提升混合云的安全性和一致性

红帽和 Google Cloud Platform

46%

的企业表示，IT 安全防护是其 2022 年的首要投资重点，而在公共云上运行应用的主要原因是数据隐私（32%）和整体数据安全防护（30%）[1]。

坚实的基础铸就可靠的安全防线

企业组织正在采用混合云解决方案，以便在各个环境中确保灵活多变并积极创新。尽管混合云仍然是最常见的云策略[1]，但管理不断增长的混合云架构所面临的 IT 挑战正变得越来越复杂。

在许多情况下，企业在多个环境中部署和管理应用与工作负载，导致配置、访问和管理控制缺乏一致性。

红帽®企业 Linux® 和 Google Cloud Platform 有助于简化您的基础架构平台、加速应用开发和交付以及实现业务自动化，以便您能够通过敏捷的混合云环境迅速适应行业、法规及全球变化。

开创性的合作伙伴关系

由于红帽和 Google 均采用开源开发模式，因此他们深知云模型对安全性的影响。红帽拥有超过 25 年的 Linux 使用经验，如果能与 Google 携手合作，您的企业组织即可提升混合云环境的安全性和一致性。

Google Cloud Platform 可提供以下优势，进而确保实现用户友好、一致且透明的安全防护：

- **内置的基础架构安全防护功能。**使用基础架构技术堆栈，通过层层递进的方式构建安全防护，以提供精准且深入的防御机制。
- **完整的数据控制。**以完全透明的方式管理信息的使用方式以及哪些人员可以访问相关信息。
- **全球化的安全防护视角。**详细了解全球范围内的威胁和攻击，并提供相应保护措施，将漏洞扼杀在摇篮里。
- **在任何地方都符合规定。**所有云区域的合规性控制都是一致的，可确保客户始终能够访问最新的服务。

红帽官方微博　红帽官方微信

1 “2022 年全球技术展望”。redhat.com，2021 年 10 月。

随着云和容器化服务部署的增加，企业组织正在应对从基础架构基础层开始的挑战，比如**稳定性、扩展**和**安全防护**。

建立一致的安全防护基础

红帽企业 Linux 可帮助您构建稳定、一致且值得信赖的基础。在混合云环境中扩展应用并推出新兴技术。

红帽企业 Linux 可帮助您实现以下目标：

- **获得敏捷性和保证。**通过不断测试和验证漏洞，同时提供支持、更新和安全补丁，在企业稳定性与开源技术的灵活性之间取得平衡。
- **从容构建。**在经过独立验证和认证的平台上开发和部署关键应用，该平台符合通用标准和联邦信息处理标准（FIPS）等政府和行业标准。
- **自动满足监管合规要求。**应用行业最佳实践，独立验证基线，并为审计员生成全面的按需报告。使用红帽 Ansible® 自动化平台，以更少的资源更高效地大规模置备、修补、配置和控制开发、测试及生产系统。
- **获得可用的洞察分析。**红帽智能分析可帮助您创建安全内容自动化协议（SCAP）策略，并高效扫描系统以确保其遵守安全防护策略。
- **在业务运维受到影响之前解决相关问题。**红帽安全团队提供持续扫描、修复软件以及对新资源的访问权限，以帮助提升您的安全防护能力。
- **减轻未经授权访问的风险。**跨 Linux 和非 Linux 基础架构集中管理身份，并配置基于角色的身份验证和授权控制。
- **降低安全防护方面的开销。**红帽企业 Linux 系统角色允许企业组织以更少的资源实施和管理安全防护最佳实践，从而大规模支持安全性和合规性要求。

了解更多

提升混合云环境的安全性和一致性。探索 Google Cloud Platform 上的红帽企业 Linux。

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

红帽官方微博　红帽官方微信

cn.redhat.com
#F31726_0622