionan las tecnologías, las amenazas y las necesidades. Los entornos de nube híbrida requieren un cambio de enfoques de seguridad y, debido a que no cuentan con un perímetro definido, los métodos tradicionales no son efectivos.

Es fundamental disponer del control de acceso y la gestión de la identidad en un solo lugar para los enfoques de seguridad que se centran en la nube, ya que utilizan el principio de privilegios mínimos para que los usuarios solo tengan los permisos que necesitan. Este enfoque requiere auditar los derechos actuales de cada cliente y luego reevaluarlos para determinar el nivel de acceso adecuado.

Además, la seguridad de la nube híbrida requiere una estrategia de seguridad en capas y con protección integral que utilice las funciones de cada capa de su entorno, las cuales incluyen los sistemas operativos, las plataformas de contenedores y las herramientas de automatización.



Sistema operativo

Busque herramientas integradas que le permitan cumplir con los requerimientos normativos de seguridad, implementar métodos de defensa físicos, mejorar la seguridad de la red, controlar el acceso de los usuarios, aislar los procesos y aumentar la protección de los datos. Algunos ejemplos son OpenSCAP, USBGuard, Security-Enhanced Linux® (SELinux), gestión de identidades y Network Bound Disk Encryption.

Plataforma de contenedores

Utilice funciones integradas en la plataforma y en Kubernetes para aumentar la seguridad de los contenedores. Por ejemplo, políticas de seguridad de los pods; controles del tráfico de la red, de entrada y salida del clúster, del acceso basados en funciones (RBAC); gestión de certificados integrada, y microsegmentación de la red.

Herramientas de automatización

Seleccione un lenguaje y una plataforma de automatización que todos en la empresa (los equipos de desarrollo, de operaciones de TI, de seguridad y de cumplimiento) puedan aprender a utilizar de manera sencilla. Busque funciones de control de acceso, inicio de sesión y auditoría.

También es importante revisar sus procesos y herramientas de seguridad actuales. Asegúrese de utilizar todas las funciones disponibles y determine si puede modificar alguna configuración para brindar una mejor protección o si requiere herramientas y procesos nuevos.

1. Realice un inventario de sus herramientas y recursos de TI actuales.
2. Lleve un registro de sus arquitecturas de seguridad y de redes, las políticas de ciberseguridad, los procesos de trabajo y la falta de personal y habilidades actuales.
3. Establezca un modelo de amenazas y defina su tolerancia a los riesgos y las estrategias de disminución del impacto ante las fallas de ciberseguridad.
4. Evalúe sus arquitecturas, políticas y procesos para identificar las áreas que requieren un cambio.
5. Analice las herramientas y los recursos que ya posee para determinar si admiten las estrategias y los procesos actualizados. Elabore un registro y una planificación de la forma en la que se abordarán las fallas de seguridad.

En las siguientes secciones, se mencionan los aspectos más importantes relacionados con la seguridad de la nube híbrida y se proporcionan consejos para mejorar la protección.

Capítulo 3

Aspecto relacionado con la seguridad n.° 1

Comience con una base sólida

¿Por qué es importante?

Cuando se implementan cargas de trabajo en varios entornos o se utilizan tecnologías de open source sin verificar, es difícil determinar dónde se encuentran los puntos vulnerables. Además, es complicado reducir el riesgo con la seguridad en varias capas sin una base sólida. Si utiliza software open source directamente de las comunidades upstream, estará vulnerable a los riesgos de seguridad y los ataques a la cadena de suministro, los cuales aprovechan las debilidades de los servicios y el software de terceros para poner en peligro al objetivo final. Estos ataques pueden presentarse de varias formas, como apoderarse del proceso de actualización e introducir un código malicioso en el software legítimo. En los últimos tres años, ha habido un aumento anual de un 742 % en promedio en los ataques a la cadena de suministro[3]. Por esta razón, es fundamental diseñar sobre una base unificada, estable y centrada en la seguridad para proteger su empresa.

Sugerencias y prácticas recomendadas

Disminuya los riesgos de seguridad en la cadena de suministro al utilizar software open source de un proveedor de open source empresarial de confianza que proporcione soporte durante todo el ciclo de vida del sistema, como Red Hat. Estos proveedores desarrollan su software con un proceso de seguridad de cadena de suministro sólido, que incluye seleccionar cuidadosamente los sistemas open source para sus clientes. Esto garantiza que la tecnología que utilicen los usuarios sea de confianza, resistente y segura de implementar.

Además, es importante ejecutar las aplicaciones fundamentales en torno a una plataforma que cuente con funciones integradas de seguridad. De esta forma, se proporcionará la seguridad básica a partir de la cual los clientes podrán ejecutar sus aplicaciones fundamentales con confianza, incluir funciones de seguridad de varias capas para disminuir los riesgos e implementar la automatización de la seguridad y el cumplimiento normativo.

Priorice una base centrada en la seguridad para las aplicaciones y los procesos al adoptar un sistema operativo, confiable, resistente y reforzado para la estabilidad y la protección, como Red Hat® Enterprise Linux®. RHEL proporciona una base estable que le permite ajustar las aplicaciones importantes con confianza, mantener el cumplimiento normativo de la seguridad e implementar tecnologías nuevas de manera uniforme en los entornos virtuales, con servidor dedicado (bare metal), de contenedores y todos los tipos de nube.

[3] Sonatype. "8th Annual State of the Software Supply Chain", 2023.

Red Hat Enterprise Linux es la base de la mayoría de los productos de la cartera de Red Hat y es el sistema operativo de confianza de muchas empresas gracias a las funciones de seguridad integrada que ofrece.

Con Red Hat Enterprise Linux puede:

Reducir el riesgo de exposición de los datos o los sistemas con las funciones de seguridad integrada, como la ejecución activa de parches en el kernel, que permite aplicar parches de seguridad sin la necesidad de reiniciar o interrumpir los tiempos de ejecución. Además, otras funciones de protección integradas son la creación de listas de aplicaciones permitidas, una práctica según la cual se especifica un índice de aplicaciones o archivos ejecutables que cuentan con permiso para ejecutarse en un sistema por un usuario en particular, y SELinux, que permite aplicar un control detallado de los archivos, los procesos, los usuarios, las aplicaciones y mucho más.

Automatizar la protección de los datos según sea necesario y mantenerlos a lo largo del tiempo con funciones de seguridad integradas, como Network Bound Disk Encryption, que le permite descifrar automáticamente los sistemas sin la necesidad de gestionar manualmente las claves. Asimismo, gracias a las políticas de cifrado para todo el sistema, puede concentrarse en mantener los datos seguros y abordar el cumplimiento normativo con configuraciones personalizables y uniformes que le permiten cumplir con los requisitos normativos particulares de su ubicación y mucho más.

Cumplir con los requisitos de cumplimiento y optimizar las auditorías. Red Hat Enterprise Linux cuenta con funciones integradas de análisis de cumplimiento y corrección de errores con OpenSCAP para llevar a cabo evaluaciones de puntos vulnerables en un sistema local y validar el cumplimiento de una gran variedad de estándares de seguridad del sector.

Gracias al enfoque de seguridad básica que brinda Red Hat Enterprise Linux, los productos en capas que se ejecutan en torno al sistema operativo, como **Red Hat OpenShift**, ofrecen una defensa integral para los contenedores y Kubernetes. Red Hat amplía las funciones de seguridad hasta la stack y los elementos de Kubernetes. De igual manera, debido a las funciones de protección integradas, **Red Hat Ansible Automation Platform** permite que las empresas implementen la automatización de la seguridad y el cumplimiento según lo necesiten.

Pasos estratégicos

Tome estas medidas cuando comience con el proceso de seguridad de la nube híbrida:

Utilice versiones disponibles en el mercado

Migre su software open source directamente de sus proyectos open source upstream a las versiones confiables disponibles en el mercado, las cuales están probadas y validadas para reducir el riesgo de errores y puntos vulnerables de seguridad. También suelen incluir soporte empresarial que distribuye rápidamente parches de seguridad y ofrece orientación para configurar su sistema de la forma más segura. Al adoptar un software open source de un proveedor de open source empresarial de confianza, podrá garantizar que este se desarrolle con un proceso de seguridad de la cadena de suministro sólido y que el soporte se brinde durante todo el ciclo de vida. Todo esto permite que las empresas utilicen esta clase de tecnología y, al mismo tiempo, reduzcan al máximo los riesgos.

Elija una plataforma con funciones de seguridad integradas

Es importante seleccionar una plataforma (como un sistema operativo o una plataforma de aplicaciones de contenedores y de automatización) con funciones de seguridad integradas. De esta forma, se proporcionará la seguridad básica a partir de la cual los clientes podrán ejecutar sus aplicaciones fundamentales con confianza, incluir funciones de seguridad de varias capas para disminuir los riesgos e implementar la automatización de la seguridad y el cumplimiento normativo según lo necesiten.

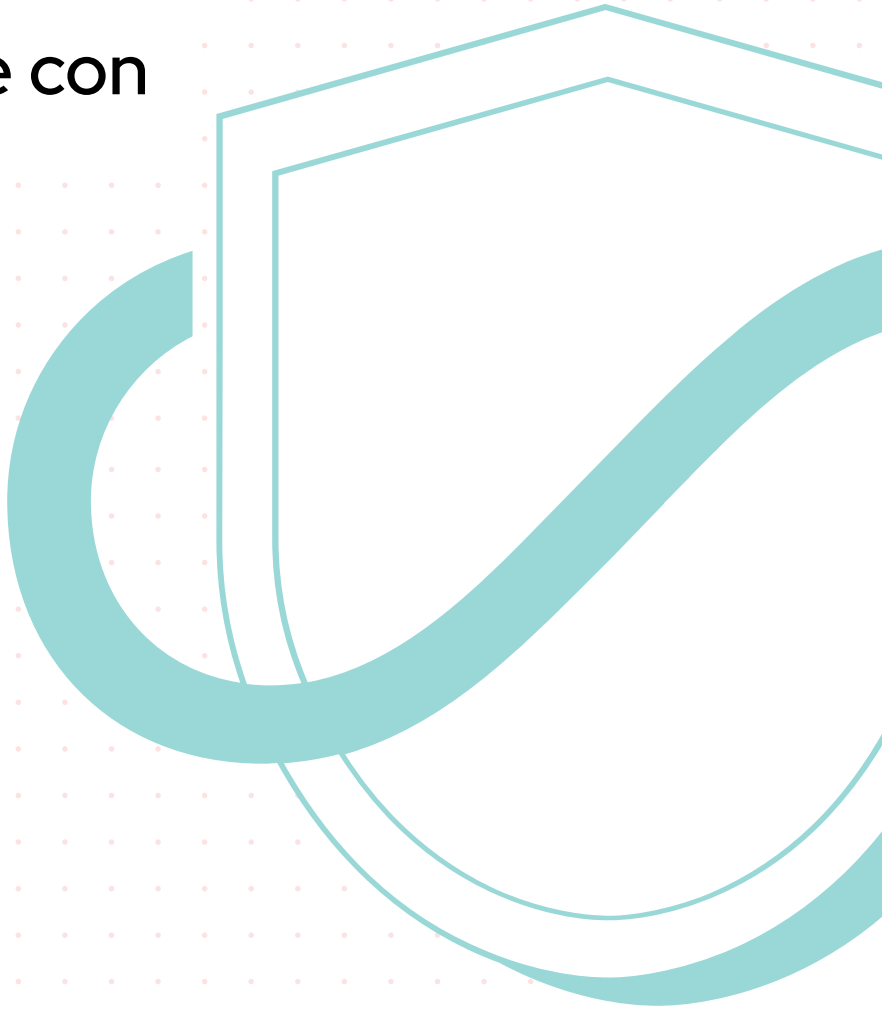
Implemente la seguridad en toda su stack tecnológica

Una vez que haya establecido una base para la seguridad, asegúrese de que las tecnologías en capas que se ejecuten en torno a ella hereden las ventajas de la protección y funcionen en conjunto para el proceso de defensa de varias capas.

Capítulo 4

Aspecto relacionado con la seguridad n.° 2

Implemente una cadena de suministro de software confiable con DevSecOps



¿Por qué es importante?

En 2023, el 12 % de las filtraciones de datos surgieron de ataques a la cadena de suministro[2]. El uso de software open source no verificado que proviene directamente de las comunidades upstream aumenta la posibilidad de que se generen puntos vulnerables de seguridad y ataques a la cadena de suministro, los cuales aprovechan las debilidades de los servicios y el software de terceros para poner en peligro al objetivo final. Estos ataques pueden presentarse de varias formas, como el secuestro de las actualizaciones y la introducción de código malicioso en software legítimo.

Los enfoques de seguridad divididos suelen generar fallas y repetición de tareas, ya que la protección se transforma en un aspecto secundario en el desarrollo de las aplicaciones y la implementación de la infraestructura. A medida que aumentan la velocidad del desarrollo y la flexibilidad de la implementación, se vuelve más importante tener en cuenta la seguridad durante todo el proceso.

Sugerencias y prácticas recomendadas

Para adoptar un enfoque centrado en la seguridad que se aplique en la cadena de suministro de software, el primer paso es desarrollar una mentalidad de DevSecOps. Con ella, los equipos de seguridad, de operaciones de TI y de desarrollo de aplicaciones trabajan en conjunto para implementar el enfoque mencionado en todo el ciclo de vida de desarrollo del software (SDLC) y de la infraestructura, los cuales se diseñan sobre una base open source reforzada para empresas en toda la nube híbrida.

[2] IBM Security, "Cost of a Data Breach Report 2023", 2023.

DevSecOps automatiza la incorporación de la seguridad en cada etapa del ciclo de vida de desarrollo del software, desde el primer diseño hasta la integración, la prueba, la implementación y la distribución.

Estas son las ventajas de la adopción de un proceso de DevSecOps:

- Ayudar a los equipos de TI y seguridad a enfrentar los desafíos relacionados con las personas, los procesos y las tecnologías
- Permitir la mejora de la eficiencia, la uniformidad, la repetición y la colaboración
- Reducir los errores humanos, lo cual termina por reducir los riesgos

Con DevSecOps, la seguridad se transforma en una responsabilidad compartida que se integra desde el principio hasta el final. En vez de tener a un solo equipo independiente como el único responsable de configurar las políticas de seguridad, el personal de los equipos de seguridad, de desarrollo y de operaciones trabajan en conjunto y comparten la supervisión, los comentarios, la información importante y todo lo que aprenden. Este enfoque permite diseñar el proceso de seguridad al comienzo del desarrollo de aplicaciones y de la implementación de infraestructuras, lo cual aumenta la protección.

Los desarrolladores de aplicaciones empresariales que diseñan funciones de software nuevas para sus empresas deben mejorar drásticamente su estrategia de seguridad y disminuir su carga cognitiva. Es necesario implementar la protección en todo el SDLC, desde que se escribe el código y durante toda la verificación integrada de la seguridad de las aplicaciones, para detectar los problemas al inicio del ciclo de vida y disminuir los tiempos de inactividad prolongados. También se debe aplicar en la etapa de diseño protegiendo los sistemas de compilación con los flujos de trabajo de integración y distribución continuas (CI/CD) centrados en la seguridad, y en las etapas de implementación y ejecución con plantillas de referencia, análisis de puntos vulnerables, firmas de los artefactos, certificaciones, información de procedencia, puntos de aplicación de políticas y listas de elementos de software (SBOM).

Además, es necesario crear una estrategia que garantice que las tecnologías de open source que utilicen los equipos provengan de fuentes confiables, se les aplique parches constantemente y de manera automatizada y se configuren teniendo en cuenta la seguridad. Asimismo, se debe promover el uso de productos open source empresariales que incluyan soporte durante todo el ciclo de vida.

Con los que ofrece Red Hat, podrá aprovechar la experiencia de más de 30 años que la empresa tiene en protección de la cadena de suministro de software open source de sus productos. Además, las empresas necesitan soluciones que les permitan implementar, gestionar y proteger la flota de clústeres de Kubernetes y diseñar, modernizar e implementar aplicaciones de manera segura, uniforme y según lo necesiten.

Red Hat OpenShift Platform Plus es una plataforma unificada que incluye Red Hat OpenShift, Red Hat Advanced Cluster Security for Kubernetes, Red Hat Advanced Cluster Management for Kubernetes, Red Hat Quay y Red Hat OpenShift Data Foundation. Esta plataforma permite que las empresas diseñen, modernicen e implementen las aplicaciones organizadas en contenedores en Kubernetes de manera segura y según sea conveniente. Se proporciona gestión de los datos, las aplicaciones, el cumplimiento y la seguridad de varios clústeres para obtener uniformidad en la cadena de suministro de software.

Pasos estratégicos

Tome estas medidas a la hora de implementar DevSecOps y las mejoras en la seguridad de la cadena de suministro de software:

Empiece de a poco y expándase
Elija un solo proyecto para comenzar. Fomente la experimentación, la repetición y las mejoras constantes para perfeccionar y optimizar su proceso. Festeje los éxitos y muestre los beneficios comprobados a las personas de la empresa.

Establezca objetivos y plazos claros y acordados
La transparencia es fundamental. Asegúrese de que todos los que participen comprendan los objetivos y los plazos del proyecto y estén de acuerdo con ellos.

Capacite al personal en varias áreas

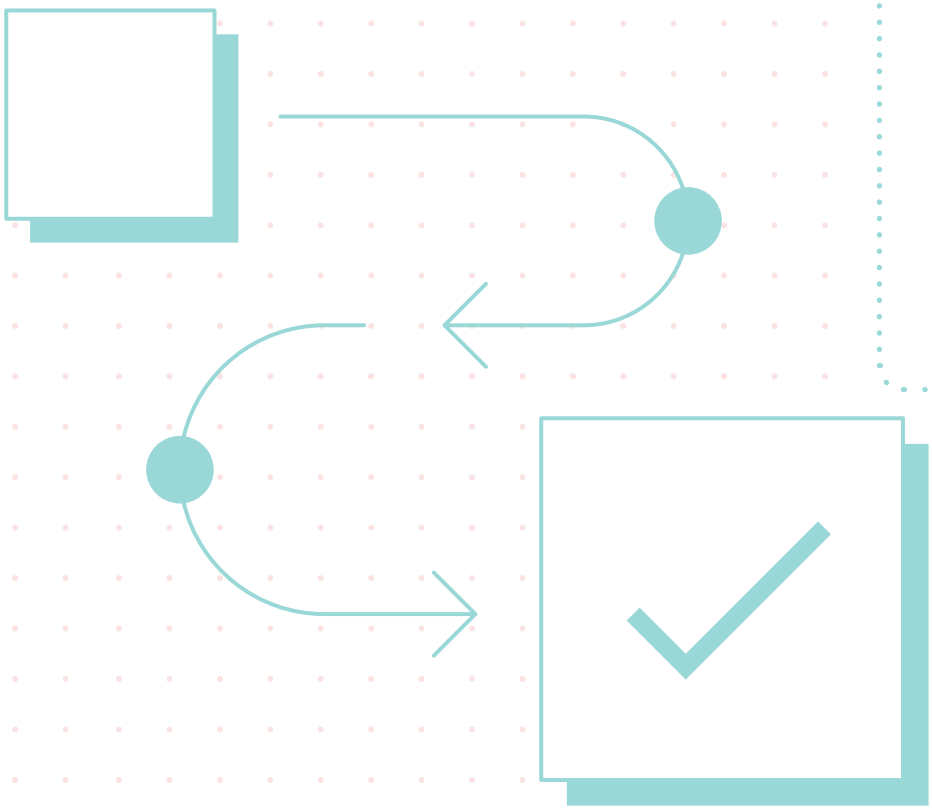
Establezca planes de capacitación sobre la seguridad, la infraestructura y el desarrollo que se actualicen regularmente y estén disponibles en todo momento para los integrantes del equipo.

Cree un grupo de trabajo para la seguridad

Diseñe un equipo integrado con experiencia en varias disciplinas para definir los casos prácticos y las estrategias de seguridad. Aprenda de los demás, aproveche los descubrimientos de otros equipos.

Implemente la seguridad en todo el SDLC con una plataforma de aplicaciones unificada

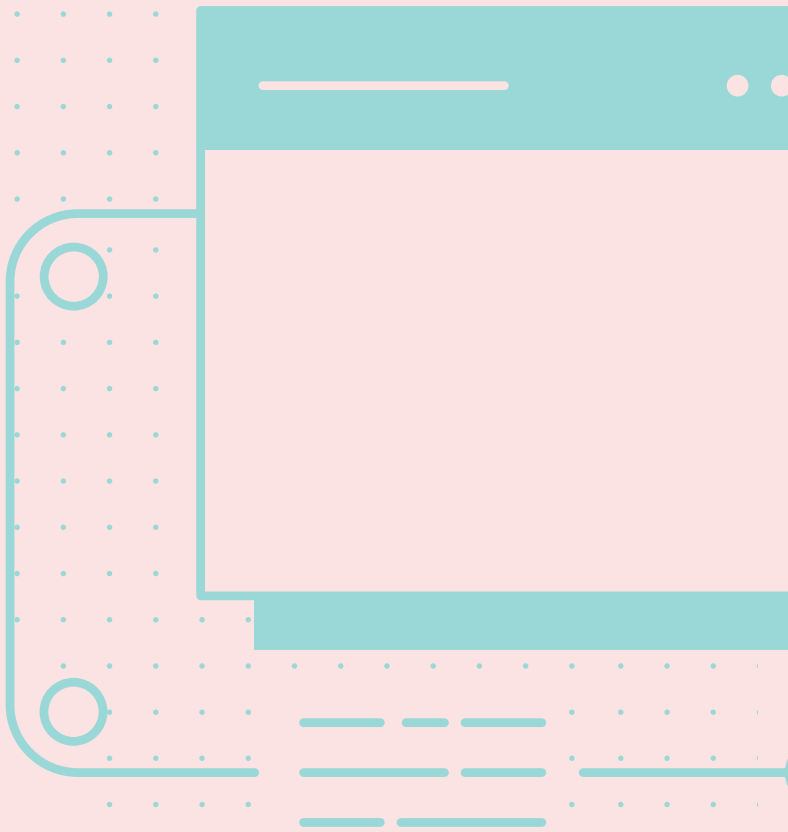
Es necesario implementar la protección en todo el SDLC, desde que se escribe el código y durante toda la verificación integrada de la seguridad de las aplicaciones, para detectar los problemas al inicio del ciclo de vida y disminuir los tiempos de inactividad prolongados. También se debe aplicar en la etapa de diseño protegiendo los sistemas de compilación con los flujos de trabajo de integración y distribución continuas (CI/CD) centrados en la seguridad, y en las etapas de implementación y ejecución con plantillas de referencia, análisis de puntos vulnerables, firmas de los artefactos, certificaciones, información de procedencia, puntos de aplicación de políticas y listas de elementos de software (SBOM).



Capítulo 5

Aspecto relacionado con la seguridad n.° 3

Utilice la automatización y la gestión para proteger la nube híbrida



¿Por qué es importante?

Los errores de configuración y el manejo inadecuado de los cambios son las principales amenazas contra la seguridad[4]. Los primeros causan que los sistemas sean propensos a recibir ataques, y lo segundo es fundamental para saber quién modificó la configuración, qué aplicaron y en qué momento del ciclo de vida del sistema.

La automatización, la gestión y la inteligencia artificial (IA) pueden ayudarlo a optimizar las operaciones cotidianas y a integrar la seguridad con los procesos, las aplicaciones y la infraestructura desde el comienzo. La implementación de una estrategia de gestión y automatización en toda la empresa permite disminuir los errores humanos y proporcionar velocidad, uniformidad, capacidad de repetición y la posibilidad de realizar comprobaciones y auditorías. Además, esta estrategia concentrada mejora la seguridad y el cumplimiento al ayudar a las empresas a integrar la seguridad con el desarrollo de aplicaciones y las operaciones de TI desde el inicio y durante todo el ciclo de vida. Todo esto les permite implementar las prácticas de DevSecOps con éxito. De hecho, incorporar ampliamente la automatización, la gestión y la IA en los procesos de seguridad reduce el costo medio de una filtración un 39,3 % en promedio, pero solo el 28 % de las empresas lo han puesto en práctica[2].

[2] IBM Security, "Cost of a Data Breach Report 2023", 2023.

[4] Cloud Security Alliance, "Top Threats to Cloud Computing: Pandemic 11 Deep Dive", octubre de 2023.

Sugerencias y prácticas recomendadas

Implemente una estrategia de automatización y gestión en toda la empresa para seguir el ritmo de los requisitos dinámicos en materia de seguridad, riesgos y cumplimiento. Al adoptar este método de manera uniforme en la nube híbrida, obtendrá mayor agilidad, capacidad de repetición, uniformidad y auditorías sencillas.

La automatización unificada reduce el riesgo de cometer errores manuales y en la configuración en toda la empresa. Este proceso, junto con la gestión, optimizan y aumentan la uniformidad de la administración de la infraestructura, el desarrollo de aplicaciones y la seguridad de las operaciones para mejorar la protección, el cumplimiento y el control de cambios. Esto le permite:

- Configurar de manera uniforme los recursos según las políticas aprobadas con anterioridad y realizarles mantenimiento preventivo de una forma repetible durante todo el ciclo de vida
- Identificar rápidamente los sistemas que requieren parches o una nueva configuración
- Optimizar la aplicación de parches o cambiar la configuración de los sistemas según parámetros definidos y de manera uniforme en una gran cantidad de sistemas
- Facilitar las auditorías y la resolución de problemas con los registros de acciones que se documentan automáticamente

Las empresas confían en la automatización de la TI para gestionar la seguridad de los entornos operativos y de nube híbrida, las aplicaciones y las operaciones de seguridad, que son cada vez más complejos. **Red Hat Ansible Automation Platform** es una plataforma de automatización integral que ofrece un marco empresarial uniforme para diseñar y llevar adelante la automatización de la TI según sus necesidades y con la seguridad como prioridad en todo momento. Permite que se mejore la eficiencia, aumenta la productividad, ayuda a controlar los riesgos y los gastos, permite que los equipos automaticen la seguridad y la uniformidad del cumplimiento en toda la empresa de manera repetible y proporciona contenido de automatización certificado para responder a las amenazas de forma coordinada con soporte empresarial de Red Hat permanente.

Además, gracias a ella, las empresas pueden gestionar los procesos de seguridad automatizados para mantenerse un paso adelante de los ataques maliciosos, ya que ofrece automatización para varias tareas, desde la gestión de la configuración hasta la corrección de errores y la aplicación de parches. Red Hat Ansible Automation Platform puede servir como punto de integración para las soluciones de seguridad, ya que incluye contenido de partners certificados, como CyberArk, IBM y Palo Alto Networks, lo cual posibilita que los usuarios automaticen la gestión y la integración de una amplia variedad de tecnologías de seguridad externas.

Gracias a la gestión de identidades y los controles de acceso para las plataformas y los procesos, puede garantizar que solo el personal autorizado ejecute tareas de automatización. Seleccione una plataforma de automatización que pueda utilizar todo el personal de la empresa. La elección de una tecnología que implemente un lenguaje de automatización común y fácil de aprender mejora:

La supervisión: todos podrán comprender lo que se logra con cada tarea automatizada

La capacidad de repetición: con una plataforma y un lenguaje accesibles, el personal autorizado puede utilizar la automatización de forma efectiva y eficiente

La colaboración: las tareas de automatización se pueden compartir con toda la empresa, lo que permite a otros equipos aprovechar el trabajo realizado y evitar la duplicación de esfuerzos.

La auditoría: varios empleados pueden verificar las tareas de automatización y ver los registros para realizar auditorías.

Pasos estratégicos

Tome estas medidas para comenzar con la automatización de la seguridad

Comience con un solo proyecto
No intente automatizar todo de una vez. Empiece con un conjunto de tareas limitado.

Seleccione tareas repetitivas
Automatice las tareas que se llevan a cabo de forma repetitiva, como la gestión de la configuración y los parches, los paquetes de software, la identificación y corrección de los puntos vulnerables de la seguridad y el cumplimiento de las políticas.

Mida los resultados, adáptese y repítalo de nuevo
Trabaje de manera iterativa para implementar la automatización, medir los resultados y adaptarse según corresponda.

Planifique la expansión con una plataforma de automatización empresarial integral con capacidad de ajuste
Asegúrese de que toda la automatización se pueda comprobar, auditar y compartir para que las otras personas que pertenecen a la empresa puedan aprovechar los beneficios y utilizar una plataforma de automatización empresarial con capacidad de ajuste.

Capítulo 6

¿Todo listo para comenzar?

La seguridad de la nube híbrida es una responsabilidad compartida para todas las empresas. Independientemente de la etapa del proceso de adopción de la nube híbrida en la que se encuentre, Red Hat le permite implementar un entorno centrado en la seguridad.

La cartera de software open source de Red Hat, con funciones de seguridad integradas, le ofrece las herramientas y las plataformas necesarias para superar los desafíos actuales y futuros en materia de seguridad y cumplimiento normativo. Red Hat también ofrece soporte listo para empresas, capacitaciones prácticas y servicios especializados que le permiten diseñar y operar un entorno de nube híbrida de manera más eficiente y segura.

Conozca la visión de Red Hat sobre la seguridad de la nube híbrida

Consulte estos recursos para obtener más información sobre la visión de Red Hat con respecto a la seguridad y el cumplimiento en la nube híbrida.

- Resumen de la seguridad de la nube híbrida
- Hybrid cloud security assessment
- Security approaches for hybrid cloud environments
- Elevate your hybrid cloud security

Sobre Lucy Huh Kerner, directora de Promoción y Estrategia Global de Seguridad, Red Hat.
Lucy Huh Kerner está a la cabeza de las iniciativas de liderazgo intelectual en materia de seguridad y de las estrategias técnicas y de comercialización para la seguridad en Red Hat y su cartera de productos en todo el mundo. Además, ayuda a crear y distribuir contenido técnico sobre la seguridad para el personal de campo, los clientes, los partners, los analistas y la prensa y ha dado charlas en varios eventos, como en conferencias relacionadas con este tema. Lucy cuenta con más de 20 años de experiencia como ingeniera de desarrollo de sistemas de hardware y software, arquitecta de soluciones y estratega de seguridad internacional, área en la que trabajó en varios aspectos.

ARGENTINA
+54 11 4329 7300

CHILE
+562 2597 7000

COLOMBIA
+571 508 8631
+52 55 8851 6400

MÉXICO
+52 55 8851 6400

ESPAÑA
+34 914 148 800

facebook.com/redhatinc
@RedHatLA
@RedHatIberia
linkedin.com/company/red-hat

es.redhat.com