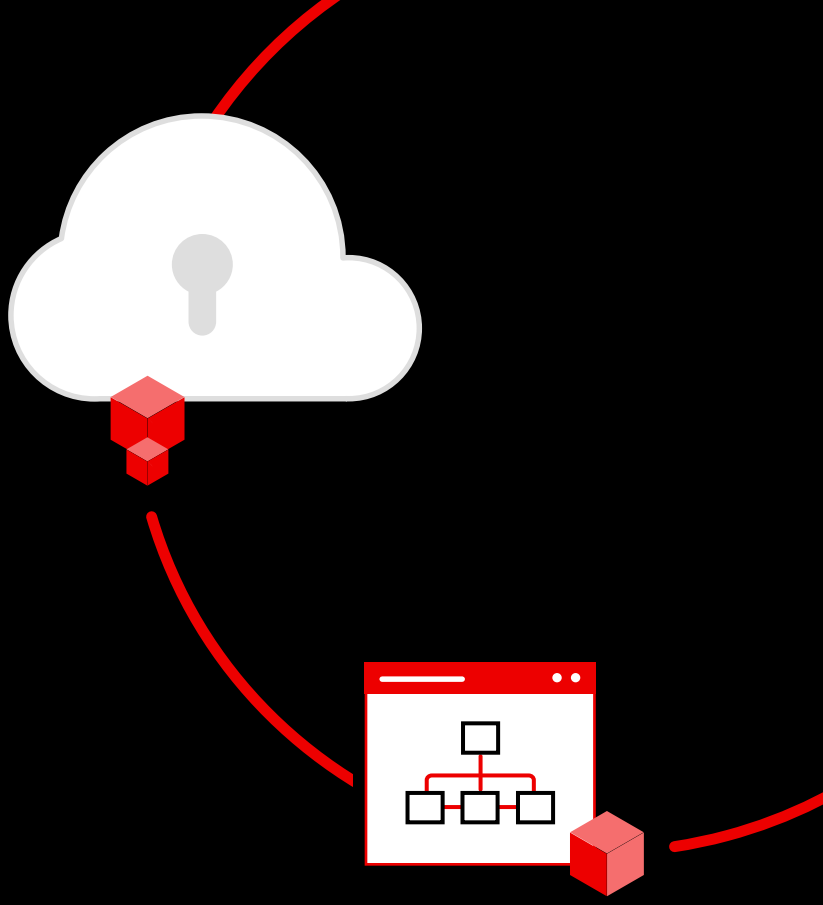
Red Hat
OpenShift
Platform Plus

打造支持 DevSecOps 的软件工厂

关于如何开启 DevSecOps 旅程的独到指南

目录



借助 DevSecOps 保护您的业务

越来越多的企业采用**云原生**、**容器**和**微服务**技术来开展创新和**数字化转型**。在转型过程中，许多企业利用 Kubernetes 进行容器编排以支持云原生运维。由于 **Kubernetes** 集群可以跨越本地和云环境中的主机，因此对于托管需要快速扩展和弹性运维的云原生应用来说， Kubernetes 是一个理想的平台。

尽管如此，Kubernetes 也带来了新的挑战，尤其是在规模化实施安全性和可管理性方面。事实上，50% 的企业 IT 高级主管将网络安全列为技术计划的三大优先事项之一。[1]

采用 DevSecOps 方法和实践可以将安全防护融进应用、流程和平台中，更好地保护您的业务。

本电子书探讨了有关借助红帽® OpenShift® 和其他红帽技术在企业内建立成功的 DevSecOps 实践的注意事项，并提供了相关的指导。

什么是云原生应用?

云原生应用是独立的小规模松散耦合服务的集合，

什么是 DevOps 和 DevSecOps?

DevOps 是指对企业文化、业务自动化和平台设计等方面进行全方位变革，实现迅捷、自动且优质的服务交付，从而专注于提升企业价值和响应能力。**DevSecOps** 是对 DevOps 协作文化的进一步扩展，旨在将安全性纳入整个应用周期内。它包含人员、流程和技术，使安全性在分布式环境中更加普及。

通过 DevSecOps，安全性成为所有团队共同承担和履行的责任，而不是仅由单个团队负责、直到开发和部署流程行将结束时才完成的一系列任务。安全、开发和运维团队携手合作，共享信息、反馈、经验教训和见解。这种方法允许从开始开发应用和部署基础设施时就集成安全性，以增强保护和降低风险。

88%

接受调查的企业使用 Kubernetes 作为容器编排器，其中 74% 将 Kubernetes 用在生产中。[2]

74%

接受调查的企业制定了 DevSecOps 计划。[2]

1 Flexera， “2021 技术支出状况报告”，2021 年 1 月。

2 红帽， “Kubernetes 安全状况报告”，2021 年。

DevSecOps 的目标

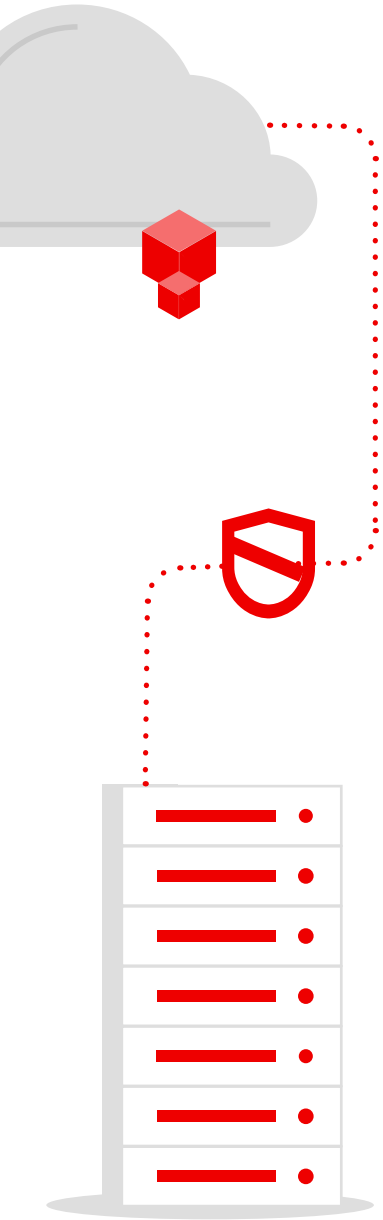
DevSecOps 的目标是快速地规模化交付和部署质量出众并以安全为重的应用、服务和功能。

扩展

速度

安全

稳定



DevSecOps 实施中的挑战

手动流程

一旦需要频繁人为介入，开发、测试和安全防护任务就会变得耗时、繁琐、易错，也难以实施。

团队之间协作有限

开发、安全防护和运维团队通常只在自己的领域内工作，造成流程分散，需要人工交接，并且无法充分了解和理解其他团队的挑战和需求。

安全防护流程贯彻不及时

传统的应用开发和发布方法只有等到流程收尾时，即部署到生产环境前，才会应用安全防护实践和检查。

应用环境错综复杂

容器、微服务和云服务等共同构成复杂的大规模应用开发、测试和生产环境，而要理解所有这些不同组件之间的衔接和安全含义颇具挑战性。

依赖于外部因素

云原生应用开发几乎都离不开一些外部依赖项，如开源代码段、库和服务等，这些外部依赖项也必须得到保护。

安全形势不断变化

安全威胁和相关法规，如业务、技术和地理位置要求等，不断快速改变，造成难以跟上发展步伐并保持合规。

人员、流程和技术至关重要

DevSecOps 不是一个团队的事，也不是一个单一流程，而是一种涵盖整个企业的能力，需要在三个领域进行变革和调整：人员、流程和技术。

人员

人员始终是任何企业级计划的核心所在，DevSecOps 也不例外。为了在整个企业中采用 DevSecOps，所有团队（包括开发、安全防护和运维）必须加入、参与并且彼此信任。

流程

流程让项目从头至尾顺利开展。制定清晰的流程来创建、部署、管理及调整应用和基础架构，并将安全防护纳入整个生命周期，对于广泛采用 DevSecOps 而言至关重要。

技术

应用平台为构建、部署及运行应用和基础架构提供所需的功能。一个支持开发、安全防护和运维团队的统一平台，可以为您建立和调整 DevSecOps 实践奠定基础。

使企业为 DevSecOps 成功做好准备

任何企业都无法在一夜之间建立完整的 DevSecOps 实践。采用 DevSecOps 是循序渐进的学习之旅，而不是孤注一掷的鲁莽尝试。需要制定合乎逻辑并可持续的策略来指导您逐步前行，并帮助您不断学习和提高。

鼓励跨团队合作。

采用激励措施并设计相应的流程，促进在整个企业内协同合作。协作使团队能够创建完整的 DevSecOps 工作流，实现更多的价值。与他人合作也有助于培养对开发、安全防护和运维的共同所有权和问责制。

记录您的当前状态。

使用 **GitOps** 等动态框架，详细记录您现有的开发、变更管理和治理流程。了解当前所处的阶段和面临的挑战，有助于您规划前进的道路。在调整流程时，务必要记录新的流程以及做出改变的原因。

评估您的流程。

识别和调整对您的 DevSecOps 目标不利的流程。其中包括效率低下或彼此迥异的持续集成/持续部署（CI/CD）设置和基础架构、过于集中的流程，以及依赖频繁手动干预的流程。

定义和衡量成功。

确定怎样才算取得 DevSecOps 成功，并明确用于跟踪进展的可衡量指标或关键绩效指标（KPI）。指标可以是应用构建和部署时间、变更发布和缺陷率、问题解决时间或应用可用性等。

分享知识和最佳实践。

创建一个由利益相关者组成的核心团队（通常称为实践社区（CoP）或卓越中心（CoE）），以便在整个企业内分享 DevSecOps 最佳实践、经验和成就。该团队还应帮助其他团队做好准备并开始采用 DevSecOps。

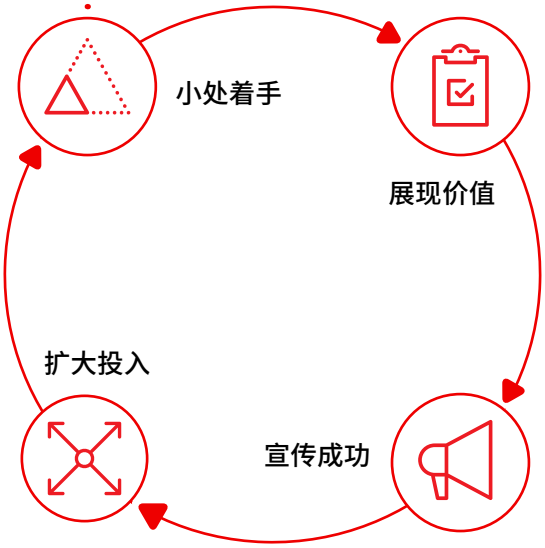
在整个企业内贯彻落实。

确保企业中的每个人都致力于采用 DevSecOps。帮助每个团队理解各项变更的缘由，并强调变更对他们的积极影响。借助高管支持和基于指标的激励措施，帮助团队在旅程中取得进展。

开始您的 DevSecOps 实践

定义好 DevSecOps 策略后，就要扬帆起航了。并不是每个开发团队都已准备好立即采用 DevSecOps。从已在采用新流程和新平台方面取得良好表现的团队着手。这些团队的成员通常也是核心利益相关者团队的理想候选者。

从小处着手，展现价值，然后谨慎扩展，如此循环重复。争取在短时间内取得渐进式成功。利用指标来监控进度，并从不太成功的项目或流程中吸取经验教训。每次取得成功时，宣传 DevSecOps 的价值，并在整个企业分享团队的经验。这样，其他人便有一个坚实的基础来借鉴各团队的经验并创造更多价值。



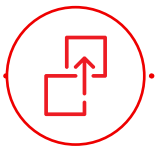
将工厂方法运用于软件交付

现代软件交付依赖于速度、一致性和质量。软件工厂方法可以帮助您实现、加速和落实在企业内采用 DevSecOps 文化所需的行为更改和举措。这种方法允许您利用一个**可信的软件供应链**和一套一致的敏捷流程（如测试驱动型开发）来快速开发和部署高质量的应用。

软件工厂的优势

软件工厂方法提供了可量化的优势：

变更交付周期短



部署频率高

故障服务恢复时间短

变更失败率低

软件交付性能量化指标[3]

软件交付性能指标	有软件工厂	无软件工厂
变更交付周期	<1 小时	1-6 个月
部署频率	按需（>1 次/天）	每隔 1-6 个月一次
服务恢复时间	<1 小时	1 天到 1 周
变更失败率	0%-15%	16%-30%

3 Google Cloud，“加速发展：2021 DevOps 现状报告”，2021 年 9 月。

软件工厂是什么样的?

软件工厂让您从不一致的手动流程转变为一致的自动化操作。

无软件工厂

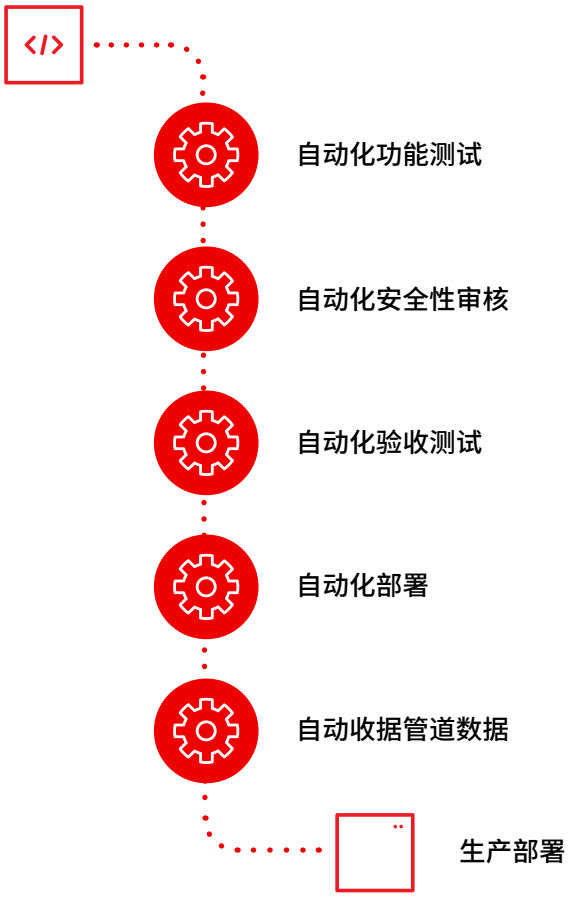
手动流程和签核会导致开发和部署缓慢、预期不明确，且安全防护贯彻不一致。即使是细微变化也可能要几天或几周才能实现，因此团队通常会试图在一次部署中进行大量更改。这会加剧变更失败和安全问题的风险。

团队间信任往往不堪一击，因为整个过程缺乏透明。安全防护和合规措施是在流程后期手动执行的，因此可能无法在开发过程中及时发现问题。结果是，应用可能要退回给开发人员，以解决意外的安全性和合规性问题。在本已紧张的阶段，这样的意外常常造成沮丧和不信任。

有软件工厂

定义清楚的自动化流程可加快开发和部署，始终如一地落实安全防护，并为所有相关团队设定明确的期望。小幅更改可在几分钟内完成部署，因此团队可以每天快速部署许多小更改，从而降低总体风险。

透明度和可见性是整个软件工厂的关键特性，开发、运维和安全防护团队之间更容易建立信任。安全防护和合规性措施在开发过程中自动得以落实，因此可以在相关流程的早期发现并解决问题。书面记录的流程和策略有助于团队了解整个过程中的期望，并防止在应用部署到生产环境时发生意外。



打造自己的软件工厂

自动化是软件工厂方法的核心。这对于运行云原生环境和采用 DevSecOps 实践而言至关重要。自动化可以帮助您以可控的方式扩展开发、交付、部署和基础架构运维。您还可以动态地调配和停用资源、环境和应用。这样，您的企业可以更快地响应变化。

考虑对 DevSecOps 工作流的每一方面进行自动化，包括开发、测试、代码质量控制、合规性验证、漏洞检测和修复流程等。使用 CI/CD 管道，自动执行应用开发和改进以及基础架构部署和管理。制定并记录安全防护和风险策略，在整个软件生命周期中针对这些策略自动执行合规性检查和修复。

借助声明式的意图驱动型自动化，您可以更快速、更轻松地扩展和调整。

声明式自动化允许您定义所需的应用或基础架构配置，而不是一组用来设置资源的指令。您只需描述最终目标，不必说明实现目标的方法。然后，应用平台就会调配并配置达到预期状态所需要的资源。它还会进行自我修复，以确保资源在不同时间保持正确配置。此外，这种方法能让您为采用 **GitOps** 做好准备； GitOps 是使用 Git 版本控制系统来管理基础架构和应用配置的一套实践。

确定自动化的对象和时间

大致与 DevSecOps 类似，部署自动化也是一段旅程，需要进行规划。按照以下步骤来开始实施自动化：

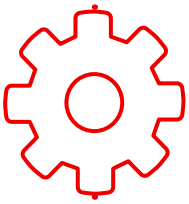
1. 详细记录您的流程。
2. 在流程中的每个手动步骤上，记录做出的决策以及具体的决策过程。决策制定可能包括阅读某些材料、考虑特定因素、咨询各种专家或采取其他行动。
3. 确定所有可以轻松自动化的手动步骤，并评估哪些程度的变更应当自动完成。例如，小的变更交由系统自动完成，而大的变更则需要经过某些团队的批准。
4. 对于无法轻松实现自动化的手动步骤，评估需要自动化的对象，并制定实施自动化的计划。

立即开始实施自动化，不需要等到确定所有可能的自动化领域后再做。对流程进行迭代式自动化本身就是一种 DevOps 流程。随着流程得到自动化、调整和完善，您将获得宝贵的技能和经验来支持整体的 DevSecOps 实践。

专注于有意义的工作

自动化并不以取代人力为目标，重点是提高生产力、一致性和工作效率。这是自动化的悖论，因为当您实施自动化后，人工介入的重要性会提高，但频率会降低。

一些人将自动化视为减少工作量的法宝，但实际上，自动化是为了让经验更丰富的 IT 员工将精力投入到更重要的问题和解决方案上，而不是困于周而复始的琐碎日常任务。



了解如何在整个企业内开展自动化

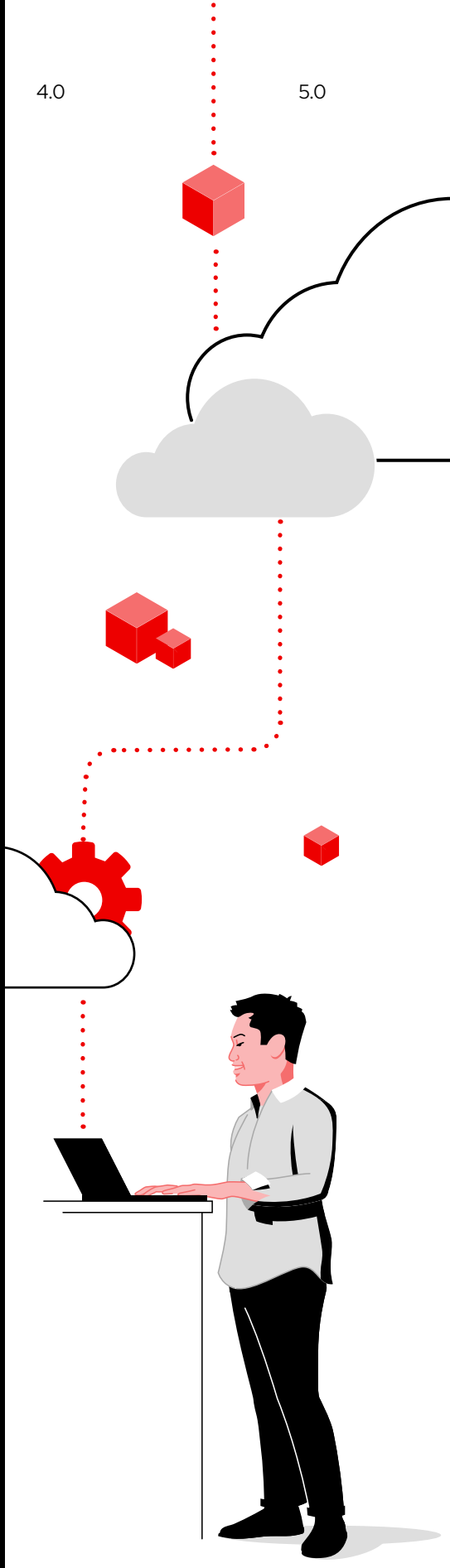
自动化可以将人员、流程和技术结合起来，提高企业的敏捷性、创新能力和价值。

阅读**自动化企业电子书**，了解您可以如何在整个企业内采用自动化。

适用于软件工厂的工具

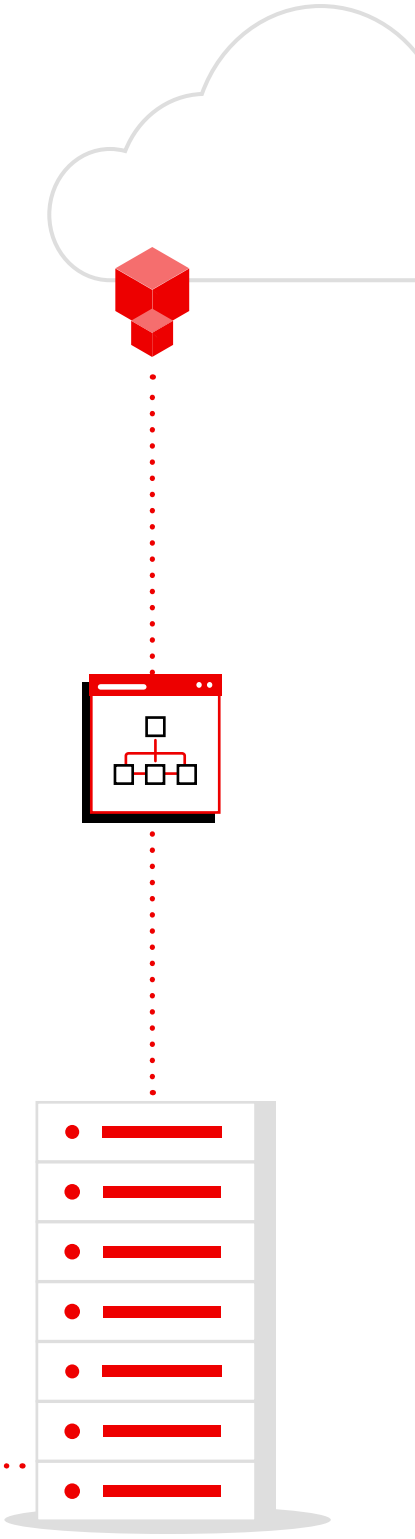
工具是软件工厂的重要组成部分。建议您在软件工厂中使用以下种类的工具并进行自动化。每一种工具都给出了示例，但也可使用其他工具。

工具类别	示例
项目管理	▸ Confluence with Jira ▸ Trello
源代码管理（SCM）	▸ Github ▸ Gitlab
集成开发环境（IDE）	▸ VS.code ▸ **红帽 OpenShift Dev Spaces**
工件存储库	▸ Nexus ▸ Artifactory
CI/CD	▸ **红帽 OpenShift Pipelines** ▸ **Jenkins**
运行时	▸ **红帽运行时** ▸ Golang
构建	▸ Maven ▸ Dotnet build
单元测试	▸ JUnit ▸ NUnit
源代码分析	▸ Sonarqube ▸ Fortify
静态应用安全测试（SAST）	▸ CheckMarx ▸ **红帽 Kubernetes 高级集群安全**
用户验收测试	▸ Cucumber ▸ Cyprus
动态应用安全测试（DAST）	▸ Veracode ▸ Synopsys
遥测、指标和日志	▸ **Prometheus** ▸ **Grafana** ▸ **Elasticsearch、Fluentd 和 Kibana（EFK）** ▸ Splunk
服务网格	▸ Linkerd ▸ **红帽 OpenShift 服务网格**



构建、部署、运行

平台架构师或 DevOps 工程师通常会代表开发人员来配置软件工厂。在构建软件工厂时，请考虑以下三个方面的安全防护最佳实践：构建、部署和运行。



构建

控制应用安全性和合规性

确保应用安全无虞对于云原生部署至关重要。

- 从受信任的来源获取外部容器和应用内容，包括运行时。
- 采用受信任的私有容器镜像仓库来管理镜像。
- 对开发和部署管道进行自动化。
- 使用诸如 TDD 等敏捷实践在代码中实现非功能性需求。
- 将安全防护与代码质量、镜像漏洞和 Kubernetes 部署分析一起集成到应用管道中。
- 自动完成应用的部署和放置。

部署

保护您的平台。

有效的安全防护需要保护您的 Kubernetes 平台并自动执行部署策略。

- 使用针对容器进行了优化的操作系统，以减小攻击面。
- 跨集群开展配置管理和策略执行的自动化。
- 使用精细的基于角色的访问控制（RBAC）实施最低权限访问。
- 对传输中和静止状态的平台及应用数据进行加密。
- 使用自动化的合规性、风险评估和修复解决方案。
- 利用 Kubernetes 容器集准入控制策略来降低部署风险。

运行

保护容器运行时的安全。

在运行时维护应用的安全性。

- 利用安全增强型 Linux®（SELinux）、安全上下文约束（SCC）、Kubernetes 命名空间、RBAC 和网络策略来隔离运行中的应用。
- 使用配额来防止资源冲突和相关的性能问题。
- 通过单点登录用户管理、入口和出口安全性管理、容器集间加密流量以及应用编程接口（API）管理，来管理应用访问并保护应用数据的安全。
- 审查和监控平台与应用活动。
- 针对具有异常行为、特权升级事件和风险流程（如加密挖矿）的容器集，自动化执行威胁检测和响应。
- 利用准入控制器来避免部署不符合安全防护策略的容器。
- 使用服务网格和网络策略来建立零信任网络。

安全防护提示

阅读**容器和 Kubernetes 安全防护分层方法**，详细了解如何保护使用 Kubernete 管理的容器化应用。

构建	部署	运行
应用生命周期	**队伍配置管理**	**队伍可观测性和警报**
漏洞分析	策略准入控制器	运行时行为分析
应用配置分析	合规性评估	网络策略建议
CI/CD 集成 API	风险分析	威胁检测和响应
可信的内容	Kubernetes 平台生命周期	容器隔离
容器镜像仓库	身份和访问权限管理	网络隔离
构建管理	平台数据	应用访问权限和数据
CI/CD 管道	部署策略	可观测性

DevSecOps

在专家助力下实施 DevSecOps

红帽结合利用经过认证的合作伙伴生态系统、深厚的专业知识和创新的平台，跨混合云环境构建、保护和部署应用。我们拥有多年的丰富经验，为企业和机构提供支持，帮助他们使用行业最佳实践和开源技术来克服技术和业务方面的挑战。

通过值得信赖的内容供应链、专业安全团队的支持和重要安全功能后援，红帽平台为 DevSecOps 解决方案提供了理想的基础。此外，我们也提供**培训和认证课程**、**互动实验室**、**咨询**和**托管服务**，帮助您更快地建立成功的 DevSecOps 实践。

无论您处在 DevSecOps 之旅的哪个阶段，红帽都能为您保驾护航。

借助我们成熟可靠的开源平台和专家服务，您可以根据当下的需求进行部署，适应未来的变化，并学习高效实施 DevSecOps 的方式方法。

详细了解为何选择红帽来实现 DevSecOps。

充分发挥 DevSecOps 投资价值

红帽服务为您提供开启、加速和扩展 DevSecOps 实践所需的资源。

- **红帽开放创新实验室**
  借助这项常驻式咨询服务，客户和红帽作为一个团队开展合作，在实现业务成果的同时学习 DevSecOps 等全新工作方法
- **红帽服务解决方案：DevSecOps**
  这项服务可帮助您利用模块化方法实施软件工厂
- **红帽服务之旅：容器采用**
  这项咨询服务可以解决关键工作流中的容器采用。
- **红帽服务之旅：自动化技术采用**
  这项服务提供一个掌控企业范围内自动化之旅的框架。

部署 DevSecOps 成功平台

红帽 OpenShift 平台 Plus 为 DevSecOps 提供技术基础和独特框架。这是一个创新的应用平台，可在本地和云端基础架构中一致地运行和扩展。红帽 OpenShift 平台 Plus 将领先的企业级 Kubernetes 平台与一致的方法相结合，方便您在自己的环境中构建、部署、运行、保护和管理应用。多集群管理工具提供对 Kubernetes 集群的完整可见性和控制力。Kubernetes 原生安全防护和 DevSecOps 功能为您的软件供应链、基础架构和工作负载提供保护。分布于全球的可扩展容器镜像仓库和集群数据管理为您的环境和信息提供安全保障。

开放式集成接口和红帽**认证合作伙伴生态系统**使您可以将现有和全新的开发、测试、运维和安全防护工具与红帽 OpenShift 平台 Plus 搭配使用。许多供应商提供**认证的红帽 OpenShift 操作器**或**认证的软件容器**，以简化其软件在红帽平台上的安装和管理。您也可以直接从**红帽市场**购买和部署许多软件产品。此外，红帽与主要的云提供商合作伙伴合作，提供全托管式**红帽 OpenShift 云服务**来简化部署和运维，同时节省内部构建成本。

红帽 OpenShift 平台 Plus 组件

Red Hat OpenShift

红帽 OpenShift 是一个企业就绪型 Kubernetes 应用平台，可以实现全栈自动化运维，以管理混合云和边缘部署。其中包含以开发人员为中心的功能，能够提高生产力并加快速度。

Red Hat Advanced Cluster Management for Kubernetes

红帽 Kubernetes 高级集群管理是一个控制台，通过内置的监管和应用生命周期管理功能，提供对整个Kubernetes 域的可见性。

Red Hat Advanced Cluster Security for Kubernetes

红帽高级集群安全防护是一个提供 Kubernetes 原生安全防护功能的解决方案，可在整个应用生命周期中增强基础架构和工作负载安全保护及可见性。

Red Hat Quay

红帽 Quay 是一个开源容器镜像仓库平台，提供存储功能，并让您可以跨数据中心和云环境构建、分发和部署容器。

Red Hat OpenShift Data Foundation

红帽 OpenShift 数据基础是一个可扩展的数据和存储服务层，为红帽 OpenShift 环境提供数据效率、弹性和安全性。

红帽 OpenShift 平台 Plus 在 DevSecOps 之旅的每一环节为您提供支持，不仅能满足您当下的需求，还能奠定一个未来发展基础，让您能够以自己的节奏稳步前行。

内置的安全防护功能

借助系统级数据收集和分析以及 60 多个可在整个应用生命周期内应用和执行的内置安全防护策略，监测运行中工作负载的安全问题和威胁。

一致的运维

在本地数据中心和云基础架构中，为红帽 OpenShift 集群应用一致的安全、配置、合规和监管运维策略。

开发人员工具

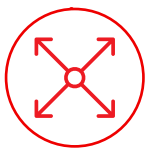
使用含有受支持的构建工具、语言、管道和框架的库，更快地创建、运行和部署应用。操作器框架可帮助集成经过测试和验证的最新开发人员工具，确保这些工具可与红帽 OpenShift 协同运行。

端到端管理

通过一个兼顾管理员和开发人员的统一界面，管理您的红帽 OpenShift 环境，适用于本地、云和边缘等多种环境，包括基于不同 Kubernetes 发行版的环境。

支持 DevSecOps

将声明式安全防护集成到开发人员工具和工作流中。利用 Kubernetes 原生控件来缓解安全威胁和执行安全策略，最大限度减少运维风险。



可扩展的数据服务

简化跨集群数据管理。红帽 OpenShift 数据基础支持文件、块和对象数据协议，为有状态应用和集群服务提供有弹性的持久存储。

零信任联网功能

实施**零信任网络**，在应用和服务之间提供弹性、安全并可观测的通信。随附**红帽 OpenShift 服务网格**并与红帽 OpenShift 集成，帮助您更轻松地保护通信安全。

红帽 OpenShift 平台 Plus 提供了有效采用 DevSecOps 所需的技术和能力。阅读**红帽 OpenShift 安全指南**，了解如何在整个技术栈中解决安全问题。

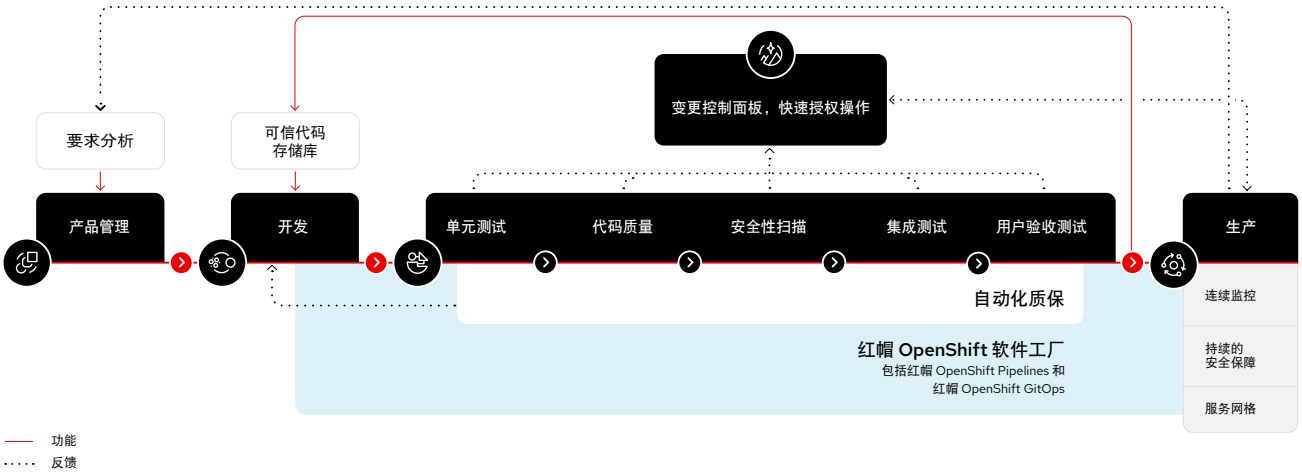
更快地开始使用红帽 OpenShift 服务

红帽 OpenShift 的云服务可以在 **AWS**、**Google Cloud**、**IBM Cloud** 和 **Microsoft Azure** 上使用，因此您可以选择最能满足自身需求的选项。每项服务都按照严格的服务级别协议（SLA），提供一个完整的全栈环境，配备所有必要的服务、简单的自助服务选项和 24x7 专家支持。

阅读**借助红帽 OpenShift 托管服务节省成本并实现更多目标**摘要，了解更多信息。

利用红帽 OpenShift 平台 Plus 为软件工厂奠定基础

红帽 OpenShift 平台 Plus 为您的软件工厂提供一个安全可靠、适应性强且可组合的基础。您可以将安全检查融入至 CI/CD 管道，为开发人员提供现有工作流中的自动防护，保护工作负载和 Kubernetes 基础架构，防止出现错误配置和不合规情形，并实现运行时威胁检测和响应。



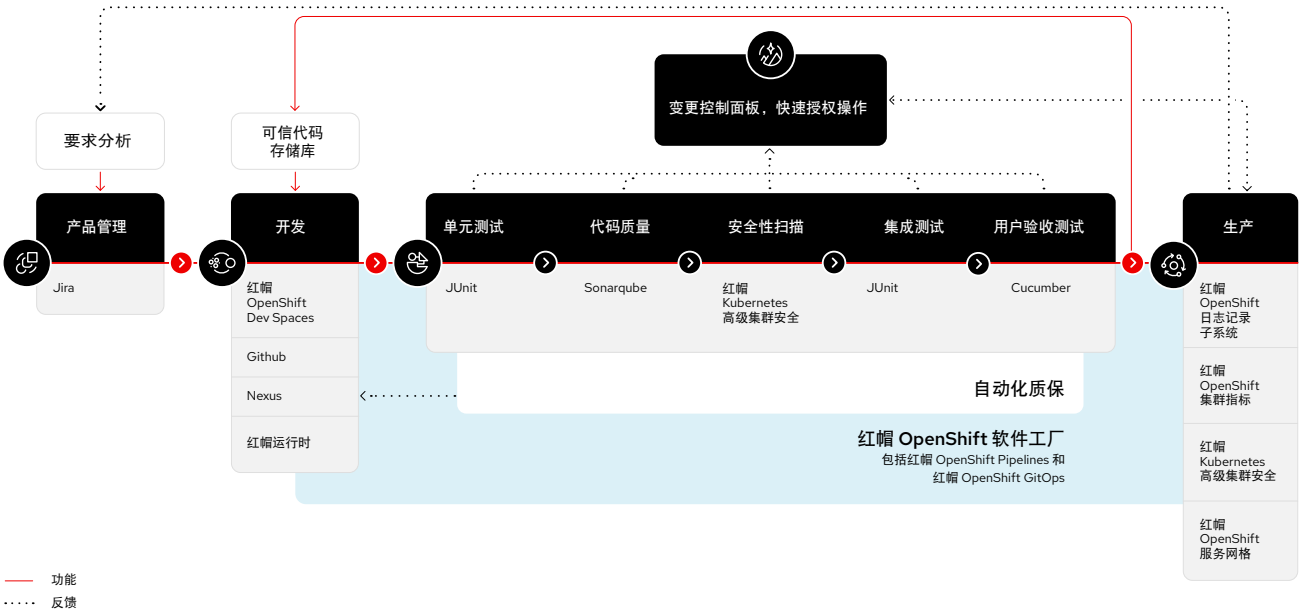
利用第三方工具生态系统组建完整的软件工厂

不同的用例需要使用软件工厂中的不同工具。有了红帽 OpenShift 平台 Plus 奠定的基础，您可以使用自己喜爱的第三方产品和技术来构造软件工厂的每一阶段，具体包括：

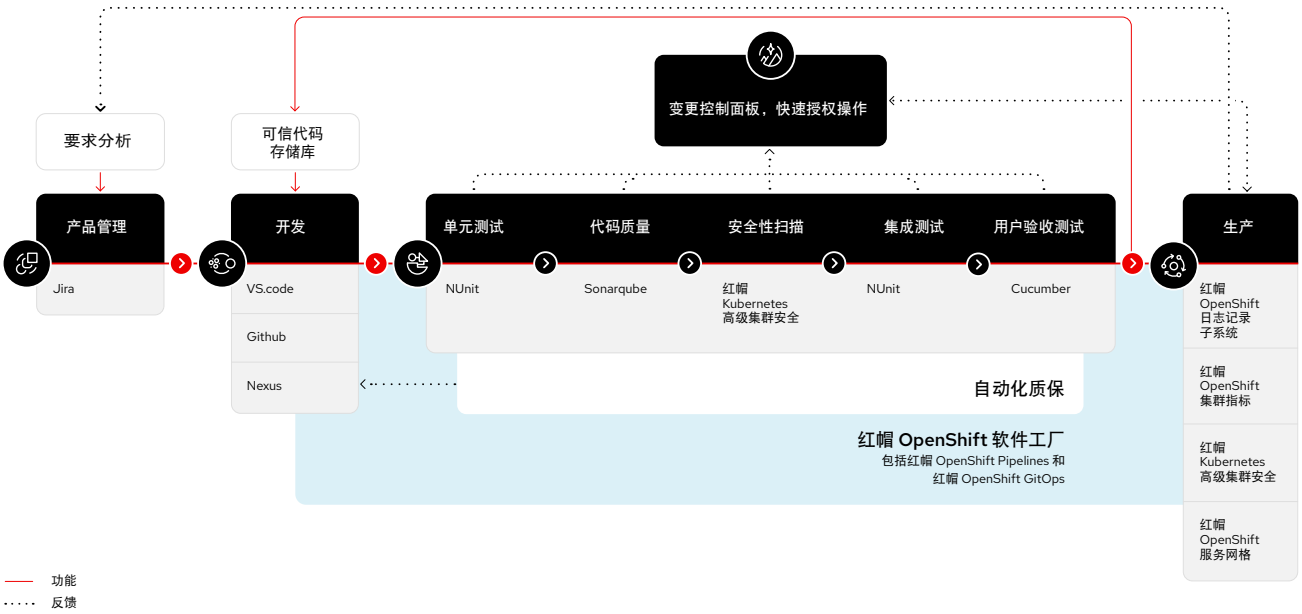
- 特权访问管理工具。
- 外部证书颁发机构。
- 外部库和密钥管理解决方案。
- 容器内容扫描程序和漏洞管理工具。
- 容器运行时分析工具。
- 安全信息和事件管理（SIEM）系统。
- 源代码控制管理工具。
- 工件存储库。
- 软件测试工具。

例如，Spring Boot 应用的云原生开发软件工厂所用的运行时、构建和测试工具，有别于 .Net Core 应用开发软件工厂所用的工具。下方演示了这两种软件工厂的可能组成，以说明红帽软件工厂基础的灵活性。

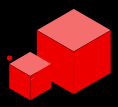
适用于基于微服务的 Spring Boot 应用云原生开发的软件工厂



适用于基于微服务的 .Net Core 应用云原生开发的软件工厂



成功案例



全球最大天然气网络之一 Snam 利用红帽 OpenShift、红帽 Quay 和微软 Azure 红帽 OpenShift 等红帽技术产品与服务来帮助推动企业数字化转型。该公司如今只需 30 分钟即可以自动化方式完成应用部署，将新软件产品的交付时间加快了 10 多倍。此外，Snam 还可以扩展任何公共云或私有云上的工作负载和应用，以满足未来的业务需求，降低潜在的云锁定风险。

> 红帽 OpenShift 是我们转型项目的奠基石，让我们能够创建一个高效、可靠的高性能 IT 平台，简化复杂系统和应用的管理。

Roberto Calandrini
Snam 架构、数字化和 AI 服务主管

了解更多

VodafoneZiggo 是荷兰领先的消费者和企业通信与娱乐服务提供商之一，部署了一个基于红帽 OpenShift 的混合云平台来统一其应用基础架构。该公司还与红帽咨询建立了关系，在红帽咨询的指导下采纳 DevSecOps 并转向更加开放、更具协作性的企业文化。VodafoneZiggo 如今能够随着业务和市场需求的发展，在多个云甚至边缘环境中更快速、更高效地进行扩展。

> 我们将红帽 OpenShift 视为云原生应用和服务的一致层面，它能协助我们提高生产力并实现持续创新。

André Beijen
VodafoneZiggo 移动网络总监

了解更多

开始采用 DevSecOps

在云原生世界中，速度、规模和安全性至关重要。

基于红帽 OpenShift 平台 Plus 的软件工厂可以帮助您建立成功的 DevSecOps 实践，从而加速开发、简化运维并保护您的业务。

免费试用红帽 OpenShift：

cloud.redhat.com/try

了解红帽 OpenShift 平台 Plus：

red.ht/openshift-platform-plus

F31657_0522_KVM

Red Hat