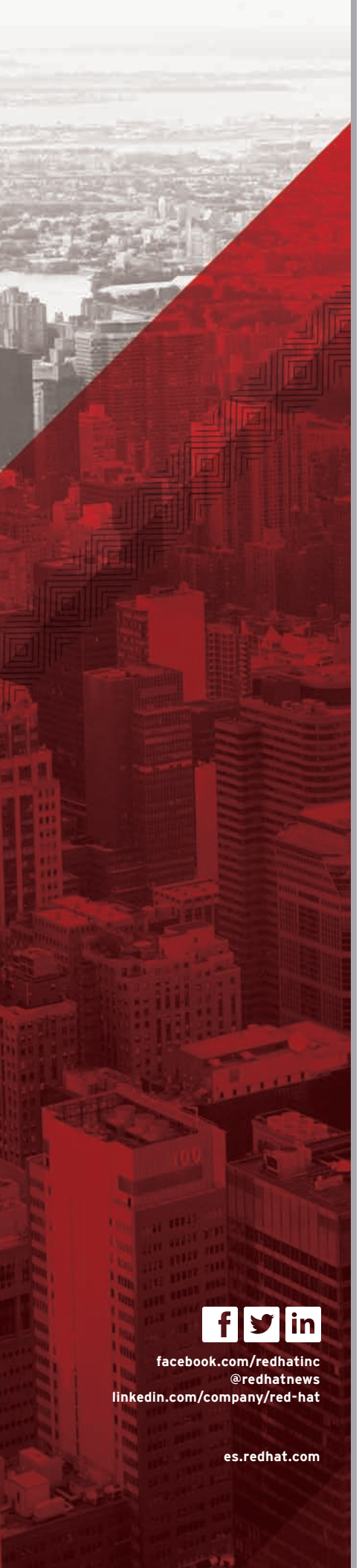


WHITEPAPER

LA SEGURIDAD Y LA INNOVACIÓN SE DAN LA MANO EN RED HAT

Gordon Haff

RESUMEN EJECUTIVO

Red Hat desarrolla software en colaboración con clientes de un amplio abanico de sectores, entre los que se incluyen servicios financieros y gubernamentales. Esto no solo promueve la innovación, sino que proporciona una valiosa orientación para las decisiones relacionadas con la seguridad de las características de los productos, los servicios o los procesos. Este planteamiento hace del software de infraestructura de Red Hat®, como Red Hat Enterprise Linux®, y de plataformas de aplicaciones, como Red Hat JBoss Enterprise Application Platform, una parte fundacional de algunos de los sectores más regulados y sensibles.

Debido al panorama actual de las amenazas, resulta más importante que nunca crear y poner en marcha sistemas seguros en todo su entorno de TI, incluidos los entornos de nube híbrida.

En este whitepaper, hablaremos del panorama actual de la seguridad y de cómo puede asociarse con Red Hat para alcanzar sus objetivos de seguridad, gestión de riesgos y cumplimiento. Esto incluye cumplir requisitos básicos comunes para mitigar las vulnerabilidades, implementar la gestión de configuración y establecer controles de acceso. Si bien estos requisitos no son nuevos, en el mundo digital de hoy en día se intensifican debido al incremento de la velocidad y el volumen de las amenazas, a la naturaleza abierta del mundo de las arquitecturas de TI y a la infraestructura, que es heterogénea e híbrida.

Por lo tanto, abordaremos el enfoque de Red Hat a la hora de crear sistemas seguros y de trabajar en comunidades upstream para corregir de manera proactiva las vulnerabilidades antes de que se conviertan en problemas. También hablaremos de Red Hat Insights, un servicio de gestión de suscripciones que puede identificar y resolver de forma proactiva los problemas técnicos de sus sistemas. Trataremos el papel de la automatización en la puesta en marcha de los procesos de seguridad y documentación del código con productos como Ansible Tower y Red Hat Satellite. Analizaremos el papel de DevOps a la hora de favorecer un proceso de TI más ágil que impulse las actualizaciones de código. Y veremos cómo Red Hat CloudForms ofrece un punto centralizado de control basado en políticas a través de entornos de TI híbrida.

Sin embargo, los sistemas de seguridad actual no están formados por características o soluciones de seguridad específicas que proporcionan una solución mágica. Se trata de adoptar una visión amplia de la seguridad (lo que significa realmente la gestión de riesgos, el cumplimiento y la gobernanza) y de su puesta en marcha de una manera adecuada para la empresa. Ese va a ser el verdadero objetivo.

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

es.redhat.com

"Los proyectos de software de código abierto que aprovechan las pruebas de desarrollo permiten que siga aumentando la calidad de su software, de modo que han elevado el listón de todo el sector".

ZACK SAMOCHA
DIRECTOR SENIOR DE PRODUCTOS
COVERITY

EL ROSTRO CAMBIANTE DE LA SEGURIDAD

El foso y las murallas de los castillos medievales suponían una barrera formidable para los posibles atacantes. Pero era una barrera que solo resultaba eficaz siempre y cuando los posibles atacantes no consiguieran encontrar un punto débil o no emplearan una táctica novedosa. La seguridad de TI tradicional también se basa principalmente en crear y proteger un fuerte perímetro para el hardware, las aplicaciones y los datos en las instalaciones. No pasa por alto las amenazas internas que surgen por mala voluntad o error. Pero no depende excesivamente de firewalls, sistemas de detección de intrusiones y controles de acceso para mantener a los "malos" a raya.

Hoy en día, la seguridad de la información debe adaptarse a un panorama cambiante. Ya se trate de ofrecer a los clientes y partners acceso a determinados sistemas y datos, como de permitir a los empleados utilizar sus propios smartphones y portátiles, utilizar aplicaciones de proveedores de software como servicio (SaaS) o aprovechar modelos de pago de servicios según consumo de proveedores de nube pública, ya no hay un solo perímetro. Utilizar de la manera más eficaz posible los activos de información de una organización puede requerir el intercambio de esa información con terceras partes autorizadas. Tanto el cumplimiento normativo como la gran intensidad y sofisticación de los ataques cibernéticos ponen aún más de relieve la necesidad de una estrategia de seguridad de TI que sea más profunda y tenga más facetas que la norma tradicional en la mayoría de las organizaciones.

Vemos que esta tendencia se refleja en la investigación de los analistas y en las charlas con clientes. Por ejemplo, el hecho de que la seguridad encabece habitualmente la lista de reticencias para la adopción de la nube pública en las encuestas no es una novedad para nadie. Sin embargo, no son los aspectos típicos de la seguridad de sistemas, como el acceso y el control, o los cortafuegos mal configurados, los que motivan estas reticencias, sino que son la jurisdicción de los datos, la capacidad para superar auditorías, el cumplimiento normativo y el cifrado integral verificable los factores que encabezan la lista. Y esos son solo los ámbitos en los que el proveedor de la nube tiene cierta responsabilidad directa.

La organización que gestiona la carga de trabajo también desempeña su propio papel en el establecimiento de la procedencia del software y la comprensión de las normativas y las certificaciones, lo que proporciona el acceso y los controles adecuados basados en políticas, la gestión de las relaciones con proveedores y, en general, el establecimiento de procesos formales y repetibles para la seguridad y la respuesta a los incidentes.

PENSAR EN LA SEGURIDAD

En este documento se abordan diversas tecnologías y capacidades relacionadas con la seguridad de la información. Sin embargo, la implementación de procesos eficaces de defensa, detección y disuasión no consiste en utilizar un determinado producto o componente. Se trata de establecer una base sólida que permita automatizar los procesos empresariales, institucionalizar buenas prácticas y solucionar problemas eficazmente cuando (no si) se producen. Como experto en seguridad, Bruce Schneier, señala que: "La seguridad no tiene que ser perfecta, pero los riesgos deben poderse gestionar".[1]

Un modelo conceptual común de las prácticas en materia de seguridad, la tríada CIA, se centra en tres aspectos de la protección (principalmente de los datos):

1. Confidencialidad: limitar el acceso a datos solo a las personas autorizadas a utilizarlos
2. Integridad: garantizar que una tercera parte no autorizada no ha alterado ni eliminado los datos
3. Disponibilidad: asegurar que los datos estarán disponibles cuando se necesiten

1 https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

"La errónea creencia de que los proveedores de nube son los únicos responsables de la seguridad de sus clientes disuade a las organizaciones de asegurarse de que sus empleados utilizan debidamente los servicios en la nube".

GARTNER
"CLOUDS ARE SECURE: ARE YOU USING THEM SECURELY?" SEPTIEMBRE DE 2015
G00281279

Los profesionales de la seguridad y de organizaciones como el National Institute of Standards and Technology[2] han desarrollado modelos más complejos que incluyen aspectos adicionales de seguridad, tales como la evaluación de los riesgos, la exactitud, la posesión física, la legalidad y la utilidad. Un tratamiento completo de las prácticas recomendadas en seguridad trasciende el ámbito de este documento. En lugar de ello, nos centraremos en tecnologías y prácticas novedosas o importantes relacionadas con arquitecturas híbridas, infraestructuras de nube nativa, el desarrollo de aplicaciones utilizando enfoques de DevOps y respuestas de seguridad y vulnerabilidad comerciales de código abierto.

La seriedad y la sofisticación de los ataques se refleja en el hecho de que puestos como el de director estratégico de seguridad de la información (CISO) son cada vez más frecuentes y de que los planes de respuesta a los incidentes están empezando a parecerse más a los asociados con la extinción de incendios. Hay varias razones para ello.

La primera es que la seguridad se debe abordar en el contexto de la empresa, en lugar de únicamente como un problema tecnológico. Esto implica, por ejemplo, definir la resistencia a los riesgos de la empresa en términos de tolerancia a las pérdidas. Un emisor de tarjetas de crédito sabe que va a tener pérdidas debido al fraude. Prevenir el fraude en su totalidad convertiría el uso de tarjetas de crédito en algo tan laborioso que nadie las usaría. En cambio, los emisores de tarjetas establecen suficientes controles para reducir las pérdidas a un nivel aceptable, al mismo tiempo que minimizan el impacto global en la experiencia del usuario.

Otra razón por la que la seguridad se toma más en serio es porque, al igual que con un incendio o un accidente de tráfico, cada minuto cuenta. Es necesario establecer con anticipación las funciones, las responsabilidades y los procesos. El conocimiento técnico es importante, pero también lo es disponer de planes de comunicación claros para compartir información con las personas que podrían verse afectadas por el incidente y con comunidades más amplias, como la prensa.

INTRODUCCIÓN A LA SEGURIDAD

La seguridad empieza con un sueño de estabilidad y seguridad, pero a menudo viene motivada por el miedo, la reticencia y la necesidad de evitar que los activos se vean comprometidos a lo largo de su ciclo de vida. Independientemente de la complejidad que puedan añadir las arquitecturas de TI actuales y el entorno de amenazas externo, es bueno empezar con tecnologías y prácticas probadas por el tiempo que se puedan ampliar al mundo actual.

El código abierto es un buen ejemplo de ello. El modelo de desarrollo de código abierto permite que sectores enteros acuerden estándares y animen a sus mejores desarrolladores a probar y mejorar constantemente la tecnología. Desarrollar software en colaboración con clientes de un amplio abanico de sectores, incluidos los servicios financieros y gubernamentales, proporciona una valiosa información que orienta los debates relacionados con la seguridad y las implementaciones de características de productos. Nadie puede resolver solo los problemas de seguridad de TI. Colaborar con las comunidades para resolver los problemas es el futuro de la tecnología.

Linux ha sido el beneficiario de una amplia gama de tecnologías relacionadas con la seguridad que se han creado con el modelo de código abierto. Algunas de estas capacidades son:

- Un firewall gestionado dinámicamente.
- SELinux para controles de acceso obligatorios.
- Una amplia gama de características de endurecimiento del kernel y del espacio de usuarios.
- Gestión de identidades y control de acceso.
- Hashes de contraseña basados en SHA-512.
- Cifrado del sistema de archivos.

2 Publicación especial 800-27 de NIST, revisión A

Además, el proceso de desarrollo de código abierto implica que, cuando se encuentran vulnerabilidades, toda la comunidad de desarrolladores y proveedores pueden colaborar para actualizar el código, introducir avisos de seguridad y realizar tareas de documentación de una manera coordinada.

Red Hat Enterprise Linux es la base de TI de algunos de los sectores más regulados y sensibles, ya que incorpora avances en seguridad de código abierto con métodos predecibles y que se pueden poner en práctica. Estos mismos procesos y prácticas se aplican en infraestructuras de nube híbrida a medida que la función del sistema operativo evoluciona y se expande para incluir nuevas prestaciones, como los contenedores de Linux. Además, los componentes se reutilizan en forma de microservicios y otras arquitecturas de bajo acoplamiento que interactúan mediante interfaces de programación de aplicaciones (API). Por ello, mantener la confianza en la procedencia de esos componentes y sus dependencias (en la creación de aplicaciones) se vuelve más importante, no menos.

APLICACIÓN DE LA SEGURIDAD

Tradicionalmente, se abordaba la seguridad como una función centralizada. Una organización podía establecer una fuente única de la verdad para los usuarios, los equipos y las identidades de servicio en un entorno completo y describir la información a la que estaban autorizados a acceder y las acciones que tenían permiso para realizar.

Hoy en día, la situación suele ser más complicada. Sigue siendo importante disponer de políticas de control de acceso que rijan las identidades de los usuarios, delegar la autoridad según sea conveniente y establecer relaciones de confianza con otros almacenes de identidades según se necesite. Sin embargo, los componentes de las aplicaciones que se ejecutan sobre Linux u otros entornos operativos pueden estar sujetas a múltiples sistemas de autorización y listas de control de acceso.

Es importante tener conocimiento y control de dichos entornos híbridos y heterogéneos. Por ejemplo, la supervisión y el cumplimiento en tiempo real de las políticas no solo permiten abordar cuestiones de fiabilidad y rendimiento antes de que los problemas se vuelvan graves, sino que también ayudan a detectar y mitigar los posibles problemas de cumplimiento. Este tipo de automatización reduce la cantidad de trabajo de administración de sistemas que se requiere. Sin embargo, también es una forma de documentar los procesos y reducir los procedimientos manuales propensos a errores. Constantemente se cita el error humano como una de las principales causas de los fallos de seguridad y las interrupciones.

La supervisión y la corrección operativas deben continuar a lo largo del ciclo de vida de un sistema. Todo empieza con el aprovisionamiento. Como con otros aspectos de la gestión de sistemas continuada, es importante mantener un historial completo de informes, auditorías y cambios.

La necesidad de disponer de planes y políticas de seguridad no termina cuando se retira la aplicación. La propiedad y las políticas relativas a los datos asociados con una aplicación deben entenderse bien de manera que puedan tomarse las medidas adecuadas para cumplir los requisitos de conservación y la comprobación del estado de los datos personales (PII).

Con las instancias tradicionales de aplicaciones de larga duración, mantener una infraestructura segura también significaba analizar y corregir automáticamente los desajustes de la configuración para establecer el estado final del host deseado. Esto sigue siendo a menudo un requisito importante. Sin embargo, con el papel cada vez más prominente que desempeñan las instancias "inmutables" de corta duración en los entornos de nube nativa, es igualmente importante crear sistemas seguros en primer lugar. Por ejemplo, puede establecer y aplicar políticas basadas en reglas en torno a servicios habilitados en las capas de una pila de software en contenedor.

Adoptar un enfoque de gestión de riesgos para la seguridad va más allá de implantar un conjunto eficaz de tecnologías. También es necesario considerar la cadena de suministro de software y tener establecido un proceso para resolver los problemas rápidamente.

Por ejemplo, es importante validar que los componentes del software provienen de una fuente de confianza. Los contenedores, un modelo ágil y simplificado para la distribución de aplicaciones, son un caso ilustrativo. Los contenedores son una manera sencilla y eficaz de ensamblar, distribuir e implementar software. La propia simplicidad puede convertirse en un malestar si el equipo de TI no garantiza que todo el software proviene de fuentes de confianza y cumple los más altos estándares de seguridad y compatibilidad.

Como describimos anteriormente, la respuesta a incidentes va mucho más allá de la ejecución de parches en el código. Sin embargo, una plataforma y un proceso de implementación de software ágiles con pruebas integradas sigue siendo una parte importante de la resolución de los problemas (y ayuda a reducir la cantidad de código erróneo que se introduce en la producción). Un canal de integración continua/distribución continua (CI/CD) que forme parte de un proceso de distribución de software de DevOps automatizado e iterativo implica que los elementos del código modular se pueden probar y publicar sistemática y puntualmente. Además, plegar explícitamente los procesos de seguridad en el flujo de trabajo de implementación de software hace que la seguridad sea una parte continuada del desarrollo del software, en lugar de simplemente un guardián que bloquea el paso a la producción.

GOBERNANZA Y CUMPLIMIENTO EN NUBES HÍBRIDAS

Si bien los temores reflexivos acerca de la falta de seguridad en las nubes públicas pueden ser ingenuos, sí que es cierto que las nubes públicas y las nubes híbridas introducen aspectos de riesgo y cumplimiento, así como retos que no tienen nada que ver con las reticencias que usted puede tener con los centros de datos tradicionales ubicados de manera local. Es importante entender sobre qué áreas sigue siendo usted responsable al utilizar las nubes públicas. En el caso de la infraestructura como servicio (IaaS), por ejemplo, necesita tener el mismo cuidado a la hora de externalizar y realizar el mantenimiento de su sistema operativo y aplicaciones como el que tiene cuando lo realiza en sus instalaciones.

Diversos marcos pueden ayudar a los ejecutivos y a los arquitectos de TI a evaluar y mitigar los riesgos asociados con el uso de proveedores de nube pública. Un buen ejemplo es la Matriz de Controles en la Nube (CCM) de la Alianza para la Seguridad en la Nube (CSA).[3]

La CCM de la CSA proporciona un marco de controles en 16 dominios, que incluye:

- Gestión de la continuidad del negocio y flexibilidad operativa.
- Cifrado y gestión de claves.
- Administración de identidades y acceso.
- Seguridad móvil.
- Gestión de amenazas y vulnerabilidades.

CCM v3.0.1 define 133 controles y acota la relación entre cada control y otros estándares, normativas y marcos de controles de seguridad aceptados en el sector, como ISO 27001/27002, ISACA PCI, COBIT, NIST, Jericho Forum y NERC CIP.

3 https://cloudsecurityalliance.org/group/cloud-controls-matrix/

Mediante el empleo de la CCM como marco de referencia, los productos y asociaciones de Red Hat son más relevantes en estos dominios:

- Control de cambios y gestión de la configuración.
- Seguridad de los datos y gestión del ciclo de vida de la información.
- Cifrado y gestión de claves.
- Administración de identidades y acceso.
- Seguridad de la infraestructura y la virtualización.
- Interoperabilidad y portabilidad.

Red Hat también trabaja con partners en todas estas áreas y proporciona soporte para otros dominios, como la gestión de amenazas e incidencias, proporcionando una respuesta eficaz y oportuna a las vulnerabilidades a medida que se descubren.

El diseño del servicio para la distribución a través de arquitecturas híbridas también se puede formar con metodologías de TI más tradicionales. Por ejemplo, la Estrategia de Servicio de la Biblioteca de Infraestructura de Tecnologías de Información (ITIL) es uno de los cinco módulos del ciclo de vida de ITIL. Puede guiarle a través del diseño, el desarrollo y la implementación de una estrategia de proveedor de servicio que se adecue a una estrategia organizativa. Por lo tanto, las prácticas de ITIL se pueden utilizar para ayudar a diseñar servicios completos que resulten apropiados para la TI híbrida.

Desde la perspectiva de la tecnología, un componente clave de la gobernanza y el cumplimiento es una plataforma de gestión de nube híbrida basada en políticas (CMP), como Red Hat CloudForms. Una CMP eficaz proporciona acceso a catálogos de servicios con aprovisionamiento automatizado delegado en funciones, aplicación de cuotas y reembolso en plataformas de virtualización y de nube. Admite una compleja orquestación y automatización de tareas y recursos basada en políticas para ayudar a garantizar la disponibilidad y el rendimiento del servicio. Todo esto ayuda al departamento de TI a conservar el control de las aplicaciones y la capacidad de la infraestructura.

DOMINIO	PRODUCTO Y CARACTERÍSTICAS DE EJEMPLO
Seguridad de aplicaciones y de interfaz	Red Hat proporciona API que se adhieren a los estándares del sector. Por ejemplo, los productos Red Hat JBoss Middleware son compatibles con las API Java™ SE y Java EE estándar, con SAML 2.0 para el inicio de sesión web único y con WS-Security para proteger los servicios web.
Garantía de auditoría y cumplimiento	Las funciones de auditoría de Red Hat CloudForms, así como las funciones de registro de una gran variedad de productos, sirven de soporte al proceso de auditoría. Red Hat también colabora con empresas que poseen productos de registro y análisis.
Control de cambios y gestión de la configuración	Tanto Red Hat Satellite como Ansible Tower ofrecen herramientas de aprovisionamiento y de gestión de la configuración.
Seguridad de los datos y gestión del ciclo de vida de la información	Funciones de Red Hat Gluster Storage como el archivado activo ayudan a dar soporte a la gestión del ciclo de vida de la información. Red Hat JBoss Data Grid emplea las funciones de autenticación y cifrado de Java SE para proteger los datos confidenciales almacenados en su almacén de datos distribuido en la memoria.

DOMINIO	PRODUCTO Y CARACTERÍSTICAS DE EJEMPLO
Cifrado y gestión de claves	Las funciones de cifrado de Red Hat Enterprise Linux incluyen hashes de contraseña basados en SHA-512, el cifrado del sistema de archivos y mejoras y certificaciones de criptografía del conjunto Suite B de la Agencia de Seguridad Nacional (NSA) de Estados Unidos. OpenJDK, que también se incluye, proporciona algoritmos criptográficos e interfaces para Red Hat JBoss Middleware según los estandarizó Java Community Process.
Gobernanza y gestión de riesgos	La automatización basada en políticas en Red Hat CloudForms es un ejemplo de una función que pueden utilizar las organizaciones para aplicar planes de gobernanza.
Administración de identidades y acceso	Una gestión centralizada de las identidades es parte de Red Hat Enterprise Linux, al igual que lo son los controles de acceso obligatorios que proporciona SELinux. La autenticación, la autorización y las funciones de auditoría a nivel de la aplicación están disponibles en Red Hat JBoss Middleware.
Infraestructura y virtualización	Red Hat Enterprise Linux, Red Hat Enterprise Virtualization, Red Hat OpenStack® Platform y Red Hat Atomic Host proporcionan una infraestructura sólida y segura.
Interoperabilidad y portabilidad	Los productos de Red Hat cumplen los estándares abiertos y proporcionan API abiertas. Los contenedores proporcionan un nuevo enfoque para la portabilidad de las cargas de trabajo en los entornos.
Seguridad móvil	Red Hat Mobile Application Platform proporciona un control centralizado de la seguridad y la gestión de las políticas.
Gestión de incidentes de seguridad, exhibición de documentos electrónicos y examen forense de la nube	Si se producen vulnerabilidades de seguridad, Red Hat proporciona a sus clientes los medios para subsanarlas y proteger sus sistemas.
Gestión de la cadena de suministro, transparencia y responsabilidad	Red Hat ayuda a proteger la cadena de suministro mediante la firma digital de todos los paquetes publicados (incluidos contenedores) y su distribución a través de canales seguros.
Gestión de amenazas y vulnerabilidades	Red Hat Insights es un servicio alojado que ayuda a identificar y a resolver de forma proactiva problemas técnicos en entornos de Red Hat Enterprise Linux y Red Hat Cloud Infrastructure. Red Hat también crea y apoya las definiciones de parches del proyecto Open Vulnerability and Assessment Language (OVAL), lo que proporciona versiones legibles por máquina de nuestros avisos de seguridad. OpenSCAP le permite controlar la configuración de seguridad de un sistema y examinarlo en busca de signos de fallos de seguridad mediante el empleo de reglas basadas en estándares y especificaciones.

Las prestaciones de Red Hat seleccionadas se asignan a dominios de seguridad de CSA (excluyendo dominios como la seguridad del centro de datos y la seguridad de los recursos humanos, ya que se centran principalmente en las prácticas empresariales y la seguridad física interna de una organización).

"Red Hat CloudForms es como una navaja suiza. Se pueden hacer muchas cosas diferentes en el entorno de TI con esta herramienta, incluidas las operaciones de información y datos sobre nuestra infraestructura. Hemos analizado las cifras para ver los recursos que hemos implementado y cuánto tiempo nos ha llevado. Nos hemos dado cuenta de que con la solución Red Hat hemos ahorrado casi 10 años de espera para entregar los recursos y nos ha supuesto casi 5 millones de dólares de ahorro tangible desde 2014. Además, gracias a Red Hat Insights podemos resolver problemas críticos antes de que se produzcan".

JASON CORNELL
DIRECTOR DE NUBE Y AUTOMATIZACIÓN DE INFRAESTRUCTURA
COX AUTOMOTIVE

ASÍ ES COMO RED HAT PUEDE AYUDARLE A CREAR UNA NUBE SEGURA

Hemos tratado algunas áreas de funcionalidad que son importantes para proteger infraestructuras de nube híbrida que utilizan productos de Red Hat. Esto incluye:

- Cifrado, controles de acceso obligatorios (SELinux) y gestión de la identidad en Red Hat Enterprise Linux 7.
- Inicio de sesión granular, basado en políticas y alertas visibles proporcionadas por Red Hat CloudForms, que permite una rápida respuesta automatizada en cargas de trabajo heterogéneas y varios tipos de nube.
- Gestión y aprovisionamiento automatizados proporcionados por Ansible Tower y Red Hat Satellite, que también supervisa los desajustes de la configuración y los corrige según sea necesario.
- La capacidad de utilizar Red Hat JBoss BRMS y Red Hat JBoss BPM Suite para crear flujos de trabajo que observan y responden a las transacciones que infringen las reglas empresariales específicas del dominio.

Por ejemplo, el Estándar de Seguridad de Datos (DSS) del Sector de Tarjeta de Pago (PCI) sigue madurando y requiere un cumplimiento más estricto de sus requisitos. A medida que las empresas implementan nuevas aplicaciones y soluciones de tecnología moderna, deben tener en cuenta las ramificaciones del cumplimiento en entornos compartidos. Red Hat CloudForms ayuda a sus clientes a tomar el control del entorno de virtualización al crear o gestionar entornos en la nube privada o híbrida. Red Hat CloudForms proporciona mecanismos sólidos para infraestructuras de nube con controles de gestión de virtualización avanzados, capacidades de gestión de nube privada o híbrida, y tecnologías de visibilidad operativa.[4] Esto incluye funciones de inicio de sesión agregado que permiten separar, registrar y asignar recursos por usuario, grupo, ubicación u otros atributos para controlar la granularidad según las políticas de Cgroups y SELinux.

Sin embargo, el enfoque de Red Hat en la seguridad es más amplio y más profundo incluso que sus importantes inversiones en tecnologías de producto. Hacer que los clientes trabajen en entornos y procesos seguros también significa tener conocimientos actualizados y participar directamente en proyectos de upstream, implementar sistemas de creación y pruebas reproducibles, distribuir paquetes de forma segura y responder con rapidez y eficacia a las vulnerabilidades.

Cuando se producen vulnerabilidades en la seguridad, nuestro Portal de clientes y los equipos de soporte técnico y de seguridad de productos ofrecen a los clientes de Red Hat distintas formas de abordar esas vulnerabilidades y salvaguardar sus sistemas. Cuando se produjeron los fallos de seguridad Heartbleed y Shellshock, los clientes de Red Hat contaron con los conocimientos, las aplicaciones y los parches necesarios para verificar su exposición y solucionar satisfactoriamente los posibles problemas en cuestión de horas desde el momento en el que los fallos se hicieron públicos.

Por ejemplo, Red Hat Insights puede ayudarle a identificar y resolver problemas técnicos de forma proactiva en entornos de Red Hat Enterprise Linux y Red Hat Cloud Infrastructure. Este servicio se centra en la seguridad y en rigurosos controles de implementación, aprovechando la red mundial de ingenieros y la amplia base de soluciones técnicas y problemas resueltos que ofrece la Red Hat Knowledgebase. El servicio analiza la información del sistema y la verifica frente a nuestra creciente base de datos de reglas deterministas. Estas reglas son el fruto del trabajo de nuestro equipo de fidelización y experiencia del cliente para identificar y documentar las mejores prácticas para optimizar las cargas de trabajo y evitar problemas. Red Hat Insights comparte esta información de forma proactiva y sugiere medidas para solucionar el problema con un formato sencillo y de uso sencillo. Red Hat Insights puede ayudarle a simplificar las operaciones y evitar posibles interrupciones de la actividad empresarial.

4 Para conocer más detalles acerca de cómo Red Hat Enterprise Linux, Red Hat Satellite y Red Hat CloudForms ofrecen una base que da soporte a la gestión continuada de los controles pertinentes y la aplicación de las políticas de PCI-DSS, consulte http://www.redhat.com/es/resources/pci-dss-compliance-red-hat

"Esperamos garantizar mayor seguridad y fiabilidad en nuestras aplicaciones de misión crítica, lo que incluye la gestión de datos para toda la red pública de hospitales y clínicas, así como la información de los planes de seguros privados".

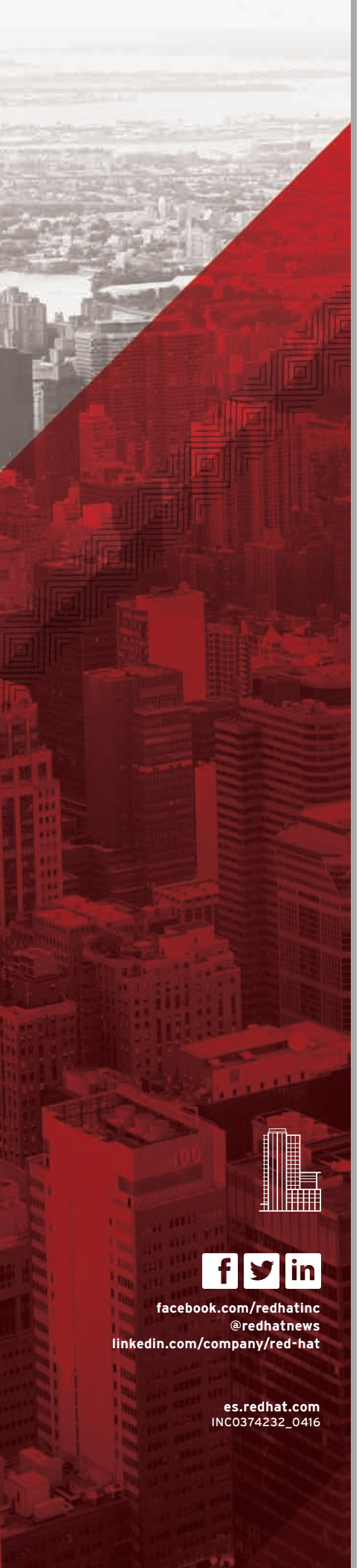
JOSÉ MARQUES
COORDINADOR GENERAL DE ANÁLISIS Y MANTENIMIENTO DEL MINISTERIO DE SALUD DE BRASIL

Red Hat también ayuda a proteger la cadena de suministro mediante la firma digital de todos los paquetes publicados y su distribución a través de canales seguros. La información sobre vulnerabilidades y erratas también se proporciona en un formato legible por máquina para que se pueda utilizar y, así, actuar en consecuencia a escala, como mediante el empleo de un escáner de protocolo de automatización de contenido de seguridad (SCAP). El registro del contenedor de Red Hat le permite saber que los componentes provienen de una fuente de confianza, los paquetes de la plataforma no se han alterado, la imagen del contenedor está libre de vulnerabilidades conocidas en los componentes de la plataforma o las capas, y la pila completa es compatible comercialmente.

El software empresarial de código abierto también requiere metodologías de revisión y puesta a prueba del código. Por ejemplo, el proceso de lanzamiento de Red Hat Enterprise Linux 7 no solo consistía en revisar los nuevos paquetes de fallos de seguridad y los problemas de embalaje, sino también en garantizar que las correcciones previas se habían incluido en la base de código upstream o que, en caso contrario, seguían estando presentes. Un sistema de compilación reproducible que registra todas las acciones permite a Red Hat saber dónde, cuándo, por qué y cómo se ha producido una versión determinada para que se pueda reproducir en el futuro, incluso años después, si es necesario.

Red Hat puede ofrecer así software de manera uniforme en parte gracias a la experiencia y a un proceso que siempre funciona. Pero también se debe a que los ingenieros de Red Hat consolidan sus conocimientos y realizan importantes contribuciones a las comunidades de upstream vinculadas a nuestros productos de suscripción. Esto nos ayuda a influir en los cambios que son importantes para nuestros clientes, incluyendo los relacionados con la seguridad.

Red Hat dispone de un equipo de seguridad de productos que analiza cada día las amenazas y las vulnerabilidades de todos nuestros productos y proporciona asesoramiento y actualizaciones pertinentes a través del Portal de Clientes. Este equipo permanece neutro y entiende las cuestiones que de verdad importan, en lugar de centrarse en los problemas principalmente teóricos. Nuestros clientes confían en nuestra experiencia para garantizar que pueden responder rápidamente y abordar las cuestiones que importan. Red Hat trabaja con otros proveedores de Linux, comunidades y empresas de software de código abierto con el fin de reducir el riesgo de sufrir problemas de seguridad compartiendo la información y la revisión por pares.



CONCLUSIÓN

La seguridad moderna trata de pasar de una estrategia que se centra en la minimización del cambio a otra que está optimizada para el cambio. Un flujo de trabajo motivado por la información debe proporcionar visibilidad en múltiples entornos, información agregada y medidas correctivas, incluso para los activos que pueden tener una duración de minutos. La seguridad debe ser un componente integral de todo el canal de distribución de software, en lugar de una casilla desconectada.

Red Hat puede ser su partner en esta transformación. Nuestros productos brindan las tecnologías y poseen las certificaciones (tales como Common Criteria y FIPS)[5] que usted necesita. Estamos profundamente integrados en la cadena de suministro de software de código abierto y poseemos la experiencia y los procesos necesarios para distribuir productos innovadores de código abierto de una manera que sea fiable, coherente y segura.

5 http://www.redhat.com/es/technologies/industries/government/standards

ACERCA DE RED HAT

Red Hat es el proveedor líder de soluciones de software de código abierto, que ha adoptado un enfoque basado en la comunidad para proporcionar tecnologías fiables y de alto rendimiento de nube, Linux, middleware, almacenamiento y virtualización. Red Hat también ofrece servicios de soporte, capacitación y consultoría que han sido premiados por su excelencia.

EUROPA, ORIENTE MEDIO Y ÁFRICA (EMEA)
00800 7334 2835
es.redhat.com
europe@redhat.com

TURQUÍA
00800-448820640

ISRAEL
1-809 449548

EAU
8000-4449549

La marca denominativa de OpenStack® y el logotipo de OpenStack son marcas de servicio/marcas comerciales registradas o marcas de servicio/marcas comerciales de OpenStack Foundation en EE. UU. y en otros países, y se utilizan con permiso de OpenStack Foundation. No estamos afiliados a OpenStack Foundation ni a la comunidad de OpenStack, y tampoco gozamos de su respaldo ni de su patrocinio.
Copyright © 2016 Red Hat, Inc. Red Hat, Red Hat Enterprise Linux, el logotipo Shadowman y JBoss son marcas comerciales de Red Hat, Inc. en Estados Unidos y en otros países. Linux® es la marca comercial registrada de Linus Torvalds en Estados Unidos y otros países.

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

es.redhat.com
INC0374232_0416