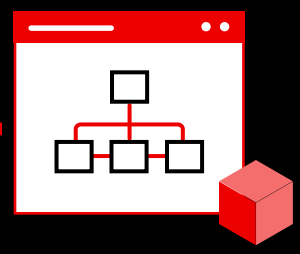
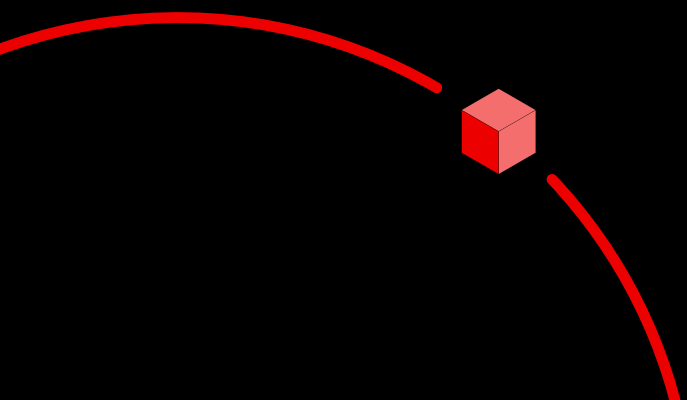
Red Hat
OpenShift
Platform Plus

Crie uma fábrica de software para dar suporte a DevSecOps

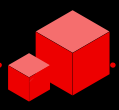
Um guia opinativo para começar sua jornada com DevSecOps

Sumário





Proteja sua empresa com DevSecOps



Cada vez mais, as organizações estão adotando tecnologias de **microsserviços**, **em container** e **nativas em nuvem** para promover inovação e **transformação digital**. Como parte dessa transformação, muitas organizações usam o Kubernetes para orquestrar containers em apoio a operações nativas em nuvem. O Kubernetes é a plataforma ideal para hospedar aplicações nativas em nuvem que exigem escala rápida e operações resilientes. O motivo disso é a capacidade de seus **clusters** abranger hosts locais e em ambientes de nuvem.

Mesmo assim, ainda há muitos desafios, especialmente em termos de segurança e capacidade de gerenciamento em escala. Por isso, 50% dos líderes de TI consideram a cibersegurança uma das prioridades para iniciativas tecnológicas.[1]

Adotar abordagens e práticas de DevSecOps ajudam a incorporar segurança a suas aplicações, processos e plataforma para proteger melhor sua empresa.

Este ebook traz considerações e orientações para a criação de uma prática bem-sucedida de DevSecOps na sua organização com o suporte das tecnologias do Red Hat OpenShift Platform Plus.

O que são aplicações nativas em nuvem?

As **aplicações nativas em nuvem** formam um conjunto de serviços pequenos, independentes e com baixo acoplamento.

O que são DevOps e DevSecOps?

O **DevOps** é uma abordagem de cultura, automação e desenvolvimento de plataforma que se concentra em aumentar o valor dos negócios e sua capacidade de resposta por meio da entrega rápida, automatizada e de alta qualidade de serviços. O **DevSecOps** estende a cultura colaborativa do DevOps para incorporar a segurança por meio dos ciclos de vida das aplicações. Além disso, ele engloba pessoas, processos e tecnologias para tornar a segurança mais abrangente em ambientes distribuídos.

Por meio do DevSecOps, a segurança se torna uma responsabilidade compartilhada e obrigatória entre equipes em vez de um conjunto de tarefas de uma equipe só e aplicada ao fim do processo de desenvolvimento e implantação. Equipes de segurança, desenvolvimento e operações trabalham juntas, têm visibilidade dos mesmos recursos e compartilham feedbacks, lições aprendidas e insights. Nesse tipo de abordagem, a segurança é integrada desde o início do desenvolvimento da aplicação e da implantação da infraestrutura, aumentando a proteção e reduzindo riscos.

88%

das organizações que participaram da pesquisa usam o Kubernetes como o orquestrador de containers, e 74% delas o usam na produção.[2]

74%

das organizações que participaram da pesquisa têm uma iniciativa de DevSecOps.[2]

1 Flexera. "2021 Flexera State of Tech Spend Report", janeiro de 2021.

2 Red Hat, "Estado de Segurança do Kubernetes", 2022.

Objetivos do DevSecOps

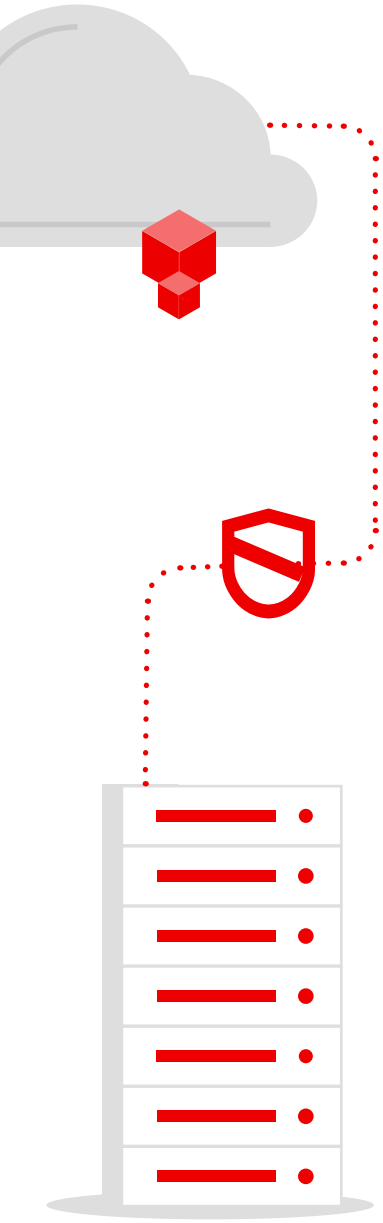
O objetivo do DevSecOps é entregar e implantar rapidamente aplicações, serviços e funcionalidades de alta qualidade, com foco em segurança e em escala.

Escala

Velocidade

Segurança

Estabilidade



Desafios na implementação de DevSecOps

Processos manuais

As tarefas relacionadas ao desenvolvimento, teste e segurança podem ser lentas, monótonas, suscetíveis a erros e difíceis de aplicar quando a intervenção humana é frequentemente necessária.

Colaboração limitada entre equipes

As equipes de desenvolvimento, segurança e operações normalmente trabalham apenas dentro de seus próprios domínios. Isso resulta em processos fragmentados, handoffs manuais e um conhecimento limitado dos desafios e necessidades das outras equipes.

Aplicação tardia dos processos de segurança

O desenvolvimento de aplicações e abordagens de inicialização tradicionais aplicam práticas e verificações de segurança apenas no final do processo, logo antes da implantação na produção.

Complexidade do ambiente de aplicação

Pode ser difícil entender as conexões e implicações de todos os componentes diferentes (como containers, microsserviços e serviços em nuvem) que compõem os complicados ambientes de produção, desenvolvimento e teste de aplicações em larga escala.

Dependências externas

O desenvolvimento de aplicações nativas em nuvem quase sempre depende de algumas dependências externas que também devem ser protegidas, incluindo seções de código, livrarias e serviços open source.

Cenário de segurança em evolução

As regulamentações e ameaças de segurança, incluindo requisitos empresariais, técnicos e geográficos, mudam em ritmo acelerado, o que dificulta se manter atualizado e em conformidade.

Pessoas, processos e tecnologia são cruciais

O DevSecOps não é uma equipe ou um único processo. É um recurso de toda a empresa que exige mudanças e alinhamento em três áreas: pessoas, processos e tecnologia.

Pessoas

As pessoas são os principais agentes de qualquer iniciativa empresarial, e isso não é diferente com a adoção de DevSecOps. Para adotar o DevSecOps, todas as equipes da organização, sejam de desenvolvimento, segurança ou operações, precisam se integrar, participar e confiar umas nas outras.

Processos

Os processos movem os projetos do início ao fim. Processos bem definidos para criar, implantar, gerenciar e adaptar aplicações e infraestrutura (e incorporar segurança durante seus ciclos de vida) são essenciais para a adoção integral de DevSecOps.

Tecnologia

Sua plataforma de aplicações oferece os recursos para criar, implantar e executar aplicações e infraestrutura. Uma plataforma unificada que oferece suporte às equipes de desenvolvimento, segurança e operações dá a você a base necessária para criar e adaptar a prática de DevSecOps.

Prepare sua organização para adotar o DevSecOps com sucesso

Nenhuma organização pode desenvolver uma prática completa de DevSecOps de um dia para o outro. A adoção de DevSecOps é uma jornada iterativa de aprendizado, não uma proposta radical. É necessária uma estratégia lógica e sustentável para guiar o progresso e ajudar você a aprender com o tempo.

Incentive a colaboração entre as equipes.

Use incentivos e processos de design para promover a colaboração na sua organização. As equipes usam a coordenação para criar fluxos de trabalho de DevSecOps completos que geram mais valor. Além disso, o trabalho entre equipes é uma forma de cultivar a responsabilidade compartilhada pelo desenvolvimento, segurança e operações.

Documente cada etapa.

Registre o desenvolvimento, gerenciamento de mudanças e processos de governança em detalhes usando frameworks dinâmicos como o **GitOps**. Se você sabe onde está e quais desafios tem, é mais fácil planejar o caminho adiante. À medida que você adapta os processos, registre os mais novos e o motivo de as mudanças terem sido feitas.

Avalie seus processos.

Identifique e adapte processos que não sejam compatíveis com os objetivos do DevSecOps. Isso inclui configurações e infraestrutura de integração/implantação contínuas (CI/CD) ineficientes e diferentes, processos muito centralizados e/ou que dependam de intervenção manual frequente.

Defina e avalie o sucesso.

Determine como deve ser o sucesso do DevSecOps para sua organização e identifique métricas para avaliar ou indicadores de desempenho (KPIs) para acompanhar o progresso. As métricas podem ser o tempo de compilação e implantação da aplicação, as taxas de defeitos e liberação de alterações, o tempo de resolução de problemas ou a disponibilidade da aplicação.

Compartilhe conhecimento e práticas recomendadas.

Crie uma equipe principal de stakeholders, usualmente chamados de comunidade de prática (CoP) ou centro de excelência (CoE), para compartilhar práticas recomendadas, experiências e conquistas de DevSecOps na sua organização. Essa equipe também deve ajudar outras que já estejam prontas para adotar DevSecOps.

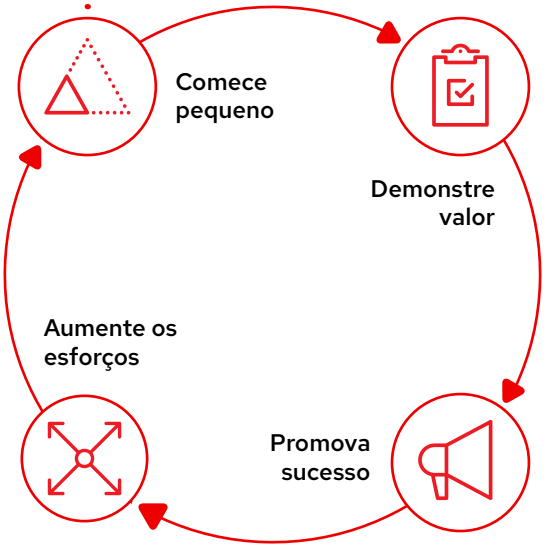
Tenha comprometimento com a sua organização.

Garanta que todos na sua organização estejam comprometidos com a adoção de DevSecOps. Ajude todas as equipes a entenderem os motivos das mudanças e enfatize o impacto positivo delas nas funções de cada um. Incentivos baseados em métricas e apoio da diretoria executiva ajudarão as equipes a progredir nessa jornada.

Comece a prática de DevSecOps

Defina uma estratégia de DevSecOps e então dê o primeiro passo. Nem todas as equipes de desenvolvimento estarão prontas para adotar o DevSecOps de imediato. Comece por equipes que antes já mostraram resultados bem-sucedidos na adoção de novos processos e plataformas. Inclusive, os membros dessas equipes normalmente são bons candidatos para a equipe principal de stakeholders.

Pode ser um passo pequeno, que demonstre valor, até se expandir gradualmente e se repetir. Trabalhe para realizar grandes feitos em pouco tempo. Monitore o progresso por meio das métricas e aprenda com projetos ou processos menos bem-sucedidos. Para cada conquista, promova o valor do DevSecOps e compartilhe a experiência da equipe com toda a organização. Essa é uma forma de estabelecer uma base para outras pessoas usarem as experiências da equipe e gerarem ainda mais valor.



Adote uma abordagem de fábrica para a entrega de software

Uma entrega moderna de software depende de velocidade, consistência e qualidade. Uma abordagem de fábrica de software ajuda a viabilizar, acelerar e reforçar as mudanças comportamentais necessárias para adotar uma cultura de DevSecOps na sua organização. Essa abordagem permite que você desenvolva e implante aplicações de alta qualidade rapidamente com uma **cadeia de suprimentos de software confiável** e um conjunto consistente de processos ágeis, como o desenvolvimento conduzido por testes.

Benefícios de uma fábrica de software

A abordagem de fábrica de software apresenta benefícios mensuráveis:

Menos tempo de provisionamento para mudanças

Mais frequência de implantação

Menor tempo de recuperação de serviços com falhas

Menor taxa de falha de alteração

Métricas quantificadas do desempenho da entrega de software[3]

Métrica do desempenho da entrega de software	Com uma fábrica de software	Sem uma fábrica de software
Tempo de provisionamento para mudanças	menos que 1 hora	1 a 6 meses
Frequência de implantação	Sob demanda (mais que 1 por dia)	Uma vez a cada 1 a 6 meses
Tempo de recuperação de serviços	menos que 1 hora	1 dia a 1 semana
Taxa de falha de alteração	0% a 15%	16% a 30%

*3 Google Cloud. "***Accelerate State of DevOps 2021***", setembro de 2021.*

Como é uma fábrica de software?

Uma fábrica de software possibilita que você evolua de processos manuais inconsistentes para operações automatizadas e consistentes.

Sem uma fábrica de software

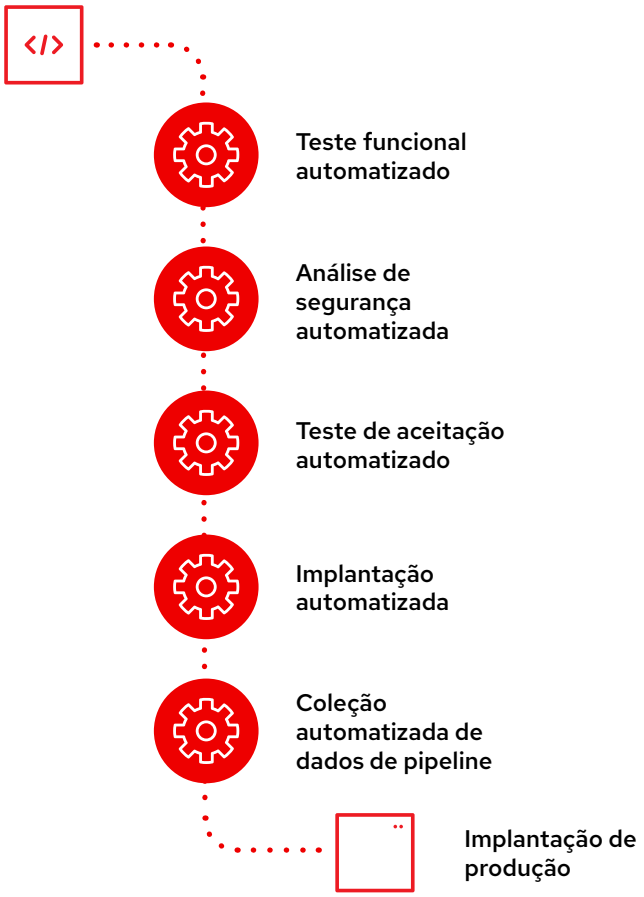
Processos e assinaturas manuais resultam em desenvolvimento e implantação lentos, expectativas incertas e reforço de segurança inconsistente. Considerando que até pequenas mudanças podem levar dias ou semanas para serem implementadas, as equipes normalmente tentam fazer o maior número de mudanças em uma só implantação. Isso aumenta o risco de falhas nas mudanças e de segurança.

A confiança entre equipes costuma ser baixa por haver pouca transparência durante o processo. Medidas de segurança e conformidade são aplicadas manual e tardiamente no processo, então falhas podem não ser identificadas durante o desenvolvimento. Como resultado disso, as aplicações acabam voltando aos desenvolvedores para que falhas de segurança e conformidade sejam corrigidas. Essas surpresas podem ser frustrantes e acabam gerando falta de confiança em uma fase já estressante por si só.

Com uma fábrica de software

Processos definidos e automatizados aceleram o desenvolvimento e implantação, reforçam a segurança de forma consistente e estabelecem expectativas claras para todas as equipes envolvidas. Considerando que mudanças pequenas podem ser lançadas em minutos, as equipes podem implantar várias delas de forma rápida e diária, resultando em menos risco em geral.

Transparência e visibilidade são funcionalidades cruciais nas fábricas de software, o que facilita o cultivo da confiança entre as equipes de desenvolvimento, operações e segurança. As medidas de segurança e conformidade são aplicadas automaticamente durante o desenvolvimento. Assim, falhas podem ser localizadas e solucionadas mais cedo no processo. A documentação de processos e políticas ajuda equipes a entender as expectativas durante o processo. Além disso, previne surpresas na hora de implantar aplicações para a produção.



Construa sua própria fábrica de software

A **automação** é o ponto principal da abordagem de fábrica de software. Ela é crucial para a operação de ambientes nativos em nuvem e para a adoção de práticas de DevSecOps. A automação ajuda a escalar o desenvolvimento, entrega, implantação e operações de infraestrutura de forma controlada. Além disso, é possível provisionar e descontinuar recursos, ambientes e aplicações de forma dinâmica. Como resultado, sua organização responde mais rápido a mudanças.

Considere automatizar todos os aspectos do fluxo de trabalho do seu DevSecOps, incluindo o desenvolvimento, teste, controle de qualidade do código, validação de conformidade, detecção de vulnerabilidades e processos de remediação. Use pipelines de CI/CD para automatizar tanto o desenvolvimento e aprimoramento de aplicações quanto o gerenciamento e implantação de infraestruturas. Defina e registre políticas de segurança e risco e automatize a verificação de conformidade e remediação contra essas políticas durante os ciclos de vida do seu software.

Automação declarativa e impulsionada por intenção ajudará você a escalar e se adaptar de forma mais rápida e fácil.

Uma automação declarativa permite que você defina a configuração de aplicação ou infraestrutura desejada em vez de um conjunto de instruções para configurar recursos. Você apenas descreve a meta, não o caminho para chegar a ela. Desse modo, sua plataforma de aplicação provisiona e configura os recursos necessários para chegar ao estado desejado. Ela também se autorremedia para garantir que os recursos continuem configurados corretamente com o tempo. Por fim, essa abordagem prepara você para o **GitOps**, um conjunto de práticas para gerenciar configurações de infraestrutura e aplicação usando a versão Git do sistema de controle.

Como decidir o que e quando automatizar

Da mesma forma que o DevSecOps como um todo, a implantação da automação também é uma jornada que exige planejamento. Siga estas etapas para começar a automação:

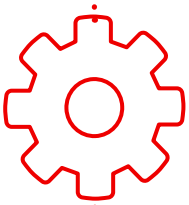
1. Documente o processo em detalhes.
2. Registre decisões e como elas são feitas a cada etapa manual do processo. A tomada de decisões pode envolver a leitura de materiais, consideração de fatores específicos, consulta com vários experts ou outras ações.
3. Identifique todas as etapas manuais que podem ser facilmente automatizadas e avalie o nível de mudanças que devem ser automatizadas. Por exemplo, você provavelmente pode automatizar mudanças pequenas, mas precisa de aprovação de outras equipes para mudanças maiores.
4. Para etapas manuais que não podem ser facilmente automatizadas, avalie o que é preciso para automatizá-las e crie um plano para a implementação de automação.

Comece a automatizar imediatamente. Não espere até identificar todas as possíveis áreas de automação. Automatizar processos iterativamente é um processo de DevOps por si só. Conforme ocorre a automação, a adaptação e o refinamento de processos, você ganha habilidades preciosas e experiência para oferecer suporte à prática geral de DevSecOps.

Concentre-se em trabalhos interessantes

A automação não serve para substituir pessoas. O foco dela é produtividade, consistência e eficiência. Esse é o paradoxo da automação: quanto mais se automatiza, menos frequente e mais importante é o envolvimento humano.

A automação pode ser vista como uma ferramenta que elimina empregos. No entanto, na realidade, ela permite que os profissionais de TI mais experientes se concentrem em problemas maiores e nas suas soluções, deixando as tarefas rotineiras e repetitivas para a automação.



Saiba como automatizar na sua empresa

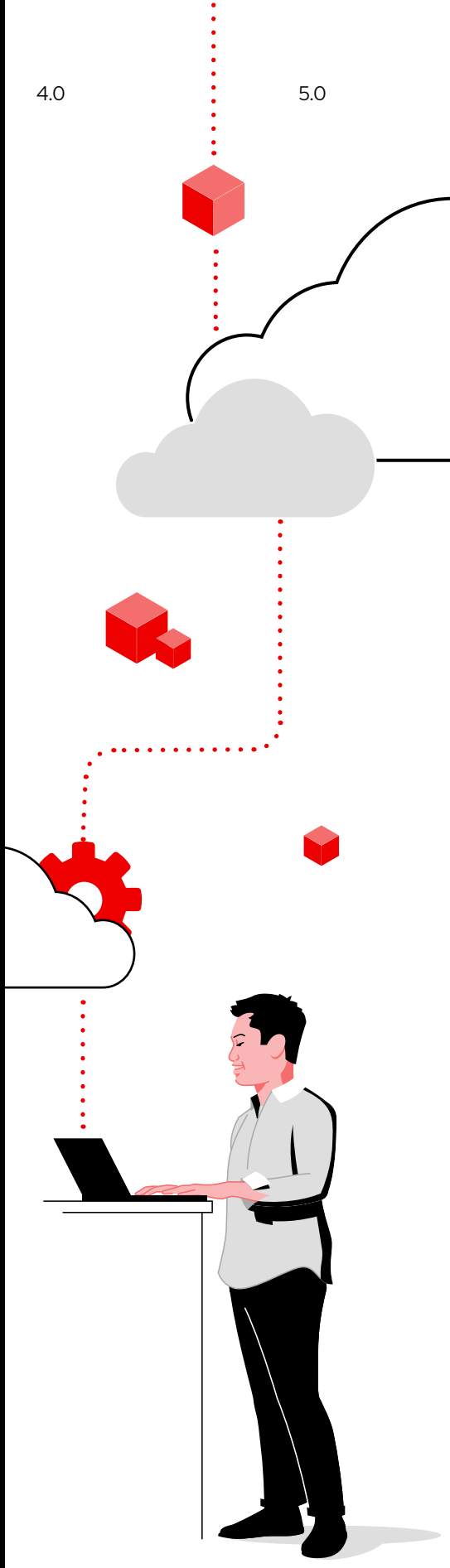
A automação é capaz de unir pessoas, processos e tecnologias para aumentar o valor, a inovação e a agilidade da empresa.

Leia o ebook **A empresa automatizada** para aprender a adotar a automação em toda a sua organização.

Ferramentas para a fábrica de software

As ferramentas são uma parte importante da fábrica de software. É recomendado o uso e automação dessas categorias de ferramentas na fábrica de software. Cada ferramenta possui exemplos, mas é possível usar outros.

Categoria da ferramenta	Exemplos
Gerenciamento de projetos	▸ Confluence com Jira ▸ Trello
Gerenciamento de código-fonte (SCM)	▸ Github ▸ Gitlab
Ambientes de desenvolvimento integrados (IDEs)	▸ VS.code ▸ **Red Hat OpenShift Dev Spaces**
Repositórios de artefatos	▸ Nexus ▸ Artifactory
CI/CD	▸ **Red Hat OpenShift Pipelines** ▸ **Jenkins**
Ambientes de execução	▸ **Red Hat Runtimes** ▸ Golang
Criação	▸ Maven ▸ Dotnet build
Teste de unidade	▸ JUnit ▸ NUnit
Análise de código-fonte	▸ Sonarqube ▸ Fortify
Teste estático de segurança de aplicações (SAST)	▸ CheckMarx ▸ **Red Hat Advanced Cluster Security for Kubernetes**
Teste de aceitação do usuário	▸ Cucumber ▸ Cyprus
Teste dinâmico de segurança de aplicações (DAST)	▸ Veracode ▸ Synopsys
Telemetria, métricas e geração de logs	▸ **Prometheus** ▸ **Grafana** ▸ **Elasticsearch, Fluentd e Kibana (EFK)** ▸ Splunk
Service mesh	▸ Linkerd ▸ **Red Hat OpenShift Service Mesh**



Crie, implante e execute

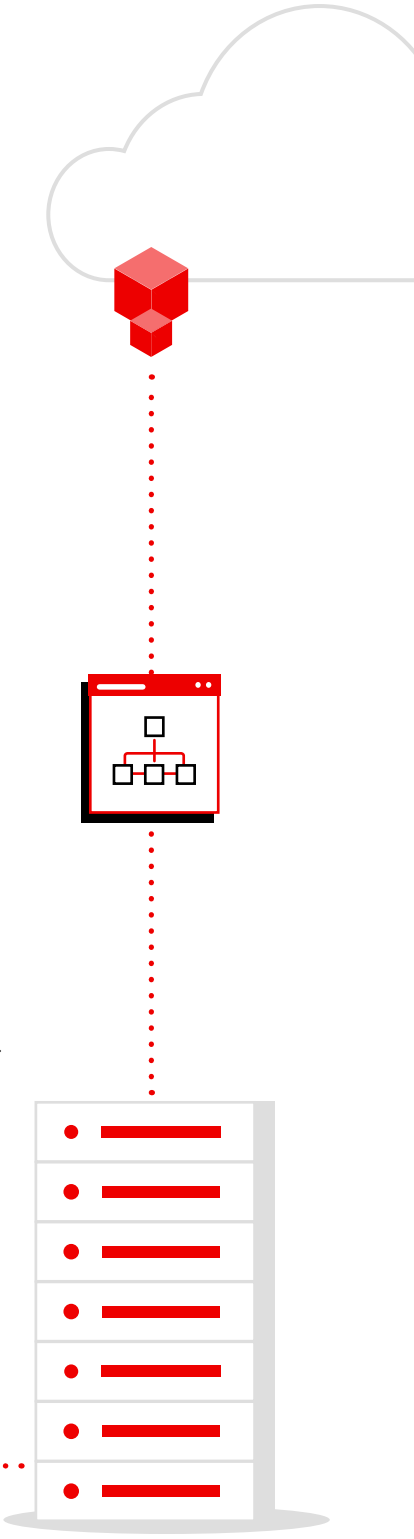
Arquitetos de plataforma ou engenheiros de DevOps frequentemente configuram fábricas de software no lugar de desenvolvedores. Durante a construção da fábrica de software, siga as práticas recomendadas de segurança nestas três áreas: criação, implantação e execução.

Criação

Controle a conformidade e aplicação de segurança.

É importante integrar a segurança às aplicações nas implantações nativas em nuvem.

- Use fontes confiáveis para conteúdos de container e aplicação, incluindo ambientes de execução.
- Adote um registro de containers confiável e privado para gerenciar imagens.
- Automatize os pipelines de desenvolvimento e implantação.
- Implemente requisitos não funcionais em códigos usando práticas ágeis, como o desenvolvimento conduzido por testes (TDD).
- Integre segurança aos pipelines da aplicação com qualidade de código, vulnerabilidade de imagem e análise da implantação do Kubernetes.
- Automatize o posicionamento e implantação da aplicação.



Implantação

Proteja sua plataforma.

Uma segurança efetiva exige a proteção da plataforma Kubernetes e políticas de implantação de automação.

- Reduza a superfície de ataque ao usar um sistema operacional otimizado para containers.
- Automatize o gerenciamento de configuração e reforço de política nos clusters.
- Implemente privilégios mínimos com controle de acesso baseado em função (RBAC) de alta granularidade.
- Criptografe dados de plataforma e aplicação em trânsito e em repouso.
- Use conformidade, avaliação de risco e remediação de soluções automatizadas.
- Reduza o risco da implantação com as políticas de controle de admissão no pod do Kubernetes

Execução

Proteja os ambientes de execução de containers.

Mantenha a segurança da aplicação no ambiente de execução.

- Isole a execução de aplicações com o Security-Enhanced Linux® (SELinux), restrições de contexto de segurança (SCC), namespaces do Kubernetes, RBAC e políticas de rede.
- Use cotas para prevenir conflitos de recursos e falhas de desempenho relacionadas.
- Gerencie o acesso à aplicação e proteja os dados dela com o gerenciamento de usuário single sign-on, entrada e saída de gerenciamento de segurança, tráfego pod a pod criptografado e gerenciamento da interface de programação de aplicação (API).
- Audite e monitore a atividade da plataforma e aplicação.
- Automatize a detecção de ameaças e a resposta a pods de comportamento anômalo, eventos de escalação de privilégio e processos arriscados, como criptomining.
- Use controladores de admissões para prevenir a implantação de containers que não estejam em conformidade com as políticas de segurança.
- Crie redes de confiança zero usando service meshes e políticas de rede.

Dica de segurança

Leia **Uma abordagem de segurança em camadas para Kubernetes e containers** para saber mais sobre a proteção de aplicações em containers gerenciadas pelo Kubernetes.

Criação	Implantação	Execução
Ciclo de vida da aplicação	**Gerenciamento de configuração de frotas**	**Alertas e observabilidade de frotas**
Análise de vulnerabilidades	Controlador de admissões de políticas	Análise comportamental do ambiente de execução
Análise de configuração de aplicações	Avaliação de conformidade	Recomendações de políticas de rede
APIs para integração de CI/CD	Caracterização de risco	Detecção e resposta a ameaças
Conteúdo confiável	Ciclo de vida da plataforma do Kubernetes	Isolamento de container
Registro de containers	Gerenciamento de identidade e acesso	Isolamento de rede
Gerenciamento de versão	Dados de plataforma	Dados e acesso de aplicação
Pipelines de CI/CD	Políticas de implantação	Observabilidade

DevSecOps

Implemente DevSecOps com especialistas

A **Red Hat** une um ecossistema de parceiros certificados, conhecimento abrangente e plataformas inovadoras para criar, proteger e implantar aplicações nos ambientes de nuvem híbrida. Nós temos anos de experiência em apoiar empresas e ajudá-las a superar desafios tecnológicos e de negócios usando práticas recomendadas do setor e tecnologias open source.

Com uma cadeia de suprimentos de conteúdo confiável, apoio de uma equipe de segurança dedicada e transferência de funcionalidades de segurança cruciais da versão upstream para a versão mais recente, as plataformas da Red Hat oferecem uma base ideal para soluções de DevSecOps. Também oferecemos **cursos de treinamento e certificações**, **laboratórios interativos**, **contratos de consultoria** e **ofertas gerenciadas** para ajudar você a criar uma prática bem-sucedida de DevSecOps com mais rapidez.

A Red Hat acompanha você na sua jornada com DevSecOps.

Com nossas plataformas open source e serviços especializados comprovados, você pode implantar o que precisa hoje, adaptar-se a mudanças futuras e aprender os métodos e abordagens necessários para uma adoção de DevSecOps eficiente e efetiva.

Descubra mais sobre por que escolher a Red Hat para DevSecOps.

Aproveite ao máximo seu investimento em DevSecOps

O Red Hat Services oferece os recursos necessários para você começar, acelerar e expandir a prática de DevSecOps.

- **Red Hat Open Innovation Labs**
  Um contrato de consultoria em formato de residência no qual clientes e associados da Red Hat se juntam para aprender novas maneiras de trabalhar e entregar resultados empresariais ao mesmo tempo, como DevSecOps
- **Solução do Red Hat Services: DevSecOps**
  Um serviço interativo que ajuda a implementar uma fábrica de software usando uma abordagem modular
- **Red Hat Services Journey: adoção de containers**
  Um serviço de consultoria que direciona a adoção de containers em principais fluxos de trabalho.
- **Red Hat Services Journey: adoção de automação**
  Um serviço de consultoria que oferece um framework para gerenciar a jornada de adoção de automação em toda a organização.

Implante uma plataforma de DevSecOps com sucesso

O **Red Hat OpenShift Platform Plus** oferece uma base tecnológica e um framework opinativo para DevSecOps. Ele é uma plataforma de aplicação inovadora que opera e escala de forma consistente em infraestruturas no local e na nuvem. O Red Hat OpenShift Platform Plus combina a plataforma empresarial líder do Kubernetes a maneiras consistentes de criar, implantar, executar, proteger e gerenciar aplicações no seu ambiente. As ferramentas de gerenciamento de vários clusters oferecem visibilidade completa e controle dos seus clusters do Kubernetes. A segurança nativa do Kubernetes e os recursos de DevSecOps protegem sua infraestrutura, cadeia de suprimentos de software e cargas de trabalho. O registro escalável e distribuído globalmente e o gerenciamento de dados de cluster protegem seu ambiente e informações.

As interfaces de integração aberta e o **ecossistema de parceiros certificados** da Red Hat permitem que você use ferramentas de desenvolvimento, teste, operações e segurança novas e já existentes com o Red Hat OpenShift Platform Plus. Muitos fornecedores oferecem **operadores certificados do Red Hat OpenShift** ou **containers de software certificados** para simplificar a instalação e o gerenciamento de softwares em plataformas da Red Hat. Também é possível comprar e implantar vários produtos de software diretamente do **Red Hat Marketplace**. Por fim, a Red Hat trabalha em parceria com os melhores provedores de nuvem para entregar serviços totalmente gerenciados do **Red Hat OpenShift.** Esses serviços otimizam a implantação e as operações, com custos inferiores ao do desenvolvimento feito internamente.

Componentes do Red Hat OpenShift Platform Plus

Red Hat OpenShift

O **Red Hat OpenShift** é uma plataforma de aplicações do Kubernetes pronta para empresas com operações automatizadas em todo o stack. Sua função é gerenciar implantações de nuvem híbrida e edge. Ele inclui recursos com foco nos desenvolvedores para aumentar a produtividade e velocidade.

Red Hat Advanced Cluster Management for Kubernetes

O **Red Hat Advanced Cluster Management for Kubernetes** é um console que oferece visibilidade em todo o seu domínio do Kubernetes, com governança integrada e recursos de gerenciamento do ciclo de vida da aplicação.

Red Hat Advanced Cluster Security for Kubernetes

O **Red Hat Advanced Cluster Security for Kubernetes** é uma solução que oferece funcionalidades de segurança nativas do Kubernetes para aumentar a proteção e visibilidade da infraestrutura e da carga de trabalho durante todo o ciclo de vida da aplicação.

Red Hat Quay

O **Red Hat Quay** é um registro open source de imagens de container que oferece armazenamento e viabiliza a criação, a distribuição e a implantação de containers por todo o data center e ambientes de nuvem.

Red Hat OpenShift Data Foundation

O **Red Hat OpenShift Data Foundation** é uma camada escalável de serviços de armazenamento e dados que gera eficiência, resiliência e segurança de dados para ambientes do Red Hat OpenShift.

O Red Hat OpenShift Platform Plus oferece suporte em todas as etapas da sua jornada com DevSecOps. Ele atende você seja em qual etapa estiver e oferece uma base para seguir em frente no seu ritmo.

Recursos de segurança integrados

Monitore cargas de trabalho em execução para lidar com problemas de segurança e ameaças a partir da coleta e análise de dados no nível do sistema e mais de 60 políticas de segurança integradas que podem ser aplicadas e reforçadas ao longo de todo o ciclo de vida da aplicação.

Operações consistentes

Aplique políticas operacionais e consistentes de segurança, configuração, conformidade e governança nos clusters do Red Hat OpenShift em várias infraestruturas de data center locais e em nuvem.

Ferramentas do desenvolvedor

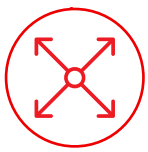
Crie, execute e implante aplicações mais rápido com a biblioteca inclusa de ferramentas compatíveis de build, linguagens, pipelines e framework. O framework de operador oferece integrações para as mais recentes ferramentas de desenvolvedor, testadas e verificadas para serem executadas no Red Hat OpenShift.

Gerenciamento de ponta a ponta

Gerencie seu ambiente do Red Hat OpenShift de forma consistente com uma interface uniforme para administradores e desenvolvedores. Essa interface trabalha em ambientes locais, de nuvem e edge, incluindo os que são baseados em diferentes distribuições do Kubernetes.

Suporte para DevSecOps

Integre uma segurança declarativa a ferramentas e fluxos de trabalho do desenvolvedor. Use controles nativos do Kubernetes para combater ameaças, reforçar políticas de segurança e minimizar riscos operacionais.



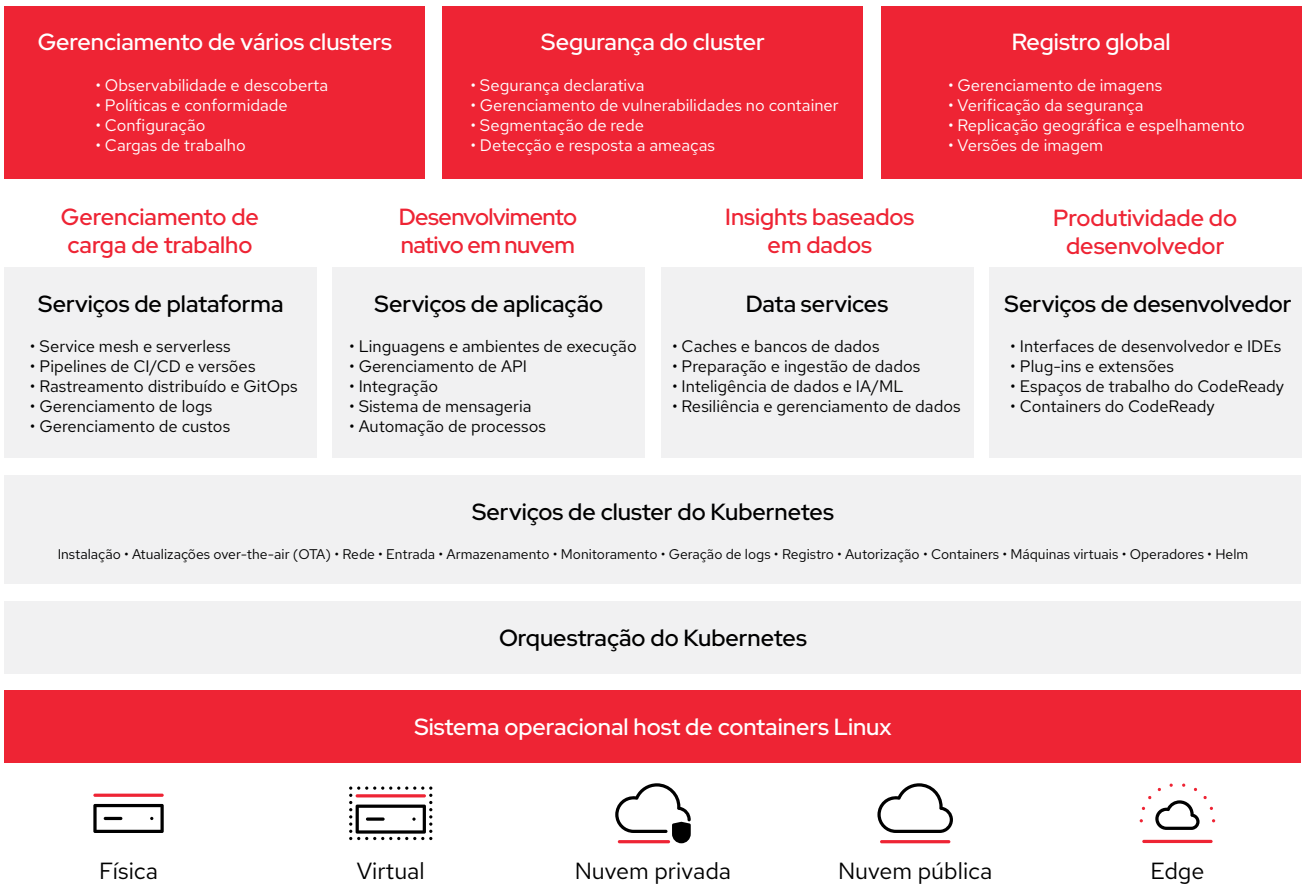
Data services escaláveis

Otimize o gerenciamento de dados nos clusters. Com suporte para protocolos de dados de arquivos, blocos e objetos, o Red Hat OpenShift Data Foundation oferece armazenamento resiliente e persistente para serviços de cluster e aplicações stateful.

Recursos de rede de confiança zero

Implemente **redes de confiança zero** para oferecer comunicações resilientes, seguras e observáveis entre aplicações e serviços. O **Red Hat OpenShift Service Mesh** está incluído e integrado ao Red Hat OpenShift para ajudar mais facilmente na proteção das comunicações.

O Red Hat OpenShift Platform Plus oferece as tecnologias e recursos necessários para uma adoção de DevSecOps eficaz. Leia o **guia de segurança do Red Hat OpenShift** para saber como a segurança é encarada no stack de tecnologia.



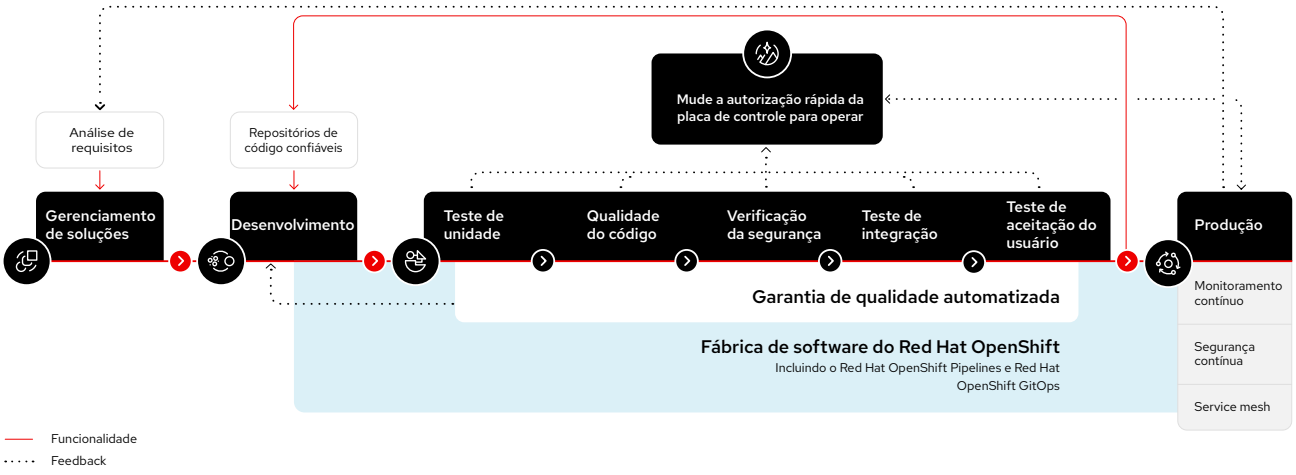
Comece mais rápido com os serviços em nuvem do Red Hat OpenShift

Esses serviços estão disponíveis na **AWS**, **Google Cloud**, **IBM Cloud** e **Microsoft Azure** para que você escolha a melhor opção para as necessidades da organização. Cada serviço oferece um stack completo de ambientes com todos os serviços necessários, opções de autosserviço simples e suporte especializado em tempo integral com rigorosos contratos de nível de serviço (SLAs).

Leia o resumo **Produza mais com os serviços em nuvem do Red Hat OpenShift** para saber mais.

Crie uma base para a fábrica de software com o Red Hat OpenShift Platform Plus

O Red Hat OpenShift Platform Plus oferece uma base confiável, adaptável e compatível para a fábrica de software. Ele permite a você incorporar verificações de segurança nos pipelines de CI/CD para oferecer aos desenvolvedores proteções automatizadas em fluxos de trabalho existentes, proteger a infraestrutura do Kubernetes e as cargas de trabalho de configurações incorretas e sem conformidade e implementar detecção e resposta a ameaças no ambiente de execução.



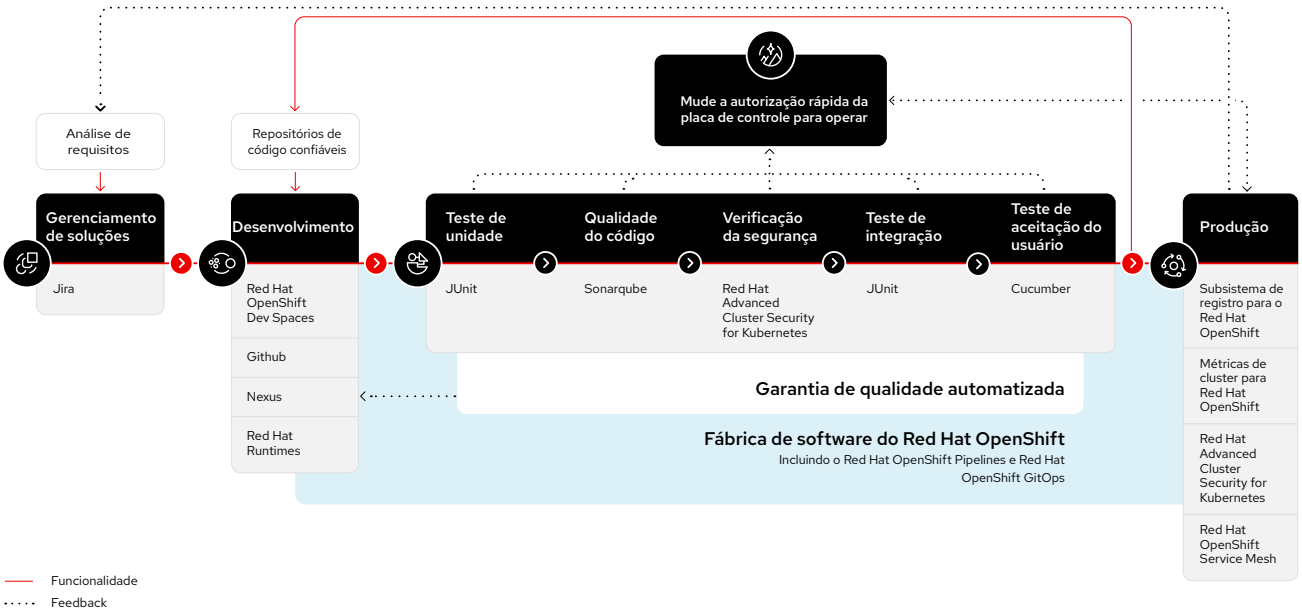
Forme fábricas de software completas com um ecossistema de ferramentas de terceiros.

Cada caso de uso exige diferentes ferramentas na fábrica de software. Com uma base do Red Hat OpenShift Platform Plus, crie cada etapa da sua fábrica de software usando tecnologias e soluções de terceiros da sua preferência, incluindo:

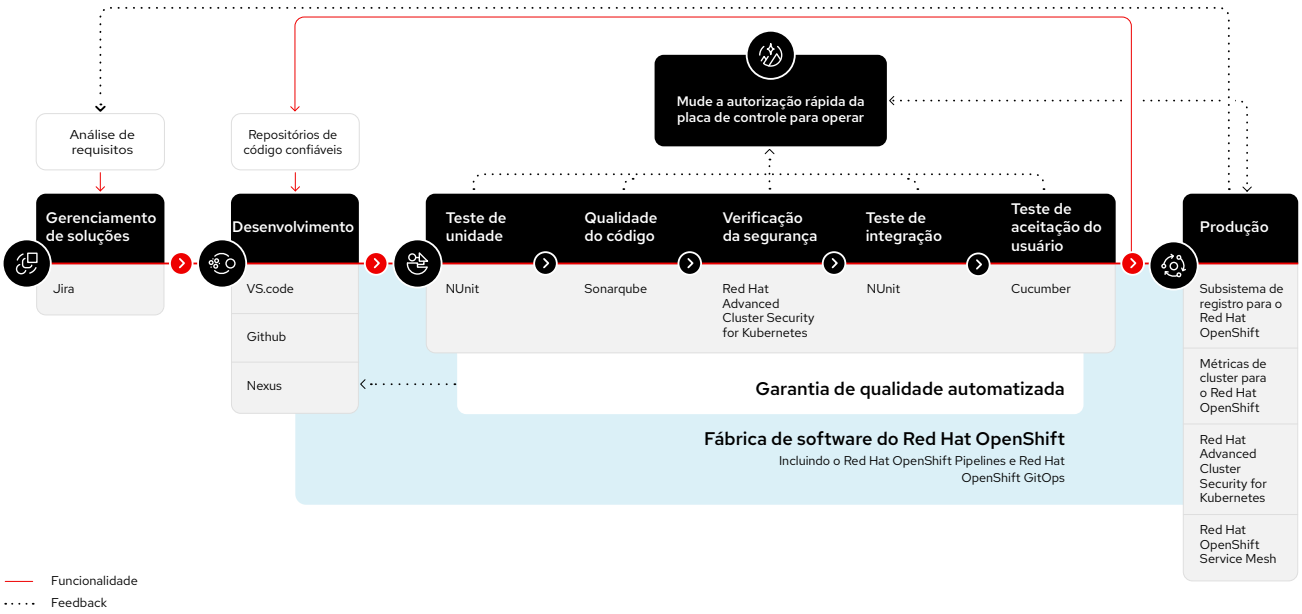
- Ferramentas de gerenciamento de acesso privilegiado (PAM)
- Autoridades de certificação externas.
- Soluções de gerenciamento de chaves e cofres externos.
- Ferramentas de gerenciamento de vulnerabilidades e verificadores de conteúdo de containers.
- Ferramentas de análise de ambientes de execução de containers.
- Sistemas de gerenciamento de eventos e informações de segurança (SIEM).
- Ferramentas de gerenciamento de controle de fonte.
- Repositórios de artefatos.
- Ferramentas de teste de software

Uma fábrica de software para desenvolvimento nativo em nuvem de aplicações do Spring Boot, por exemplo, usa ferramentas de ambientes de execução, build e teste diferentes das de uma fábrica para aplicações .Net Core. Para ilustrar a flexibilidade da base da fábrica de software da Red Hat, mostramos abaixo composições possíveis para essas duas fábricas de software:

Fábrica de software para desenvolvimento nativo em nuvem de aplicações do Spring Boot baseadas em microsserviços.



Fábrica de software para desenvolvimento nativo em nuvem de aplicações do .Net Core baseadas em microsserviços.



Veja casos de sucesso

A **Snam**, uma das maiores redes de gás natural do mundo, adotou os serviços e tecnologias da Red Hat, como o Red Hat OpenShift, o Red Hat Quay e o **Microsoft Azure Red Hat OpenShift**, para ajudar na transformação digital da organização. A empresa agora pode implantar aplicações de maneira automatizada em até 30 minutos, acelerando em mais de 10 vezes o tempo de entrega de novas soluções de software. A Snam também pode escalar cargas de trabalho e aplicações em qualquer nuvem pública ou privada de modo a se adequar a futuros requisitos empresariais, assim reduzindo potenciais riscos de depender da nuvem.

> O Red Hat OpenShift é uma peça fundamental do nosso projeto de transformação. Afinal, ele possibilita a criação de uma plataforma de TI eficiente, confiável e de alto desempenho, o que simplifica o gerenciamento de aplicações e sistemas complexos.

Roberto Calandrini
Chefe de arquitetura, Serviços de IA e digitais, Snam

Mais informações

A **VodafoneZiggo** é uma das fornecedoras líderes de serviços de comunicação e entretenimento para pessoas e empresas nos Países Baixos. Ela implantou uma plataforma de nuvem híbrida baseada no Red Hat OpenShift para unificar a infraestrutura de aplicação da organização. Além disso, a empresa contatou a Red Hat Consulting para buscar orientações durante o processo de adoção de DevSecOps e de mudança para uma cultura mais aberta e colaborativa. A VodafoneZiggo agora é capaz de escalar horizontalmente de forma mais rápida e eficiente em várias nuvens e para a edge à medida que as necessidades empresariais evoluem.

> Nós vemos o Red Hat OpenShift como uma camada consistente para aplicações e serviços nativos em nuvem, os quais nos permitem aumentar a produtividade e oferecer inovações continuamente.

André Beijen
Diretor, Rede mobile, VodafoneZiggo

Mais informações

Comece agora mesmo com DevSecOps

Velocidade, escala e segurança são cruciais em um mundo nativo em nuvem.

Uma fábrica de software baseada no Red Hat OpenShift Platform Plus ajuda você a criar uma prática de DevSecOps bem-sucedida que acelera o desenvolvimento, otimiza as operações e protege sua empresa.

Experimente o Red Hat OpenShift gratuitamente:

cloud.redhat.com/try

Veja mais sobre o Red Hat OpenShift Platform Plus:

red.ht/openshift-platform-plus

F31657_0522_KVM

Red Hat