Automatice la seguridad de los datos

Aplicaciones para el sector de servicios financieros en la multicloud

La gestión de la seguridad y el cumplimiento en varias nubes reduce múltiples riesgos

Durante los últimos años, ciertos beneficios, como la agilidad y la flexibilidad, llevaron al sector de los servicios financieros a adoptar en poco tiempo aplicaciones desarrolladas originalmente en la nube. Sin embargo, optar por las implementaciones en la nube y la multicloud genera problemas de seguridad y cumplimiento, sobre todo cuando se trata de los datos de los clientes. Si bien la protección de los datos es una de las principales preocupaciones para las empresas, en los servicios financieros también implica proteger el dinero de los clientes.

El costo de las filtraciones de datos aumentará de USD 3 billones por año a más de USD 5 billones para el 2024, lo cual representa un crecimiento anual promedio del 11 %[1].

Juniper Research

Los bancos, los proveedores de servicios de pago, las aseguradoras y otras empresas de servicios financieros deben cumplir con una serie de normas de seguridad y privacidad, las cuales son cada vez más estrictas. Entre ellas se encuentran el Estándar de Seguridad de Datos (DSS) para la Industria de Tarjetas de Pago (PCI) y el Reglamento General de Protección de Datos (GDPR). A pesar de ser una ley europea, muchas empresas del mundo se esfuerzan para cumplir con el GDPR, el cual requiere realizar seguimientos, presentar informes y generar documentación de forma rigurosa.

Muchas de estas leyes contienen requisitos específicos sobre cómo las empresas deben resguardar la información personal de los clientes y, además, les exigen demostrar que protegieron sus datos en caso de pérdidas o filtraciones. Por ejemplo, la Ley de información sobre filtraciones de seguridad de California (SB-1386) fue la primera ley estatal en exigir la divulgación de las filtraciones y ha sido adoptada por otros estados de los Estados Unidos. Dispone que las empresas notifiquen a las personas afectadas "lo antes posible y sin demoras injustificadas, de acuerdo con las necesidades legítimas de las fuerzas del orden"[2], aunque también ofrece protección legal si se demuestra que los datos comprometidos estaban cifrados al momento de la pérdida.

El incumplimiento de este tipo de normas de privacidad de la información puede resultar costoso para las empresas de servicios financieros. Las filtraciones de datos tienen costos directos e indirectos. Un informe reciente de Juniper Research demostró que el costo de las filtraciones de datos aumentará de USD 3 billones por año a más de USD 5 billones para el 2024, lo cual representa un crecimiento anual promedio del 11 %[3]. Esto se debe principalmente al aumento de las multas por filtraciones de datos a medida que las regulaciones se vuelven más estrictas.

Las empresas también corren el riesgo de sufrir grandes pérdidas comerciales, ya que cada vez dependen más del ámbito digital. Por ejemplo, muy pocas personas en el sector de los servicios financieros olvidarán el costo, el daño a la marca y la distracción comercial que sufrió Equifax cuando no logró proteger la información personal de los clientes.

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

1 *Juniper Research. The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024, agosto de 2019.*

2 *Proyecto de ley 1386 del Senado de California SEC. 2. Sección 1798.29, promulgada en septiembre del 2002.*

3 *Juniper Research. The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024, agosto de 2019.*

Los entornos multicloud exigen una estrategia de automatización del cumplimiento

Los entornos de nube híbrida y multicloud se convirtieron rápidamente en un estándar para las empresas de servicios financieros. Según un informe reciente de Enterprise Cloud Index, los servicios financieros superaron a los demás sectores en la adopción de la nube híbrida, ya que alcanzaron al 21 % del mercado, en comparación con un promedio mundial del 18 %[5]. En estos entornos mixtos, supervisar el cumplimiento del sistema de forma manual resulta muy difícil y, en muchos casos, prácticamente imposible.

Otro informe reciente del SANS Institute demostró que el 54 % de las empresas encuestadas estaban adaptando sus estrategias de nube para cumplir con las normas cambiantes[6]. Aun así, las instituciones financieras deben migrar a la nube para mantener su competitividad.

El 54 % de las empresas encuestadas estaban adaptando sus estrategias de nube para cumplir con las normas cambiantes[4].

SANS Institute

Los equipos de TI que no cuentan con una estrategia de automatización efectiva se enfrentan a una serie de posibles inconvenientes relacionados con la verificación manual de la seguridad y el cumplimiento de los sistemas. Los procesos manuales pueden dar lugar a cambios de configuración y acciones no adecuados que carecen de información sobre el seguimiento de auditoría, un elemento clave del cumplimiento.

Estos procesos:

- Llevan mucho tiempo y son tediosos.
- Son propensos a los errores humanos.
- No se pueden repetir, compartir ni verificar.
- Son vulnerables a los errores de auditoría, debido a la información incompleta y poco uniforme del registro de cambios.
- Inhiben la comunicación entre los equipos de operaciones y de seguridad.

Afortunadamente, una estrategia sólida de automatización permite que las empresas mejoren sus sistemas de seguridad y cumplimiento, lo que reduce el riesgo general para el negocio. Si es efectiva, también ayuda a gestionar y optimizar los entornos multicloud complejos.

La automatización permite que las instituciones financieras gestionen la seguridad y el cumplimiento de manera más completa y eficiente, y también ayuda a evitar los errores humanos, ya que automatiza la aplicación de parches de software y la configuración del sistema. Tal como afirma Verizon en su informe Data Breach Investigations Report de 2019, "Los criminales cibernéticos se aprovechan de los errores humanos"[7]. Esta es otra forma en que la automatización respalda el cumplimiento y el enfoque general de seguridad.

4 *SANS Institute. SANS 2019 Cloud Security Survey, 2019.*

5 *Nutanix. Enterprise Cloud Index, 2019.*

6 *SANS Institute. SANS 2019 Cloud Security Survey, 2019.*

7 *Verizon. 2019 Data Breach Investigations Report, 2019.*

El cumplimiento como código: la automatización de la seguridad en la nube

Las estrategias automatizadas llevan a DevSecOps al siguiente nivel lógico: automatizar el cumplimiento normativo como parte del proceso. En el último tiempo, parece ser que las empresas de TI implementan todos sus procesos como código, y en el caso del cumplimiento no es muy diferente. Comienza a suceder lo mismo que cuando DevOps puro se transformó en DevSecOps, donde se automatizaron diversas validaciones de seguridad. Como en los servicios financieros hay requisitos esenciales de cumplimiento, no resulta extraño que las empresas del sector deban automatizarlo de la misma manera que codificaron la seguridad con DevSecOps. Esto dio como resultado DevSecComplianceOps.

Incorporar el cumplimiento a nivel mundial no es una tarea sencilla, especialmente si se tiene en cuenta que los requisitos normativos varían según la región. Por ejemplo, un banco internacional no solo tendrá que cumplir con los requisitos normativos globales, sino también con las disposiciones locales. Si se encuentra en Europa, es posible que deba cumplir con estándares adicionales específicos de sus filiales en Alemania. A diferencia del caso de DevSecOps, donde el código que se escribió para la seguridad funciona igual de bien en Malasia que en Alemania, muchas empresas de servicios financieros deben satisfacer los requisitos internacionales y locales de cumplimiento.

Como ese banco se encuentra en varias regiones, puede tener diferentes requisitos para proteger los datos con el firewall. Es posible que necesite prepararse para las normas futuras que podrían requerir mantener los datos en más de una nube pública, lo cual garantiza la continuidad y la resistencia empresarial. Como los requisitos normativos cambian constantemente, se vuelve aún más importante automatizar el cumplimiento para gestionar la complejidad en diversas regiones y tipos de nubes.

Reducir los riesgos y agilizar el cumplimiento de las normas de manera eficiente supone incorporar reglas de cumplimiento al código de la aplicación desde el primer momento. Este nuevo enfoque de DevSecComplianceOps permite que los equipos de TI logren una automatización localizada dentro de un marco globalizado, en un entorno escalable y más resistente.

Red Hat e Intel ayudan a automatizar la seguridad y el cumplimiento

Juntos, Red Hat e Intel ofrecen los sistemas de hardware y software complementarios que se necesitan para la automatización. Estos dos innovadores también han trabajado juntos en soluciones que combinan las tecnologías de infraestructura como código. Durante varios años, se han gestado iniciativas de estrecha colaboración que ofrecen soluciones muy integradas con ventajas adicionales.

Red Hat® Ansible® Automation Platform utiliza la tecnología de la plataforma de aplicaciones en contenedores de Red Hat OpenShift® para automatizar las implementaciones del código y la infraestructura en todos los entornos de nube. En combinación con Intel Software Guard Extensions (Intel SGX), que permite el cifrado de la memoria y el aislamiento basado en el hardware, los datos residen en "enclaves" confiables de la memoria. También se puede implementar en regiones locales de manera automática y uniforme. El uso de este entorno de datos automatizado, coherente y con seguridad mejorada como base para la empresa digital protege aún más el código, de modo que los desarrolladores puedan ofrecer soluciones más seguras.

Históricamente, las cargas de trabajo reguladas debían ejecutarse en un entorno exclusivo de confianza, lo que suponía una infraestructura específica dentro del banco. Gracias a la tecnología que protege los datos en uso, las cargas de trabajo pueden compartir los servidores en una o varias nubes. En otras palabras, usted puede ejecutar su carga de trabajo con confianza incluso en un entorno que no es confiable.

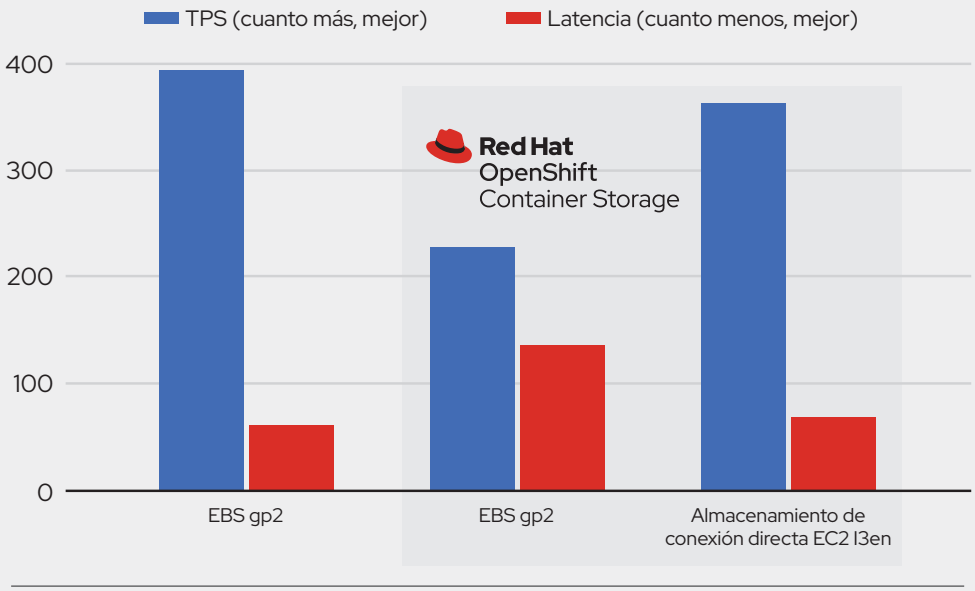

Figura 1. Sistema compatible con Intel SGX

Por ejemplo, si tenemos en cuenta los estrictos requisitos de cumplimiento del GDPR, utilizar métodos diferentes para proteger los datos en Europa y en Estados Unidos sería poco efectivo. Intel SGX permite que los desarrolladores creen un enclave más seguro en la memoria, de modo que incluso si los atacantes obtienen acceso físico a un servidor o mejoran sus privilegios administrativos con fines maliciosos, no podrán ver lo que se ejecuta en la memoria.

También les permite crear un sistema automatizado en código en Red Hat OpenShift con Red Hat Ansible Automation Platform. Este enfoque muestra que, durante un ataque a un servidor, el malhechor no puede ver lo que se está ejecutando en ese enclave. Del mismo modo, en las nubes en las que depende de un tercero, estos enclaves refuerzan la confianza, incluso cuando el entorno no es completamente confiable.

Antes del GDPR, los bancos podían ingresar al centro de datos y deshacerse de un disco físico que había dejado de funcionar. Sin embargo, ahora los clientes pueden exigir que elimine sus datos, y usted debe proporcionar pruebas verificables de que los eliminó o destruyó. Una práctica común es crear un mecanismo compensatorio que permite demostrar a los reguladores que esa información se cifró, por lo que ya no está más disponible.

Por ejemplo, imagínese que un empleado de una empresa de café se olvida en un taxi una computadora portátil con la información de las tarjetas de crédito de millones de clientes. De acuerdo con la mayoría de las leyes sobre violación de la privacidad, el banco debería indemnizar a las víctimas y dar a conocer la filtración al público en general. Sin embargo, esto no sería necesario si pudiese demostrar que la computadora tenía un software de protección del extremo que garantizaba el cifrado del disco duro. Por lo tanto, el software presenta pruebas del cifrado como mecanismo compensatorio.

El cumplimiento como código puede ofrecer un mecanismo de compensación similar en cualquier nube. Durante el desarrollo, la aplicación creada originalmente en la nube que utiliza Intel SGX con Ansible Automation Platform ofrece un contenedor de automatización del cumplimiento en torno a Red Hat OpenShift.

Conclusión

Gracias a Red Hat e Intel, su equipo puede unificar su canal de integración e implementación continuas (CI/CD) e incorporar el cumplimiento como código desde el diseño. Esto reduce el riesgo de errores humanos en el entorno de DevOps. El enfoque de DevSecComplianceOps acerca a los equipos de desarrollo y de operaciones, ya que automatiza el diseño, las pruebas y la implementación de las aplicaciones.

Al unificar este proceso, DevSecComplianceOps permite compartir y comprobar la repetibilidad principal y proporciona una plataforma común de automatización en los distintos equipos y nubes. En conjunto, estas funciones brindan la información que necesitan los equipos de seguridad, redes, Windows y Linux®, entre otros, para realizar sus aportes en la aplicación de la seguridad con el cumplimiento como código.

El enfoque del cumplimiento como código ofrece varios beneficios.

- Posibilidad de rastrear y repetir el cumplimiento normativo.
- Menos tiempo dedicado a las tareas repetitivas.
- Reducción del riesgo de downtime por medio de un enfoque coherente de gestión de la infraestructura.
- Minimización de los riesgos de errores sistemáticos mediante la automatización de los procesos de análisis, detección y resolución de problemas.
- Reducción del riesgo de errores humanos.
- Aceleración de los procesos de TI (por lo general, de días a minutos).
- Configuración y gestión uniformes en los entornos multicloud.

Obtenga más información

Estos ejemplos muestran de forma simplificada cómo las empresas de servicios financieros pueden proteger los datos y la información personal en las cargas de trabajo multicloud actuales utilizando el cumplimiento como código. Obtenga más información sobre cómo Red Hat e Intel permiten automatizar el canal de CI/CD sin comprometer la seguridad ni el cumplimiento.

ACERCA DE RED HAT

Red Hat es el proveedor líder de soluciones de software de open source para empresas, que adopta un enfoque basado en la comunidad para ofrecer tecnologías confiables y de alto rendimiento de Linux, nube híbrida, contenedores y Kubernetes. Red Hat ayuda a los clientes a integrar aplicaciones de TI nuevas y existentes, desarrollar aplicaciones nativas de la nube, estandarizar en nuestro sistema operativo líder del sector y automatizar, proteger y gestionar entornos complejos. Sus servicios galardonados de soporte, capacitación y consultoría convierten a Red Hat en un asesor de confianza para las empresas de Fortune 500. Como partner estratégico de proveedores de nube, integradores de sistemas, proveedores de aplicaciones, clientes y comunidades de open source, Red Hat puede ayudar a las organizaciones a prepararse para el futuro digital.

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

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

es.redhat.com
#F24716_0820