Red Hat
Advanced Cluster Security
for Kubernetes

适用于 Kubernetes 的红帽高级集群安全防护

借助业内唯一的 Kubernetes 原生容器安全防护，更好地保护 Kubernetes 和云原生应用的安全

想要保护云原生应用，我们需要对安全防护方法做出重大改变：我们必须在应用开发生命周期的早期应用控制，利用基础架构自身应用控制，并跟上越来越紧密的发布时间表。

适用于 Kubernetes 的红帽®高级集群安全防护由 StackRox 技术提供支持，并在构建、部署和运行时为重要应用提供安全防护。软件将部署到基础架构，并集成 DevOps 工具和工作流，提供更好的安全性和合规性。该策略引擎包括数百个内置控制功能，可强制执行 DevOps 和安全防护最佳实践、行业标准，例如 CIS 基准和美国国家标准与技术研究院 (NIST) 指南、容器和 Kubernetes 的配置管理，以及运行时安全。

适用于 Kubernetes 的红帽高级集群安全防护 为容器安全防护提供了 Kubernetes 原生架构，并使 DevOps 和 InfoSec 团队能够实施防护。

功能和优势

- Kubernetes 原生安全防护。
- 增强保护。
- 消除盲点，并为工作人员提供对关键漏洞和威胁途径的洞见。
- 缩短时间和降低成本。
- 利用 Kubernetes 提供的丰富情境，减少实施安全防护所需的时间和精力，并简化安全分析、调查和修复程序。
- 改进可扩展性和可移植性。
- 提供 Kubernetes 原生可扩展性和复原能力，避免带外安全控制导致的运维冲突和复杂性。

红帽官方微博　红帽官方微信

Red Hat
Advanced Cluster Security
for Kubernetes

优势详解

领域	优势
可视性	▸ 提供部署的完整视图，包括镜像、容器集和配置 ▸ 发现并显示在所有集群跨度的命名空间、部署和容器集中的网络流量 ▸ 收集每个容器中的关键系统级事件
漏洞管理	▸ 根据特定的语言、软件包、镜像层，扫描镜像中的已知漏洞 ▸ 将漏洞与运行中的部署关联，而不仅仅是镜像 ▸ 根据漏洞细节强制执行策略：在构建时使用持续集成/连续交付 (CI/CD) 集成，在部署时使用动态许可控制，在运行时使用原生 Kubernetes 控制
合规	▸ 评估 CIS 基准、支付卡行业 (PCI)、健康保险携带与责任法案 (HIPAA) 以及 NIST SP 800-190 的数百种控制的合规性 ▸ 提供每个标准控制的整体合规性仪表板概览，并支持导出证据，满足审计员的需求 ▸ 提供合规详细信息视图，确定不符合特定标准和控制的集群、节点或命名空间
网络分段	▸ 可视化命名空间、部署和容器集之间的允许流量与活动流量，包括外部风险 ▸ 在实施前模拟网络策略变化，以最大限度减少对环境的运维风险 ▸ 基线网络活动，建议全新的 Kubernetes 网络策略，消除不必要的网络连接 ▸ 利用 Kubernetes 内置的网络执行功能，确保一致、可移植和可扩展的分段
风险预测	▸ 根据安全风险对正在运行的部署排序，充分利用 Kubernetes 数据，利用配置或部署细节以及运行时活动对漏洞进行优先排序 ▸ 跟踪 Kubernetes 部署安全态势的改进情况，验证安全团队操作的影响
配置管理	▸ 提供预建的 DevOps 和安全策略，识别与网络风险、特权容器、以根用户身份运行的进程相关的配置违规，并确保符合行业标准 ▸ 分析 Kubernetes 基于角色的访问控制 (RBAC) 设置，确定用户或服务帐户的特权和错误配置 ▸ 跟踪机密信息，并检测哪些部署使用机密信息限制访问 ▸ 强制执行配置策略，在构建时使用 CI/CD 集成，并在部署时使用动态许可控制

领域	优势
运行时检测和响应	▸ 监控容器内的系统级事件，检测显示威胁的异常活动，并使用 Kubernetes 原生控制进行自动响应 ▸ 基线容器中的流程活动，自动将流程列入白名单，无需手动加入白名单 ▸ 使用预构建的策略，检测加密开采、权限升级和各种漏洞 ▸ 使用外部 Berkeley Packet Finder (eBPF) 或每个主要 Linux 发行版的内核模块，实现灵活的系统级数据收集
集成	▸ 提供丰富的应用程序接口 (API) 和预建插件，集成 DevOps 系统，包括 CI/CD工具、镜像扫描程序、注册表、容器运行时间、安全集成事件管理 (SIEM) 解决方案和通知工具

关于红帽

红帽是世界领先的企业开源软件解决方案供应商，依托强大的社区支持，为客户提供稳定可靠而且高性能的 Linux、混合云、容器和 Kubernetes 技术。红帽帮助客户集成现有和新的 IT 应用，开发云原生应用，在业界领先的操作系统上开展标准化作业，并实现复杂环境的自动化、安全防护和管理。凭借一流的支持、培训和咨询服务，红帽成为《财富》500 强公司备受信赖的顾问。作为众多云提供商、系统集成商、应用供应商、客户和开源社区的战略合作伙伴，红帽致力于帮助企业做好准备，拥抱数字化未来。

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
#F27185_0221