La seguridad y el cumplimiento normativo de Red Hat Enterprise Linux

Base segura para la ejecución de las cargas de trabajo de la nube híbrida abierta

Red Hat Enterprise Linux le permite mejorar la protección, aumentar el cumplimiento de las normas y estar preparado para las auditorías, ya que respalda los principales requisitos normativos y de seguridad para los sistemas operativos:

- Funciones de seguridad modernas y en varias capas para reducir los riesgos
- Automatización de la ejecución de parches y la aplicación de correcciones para minimizar el tiempo de inactividad
- Validación y procesos seguros del ciclo de vida de desarrollo
- Herramientas de cumplimiento integradas para respetar las normas de seguridad
- Controles de seguridad uniformes en toda la nube híbrida
- Protección de las cargas de trabajo en los entornos de nube pública

La protección del sistema operativo es fundamental

Debido al aumento constante de la cantidad y la complejidad de los ataques informáticos, es esencial que la seguridad esté integrada en cada parte de la infraestructura. Los sistemas operativos (SO) son la base en la que se ejecutan todas las aplicaciones, por eso es necesario aplicar diversas funciones de seguridad en ellos para que estén protegidos de los puntos vulnerables y que cumplan con los requisitos normativos.

Red Hat® Enterprise Linux® ofrece una base más segura desde la cual puede ajustar las aplicaciones actuales e implementar tecnologías nuevas de manera uniforme en entornos virtuales, con servidores dedicados (bare metal), de nube y en el extremo de la red. Además, sus funciones de cumplimiento y seguridad integradas le permiten:

- **Reducir los riesgos:** gestione la seguridad y disminuya el riesgo de que se produzcan filtraciones de información para evitar que sus datos, sus sistemas y su reputación se vean comprometidos.
- **Brindar mayor protección:** automatice y mantenga los controles de seguridad según sea necesario y con un tiempo de inactividad mínimo.
- **Cumplir con los requisitos normativos:** optimice las normas de cumplimiento para las empresas con entornos estrictamente regulados.

Reduzca los riesgos relacionados con la exposición de sus datos y sistemas o con el daño a su reputación

Parches y actualizaciones importantes de seguridad: aumente el tiempo de actividad y resistencia con la ejecución activa de parches en el kernel y la corrección de los puntos vulnerables. Aborde rápidamente los problemas urgentes e importantes de seguridad sin tener que reiniciar los sistemas, para evitar interrupciones en las aplicaciones esenciales.

Lista de aplicaciones permitidas (fapolicyd): cree una lista con los programas de confianza que pueden ejecutarse en una máquina o red para evitar el acceso no autorizado. Aproveche las políticas de seguridad predefinidas o personalice las suyas para detectar o impedir la ejecución de aplicaciones alteradas.

Protección de la cadena de suministros: utilice prácticas de desarrollo más seguras que incluyan el análisis estático de todo el código fuente para reducir los riesgos durante el ciclo de vida del sistema de software. De esta manera, podrá disminuir las fallas de seguridad antes de la distribución de las aplicaciones y mejorar el proyecto open source upstream.

Gestión flexible de los puntos vulnerables: utilice Red Hat Insights para integrar la gestión flexible de los puntos vulnerables y de la configuración de la seguridad. Personalice las políticas de seguridad, impleméntelas en todos los sistemas, realice controles para evitar las exposiciones y aplique las correcciones necesarias cuando corresponda.

Automatice los controles de seguridad según sea necesario y manténgalos a lo largo del tiempo

Base de confianza de hardware segura: utilice una base de confianza de hardware para garantizar que el software que utilizan sus sistemas no haya sido alterado ni manipulado. Proporcione una configuración uniforme de la seguridad del hardware para los tokens de hardware externos, como las tarjetas inteligentes y los módulos de seguridad de hardware (HSM).

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

Cifrado de discos vinculado a la red (NBDE): automatice el desbloqueo de los sistemas cifrados en las instalaciones o en la nube híbrida sin tener que gestionar las claves de cifrado de forma manual. Esta medida de seguridad adicional para los datos garantiza que solo se pueda acceder a ellos si se encuentran protegidos.

Cifrado flexible y moderno: proteja sus datos con ajustes criptográficos personalizables y uniformes en todo el sistema para cumplir con los requisitos normativos, y gestione la criptografía del sistema con un método sencillo de un solo comando.

Controles obligatorios de acceso de SELinux: minimice el riesgo de aumentos inapropiados de privilegios utilizando controles de acceso específicos para los archivos, los procesos, los usuarios y las aplicaciones. Personalice el acceso según la aplicación o el contenedor. Este nivel de control no solo refuerza la integridad y la confidencialidad de los datos, sino que también protege los procesos de los accesos que no son confiables.

Gestión centralizada de las identidades: utilice los controles de acceso basado en funciones o en políticas en todo el entorno según sea necesario, para gestionar la autenticación y la autorización de los usuarios. Combine esta función fácilmente con otros directorios o soluciones de gestión de acceso e identidades.

Cumpla con los requisitos normativos y optimice las auditorías

Certificaciones de seguridad verificadas: satisfaga los requisitos de cumplimiento de los clientes. El objetivo de Red Hat es que las versiones secundarias de Red Hat Enterprise Linux se validen de forma independiente de acuerdo con las normas FIPS, y que todos los lanzamientos con EUS obtengan la certificación de Common Criteria.

Herramientas de cumplimiento integradas: analice las configuraciones y los puntos vulnerables en un sistema local para validar el cumplimiento normativo. Luego, cree informes y estándares con OpenSCAP, y recurra a la automatización para corregir los sistemas que no cumplan con las normas. Combine estas herramientas con Red Hat Smart Management y Red Hat Insights para gestionar el cumplimiento normativo según sea necesario.

Grabación de las sesiones: registre la actividad administrativa en un archivo de video para cumplir con los requisitos de auditoría de seguridad o para reproducir la sesión en caso de que se deba resolver un problema tras un incidente. Puede elegir fácilmente a los usuarios o los grupos que desee grabar.

Funciones del sistema: automatice la configuración de la seguridad y mantenga la uniformidad en todos los sistemas a lo largo del tiempo para garantizar la protección y el cumplimiento normativo según sea necesario. Implemente y gestione la seguridad de Red Hat Enterprise Linux con menos recursos que antes utilizando las funciones para SELinux, los certificados, el cifrado NBDE, la grabación de sesiones, el protocolo SSH, las políticas de cifrado, etc.

Descubra todo lo que Red Hat Enterprise Linux tiene para ofrecer

Comuníquese con un representante de ventas de Red Hat o haga clic para conocer la forma en la que Red Hat Enterprise Linux puede ayudarlo a gestionar la seguridad y el cumplimiento normativo en toda su infraestructura de nube híbrida.

ACERCA DE RED HAT

Con Red Hat, los clientes pueden llevar la estandarización a todos los entornos, desarrollar aplicaciones directamente en la nube e integrar, automatizar, proteger y gestionar los entornos complejos a través de los servicios galardonados de soporte, capacitación y consultoría.

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
#F29077_0621