# 提升云安全性的四种方式

**红帽 OpenShift 云服务助您采用注重安全的方法**

许多企业正在实施技术和流程的现代化来保持竞争力。不过，这可能会让云环境的维护和安全防护变得困难。云安全性是最终用户与云提供商共担的责任，最终用户若不遵循最佳实践常会导致安全问题。内置安全功能的托管式云服务有助于简化现代化改造工作。

通过以下 4 种方式来帮助企业提升云安全性。

## 1 加速实施集成安全防护

在整个云环境中将安全防护视为优先任务。借助安全软件供应链、自动化 DevSecOps 实践和运行时应用安全防护，尽早落实安全防护工作并贯彻到整个开发周期。

红帽 ® OpenShift® 云服务提供内置的安全功能，帮助企业完成以下工作：

- 利用全托管服务中内置的自动化安全维护、持续监控和预防性修复，简化软件部署并降低运维复杂性。
- 评估 Kubernetes 平台配置，并通过集成平台配置和生命周期管理、身份和访问管理、平台数据安全防护和附加存储，使用自动化部署策略保护平台安全。
- 确保将开发运维最佳实践和内部控制融入安全防护平台的配置检查中。

## 2 委派风险管理并提高生产力

将团队工作重心转回到高价值行动上，提升工作效率并加快应用开发。作为一项共同责任，转移安全防护和基础架构管理需求可以：

- 使应用开发和部署时间缩短最多 70%，而且有助于团队快速扩展并持续改进应用。[1]
- 解放原先负责管理基础架构的开发运维团队，提升运维工作效率。
- 帮助开发人员将更新化整为零，减轻在有限时间内开展密集测试的压力。
- 在混合云环境中打造精简和优化的开发体验。

[1]Forrester Consulting（红帽赞助），“红帽 OpenShift 云服务的总体经济影响”，2022 年 1 月。

## 3 借助自动化和主动管理来降低风险

消除为应用平台招募专职安全专家的需求，减少维护云环境所需的成本和资源。全托管云服务可以帮助您：

- 专注于价值驱动和成长相关的任务，了却手动应用安全更新和补丁的负担，这些工作由红帽站点可靠性工程（SRE）团队负责管理。
- 减轻对内部基础架构管理的需求，这些管理工作给开发团队的工作增加了许多责任和风险。在采用 OpenShift 云服务的企业中，开发人员回收了 20% 的时间[1]。
- 减少 Kubernetes 和容器平台中的配置错误，据 IT 专业人士所说，这些配置错误带来的困扰几乎是网络攻击的三倍。

## 4 选择在安全方面经验丰富的提供商

保持一致且可靠的用户体验，与任何主流运营商搭配运行，如 Amazon Web Services（AWS）、Microsoft Azure、IBM Cloud 和 Google Cloud 等。

红帽深耕于开源安全防护，借助以下手段来帮助您将安全性整合到整个生命周期、基础架构和应用堆栈中：

- 默认采用零信任策略的深度防御战略，并通过合作伙伴生态系统拓展安全理念。
- 安全防护整合到人员、流程和技术中，以管理、自动化和调整基础架构，从而保持安全和合规。
- 全球 SRE 团队 24x7 全天待命，提供应用平台管理和安全防护，以及管理和数据服务。
- 云安全服务最大程度减少服务中断和系统故障，提供由财务支持的 99.95% 正常运行时间 SLA。

---

**立即开始**

阅读《红帽 OpenShift 安全指南》，了解红帽 OpenShift 云服务的可靠性。

[1] Forrester Consulting（红帽赞助），“红帽 OpenShift 云服务的总体经济影响”，2022 年 1 月。

**关于红帽**

红帽帮助客户跨环境实现标准化，支持他们开发云原生应用，并利用红帽一流的支持、培训和咨询服务，实现复杂环境的集成、自动化、安全防护和管理。

红帽官方微博

红帽官方微信

**销售及技术支持**

800 810 2100
400 890 2100

**红帽北京办公地址**

北京市朝阳区东大桥路 9 号侨福芳草地大厦 A 座 8 层　邮编: 100020
8610 6533 9300

cn.redhat.com
#F31854_202207