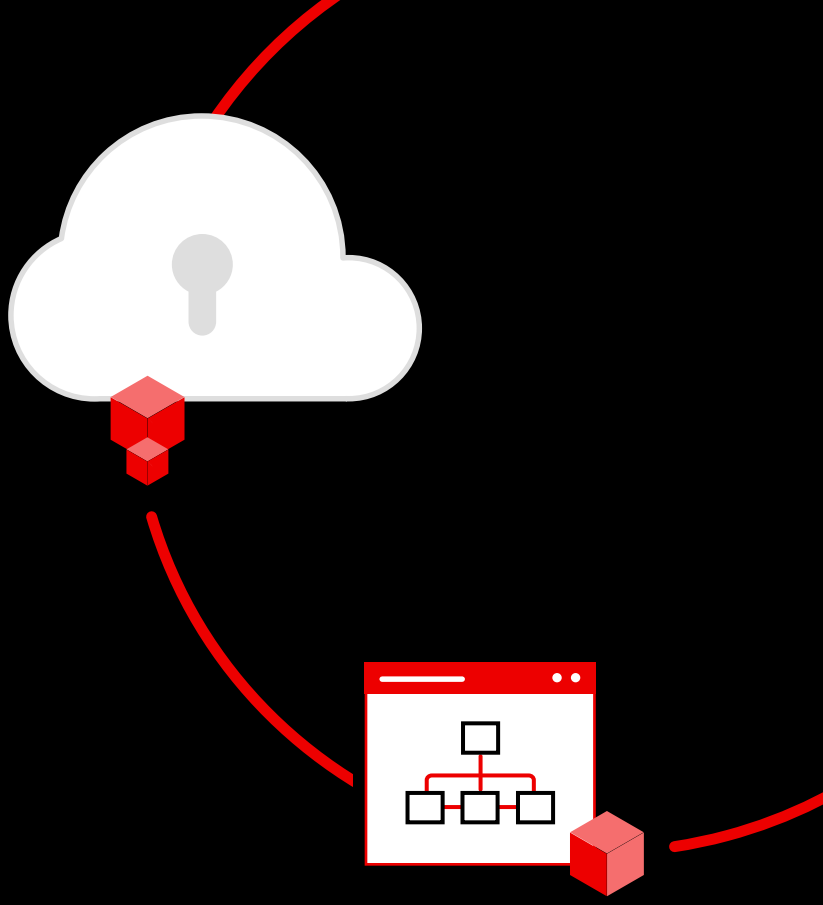
Red Hat
OpenShift
Platform Plus

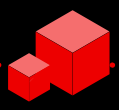
Entwicklung einer Softwarefabrik zur Unterstützung von DevSecOps

Ein Guide mit vorgegebenem Framework für Ihren Einstieg in DevSecOps

Inhalt



DevSecOps zum Schutz ihres Unternehmens



Immer mehr Organisationen führen **cloudnative**, **Container-** und **Microservice-**Technologien ein, um Innovationen und die **digitale Transformation** des Unternehmens zu fördern. Viele setzen dabei für die Container-Orchestrierung und zur Unterstützung cloudnativer Abläufe auf Kubernetes. **Kubernetes-Cluster** können Hosts mehrerer Onsite- und Cloud-Umgebungen umfassen. Daher ist Kubernetes eine optimale Plattform für das Hosting cloudnativer Anwendungen, die eine schnelle Skalierung und resiliente Abläufe erfordern.

Nichtsdestotrotz gehen damit neue Herausforderungen einher, vor allem hinsichtlich der Sicherheit und Verwaltbarkeit in großem Umfang. Tatsächlich nennen 50 % der leitenden IT-Führungskräfte Cybersicherheit unter ihren drei wichtigsten technologischen Initiativen.[1]

Die Einführung von DevSecOps-Ansätzen und -Praktiken kann Sie dabei unterstützen, Sicherheit in Ihre Anwendungen, Prozesse und Plattformen zu integrieren und Ihr Unternehmen dadurch besser zu schützen.

Dieses E-Book beleuchtet wichtige Überlegungen und bietet Ihrer Organisation eine Orientierungshilfe für den Aufbau erfolgreicher DevSecOps-Praktiken mit Red Hat® OpenShift® und anderen Red Hat Technologien.

Was sind cloudnative Anwendungen?

Eine **cloudnative Anwendung** ist eine Ansammlung kleiner, unabhängiger und lose gekoppelter Services.

Was sind DevOps und DevSecOps?

Das **DevOps**-Konzept umfasst die Aspekte Unternehmenskultur, Automatisierung und Plattformdesign mit dem Schwerpunkt, den geschäftlichen Mehrwert und die Reaktionsfähigkeit durch die schnelle Bereitstellung hochwertiger Services zu steigern. **DevSecOps** erweitert diese auf Zusammenarbeit basierende Kultur von DevOps um den Faktor Sicherheit und integriert diese in den gesamten Anwendungs-Lifecycles. Der Ansatz bezieht Menschen, Prozesse und Technologie mit ein und sorgt so für eine umfassendere Sicherheit auch in verteilten Umgebungen.

Ohne DevSecOps ist Sicherheit eine Reihe von Aufgaben, für die ein einziges Team zuständig ist und die am Ende des Entwicklungs- und Bereitstellungsprozesses angewandt werden. Mit DevSecOps wird Sicherheit zu einer gemeinsamen und erzwungenen Verantwortlichkeit mehrerer Teams. Sicherheits-, Entwicklungs- und Operations-Teams arbeiten zusammen und tauschen dabei Informationen, Feedback, Erfahrungen und Insights aus. Mit diesem Ansatz kann die Sicherheit von Anfang an bei der Anwendungsentwicklung und Infrastrukturbereitstellung integriert werden, was den Schutz erhöht und Risiken senkt.

88 %

der befragten Organisationen nutzen Kubernetes für die Container-Orchestrierung, 74 % in der Produktion.[2]

74 %

der befragten Organisationen haben eine DevSecOps-Initiative.[2]

*1 Flexera. „**2021 Flexera State of Tech Spend Report**“, Januar 2021.*

*2 Red Hat. „**State of Kubernetes security report**“, 2021.*

Ziele von DevSecOps

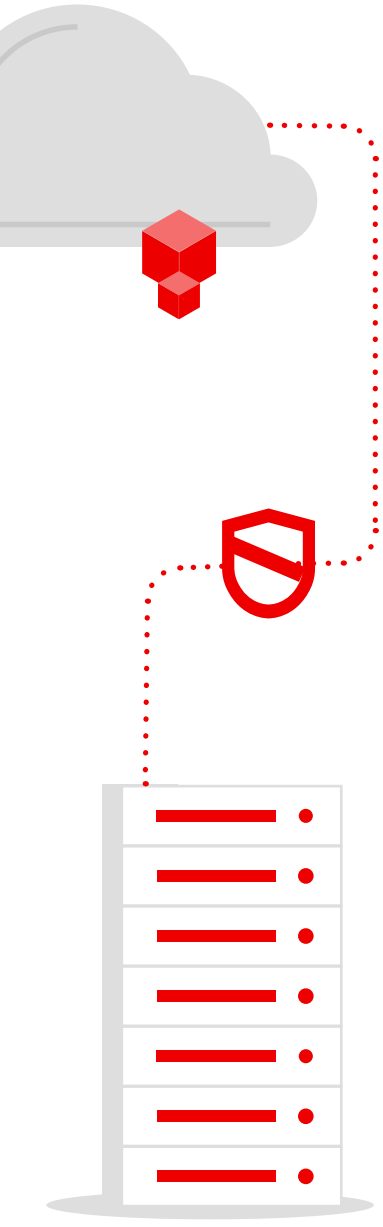
Ziel von DevSecOps ist die qualitativ hochwertige, sicherheitsorientierte Bereitstellung von Anwendungen, Services und Funktionen in großem Umfang.

Umfang

Geschwindigkeit

Sicherheit

Stabilität



Herausforderungen der DevSecOps-Implementierung

Manuelle Prozesse

Entwicklungs-, Test- und Sicherheitsaufgaben können zeitaufwändig, mühsam, fehleranfällig und schwer durchsetzbar sein, wenn menschliches Eingreifen erforderlich ist.

Eingeschränkte Zusammenarbeit von Teams

Entwicklungs-, Sicherheits- und Operations-Teams arbeiten oft nur in ihrem eigenen Bereich. Das führt zu fragmentierten Prozessen, manuellen Übergaben sowie begrenzten Kenntnissen und mangelndem Verständnis der Herausforderungen und Anforderungen anderer Teams.

Späte Anwendung von Sicherheitsprozessen

Bei traditionellen Ansätze zur Entwicklung und zum Launch von Anwendungen erfolgen Sicherheitspraktiken und -prüfungen erst am Ende des Prozesses – als letzter Schritt vor dem Deployment in die Produktion.

Komplexe Anwendungsumgebungen

Umfangreiche, komplizierte Entwicklungs-, Test- und Produktivumgebungen für Anwendungen können aus vielen Containern, Microservices und Cloud-Services bestehen. Die Verbindungen und Sicherheitsauswirkungen dieser verschiedenen Komponenten zu verstehen, kann daher zur Herausforderung werden.

Externe Abhängigkeiten

Die cloudnative Anwendungsentwicklung beruht fast immer auf einer gewissen Anzahl externer Abhängigkeiten – einschließlich Open Source, Code, Libraries und Services – die ebenfalls geschützt werden müssen.

Weiterentwicklung der Sicherheitslandschaft

Sicherheitsbedrohungen und -vorschriften – einschließlich geschäftlicher, technischer und geografischer Anforderungen – verändern sich in einem rasanten Tempo. Das erschwert es Unternehmen, auf dem Laufenden und regelkonform zu bleiben.

Menschen, Prozesse und Technologie sind wesentlich

Bei DevSecOps handelt es sich nicht um ein Team oder einen einzelnen Prozess, sondern um eine unternehmensweite Funktion, die Veränderungen und Abgleich in drei Bereichen erforderlich macht: Menschen, Prozesse und Technologie.

Menschen

Bei allen unternehmensweiten Initiativen steht das Personal im Mittelpunkt. Bei DevSecOps verhält sich das nicht anders. Um DevSecOps im gesamten Unternehmen einzuführen, müssen alle Teams – einschließlich Entwicklung, Sicherheit und Operations – einbezogen werden, zusammenarbeiten und sich gegenseitig vertrauen.

Prozesse

Prozesse sorgen dafür, dass Projekte ordnungsgemäß abgewickelt werden. Klare Prozesse für die Entwicklung, Bereitstellung, Verwaltung und Anpassung von Anwendungen und Infrastruktur – und auch für die Integration von Sicherheit in den gesamten Lifecycle – sind für eine umfassende DevSecOps-Einführung wesentlich.

Technologie

Ihre Anwendungsplattform stellt die Funktionen für die Entwicklung, Bereitstellung und Ausführung von Anwendungen und Infrastruktur zur Verfügung. Eine einheitliche Plattform, die Entwicklungs-, Sicherheits- und Operations-Teams unterstützt, kann Ihnen eine Basis geben, mit der Sie Ihre DevSecOps-Praktiken aufbauen und anpassen können.

Vorbereitung für erfolgreiche DevSecOps

Kein Unternehmen kann umfassende DevSecOps-Praktiken von heute auf morgen entwickeln. Bei der Einführung von DevSecOps handelt es sich um einen iterativen Lernprozess, nicht um ein Alles-oder-nichts-Unterfangen. Sie brauchen daher eine logische, nachhaltige Strategie, die Sie auf Ihrem Weg begleitet und Ihren Lernprozess unterstützt.

Teamübergreifende Zusammenarbeit fördern

Schaffen Sie Anreize und nutzen Sie Design-Prozesse, um die Zusammenarbeit innerhalb Ihres Unternehmens zu fördern. Durch Koordination können Teams komplette DevSecOps-Workflows erstellen, die eine größere Wertschöpfung ermöglichen. Durch die Zusammenarbeit mit anderen Mitarbeitenden entwickelt sich eine gemeinsame Verantwortung für Entwicklung, Sicherheit und Betrieb.

Den aktuellen Zustand dokumentieren

Sie sollten Ihre vorhandenen Prozesse in den Bereichen Entwicklung, Änderungsmanagement und Governance ausführlich mit dynamischen Frameworks wie **GitOps** dokumentieren. Wenn Sie den aktuellen Zustand und die Herausforderungen Ihres Unternehmens kennen, können Sie den Weg in die Zukunft besser planen. Dokumentieren Sie im Rahmen der Anpassung Ihrer Prozesse unbedingt die neuen Prozesse und auch, warum Sie Änderungen vorgenommen haben.

Prozesse bewerten

Identifizieren und passen Sie Prozesse an, die Ihre DevSecOps-Ziele nicht unterstützen. Dazu gehören auch ineffiziente oder nicht zueinanderpassende CI/CD-Set-ups (Continuous Integration/Continuous Deployment) und Infrastrukturen, übermäßig zentralisierte Prozesse sowie solche, die ein häufiges manuelles Eingreifen erfordern.

Erfolg definieren und messen

Bestimmen Sie, was DevSecOps-Erfolg für Ihr Unternehmen bedeutet, und legen Sie messbare Metriken oder KPIs (Key Performance Indicators) fest, an denen Sie Ihren Fortschritt messen können. Beispiele für Metriken: Build- und Deployment-Zeit von Anwendungen, Häufigkeit von Fehlern sowie von Releases mit Änderungen, Problembehebungszeit oder Anwendungsverfügbarkeit.

Wissen und Best Practices teilen

Stellen Sie ein Kernteam aus Experten zusammen, die Best Practices, Erfahrungen und Ergebnisse von DevSecOps innerhalb des Unternehmens gemeinsam nutzen. Dieses Team wird oft als Community of Practice (CoP) oder Center of Excellence (CoE) bezeichnet. Dieses Team sollte auch andere Teams unterstützen, die für die Einführung von DevSecOps bereit sind und ihre ersten Schritte unternehmen wollen.

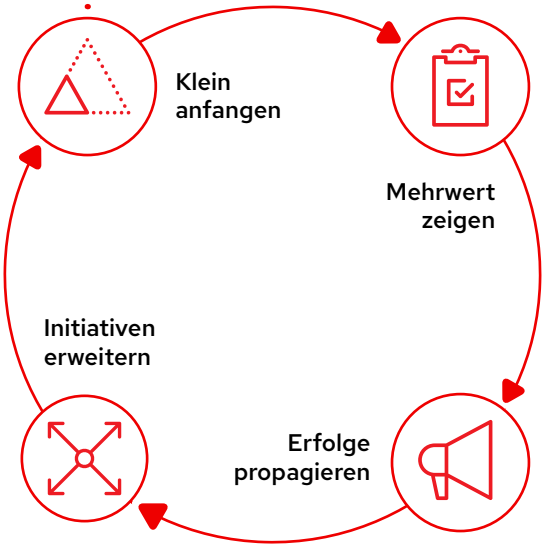
Unternehmensweit Engagement zeigen

Stellen Sie sicher, dass jede und jeder in Ihrer Organisation sich für die Einführung von DevSecOps einsetzen. Dabei sollten Sie jedem Team die Gründe für die einzelnen Veränderungen verständlich machen und die positiven Auswirkungen auf ihre jeweiligen Rollen hervorheben. Mit Sponsorships und metrikbasierten Anreizen können Sie die Teams auf ihrem Weg unterstützen.

Einführung von DevSecOps-Praktiken

Nachdem Sie Ihre Strategie definiert haben, können Sie mit der DevSecOps-Einführung beginnen. Nicht alle Entwickler-Teams werden für eine sofortige Einführung bereit sein. Beginnen Sie mit den Teams, die bereits messbaren Erfolg bei der Einführung neuer Prozesse und Plattformen vorweisen können. Die Mitglieder dieser Teams eignen sich außerdem oft gut als Kandidatinnen und Kandidaten für Ihr zentrales Stakeholder-Team.

Fangen Sie klein an, zeigen Sie den erzielten Mehrwert, erweitern Sie die DevSecOps-Initiativen vorsichtig, und wiederholen Sie den Prozess. Arbeiten Sie so, dass Sie schrittweise Erfolge innerhalb kurzer Zeit erreichen. Überwachen Sie den Fortschritt mit Ihren Metriken und lernen Sie von weniger erfolgreichen Projekten oder Prozessen. Propagieren Sie bei jedem erzielten Erfolg den Vorteil von DevSecOps, und teilen Sie die Erfahrung Ihres Teams im gesamten Unternehmen. Dadurch entsteht eine Basis, bei der andere auf die Erfahrungen Ihres Teams aufbauen und die Wertschöpfung weiter erhöhen können.



Ein Fabrik-Ansatz für die Softwarebereitstellung

Geschwindigkeit, Konsistenz und Qualität bilden die Grundlage der modernen Softwarebereitstellung. Mit einem Softwarefabrik-Ansatz können Sie die Verhaltensänderungen und neuen Verhaltensweisen, die zur Einführung einer DevSecOps-Unternehmenskultur erforderlich sind, fördern, beschleunigen und auch erzwingen. Außerdem ermöglicht dieser Ansatz eine schnelle Entwicklung und Bereitstellung hochwertiger Anwendungen mit einer **bewährten Softwarelieferkette** und einheitlichen agilen Prozessen wie Test Driven Development (TDD).

Vorteile einer Software-Fabrik

Dieser Ansatz bietet messbare Vorteile:

Schnelle Einführung von Änderungen

Häufige Deployments

Schnelle Wiederherstellung von Services nach Ausfall

Niedrige Änderungsfehlerrate

Quantifizierbare Performance-Metriken für die Softwarebereitstellung[3]

Performance-Metrik für die Softwarebereitstellung	Mit einer Software-Fabrik	Ohne Software-Fabrik
Einführungsdauer von Änderungen	< 1 Stunde	1 – 6 Monate
Häufigkeit von Deployments	Nach Bedarf (> 1 pro Tag)	Alle 1 – 6 Monate
Wiederherstellung von Services	< 1 Stunde	1 Tag bis 1 Woche
Änderungsfehlerrate	0 % – 15 %	16 % – 30 %

*3 Google Cloud. „**Accelerate State of DevOps 2021**", September 2021.*

Was macht eine Softwarefabrik aus?

Mit einer Softwarefabrik stellen Sie von uneinheitlichen, manuellen Prozessen auf konsistente, automatisierte Abläufe um.

Ohne Software-Fabrik

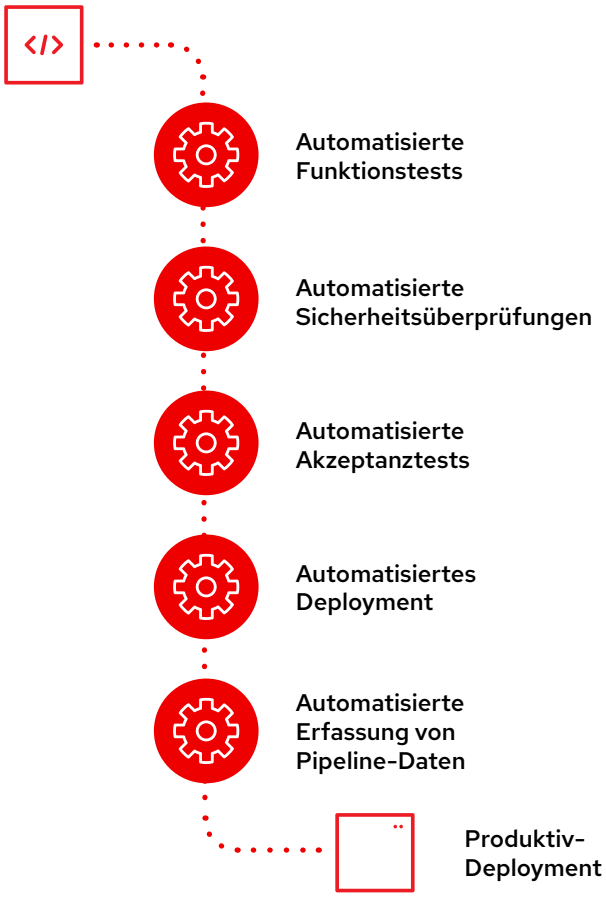
Manuelle Prozesse und Genehmigungen führen oft zu einer langsamen Entwicklung und Bereitstellung, unklaren Erwartungen und einer uneinheitlichen Durchsetzung von Sicherheitsrichtlinien. Da so die Implementierung selbst kleiner Änderungen Tage oder Wochen dauern kann, versuchen Teams oft, viele Änderungen in einem einzigen Deployment vorzunehmen. Dadurch steigt aber das Risiko für fehlgeschlagene Änderungen und Sicherheitsprobleme.

Das Vertrauen zwischen Teams ist durch eine mangelnde Transparenz des gesamten Prozesses oft dürftig. Sicherheits- und Compliance-Maßnahmen werden manuell und spät im Prozess angewandt, so dass Probleme nicht immer während der Entwicklung erkannt werden. Das kann dazu führen, dass Anwendungen zur Behebung von unerwarteten Sicherheits- und Compliance-Problemen an Entwicklungs-Teams zurückgegeben werden. Derartige Überraschungen sorgen in einer bereits stressigen Phase oft für Frustration und Misstrauen.

Mit einer Software-Fabrik

Definierte, automatisierte Prozesse beschleunigen Entwicklung und Deployment, sorgen für eine einheitliche Durchsetzung der Sicherheit und schaffen klare Erwartungen für alle beteiligten Teams. Da sich damit kleine Änderungen innerhalb von Minuten einführen lassen, können diese von den Teams täglich schnell bereitgestellt werden, was insgesamt zu einem geringeren Risiko führt.

Transparenz und Sichtbarkeit sind wichtige Funktionen in der gesamten Softwarefabrik, da sich damit leichter Vertrauen zwischen Entwicklungs-, Operations- und Sicherheitsteams aufbauen lässt. Da Sicherheits- und Compliance-Maßnahmen während der Entwicklung automatisch angewandt werden, können Probleme früher erkannt und behoben werden. Mithilfe von dokumentierten Prozessen und Richtlinien können die Teams die Erwartungen in den verschiedenen Phasen besser verstehen. Außerdem lassen sich so Überraschungen beim Deployment der Anwendungen in die Produktion vermeiden.



Entwicklung Ihrer Softwarefabrik

Automatisierung bildet die Grundlage des Softwarefabrik-Ansatzes. Sie ist für den Betrieb von cloudnativen Umgebungen und die Einführung von DevSecOps-Praktiken wesentlich. Mithilfe von Automatisierung können Sie Entwicklungs-, Release-, Deployment- und Infrastrukturabläufe kontrolliert skalieren. Außerdem lassen sich damit Ressourcen, Umgebungen und Anwendungen dynamisch bereitstellen und außer Betrieb nehmen. Das Ergebnis: Ihre Organisation kann schneller auf Veränderungen reagieren.

Sie können im Prinzip alle Aspekte Ihres DevSecOps-Workflows automatisieren: Entwicklung, Tests, Codequalitätskontrolle, Compliance-Validierung, Schwachstellenerkennung, Problembehebung und mehr. Mit CI/CD-Pipelines lassen sich sowohl Anwendungsentwicklung und -verbesserung als auch Infrastruktur-Deployment und -Management automatisieren. Definieren und dokumentieren Sie Sicherheits- und Risikorichtlinien und automatisieren Sie dann Compliance-Überprüfungen und Korrekturmaßnahmen anhand dieser Richtlinien – und zwar im gesamten Software-Lifecycle.

Deklarative, zielgerichtete Automatisierung für eine schnelle, einfache Skalierung und Anpassung

Mit einer deklarativen Automatisierung können Sie gewünschte Anwendungs- oder Infrastrukturkonfigurationen definieren, anstatt Anleitungen für die Einrichtung von Ressourcen festzulegen. Dabei beschreiben Sie einfach das Endziel anstelle der Methoden, wie dieses zu erreichen ist. Ihre Anwendungsplattform provisioniert und konfiguriert dann die Ressourcen, die zum Erreichen des gewünschten Zustands erforderlich sind. Die Plattform behebt Probleme außerdem selbst und stellt so sicher, dass Ihre Ressourcen auf Dauer richtig konfiguriert bleiben. Schließlich bereitet dieser Ansatz Sie für **GitOps** vor, einer Reihe von Praktiken zur Verwaltung von Infrastruktur- und Anwendungskonfigurationen mit dem Git-Versionskontrollsystem.

Entscheidungen über das Was und Wann der Automatisierung

Wie bei DevSecOps als Ganzem, so ist auch beim Deployment von Automatisierung sorgfältige Planung erforderlich. Die folgenden Schritte können Ihnen den Einstieg in die Automatisierung erleichtern:

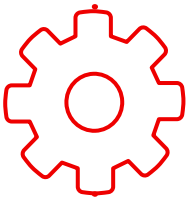
1. Dokumentieren Sie Ihren Prozess genau.
2. Halten Sie für jeden manuellen Schritt Ihres Prozesses fest, was entschieden und wie die Entscheidung getroffen wird, etwa indem bestimmte Ressourcen gelesen, besondere Faktoren berücksichtigt oder verschiedene Fachleute befragt werden.
3. Identifizieren Sie alle manuellen Schritte, die sich einfach automatisieren lassen, und bewerten Sie, auf welchem Level Änderungen automatisiert werden sollen. So könnten Sie beispielsweise kleine Änderungen automatisieren, aber für größere Änderungen die Genehmigung bestimmter Teams erforderlich machen.
4. Bei manuellen Schritten, die sich nicht einfach automatisieren lassen, sollten Sie prüfen, was für deren Automatisierung erforderlich wäre, und dann einen Plan zur Implementierung der Automatisierung aufstellen.

Beginnen Sie umgehend mit der Automatisierung und warten Sie nicht, bis Sie alle Bereiche identifiziert haben, in denen Automatisierung möglich ist. Die iterative Automatisierung von Prozessen ist an sich schon ein DevOps-Prozess. Beim Automatisieren, Anpassen und Verbessern Ihrer Prozesse werden Sie nützliche Kompetenzen sowie Erfahrung zur Förderung Ihrer gesamten DevSecOps-Praktiken gewinnen.

Mehr Zeit für interessante Aufgaben

Durch Automatisierung sollen keine Menschen ersetzt werden, sondern die Produktivität, Konsistenz und Effizienz verbessert werden. Dies ist das Paradoxon der Automatisierung: Durch den Einsatz der Automatisierung wird die menschliche Beteiligung zwar seltener, aber umso wichtiger.

Anstatt Automatisierung als etwas zu betrachten, das Arbeitsplätze eliminiert, ist es in Wirklichkeit so, dass erfahrenes IT-Personal mithilfe der Automatisierung größere Probleme und deren Lösung in Angriff nehmen kann, statt sich täglich immer wieder um dieselben Aufgaben kümmern zu müssen.



Automatisierung unternehmensweit einsetzen

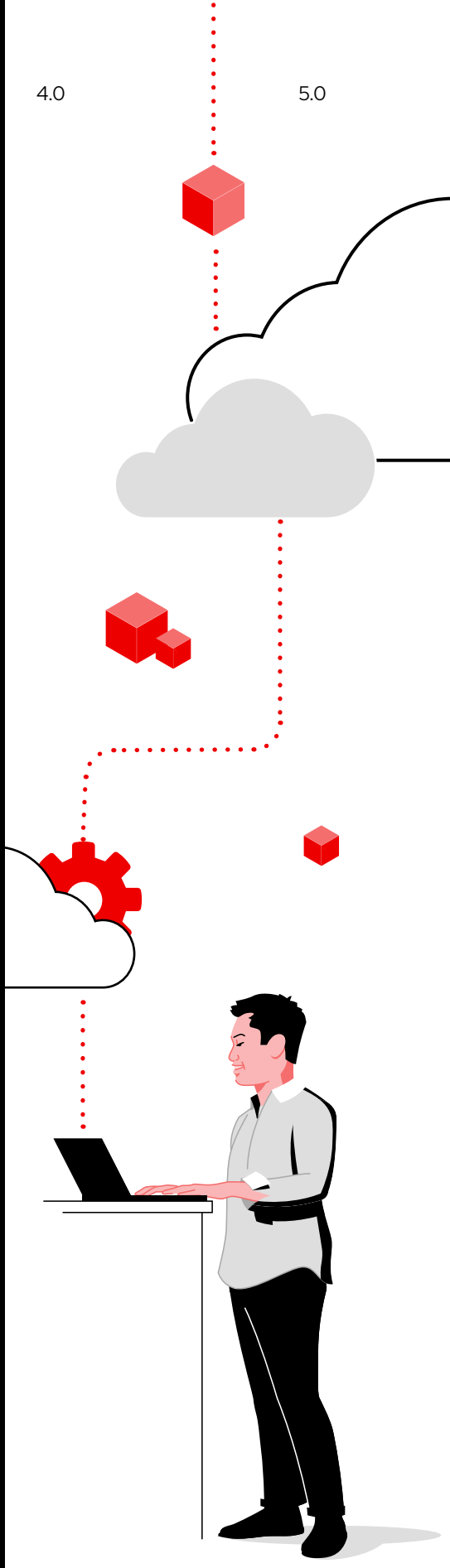
Mithilfe von Automatisierung können Sie Ihre Menschen, Prozesse und Technologien zusammenbringen und so für mehr geschäftliche Agilität und Innovationen sorgen und Ihren Geschäftswert erhöhen.

Lesen Sie das E-Book „**Das automatisierte Unternehmen**“, um mehr über die unternehmensweite Einführung von Automatisierung zu erfahren.

Tools für Ihre Software-Fabrik

Tools sind ein wichtiger Teil Ihrer Software-Fabrik. Wir empfehlen Ihnen, die folgenden Kategorien an Tools in Ihrer Softwarefabrik zu verwenden – und zu automatisieren. Dabei werden für jede Art von Tools Beispiele gegeben, Sie können aber auch andere nutzen.

Tool-Kategorie	Beispiele
Projektmanagement	▸ Confluence mit Jira ▸ Trello
Quellcodemanagement (SCM)	▸ GitHub ▸ GitLab
Integrierte Entwicklungsumgebungen (Integrated development environments, IDEs)	▸ VS.code ▸ **Red Hat OpenShift Dev Spaces**
Artefakt-Repositories	▸ Nexus ▸ Artifactory
CI/CD	▸ **Red Hat OpenShift Pipelines** ▸ **Jenkins**
Runtimes	▸ **Red Hat Runtimes** ▸ Golang
Build	▸ Maven ▸ Dotnet build
Testen von Einheiten	▸ JUnit ▸ NUnit
Quellcodeanalyse	▸ Sonarqube ▸ Fortify
Sicherheitstests für statische Anwendungen (Static Application Security Testing, SAST)	▸ CheckMarx ▸ **Red Hat Advanced Cluster Security for Kubernetes**
Nutzungakzeptanztests	▸ Cucumber ▸ Cyprus
Sicherheitstests für dynamische Anwendungen (Dynamic Application Security Testing, DAST)	▸ Veracode ▸ Synopsys
Telemetrie, Metriken und Protokollierung	▸ **Prometheus** ▸ **Grafana** ▸ **Elasticsearch, Fluentd und Kibana (EFK)** ▸ Splunk
Service Mesh	▸ Linkerd ▸ **Red Hat OpenShift Service Mesh**



Entwicklung, Deployment, Ausführung

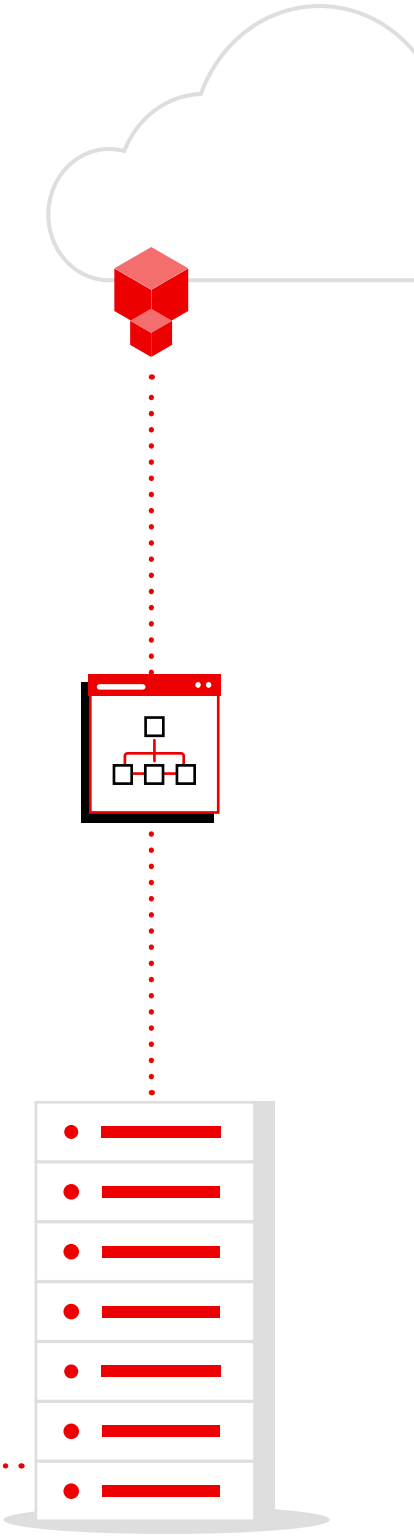
Oft konfigurieren Plattformarchitektinnen und -architekten oder DevOps-Ingenieurinnen und -Ingenieure Softwarefabriken für Entwicklungs-Teams. Wenn Sie Ihre Softwarefabrik aufbauen, sollten Sie Best Practices für Sicherheit in den folgenden drei Bereichen berücksichtigen: Entwicklung, Deployment und Ausführung.

Entwicklung

Kontrollieren Sie die Sicherheit und Compliance von Anwendungen.

Für cloudnative Deployments ist es wichtig, dass Sie Sicherheit von Anfang an in Ihre Anwendungen integrieren.

- Verwendung vertrauenswürdiger Quellen für externe Container- und Anwendungsinhalte (einschließlich Runtimes)
- Einführung einer vertrauenswürdigen, privaten Container Registry für die Image-Verwaltung
- Automatisierung von Entwicklungs- und Deployment-Pipelines
- Implementierung nicht funktionaler Anforderungen in Code mithilfe agiler Praktiken wie TDD
- Integration von Sicherheit in Anwendungs-Pipelines durch die Analyse der Codequalität sowie von Image-Schwachstellen und Kubernetes-Deployments
- Automatisierung von Anwendungs-Deployments und -platzierung



Deployment

Schützen Sie Ihre Plattform.

Für eine wirksame Sicherheit ist es erforderlich, dass Sie Ihre Kubernetes-Plattform schützen und Deployment-Richtlinien automatisieren.

- Reduzierung der Angriffsfläche durch ein für Container optimiertes Betriebssystem
- Automatisierung des Konfigurationsmanagements und der Richtlinienerzwingung in Clustern
- Implementierung des Zugriffs nach dem Prinzip der geringsten Privilegien mit RBAC (Role-based Access Control)
- Verschlüsselung von Plattform- und Anwendungsdaten bei der Übertragung und im Ruhezustand
- Verwendung von automatisierten Lösungen für Compliance, Risikobeurteilung und Problembehebung
- Reduzierung von Deployment-Risiken mit Richtlinien für die Zugangskontrolle von Kubernetes-Pods

Ausführung

Sichern Sie Ihre Container-Runtimes.

Sorgen Sie für die Beibehaltung der Anwendungssicherheit zur Laufzeit.

- Isolierung von ausgeführten Anwendungen mit SELinux (Security-Enhanced Linux®), SCC (Security Context Constraints), Kubernetes-Namespaces, RBAC und Netzwerkrichtlinien
- Verwendung von Quotas zur Vermeidung von Ressourcenkonflikten und damit zusammenhängenden Performance-Problemen
- Verwaltung des Anwendungszugangs und Schutz der Anwendungsdaten durch SSO-Nutzerverwaltung (Single Sign-On), Ingress- und Egress-Sicherheitsverwaltung, verschlüsseltem Pod-zu-Pod-Datenverkehr und API-Verwaltung (Application Programming Interface)
- Audits und Überwachung der Plattform- und Anwendungsaktivität
- Automatisierung der Bedrohungserkennung und -reaktion bei Pods mit anomalem Verhalten, privilegierten Eskalations-Events und riskanten Prozessen wie Cryptomining
- Verwendung von Zugangskontrollen zur Verhinderung der Bereitstellung von Containern, die Sicherheitsrichtlinien nicht erfüllen
- Aufbau von Zero Trust-Netzwerken mit Service Meshes und Netzwerkrichtlinien

Sicherheitstipp

Im Whitepaper „**Ein mehrschichtiger Sicherheitsansatz für Container und Kubernetes**“ erfahren Sie, wie Sie mit Kubernetes gemanagte containerisierte Anwendungen besser schützen können.

Entwicklung	Deployment	Ausführung
Anwendungs-Lifecycle	**Flotten-Konfigurationsmanagement**	**Flottentransparenz und Warnungen**
Schwachstellenanalyse	Zugangskontrolle durch Richtlinien	Runtime-Verhaltensanalyse
Analyse der Anwendungskonfiguration	Compliance-Bewertung	Empfehlungen für Netzwerkrichtlinien
APIs für die CI/CD-Integration	Risikoprofiling	Erfassung von und Reaktion auf Bedrohungen
Vertrauenswürdige Inhalte	Lifecycle der Kubernetes-Plattform	Container-Isolierung
Container Registry	Identitäts- und Zugriffsmanagement	Netzwerkisolierung
Build-Management	Plattformdaten	Anwendungszugriff und -daten
CI/CD-Pipelines	Deployment-Richtlinien	Transparenz

DevSecOps

Implementierung mit DevSecOps-Fachkräften

Red Hat bietet ein zertifiziertes Partnernetzwerk, ein umfangreiches Fachwissen und innovative Plattformen für die Entwicklung, Sicherung und Bereitstellung von Anwendungen in Hybrid Cloud-Umgebungen. Wir verfügen über jahrelange Erfahrung in der Unterstützung von Unternehmen bei der Bewältigung ihrer technologischen und geschäftlichen Herausforderungen mithilfe von branchenspezifischen Best Practices und Open Source-Technologien.

Red Hat Plattformen bieten eine Lieferkette vertrauenswürdiger Inhalte, Support durch ein dediziertes Sicherheitsteam und Backports wichtiger Sicherheitsfunktionen, was sie zu einer optimalen Basis für DevSecOps-Lösungen macht. Wir bieten außerdem **Trainings- und Zertifizierungskurse**, **interaktive Labs**, **Consulting-Services** und **gemanagte Angebote**, mit denen Sie Ihre DevSecOps-Praktiken schneller entwickeln können.

Red Hat passt sich bei der DevSecOps-Einführung an Ihre Anforderungen an.

Mit unseren bewährten Open Source-Plattformen und fachkundigen Services können Sie heute erforderliche Deployments ausführen, sich bei zukünftigen Veränderungen anpassen und die Methoden und Ansätze lernen, die Sie für eine effiziente und wirksame DevSecOps-Einführung brauchen.

Mehr über die Einführung von DevSecOps mit Red Hat erfahren.

Maximierung Ihrer DevSecOps-Investitionen

Red Hat Services kann Ihnen die erforderlichen Ressourcen zur Verfügung stellen, damit Sie Ihre DevSecOps-Praktiken starten, beschleunigen und ausweiten können.

- **Red Hat Open Innovation Labs**
  Eine Consulting-Service im Workshop-Format, bei dem Kunden und Beschäftigte von Red Hat als Team zusammenarbeiten, um neue Arbeitsweisen – wie DevSecOps – zu erlernen und gleichzeitig geschäftliche Ergebnisse zu erreichen.
- **Red Hat Services Solution: DevSecOps**
  Ein Service-Projekt, das Sie bei der Implementierung einer Softwarefabrik mit einem modularen Ansatz unterstützt.
- **Red Hat Services Journey: Container Adoption**
  Ein Consulting-Service zur Einführung von Containern in wichtigen Arbeitsbereichen.
- **Red Hat Services Journey: Automation Adoption**
  Ein Consulting-Service, der ein Framework für das Management Ihrer unternehmensweiten Automatisierung bietet.

Eine Plattform für erfolgreiche DevSecOps

Red Hat OpenShift Platform Plus stellt eine technologische Basis und ein vorgegebenes Framework für DevSecOps bereit. Diese innovative Anwendungsplattform bietet Ihnen eine konsistente Ausführung und Skalierung in Onsite- und Cloud-Infrastrukturen. Red Hat OpenShift Platform Plus bietet Ihnen eine führende Kubernetes-Plattform für Unternehmen, mit der sich Anwendungen in Ihrer gesamten Umgebung konsistent entwickeln, bereitstellen, ausführen, schützen und verwalten lassen. Multicluster-Managementtools bieten eine umfassende Transparenz und Kontrolle Ihrer Kubernetes-Cluster. Kubernetes-native Sicherheit und DevSecOps-Funktionen schützen Ihre Software-Lieferkette, Infrastruktur und Workloads. Die skalierbare, global verteilte Registry und Clusterdatenverwaltung sichert Ihre Umgebungen und Daten.

Dank der offenen Integrationsoberflächen und dem **zertifizierten Partnernetzwerk** von Red Hat können Sie sowohl vorhandene als auch neue Entwicklungs-, Test-, Betriebs- und Sicherheits-Tools mit Red Hat OpenShift Platform Plus nutzen. Viele Anbieter verfügen über **zertifizierte Red Hat OpenShift Operatoren** oder **zertifizierte Software-Container** zur Vereinfachung der Installation und Verwaltung ihrer Software auf Red Hat Plattformen. Außerdem können Sie viele Softwareprodukte direkt über den **Red Hat Marketplace** erwerben und bereitstellen. Außerdem arbeitet Red Hat mit wichtigen Cloud-Anbietern zusammen, um vollständig gemanagte **Red Hat OpenShift Cloud-Services** bereitstellen zu können, die das Deployment und den Betrieb optimieren. Gleichzeitig werden die Kosten der internen Installation reduziert.

Red Hat OpenShift Platform Plus Komponenten

Red Hat OpenShift

Red Hat OpenShift ist eine unternehmensgerechte Kubernetes-Anwendungsplattform, auf der Operationen für den gesamten Stack automatisiert werden, um Hybrid Cloud- und Edge-Deployments einfacher verwalten zu können. Mit enthalten sind dabei Funktionen, die auf Entwicklerinnen und Entwickler ausgerichtet sind und die Produktivität und Geschwindigkeit steigern können.

Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes ist eine Konsole, die Ihnen einen umfassenden Überblick über Ihre Kubernetes-Domain sowie integrierte Governance und Anwendungs-Lifecycle-Management-Funktionen bietet.

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes ist eine Lösung mit Kubernetes-nativen Sicherheitsfunktionen, die den Schutz Ihrer Infrastruktur und Workloads ausweitet und Ihnen einen umfassenden Überblick über den Anwendungs-Lifecycle bietet.

Red Hat Quay

Red Hat Quay ist eine Open Source-Registry für Container Images, mit der Sie Storage erhalten und Container in Rechenzentren und Cloud-Umgebungen erstellen, verteilen und bereitstellen können.

Red Hat OpenShift Data Foundation

Red Hat OpenShift Data Foundation ist eine skalierbare Schicht aus Daten- und Storage-Services, die Red Hat OpenShift Umgebungen Effizienz, Resilienz und Sicherheit bietet.

Red Hat OpenShift Platform Plus unterstützt Sie in allen Phasen Ihrer DevSecOps-Einführung. Es passt sich an Ihren aktuellen Stand an und gibt Ihnen eine Basis, mit der Sie sich in Ihrem eigenen Tempo entwickeln können.

Integrierte Sicherheitsfunktionen

Überwachen Sie Ihre aktiven Workloads auf Sicherheitsprobleme und Bedrohungen hin – durch Erfassung und Analyse von Daten auf Systemebene und mit mehr als 60 integrierten Sicherheitsrichtlinien, die während des gesamten Lifecycles Ihrer Anwendung angewendet und durchgesetzt werden können.

Konsistente Abläufe

Wenden Sie konsistente operative Richtlinien für Sicherheit, Konfiguration, Compliance und Governance in Red Hat OpenShift Clustern in Onsite-Rechenzentren und Cloud-Infrastrukturen an.

Entwicklertools

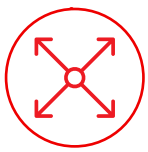
Mit der enthaltenen Library an unterstützten Build-Tools, Sprachen, Pipelines und Frameworks können Sie Anwendungen schneller entwickeln, ausführen und bereitstellen. Das Operator-Framework bietet Integrationen für aktuelle Entwicklertools, die für die Nutzung mit Red Hat OpenShift getestet und verifiziert wurden.

End-to-End-Management

Sorgen Sie für eine konsistent Verwaltung Ihrer Red Hat OpenShift Umgebung mit einer einheitlichen Oberfläche für Administrations- und Entwicklungsteams, die in Onsite-, Cloud- und Edge-Umgebungen funktioniert – einschließlich solcher, die auf anderen Kubernetes-Distributionen basieren.

Support für DevSecOps

Integrieren Sie deklarative Sicherheitsfunktionen in Entwicklertools und -workflows. Mit Kubernetes-nativen Kontrollen können Sie auf Bedrohungen reagieren und Sicherheitsrichtlinien durchsetzen und so operative Risiken minimieren.



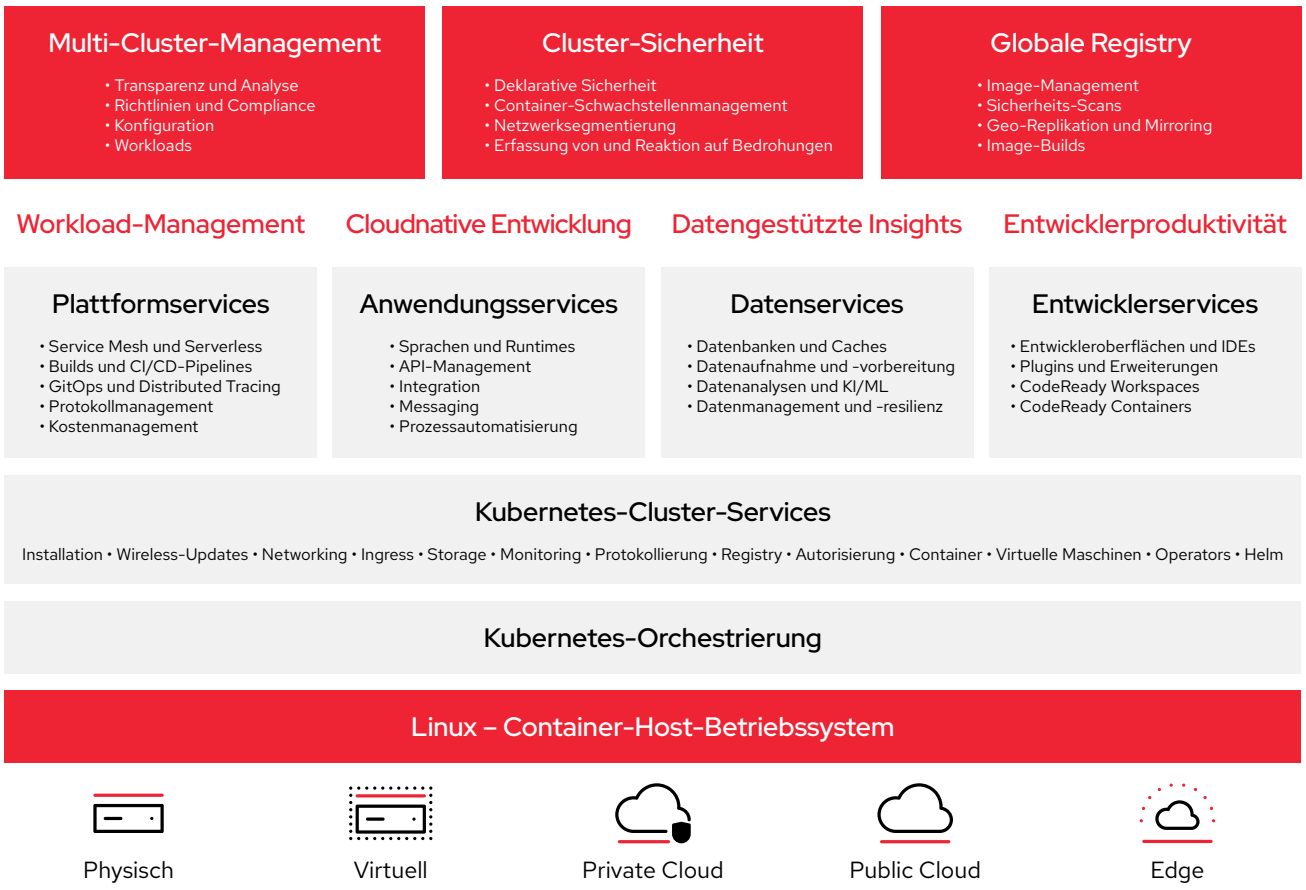
Skalierbare Datenservices

Optimieren Sie das Datenmanagement Ihrer Cluster. Durch die Unterstützung von Datei-, Block- und Objektdatenprotokollen stellt Red Hat OpenShift Data Foundation einen resilienten persistenten Storage für zustandsbehaftete Anwendungen und Clusterservices zur Verfügung.

Zero Trust-Netzwerkfunktionen

Implementieren Sie **Zero Trust-Netzwerke** für die resiliente, sichere, beobachtbare Kommunikation zwischen Anwendungen und Services. **Red Hat OpenShift Service Mesh** ist in Red Hat OpenShift enthalten und integriert, damit Sie Ihre Kommunikation einfacher schützen können.

Red Hat OpenShift Platform Plus stellt Ihnen die Technologien und Funktionen zur Verfügung, die Sie für eine effektive DevSecOps-Einführung benötigen. Im **Red Hat OpenShift Sicherheits-Guide** erfahren Sie mehr zur Sicherheit im gesamten Technologie-Stack.



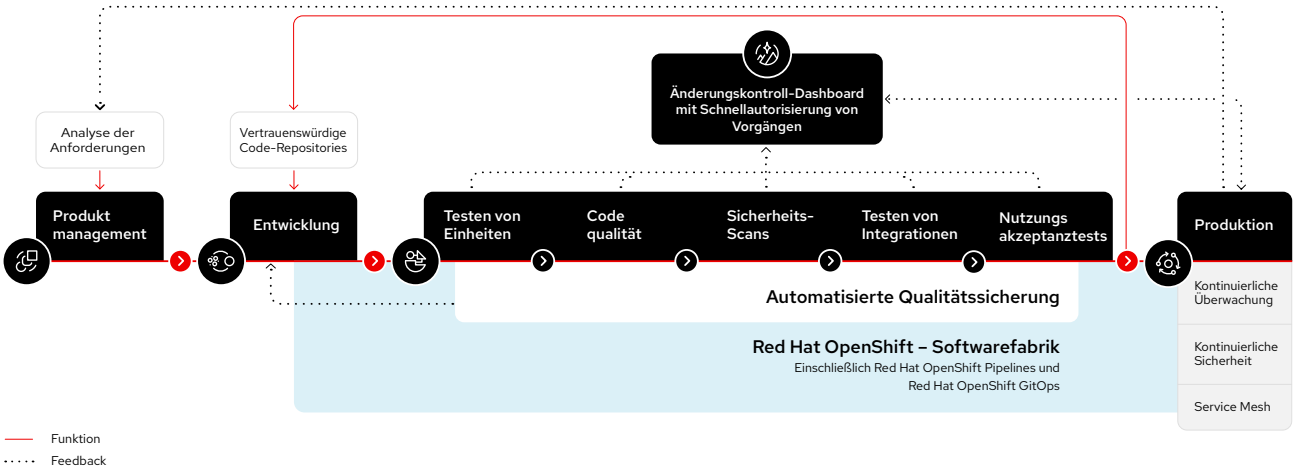
Den Einstieg schneller schaffen – mit Red Hat OpenShift Cloud-Services

Red Hat OpenShift Cloud-Services sind in **AWS**, **Google Cloud**, **IBM Cloud** und **Microsoft Azure** verfügbar. So können Sie die Option wählen, die den Anforderungen Ihres Unternehmens am besten gerecht wird. Jeder Service liefert eine komplette Full Stack-Umgebung mit allen notwendigen Services, einfachen Self-Service-Optionen und rund um die Uhr verfügbarem, kompetenten Support mit strengen SLAs (Service Level Agreements).

In der Kurzdarstellung „**Mehr Effizienz mit gemanagten Services von Red Hat OpenShift**“ finden Sie weitere Informationen.

Entwicklung einer Basis für Ihre Softwarefabrik mit Red Hat OpenShift Platform Plus

Red Hat OpenShift Platform Plus stellt eine zuverlässige, adaptive, kombinierbare Basis für Ihre Softwarefabrik zur Verfügung. Damit können Sie Sicherheitsprüfungen in Ihre CI/CD-Pipelines integrieren, um Entwicklerinnen und Entwicklern automatisierte Rahmenbedingungen in vorhandenen Workflows zu geben, ihre Workloads und Kubernetes-Infrastruktur vor Fehlkonfigurationen und Compliance-Verstößen zu schützen und die Erkennung von und Reaktion auf Bedrohungen der Runtime zu implementieren.



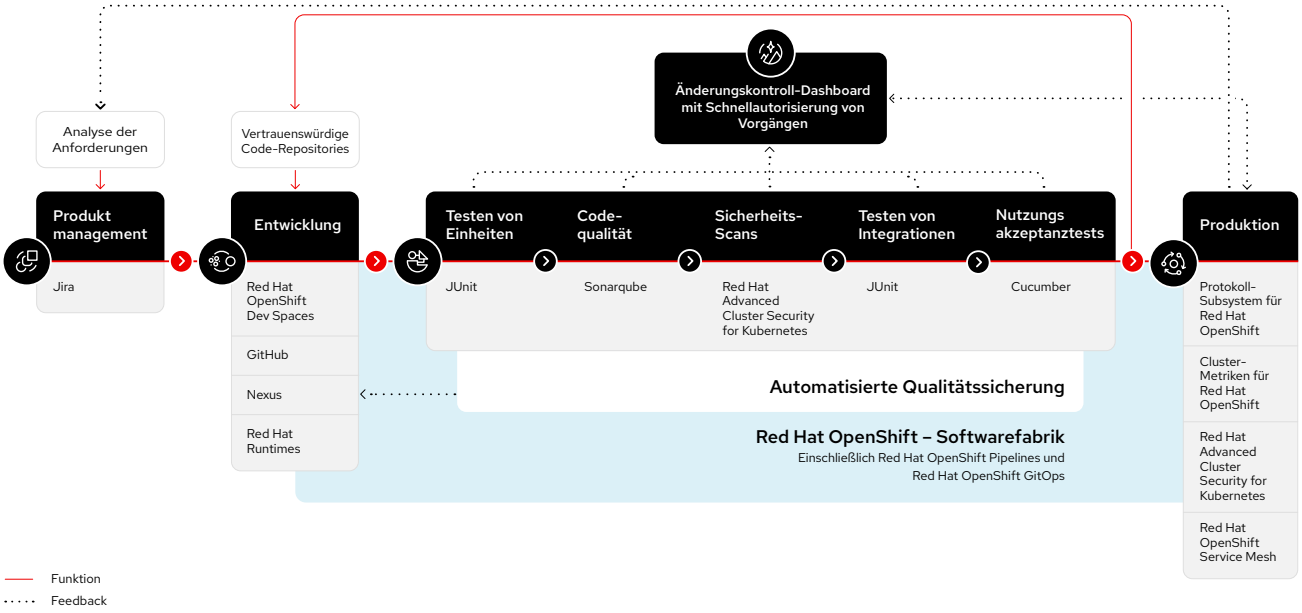
Aufbau vollständiger Softwarefabriken mit einem System von Drittanbietertools

Unterschiedliche Use Cases erfordern unterschiedliche Tools innerhalb Ihrer Softwarefabrik. Mit Red Hat OpenShift Platform Plus als Ihrer Basis können Sie jede Phase Ihrer Softwarefabrik mit Ihren bevorzugten Drittanbieterprodukten und -technologien erstellen, darunter:

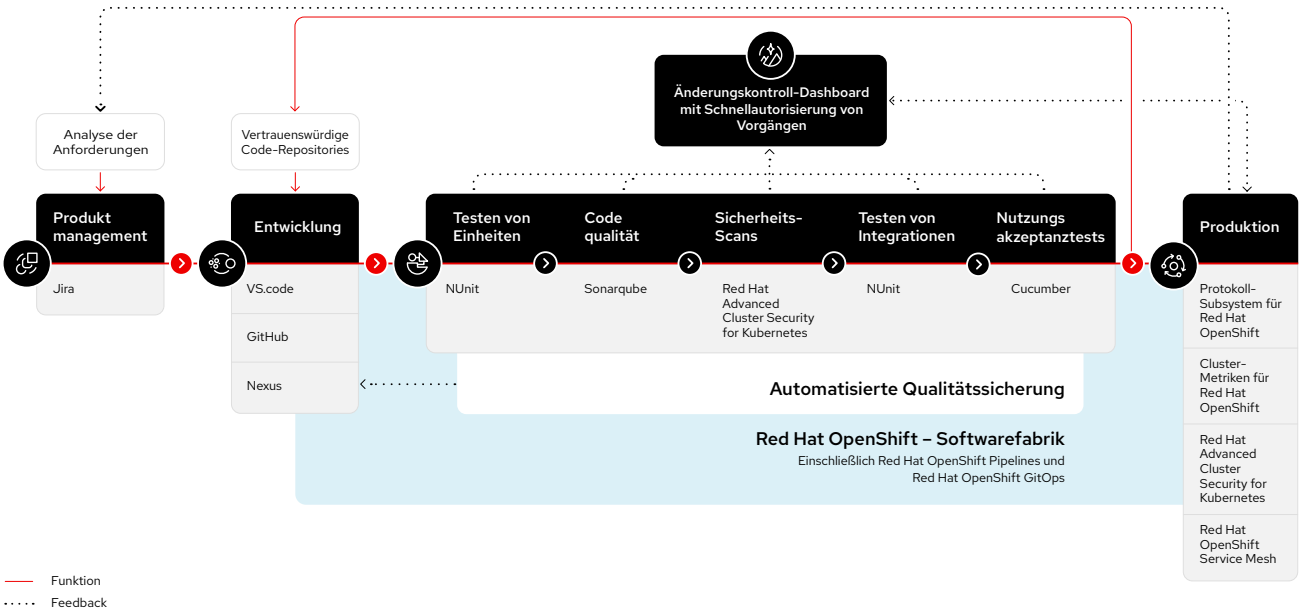
- PAM-Tools (Privileged Access Management)
- Externe Zertifizierungsstellen
- Externe Vaults und Schlüssel-Management-Lösungen
- Scanner für Container-Inhalte und Tools für das Schwachstellenmanagement
- Analysetools für Container Runtimes
- SIEM-Systeme (Security Information and Event Management)
- Managementtools für die Versionskontrolle
- Artefakt-Repositories
- Softwaretesttools

So würde eine Softwarefabrik für die cloudnative Entwicklung von Spring Boot-Anwendungen andere Runtime-, Build- und Testtools verwenden als eine Softwarefabrik für .Net Core-Anwendungen. Mögliche Strukturen für diese beiden Softwarefabriken sind im Folgenden dargestellt und veranschaulichen die Flexibilität einer auf Red Hat Lösungen basierenden Softwarefabrik.

Softwarefabrik für die cloudnative Entwicklung von auf Microservices basierenden Spring Boot-Anwendungen



Softwarefabrik für die cloudnative Entwicklung von auf Microservices basierenden .Net Core-Anwendungen



Erfolgsbeispiele aus der Praxis

Snam, eines der größten Erdgasnetzwerke der Welt, führte Red Hat Technologien und Services wie Red Hat OpenShift, Red Hat Quay und **Microsoft Azure Red Hat OpenShift** ein, um die digitale Transformation des Unternehmens voranzutreiben. Das Unternehmen kann Anwendung jetzt automatisch innerhalb von nur 30 Minuten bereitstellen, was die Release-Zeit für neue Softwareprodukte um mehr als das Zehnfache verbessert. Da Snam außerdem Workloads und Anwendungen in verschiedenen Public oder Private Clouds skalieren kann, ist das Unternehmen für die Erfüllung zukünftiger geschäftlicher Anforderungen gut aufgestellt und kann die potenziellen Risiken einer Cloud-Anbieterbindung reduzieren.

> Red Hat OpenShift ist ein wichtiger Eckpfeiler unseres Transformationsprojekts. Wir konnten damit eine effiziente, hochleistungsfähige und zuverlässige IT-Plattform entwickeln und die Verwaltung unserer komplexen Systeme und Anwendungen vereinfachen.

Roberto Calandrini
Head of Architecture, Digital and AI Services, Snam

Mehr erfahren

VodafoneZiggo, ein in den Niederlanden führender Anbieter von Kommunikations- und Unterhaltungsservices für Verbraucherinnen und Verbraucher sowie Unternehmen, stellte eine auf Red Hat OpenShift basierende Hybrid Cloud-Plattform bereit, um seine Anwendungsinfrastruktur zu vereinheitlichen. Das Unternehmen beauftragte zudem Red Hat Consulting damit, die umfassende Einführung von DevSecOps in der Organisation sowie die Umstellung auf eine offenere Kultur der Zusammenarbeit anzuleiten und zu begleiten. VodafoneZiggo kann jetzt schneller und effizienter in einer Vielzahl von Clouds und am Netzwerkrand skalieren und mit den Anforderungen des Unternehmens und des Markts mithalten.

> Wir sehen Red Hat OpenShift als eine konsistente Schicht für cloudnative Anwendungen und Services, die uns ermöglicht, die Produktivität zu steigern und kontinuierliche Innovationen zu schaffen.

André Beijen
Director, Mobile Network, VodafoneZiggo

Mehr erfahren

Einstieg in DevSecOps

Geschwindigkeit, Skalierung und Sicherheit sind in einer cloudnativen Welt entscheidend.

Eine auf Red Hat OpenShift Platform Plus basierende Softwarefabrik kann Sie bei der Einführung von erfolgreichen DevSecOps-Praktiken unterstützen, mit denen Sie die Entwicklung beschleunigen, Abläufe optimieren und Ihr Unternehmen schützen.

Red Hat OpenShift® kostenlos testen:

cloud.redhat.com/try

Mehr über Red Hat OpenShift Platform Plus erfahren:

red.ht/openshift-platform-plus

F31657_0522_KVM

Red Hat