Aumente a segurança na nuvem híbrida

Proteja seus negócios com considerações essenciais de segurança nativa em nuvem

/Mantenha suas opções abertas

Red Hat

Por Lucy Kerner, diretora de evangelização e estratégia global de segurança da Red Hat

Conteúdo

Capítulo 1

Implante uma nuvem híbrida com foco em segurança

A adoção da nuvem continua a crescer em uso e popularidade. Hoje, 65% das organizações afirmam que usam significativamente a nuvem, e 72% das empresas têm uma estratégia de nuvem híbrida.[1]

A nuvem híbrida é uma arquitetura de TI que incorpora algum nível de portabilidade, orquestração e gerenciamento de cargas de trabalho em dois ou mais ambientes separados, mas que estão conectados, incluindo bare metal, ambientes virtualizados, nuvem privada e nuvem pública. Com a arquitetura de nuvem híbrida, você pode executar cargas de trabalho em qualquer ambiente conectado, movendo e usando recursos nesses ambientes de forma intercambiável.

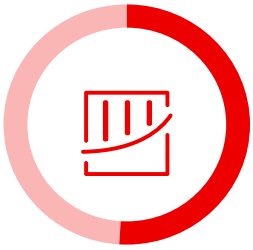
As organizações adotam ambientes de nuvem híbrida para

- Conectar infraestruturas, plataformas, aplicações e ferramentas de diferentes fornecedores.
- Aprimorar a eficiência e a escalabilidade.
- Reduzir custos
- Aumente a agilidade
- Otimizar a alocação de dados

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

Independentemente da etapa em que você esteja na jornada para adotar a nuvem híbrida, a segurança é uma grande preocupação, com 79% das empresas citando a segurança da nuvem como um desafio.[1] Normalmente, as vulnerabilidades de segurança da nuvem híbrida resultam em perda da supervisão e do controle dos recursos, incluindo uso não autorizado da nuvem pública, falta de visibilidade dos recursos, controle de mudanças inapropriado, gerenciamento ineficaz das configurações, controles de acesso ineficiente, erros humanos e muito mais. Usuários não autorizados podem se aproveitar dessas lacunas e acessar dados confidenciais e recursos internos, podendo causar um grande prejuízo.

A média global de gastos com violações de dados atingiu um novo recorde em 2023: **US$ 4,45 milhões**, com a perda de contas de negócios sendo responsável por **29,2%** desse custo.[2]



51%

das empresas afirmam que pretendem aumentar os investimentos em segurança devido a uma violação.[2]

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

Tanto o custo médio por registro envolvido em uma violação de dados quanto o tempo necessário para conter essas violações cresceram em 2023.[2] Ao adaptar seus métodos para considerar as diferença entre arquitetura de nuvem e on-premises, você pode implantar uma nuvem híbrida com foco em segurança para ajudar a superar esses desafios crescentes. Este ebook discute novas abordagens e considerações de segurança da nuvem híbrida.

277 dias

é o tempo médio para identificar e conter uma violação de dados em 2023.[2]

EUA

$ 1,02 milhões

são economizados quando uma violação é identificada e contida em até 200 dias.[2]

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

Capítulo 2

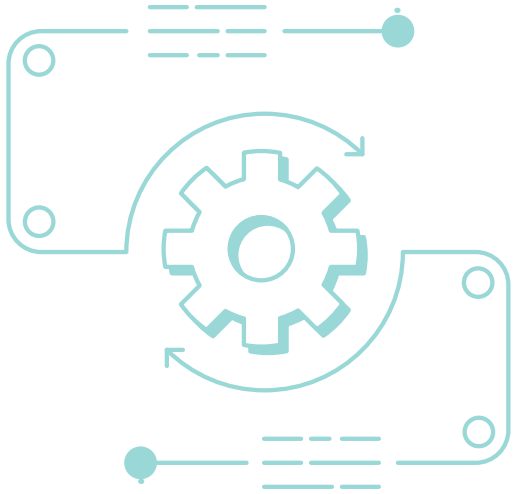
Segurança é um processo, não um produto

A eficácia das medidas de segurança depende de uma abordagem holística que incorpore pessoas, processos e tecnologias. O simples ato de implantar produtos e ferramentas com foco em segurança não é o suficiente para proteger sua infraestrutura, nuvem ou negócios. Você também deve considerar estratégias e processos de segurança para maximizar a eficácia dos seus produtos e reduzir riscos.

Você pode adotar essas estratégias e processos ao longo do tempo, à medida que as tecnologias, ameaças e necessidades evoluem. Ambientes de nuvem híbrida exigem que você mude suas abordagens de segurança, e como eles não têm um perímetro definido, as abordagens de segurança tradicionais são ineficientes.

Ter um controle de acesso e um gerenciamento de identidades centralizados é fundamental para as abordagens de segurança voltadas para a nuvem. É aplicado o princípio de menor privilégio para fornecer acesso aos usuários somente quando necessário. Essa abordagem exige a auditoria dos direitos de acesso atuais de cada usuário e uma reavaliação para determinar o nível de acesso.

Além disso, a segurança em nuvem híbrida também requer uma estratégia de segurança em camadas com defesa em profundidade que usa os recursos e cada camada em seu ambiente, incluindo sistemas operacionais, plataforma de aplicações em containers e ferramentas de automação.



Sistema operacional

Busque ferramentas integradas que ajudem você a atender aos requisitos de conformidade de segurança, implementar segurança física, aprimorar a segurança de rede, controlar o acesso de usuários, isolar processos e aumentar a segurança dos dados. Por exemplo, OpenSCAP, USBGuard, Security-Enhanced Linux® (SELinux), gerenciamento de identidade e Network Bound Disk Encryption.

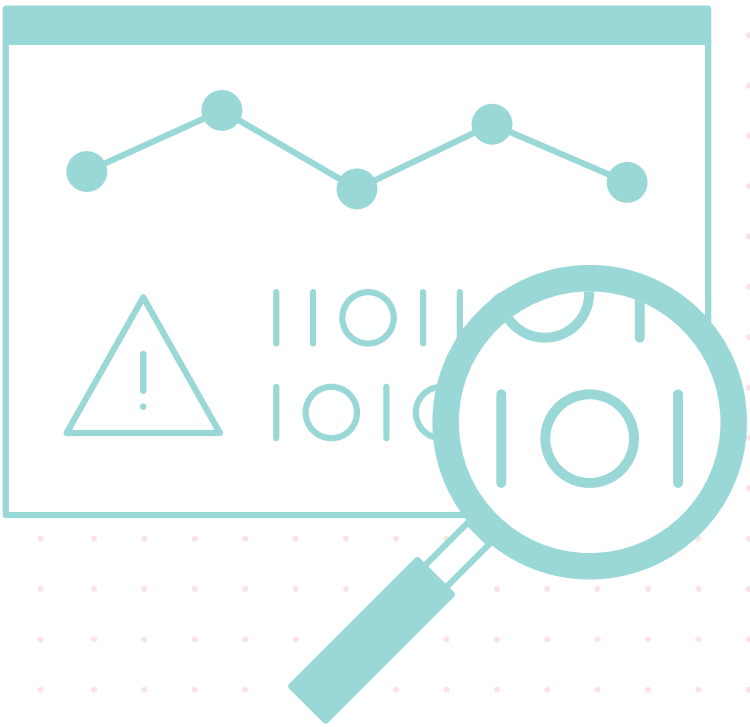
Plataforma de aplicações em containers

Use recursos integrados em sua plataforma e o Kubernetes para aumentar a segurança de containers. Por exemplo, políticas de segurança de pod, controles de tráfego de rede, controles de entrada e saída do cluster, controles de acesso baseado em função (RBACs), gerenciamento de certificados integrados e microssegmentação de rede.

Ferramentas de automação

Escolha uma plataforma e um linguagem de automação que todos em sua organização, incluindo equipes de desenvolvimento, operações de TI, segurança e conformidade, possam aprender a usar com facilidade. Busque recursos de controle de acesso, geração de logs e auditoria.

Também é importante revisitar seus processos e suas ferramentas de segurança existentes. Certifique-se de que você está usando todas as funcionalidades disponíveis e determine se é possível modificar ou redefinir alguma configuração para melhorar a proteção, ou se é necessário implementar novos processos e ferramentas.



1. Crie um inventário de seus ativos e ferramentas de TI atuais.
2. Registre suas atuais arquiteturas de rede e segurança, políticas de cibersegurança, processos de trabalho e lacunas de habilidades e talentos.
3. Defina um modelo de ameaças e determine sua tolerância a riscos e suas estratégias de mitigação para violações de segurança.
4. Avalie suas arquiteturas, políticas e processos para identificar áreas que precisam de mudanças.
5. Avalie suas ferramentas e seus ativos atuais para determinar se são capazes de acomodar suas estratégias e processos atualizados. Registre e planeje como abordar possíveis lacunas de segurança.

As seções a seguir abordam considerações importantes sobre segurança em nuvem híbrida e oferecem dicas para melhorar sua proteção.

Capítulo 3

Considerações de segurança 1

Comece com uma base sólida

Por que isso é importante?

Quando suas cargas de trabalho estão divididas em vários ambientes ou tecnologias open source não examinadas são usadas em seu ambiente, pode ser difícil identificar onde se encontram as vulnerabilidades. Além disso, será difícil reduzir os riscos de uma segurança em várias camadas sem uma base de segurança sólida. Usar software open source diretamente de comunidades upstream pode dar brecha para riscos de segurança e ataques à cadeia de suprimentos, que exploram pontos vulneráveis em serviços e software de terceiros para atingir um alvo final. Esses ataques acontecem de várias maneiras, como sequestro e atualizações de software e injeção de código mal-intencionado em softwares legítimos. Inclusive, houve um aumento anual de 742% nos ataques à cadeia de suprimentos e software nos últimos três anos.[3] Por esse motivo, adotar uma base unificada, estável e focada em segurança é essencial para proteger seus negócios.

Recomendações e práticas recomendadas

Reduza os riscos de segurança da cadeia de suprimentos de software com um software open source de um fornecedor de open source empresarial confiável, como a Red Hat, que oferece suporte de nível empresarial durante todo o ciclo de vida do software. Uma fornecedor de open source empresarial desenvolve seu software com um processo de segurança robusto da cadeia de suprimentos de software, que inclui selecionar o software open source em nome dos clientes. Isso garante que o software open source usado pelo cliente seja confiável, resiliente e seguro para consumo.

Além disso, é importante executar aplicações críticas em uma plataforma que tenha recursos de segurança integrados. Assim, os clientes terão uma segurança de base confiável para executar aplicações críticas, incluir recursos de segurança de várias camadas para reduzir riscos e implementar automação de conformidade e segurança.

Priorize uma base focada em segurança para aplicações e processos adotando um sistema operacional resiliente e confiável que é fortalecido pela estabilidade e segurança de soluções como o Red Hat® Enterprise Linux®. Isso fornece uma base estável para você escalar com confiança aplicações importantes, manter a conformidade de segurança e implementar novas tecnologias de maneira consistente em ambientes bare-metal, virtuais, em containers e em todos os tipos de ambientes de nuvem.

[3] Sonatype. "9th Annual State of the Software Supply Chain", 2023.

O **Red Hat Enterprise Linux** é a base de grande parte do portfólio da Red Hat. Devido aos recursos de segurança que oferece, ele é o sistema operacional que várias empresas confiam.

Com o Red Hat Enterprise Linux, você pode:

Reduzir os riscos de dados ou sistemas expostos com recursos de segurança integrados, como aplicação de patches no kernel em tempo real. Dessa forma, é possível aplicar patches de segurança sem a necessidade de reinicializar ou interromper o runtime. Há também outros recursos de segurança integrados, como listas de permissão de aplicações, que consistem em especificar o índice de aplicações ou arquivos executáveis aprovados que têm permissão para serem executados no sistema por um usuário específico, o SELinux para aplicar controle sobre os arquivos, processos, usuários, aplicações e muito mais com alta granularidade.

Automatizar a proteção de dados em escala e mantê-la ao longo do tempo com recursos de segurança integrados, como o Network Bound Disk Encryption, que permite a automação do desbloqueio de sistemas criptografados sem a necessidade de gerenciar chaves de criptografia. Além disso, com as políticas de criptografia implantadas em todo o sistema, você pode focar em manter os dados protegidos e atender aos requisitos de conformidade com configurações criptográficas consistentes e personalizáveis que suprem suas demandas de políticas específicas do site e muito mais.

Atenda aos requisitos de conformidade e otimize as auditorias. O Red Hat Enterprise Linux oferece verificação e correção de conformidade integradas com o OpenSCAP. Assim, você executa verificações de configuração e vulnerabilidade em um sistema local para validar a conformidade em relação a uma grande variedade de padrões de segurança do setor.

Com a abordagem de segurança de base oferecida pelo Red Hat Enterprise Linux, as soluções em camadas executadas nele, como o **Red Hat OpenShift**, proporcionam proteção profunda para containers e Kubernetes. A Red Hat estende os recursos de segurança até a stack e os componentes do Kubernetes. Da mesma forma, com recursos de segurança integrados, o **Red Hat Ansible Automation Platform** permite que empresas implementem automação de segurança e conformidade em escala.

Etapas táticas

Quando estiver começando sua jornada de segurança em nuvem híbrida, tome estas medidas:

Escolha versões disponíveis comercialmente

Migre seu software open source diretamente de projetos open source de upstream para versões confiáveis disponíveis comercialmente. Essas versões são testadas e validadas para reduzir os riscos de bugs e vulnerabilidades de segurança. Além disso, podem incluir suporte empresarial que fornece rapidamente patches de segurança e oferece orientação de como configurar seu software para que fique seguro. Ao adotar um software open source de um fornecedor de open source empresarial confiável, você tem a garantia de que o software foi desenvolvido com um processo de segurança robusto para a cadeia de suprimentos de software e que você receberá suporte de nível empresarial durante todo o ciclo de vida do software. Tudo isso permite que empresas utilizem software open source e, ao mesmo tempo, minimizem os riscos de segurança.

Escolha uma plataforma com funcionalidades de segurança integradas

É fundamental escolher uma plataforma (como sistema operacional, plataforma de aplicação de containers e plataforma de automação) com recursos de segurança integrados. Assim, os clientes terão uma segurança de base confiável para executar aplicações críticas, incluir recursos de segurança de várias camadas para reduzir riscos e implementar automação de conformidade e segurança em escala.

Implemente segurança em todo o stack de tecnologia.

Depois que você estabelecer uma base para a segurança, certifique-se de que as tecnologias em camadas executadas nessa base herdam os benefícios de segurança e trabalham em conjunto para proporcionar uma segurança multicamadas.

Capítulo 4

Considerações de segurança 2

Implemente uma cadeia de suprimentos confiável com o DevSecOps

Por que isso é importante?

Em 2023, 12% das violações de dados ocorreram devido a um ataque à cadeia de suprimentos de software.[2] Usar software open source diretamente de comunidades upstream pode dar brecha para vulnerabilidades de segurança e ataques à cadeia de suprimentos, que exploram pontos vulneráveis em serviços e software de terceiros para atingir um alvo final. Esses ataques acontecem de várias formas, como sequestro de atualizações de software e injeção de código mal-intencionado em softwares legítimos.

Como a segurança não costuma ser uma prioridade quando se trata de desenvolvimento de aplicações e implantação de infraestrutura, é comum que as abordagens de segurança compartimentalizadas gerem lacunas de segurança e esforço em dobro. Com o aumento da velocidade do desenvolvimento e da flexibilidade das implantações, ficou ainda mais importante considerar a segurança durante todo o processo.

Recomendações e práticas recomendadas

Para adotar uma abordagem focada em segurança na sua cadeia de suprimentos de software, a primeira etapa é desenvolver uma mentalidade de DevSecOps. De acordo com a mentalidade de DevSecOps, as equipes de desenvolvedores de aplicações, operações de TI e segurança devem trabalhar em conjunto para implementar a cadeia de suprimentos de software em todo o ciclo de vida de desenvolvimento do software (SDLC) e no ciclo de vida da infraestrutura, fundamentado em uma base de open source fortalecida para segurança empresarial em uma nuvem híbrida.

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

O DevSecOps automatiza a integração de segurança em todas as etapas do ciclo de vida do desenvolvimento de software, do projeto inicial até a integração, testes, implantação e entrega.

Benefícios de adotar um processo de DevSecOps:

- Ajuda as equipes de TI e segurança a superar os desafios relacionados a pessoas, processos e tecnologias.
- Possibilita maior eficiência, consistência, capacidade de repetição e colaboração.
- Reduz erros humanos e, consequentemente, os riscos.

Com o DevSecOps, a segurança se torna uma responsabilidade compartilhada que é integrada do início ao fim. Em vez e uma única equipe desconectada ficar responsável pela configuração da política de segurança, os membros das equipes de segurança, desenvolvimento e operações trabalham juntos, compartilhando visibilidade, feedback, aprendizado e insights. Nesse tipo de abordagem, os processos de segurança são integrados desde o início do desenvolvimento da aplicação e da implantação da infraestrutura, aumentando a proteção.

Os desenvolvedores de aplicações que criam novos recursos de software para as organizações precisam aprimorar significativamente a postura de segurança, bem como reduzir a carga cognitiva. A segurança precisa ser implementada em todo o SDLC: no etapa do código, por meio de verificações de segurança de aplicações integradas para detectar problemas logo no início no SDLC e reduzir downtimes prolongados; na etapa de versão, protegendo sistemas de versão usando fluxos de trabalho de integração e entrega contínuas (CI/CD) focados em segurança; e nas etapas de implantação e runtime com templates de golden path (caminho dourado), análise de vulnerabilidades, assinaturas de artefatos, atestados, procedência, pontos de execução de políticas e listas de materiais de software (SBOMs).

Também é necessário criar uma estratégia para garantir que as tecnologias open source usadas por suas equipes venham de fontes confiáveis, recebam patches de forma contínua e automática e sejam configuradas com foco em segurança. Além disso, você deve incentivar o uso de ofertas de open source empresarial que incluam suporte empresarial em todo o ciclo de vida útil.

Ao usar ofertas open source empresariais, como as que a Red Hat oferece, você aproveita mais de 30 anos de experiência que a empresa tem em proteger a cadeia de suprimentos de software open source de suas soluções. Além disso, as empresas precisam de soluções para implantar, gerenciar e proteger as frotas de clusters Kubernete, bem como uma maneira unificada de criar, modernizar e implantar aplicações de forma segura e em escala.

O **Red Hat OpenShift Platform Plus** é uma plataforma unificada que inclui o Red Hat OpenShift, Red Hat Advanced Cluster Security for Kubernetes, Red Hat Advanced Cluster Management for Kubernetes, Red Hat Quay e Red Hat OpenShift Data Foundation. Essa plataforma ajuda empresas a criar, modernizar e implantar aplicações em containers no Kubernetes de maneira segura e em escala. Segurança multicluster, conformidade, gerenciamento de dados e aplicações são incluídos para possibilitar consistência em toda a cadeia de suprimentos do software.

Etapas táticas

Siga estas ações ao implementar aprimoramentos de DevSecOps e de segurança da cadeia de suprimentos de software.

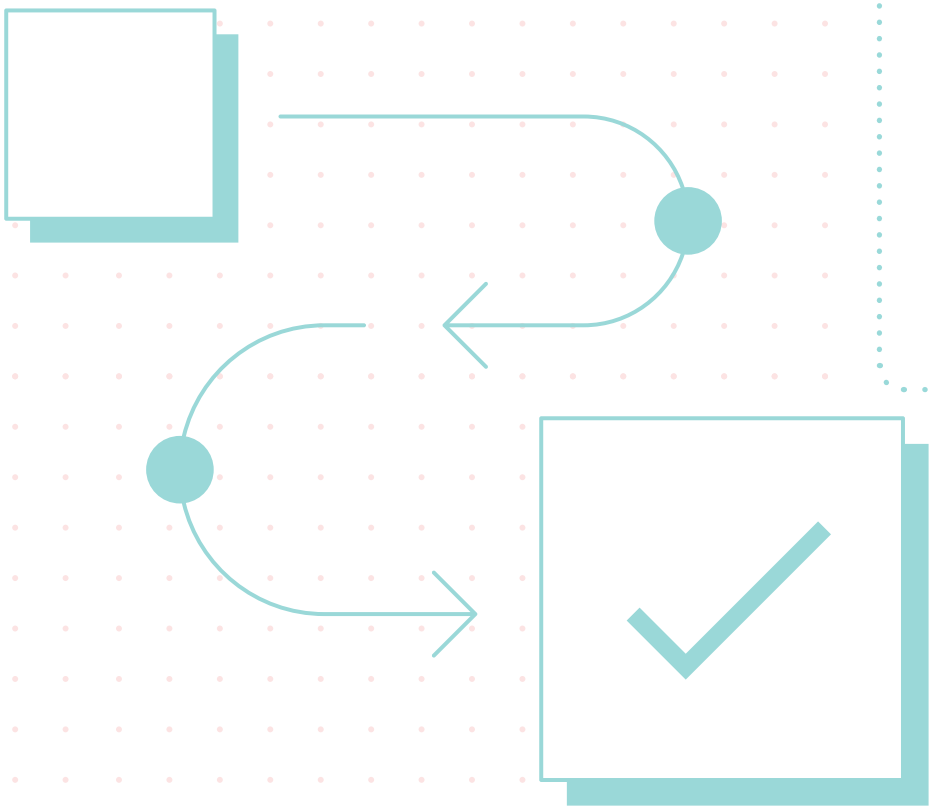
Comece com pouco e cresça aos poucos.
Escolha um único projeto para começar. Incentive experimentos e aprimoramentos iterativos e contínuos para aperfeiçoar e otimizar seu processo. Celebre as conquistas e valorize as pessoas na sua organização.

Defina metas e linhas do tempo que todos concordem.
Transparência é fundamental. Certifique-se de que todos os envolvidos entendam e concordem com as metas e as linhas do tempo do projeto.

Treine sua equipe em várias áreas.
Defina trajetórias de aprendizagem sobre segurança, infraestrutura e desenvolvimento que sejam atualizadas com frequência e que possam ser acessadas a qualquer momento por todos os membros da equipe.

Crie um grupo de trabalho de segurança.
Crie uma equipe integrada e multidisciplinar para definir casos de uso e estratégias de segurança. Aprenda com outras pessoas. Aproveite as descobertas feitas por outras organizações.

Implemente segurança em todo o SDLC com uma plataforma de aplicação unificada.
A segurança precisa ser implementada em todo o SDLC: no etapa do código, por meio de verificações de segurança de aplicações integradas para detectar problemas logo no início no SDLC e reduzir downtimes prolongados; na etapa de versão, protegendo sistemas de versão usando fluxos de trabalho de integração e entrega contínuas (CI/CD) focados em segurança; e nas etapas de implantação e runtime com templates de golden path (caminho dourado), análise de vulnerabilidades, assinaturas de artefatos, atestados, procedência, pontos de execução de políticas e listas de materiais de software (SBOMs).



Capítulo 5

Considerações de segurança 3

Use automação e gerenciamento para proteger sua nuvem híbrida

Por que isso é importante?

Configurações incorretas e controle de alterações inadequado representam as principais ameaças de segurança.[4] Configurações incorretas podem, inclusive, deixar os sistemas vulneráveis a ataques. O controle de alterações é essencial para entender quem modificou as alterações, quando isso foi feito e o que foi mudado nos ciclo de vida do sistema.

Automação, gerenciamento e IA podem ajudar sua empresa a simplificar as operações diárias e a integrar a segurança em processos, aplicações e infraestrutura desde o início. Ter uma estratégia de automatização e gerenciamento em vigor na sua organização pode ajudar a reduzir erros humanos e oferecer velocidade, consistência, capacidade de repetição e a opção de fazer verificações e auditorias. Além disso, uma estratégia centralizada de automação e gerenciamento ajuda a aprimorar a segurança e a conformidade, ajudando empresas a integrar a segurança no desenvolvimento de aplicações e nas operações de TI em todo o ciclo de vida. Assim, as organizações conseguem implementar o DevSecOps com sucesso. Na verdade, incorporar automação, gerenciamento e IA aos processos de segurança pode reduzir o custo médio de uma violação em 39,3%, mas apenas 28% das organizações já colocaram isso em prática.[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", outubro de 2023.

Recomendações e práticas recomendadas

Implemente uma estratégia de automação e gerenciamento em toda a empresa para acompanhar o ritmo dos requisitos dinâmicos de segurança, risco e conformidade. Ao adotar uma estratégia consistente de automação e gerenciamento para sua nuvem híbrida, você aproveita maior agilidade, capacidade de repetição, consistência e auditoria simplificada.

Uma estratégia unificada de automação e gerenciamento reduz o risco de configurações incorretas e erros manuais em toda a sua organização. A automação e o gerenciamento otimizam e aumentam a consistência do gerenciamento de infraestruturas, desenvolvimento de aplicações e operações de segurança para aprimorar a proteção, a conformidade e o controle de alterações. Isso permite a você:

Configurar recursos de modo consistente de acordo com políticas pré-aprovadas e mantê-las proativamente de modo repetível durante o ciclo de vida.

Identificar rapidamente sistemas que exigem aplicações de patches ou reconfiguração.

Otimize a aplicação de patches e as configurações do sistema de acordo com linhas de base definidas e de modo consistente em diversos sistemas.

Facilite auditorias e soluções de problemas com registros de ações gravados automaticamente.

As empresas dependem da automação da TI para gerenciar a segurança em ambientes operacionais, aplicações, operações de segurança e nuvem híbrida cada vez mais complexos. **O Red Hat Ansible Automation Platform** é uma plataforma de automação de ponta a ponta que oferece um framework empresarial consistente para criar e operar a automação da TI em escala, priorizando a segurança em cada etapa do processo. Ele ajuda a aprimorar a eficiências, aumenta a produtividade, auxilia no controle de riscos e gastos e permite que equipes automatizem a consistência de segurança e conformidade em toda a empresa de forma repetível, além de oferecer conteúdo de automação certificado para responder a ameaças de maneira coordenada com o suporte empresarial em tempo integral da Red Hat.

O Red Hat Ansible Automation Platform oferece tudo, de gerenciamento de configurações até aplicação de patches e correções, tudo automatizado. Isso ajuda as organizações a gerenciar processos de segurança automatizados para antecipar ataques maliciosos. Além disso, o Red Hat Ansible Automation Platform pode funcionar como um ponto de integração para soluções de segurança, utilizando conteúdo de parceiros certificados como CyberArk, IBM e Palo Alto Networks. Isso permite que os usuários automatizem a gestão e integração de uma ampla variedade de tecnologias de segurança externas.

Com gerenciamento de identidades e controles de acesso para seus processos e sua plataforma de automação, você garante que somente o pessoal autorizado execute tarefas de automação. Escolha uma plataforma de automação que todos em sua organização possam usar. Escolher uma plataforma que implementa uma linguagem de automação comum e fácil de usar pode aprimorar:

Visibilidade. Todos entendem o que cada tarefa automatizada faz.

Capacidade de repetição. Uma plataforma e uma linguagem acessíveis permitem que todos os funcionários aprovados usem a automação de forma eficaz e eficiente.

Colaboração. As tarefas de automação podem ser compartilhadas em toda a organização, de modo que outras equipes tenham acesso a trabalhos concluídos e evitar esforços duplicados.

Auditoria. Vários funcionários podem verificar tarefas de automação e visualizar registros para auditoria.

Etapas táticas

Siga estas ações para começar a colocar em prática a automação de segurança.

Comece com apenas um projeto.
Não automatize tudo de uma vez. Escolha um conjunto limitado de tarefas para começar.

Escolha tarefas repetitivas.
Automatize tarefas que são executadas de maneira repetitiva, como gerenciamento de configurações, gestão de patches e pacotes de software, identificação e correção de vulnerabilidades de segurança e aplicação de políticas.

Avalie, adapte e repita.
Trabalhe de forma iterativa para implementar automação, avaliar resultados e fazer as adaptações necessárias.

Planeje expansões usando uma plataforma de automação empresarial de ponta a ponta para escalar.
Certifique-se de que toda a automação seja verificável, auditável e compartilhável. Assim, outras pessoas na organização possam aproveitar os ganhos e usar uma plataforma de automação empresarial de ponta a ponta para escalar.

Capítulo 6

Vamos começar?

A segurança de nuvem híbrida é uma responsabilidade compartilhada por todos na organização. Independentemente de onde você esteja na jornada para adotar a nuvem híbrida, a Red Hat pode ajudar a implantar uma nuvem híbrida com foco em segurança.

Com recursos de segurança incorporados e integrados, o portfólio de software open source com nível de produção da Red Hat oferece as ferramentas e plataformas de que você precisa para superar os desafios de segurança e conformidade atuais e futuros. A Red Hat também oferece suporte empresarial, treinamentos hands-on e serviços especializados para ajudar você a criar e operar seu ambiente de nuvem híbrida de maneira eficiente e segura.

Descubra a abordagem da Red Hat para a segurança em nuvem híbrida

Consulte esses recursos para mais informações sobre a abordagem da Red Hat para segurança e conformidade em uma nuvem híbrida.

- Visão geral da segurança em nuvem híbrida
- Avaliação da segurança em nuvem híbrida
- Abordagens de segurança para ambientes de nuvem híbrida
- Aprimore sua segurança em nuvem híbrida

Sobre Lucy Kerner, diretora de evangelização e estratégia global de segurança da Red Hat
Lucy Huh Kerner lidera o pensamento estratégico de segurança e a estratégia técnica e de entrada no mercado para segurança no portfólio global e em toda a Red Hat. Além disso, ela ajuda a criar e fornecer conteúdo técnico relacionado à segurança para o mercado, clientes, parceiros, analistas e jornalistas, além de já ter dado palestras em diversos eventos, incluindo conferências sobre segurança. Lucy tem mais de 20 anos de experiência profissional como engenheira de desenvolvimento de software e hardware, arquiteta de soluções e estrategista de segurança global, tendo trabalhado com vários aspectos da segurança.

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

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

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

br.redhat.com

© 2024 Red Hat, Inc. Red Hat, o logotipo da Red Hat, OpenShift e Ansible são marcas comerciais ou registradas da Red Hat, Inc. e suas subsidiárias nos Estados Unidos e em outros países. Linux® é uma marca registrada da Linus Torvalds nos Estados Unidos e em outros países.