Automatização da segurança de dados

Aplicações de serviços financeiros multicloud

Gerenciar segurança e conformidade em diversas nuvens significa mitigar vários riscos

O custo anual das violações de dados aumentará de US$ 3 trilhões para mais de US$ 5 trilhões em 2024, um crescimento anual médio de 11%.[1]

Juniper Research

Nos últimos anos, benefícios como agilidade e elasticidade foram os principais motivadores para a rápida adoção de aplicações nativas em nuvem pelo setor de serviços financeiros. No entanto, a mudança para implantações em nuvem e multi-nuvem traz à tona questões de segurança e conformidade, especialmente quando se trata de dados de clientes. A proteção aos dados é uma das principais preocupações para qualquer empresa. Mas, no setor de serviços financeiros, manter a segurança dos dados significa proteger também o patrimônio financeiro dos clientes.

Bancos, provedores de serviços de pagamento e outras instituições de serviços financeiros precisam cumprir com uma série de padrões de segurança e privacidade cada vez mais rígidos. Dois desses padrões são: o Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS) e o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. Embora seja uma lei europeia, muitas empresas globais estão elevando o nível de suas políticas para cumprir com os padrões estabelecidos pelo GDPR. Isso exige processos rigorosos de monitoramento, comunicação e documentação para manter a conformidade.

Muitas dessas novas leis contêm requisitos específicos sobre como as organizações devem proteger os dados referentes a informações de identificação pessoal (PII). Eles também exigem que as empresas provem que protegeram os dados dos clientes mesmo em caso de perda ou roubo de dados. Como exemplo, podemos citar o Security Breach Information Act (SB-1386) da Califórnia, também adotado por outros estados dos EUA, que foi a primeira lei estadual a exigir que as violações fossem divulgadas publicamente. Essa lei obriga as organizações a notificar as pessoas atingidas "no tempo mais oportuno possível e sem atrasos injustificados, conforme as necessidades legítimas de execução da lei".[2] Entretanto, a norma oferece um porto seguro especificamente no caso da organização comprovar que os dados comprometidos estavam criptografados no momento da violação.

As empresas de serviços financeiros podem pagar caro por não cumprir as normas de privacidade de dados, como as mencionadas acima. As violações de dados resultam em custos tangíveis e intangíveis. Em um relatório recente, a Juniper Research constatou que o custo por ano das violações de dados aumentará de US$ 3 trilhões para mais de US$5 trilhões em 2024, o que representa um crescimento anual médio de 11%.[3] Esse aumento será motivado principalmente pelas multas mais altas impostas por normas mais rígidas.

As empresas também correm o risco de sofrer perdas significativas nos negócios à medida que se tornam mais dependentes da esfera digital. Por exemplo, muitas entidades do setor ainda se lembram do prejuízo financeiro e de imagem sofrido pela Equifax por não ter protegido adequadamente as informações de identificação pessoal dos seus clientes.

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

2 *California Senate Bill 1386, SEC. 2. Section 1798.29, promulgada em setembro de 2002.*

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

Ambientes multicloud exigem uma estratégia de automação para manter a conformidade

Os ambientes híbridos e de multicloud se tornaram em pouco tempo o padrão para as empresas de serviços financeiros. De acordo com o recente relatório Enterprise Cloud Index, o setor de serviços financeiros ultrapassou todos os outros em termos de adoção da nuvem híbrida, alcançando a marca de 21% do mercado em comparação com a média global de 18%.[5] Nesses ambientes mistos, monitorar manualmente a conformidade do sistema é uma tarefa ainda mais difícil e, em muitos casos, praticamente impossível.

Em outro relatório recente, o SANS Institute observou que mais da metade (54%) das organizações pesquisadas estavam ajustando suas estratégias de nuvem para atender à evolução das normas.[6] E, mesmo assim, as instituições financeiras precisam migrar para a nuvem a fim de continuarem competitivas.

54% das organizações pesquisadas estavam ajustando suas estratégias de nuvem para atender à evolução das normas.[4]

SANS Institute

Sem uma estratégia de automação eficaz, as equipes de TI enfrentam uma série de possíveis contratempos relacionados à verificação manual dos sistemas para evitar problemas de segurança e conformidade. Os processos manuais podem resultar em ações inadequadas e alterações de configuração que não possuem informações do registro de auditoria, um componente imprescindível para manter a conformidade.

Processos manuais são:

- Demorados e tediosos;
- Propensos a falhas humanas;
- Não reproduzíveis, compartilháveis ou verificáveis;
- Suscetíveis a falhas no processo de auditoria por produzirem informações de changelog incompletas ou inconsistentes;
- Desfavoráveis à comunicação entre as equipes de segurança e de operações.

Felizmente, com uma estratégia de automação sólida, as organizações podem aprimorar os processos de segurança e conformidade e, dessa forma, reduzir os riscos gerais para os negócios. Uma estratégia de automação eficaz também ajuda a gerenciar e simplificar ambientes multicloud complexos.

Com a automação, as instituições financeiras podem gerenciar operações de segurança e conformidade de modo mais abrangente e eficiente. Além disso, essa tecnologia ajuda a evitar as falhas humanas por meio da automação da aplicação de patches de software e da configuração de sistemas. Como exposto pela Verizon em seu Data Breach Investigations Report de 2019, "os cibercriminosos se aproveitam das falhas humanas".[7] Essa é mais uma área em que a automação ajuda a reforçar as medidas de conformidade e segurança em geral.

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.*

Conformidade como código: automação da segurança baseada na nuvem

As estratégias de automação levam a implementação de métodos de DevSecOps para o próximo nível lógico: a automação da conformidade como parte do processo. É fácil observar que, nos últimos anos, as equipes de TI passaram a implementar todos os processos como código. Isso também pode ser aplicado aos processos de conformidade. Da mesma forma como o DevOps evoluiu para o DevSecOps, em que várias validações de segurança são automatizadas, o mesmo está começando a acontecer com a conformidade. Levando em consideração os inúmeros requisitos, não é de surpreender que as empresas do setor de serviços financeiros tenham percebido a necessidade de automatizar os processos de conformidade à medida que passaram a adotar o DevSecOps e a incorporar as medidas de segurança no código. O resultado é o que chamamos de abordagem de DevSecComplianceOps.

Desenvolver processos de conformidade de escala global não é uma tarefa fácil, principalmente se levarmos em consideração os requisitos regulatórios específicos de cada local. Um banco multinacional precisará atender às exigências regulatórias de várias partes do mundo, além das regulamentações regionais. Por exemplo, um banco que opera na Europa precisa cumprir também com outros padrões de conformidade que são impostos especificamente às suas filiais na Alemanha. Diferentemente da situação de DevSecOps, em que um mesmo código para processos de segurança funciona bem na Malásia ou na Alemanha, muitas organizações de serviços financeiros precisam atender aos requisitos de conformidade globais e locais.

Levando em consideração a atuação desse mesmo banco em várias localidades geográficas, a instituição precisará cumprir com diferentes exigências para manter os dados protegidos por um firewall. Além disso, talvez seja necessário desenvolver um plano para atender a regulamentações futuras que exijam que os dados sejam mantidos em mais de uma nuvem pública, a fim de assegurar a resiliência e a continuidade dos negócios. Essas mudanças constantes nos requisitos regulatórios fazem com que a automação da conformidade seja uma medida ainda mais importante para gerenciar complexidades nas várias regiões e em diferentes tipos de nuvens.

Para reduzir os riscos e simplificar os processos com eficácia, é necessário incorporar as normas de conformidade ao código das aplicações desde o início. Ao adotar essa nova abordagem de DevSecComplianceOps, as equipes de TI podem implementar automações localizadas dentro de um framework globalizado e em um ambiente fortalecido e escalável.

A Red Hat e a Intel ajudam a automatizar a segurança e a conformidade

Juntas, a Red Hat e a Intel oferecem os componentes de hardware e software complementares necessários para a automação. Essas duas empresas inovadoras já colaboraram em outras soluções conjuntas que combinam tecnologias de infraestrutura como código. Essa parceria sólida produziu iniciativas que estão em desenvolvimento há vários anos e resultaram em soluções totalmente integradas com benefícios extras.

O Red Hat® Ansible® Automation Platform automatiza a implantação da infraestrutura e do código em qualquer ambiente de nuvem com o uso da tecnologia de plataforma de aplicações em container do Red Hat OpenShift®. Em combinação com o Intel Software Guard Extensions (Intel SGX), que permite o isolamento baseado em hardware e a criptografia de memória, os dados passam a residir em "territórios isolados" e de confiança na memória. Também é possível implantar essa solução conjunta de modo automático e consistente em localidades diferentes. Usar esse ambiente de dados automatizado, consistente e seguro como base para os negócios digitais oferece mais proteção ao código e ajuda os desenvolvedores a produzirem soluções mais seguras.

Historicamente, as cargas de trabalho submetidas a requisitos regulatórios eram executadas em um ambiente dedicado e de confiança, o que normalmente significava ter uma infraestrutura exclusiva para isso dentro do banco. Com o surgimento da tecnologia que protege os dados em uso, as cargas de trabalho podem compartilhar os mesmos servidores em uma ou mais nuvens. Em outras palavras, você pode executar sua carga de trabalho de maneira confiável mesmo em um ambiente não confiável.

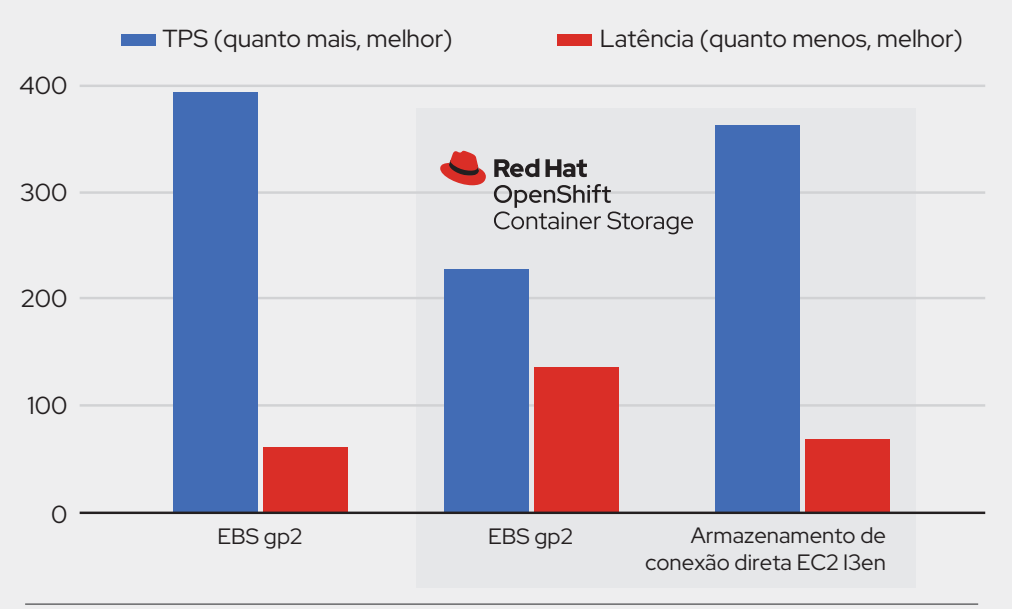

Figura 1. Sistema pronto para o Intel SGX

Por exemplo, levando em consideração os rigorosos requisitos de conformidade do GDPR, usar métodos diferentes para proteger dados na Europa e nos EUA seria uma medida ineficaz. Com o Intel SGX, os desenvolvedores podem criar um território isolado mais seguro na memória. Assim, mesmo se invasores tiverem acesso físico ao servidor ou forem capazes de elevar seus próprios privilégios administrativos de forma mal-intencionada, eles não conseguirão ver o que está sendo executado na memória.

Os desenvolvedores podem criar um sistema automatizado como um código do Red Hat OpenShift usando o Red Hat Ansible Automation Platform. Com essa abordagem, é possível verificar evidências de que um invasor foi impedido de ver o que está em execução em um determinado território isolado depois de um ataque ao servidor. De forma semelhante, é possível usar esses territórios isolados em qualquer nuvem administrada por terceiros para reforçar a confiança quando o ambiente não é totalmente confiável.

Antes do GDPR, os bancos podiam descartar como quisessem um disco físico danificado no datacenter. No entanto, depois do GDPR, os clientes passaram a ter o direito de exigir que os bancos excluam dados pessoais e disponibilizem provas auditáveis de que esses dados foram apagados ou destruídos. Uma prática comum é criar um mecanismo compensatório para entregar às autoridades reguladoras as provas de que tais dados não estão mais disponíveis porque foram criptografados.

Para exemplificar, imagine que um funcionário de uma empresa de café tenha esquecido em um táxi um laptop com informações de cartão de crédito de milhões de clientes. De acordo com a maioria das leis sobre violação de privacidade, o banco seria obrigado a ressarcir as vítimas e a notificar publicamente a violação. No entanto, se o laptop tiver um software de proteção de endpoint que assegure a criptografia do disco rígido, não haveria mais nenhuma obrigação quanto a ressarcir ou notificar os clientes afetados. Como um mecanismo compensatório, o software dá todas as provas de que a criptografia foi feita.

Em qualquer nuvem, a implementação de uma abordagem de conformidade como código pode ser considerada um mecanismo compensatório semelhante ao exemplo. No desenvolvimento, a aplicação nativa em nuvem que usa o Intel SGX com o Ansible Automation Platform oferece um wrapper de automação de conformidade para o Red Hat OpenShift.

Conclusão

A Red Hat e a Intel podem ajudar sua equipe a estreitar o pipeline de integração e implantação contínuas (CI/CD) e integrar o código como conformidade desde a concepção. Como resultado, os riscos de falhas humanas no ambiente de DevOps podem ser reduzidos. Essa abordagem de DevSecComplianceOps aproxima as equipes de desenvolvimento e de operações por meio da automação das tarefas de compilação, testes e implantação de aplicações.

A consistência na automação, viabilizada pelos métodos de DevSecComplianceOps, possibilita o compartilhamento e a verificação das diretrizes de reprodutibilidade e oferece uma plataforma comum de automação para diferentes equipes e nuvens. Juntos, esses recursos dão às equipes de segurança, redes, Windows, Linux® e outras áreas as informações de que precisam para desempenhar seu papéis individuais no reforço à segurança por meio da conformidade como código.

A abordagem de código como conformidade oferece diversos benefícios.

- Capacidade de reprodução e rastreamento para fins de conformidade
- Menos tempo gasto em tarefas repetitivas
- Redução do risco de períodos de downtime com a adoção de uma abordagem consistente de gerenciamento da infraestrutura
- Redução do risco de erros sistemáticos por meio de análises, detecções e soluções automatizadas
- Redução de risco de falhas humanas
- Processos de TI mais rápidos (muitas vezes, passando de dias para minutos)
- Gerenciamento e configuração consistentes em ambientes de multicloud

Saiba mais

Os exemplos aqui mencionados são alguns cenários simplificados de como entidades de serviços financeiros podem proteger os dados e as informações pessoais utilizadas em suas atuais cargas de trabalho multicloud usando uma abordagem de conformidade como código. Saiba mais sobre como a Red Hat e a Intel ajudam a aproveitar o potencial da automação do pipeline de CI/CD sem comprometer a segurança ou a conformidade.

SOBRE A RED HAT

A Red Hat é a líder mundial no fornecimento de soluções corporativas de software open source. Por meio da estreita parceria com as comunidades, a Red Hat oferece tecnologias confiáveis e de alto desempenho em Linux, cloud híbrida, containers e Kubernetes. A Red Hat ajuda os clientes a integrar aplicações de TI novas e existentes, desenvolver aplicações nativas em cloud e definir padrões com nosso sistema operacional líder do setor, além de automatizar, proteger e gerenciar ambientes complexos. Com serviços de consultoria, treinamento e suporte premiados, a Red Hat tem a confiança das empresas da Fortune 500. Como um parceiro estratégico para provedores de cloud, integradores de sistema, fornecedores de aplicações, clientes e comunidades open source, a Red Hat ajuda as organizações a se preparar para o futuro digital.

facebook.com/redhatinc
@redhatbr
linkedin.com/company/red-hat-brasil

AMÉRICA LATINA
+54 11 4329 7300
latammktg@redhat.com

BRASIL
+55 11 3629 6000
marketing-br@redhat.com

br.redhat.com
#F24716_0820