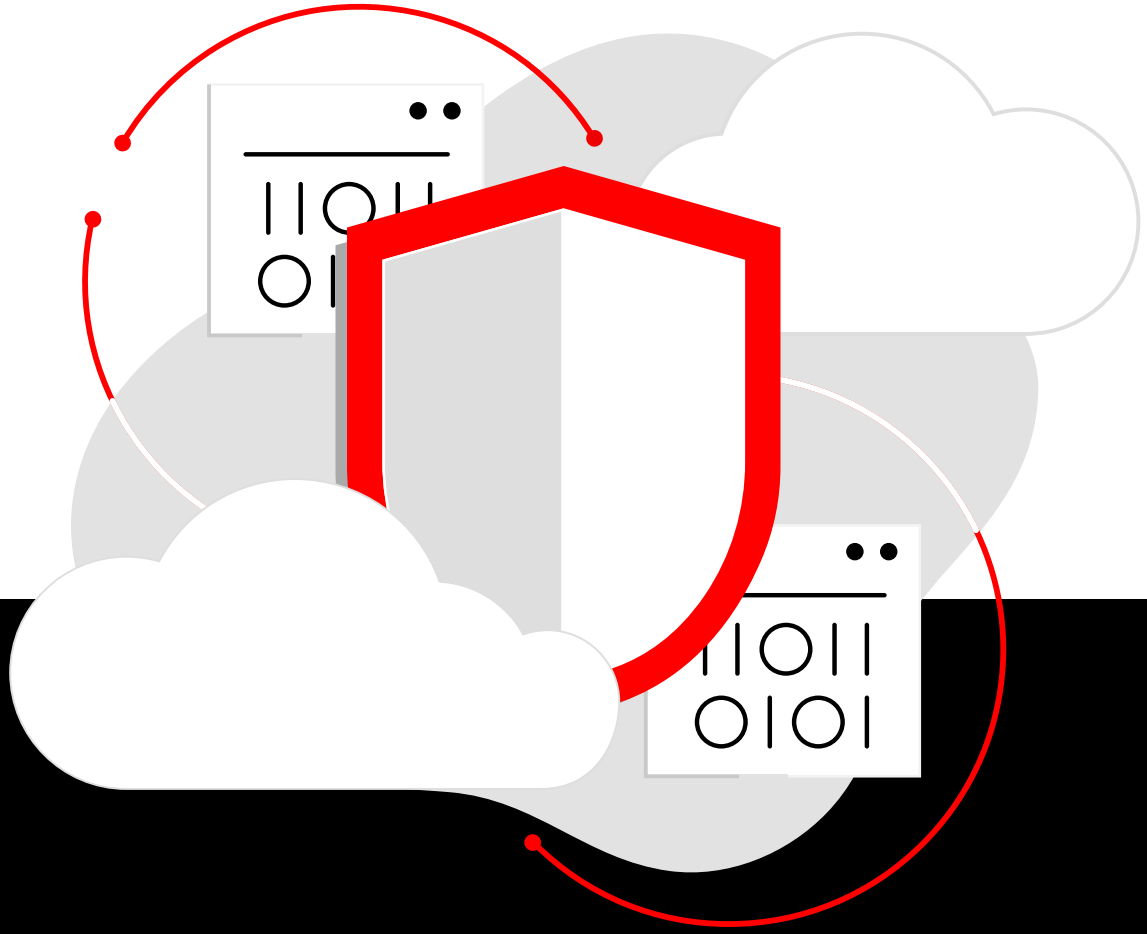
Red Hat



践行 DevSecOps，实现应用生命周期的现代化和安全保障

目录

第 1 页
应用安全在数字世界中至关重要

第 3 页
红帽的 DevSecOps 策略

第 4 页
使用红帽产品构建开放的 DevSecOps 基础

第 5 页
利用经过认证的安全合作伙伴生态系统获得灵活性和可靠性

第 6 页
创建完整的 DevSecOps 解决方案

第 7 页
选择符合需求的安全方法和产品

第 8 页
合作伙伴亮点：
Sysdig

第 9 页
合作伙伴亮点：
Synopsys

第 10 页
合作伙伴亮点：
Palo Alto Networks

第 11 页
合作伙伴亮点：
CyberArk

第 12 页
合作伙伴亮点：
Tigera

第 13 页
合作伙伴亮点：
Aqua Security

第 14 页
准备开启您的 DevSecOps 之旅？

简介

应用安全在数字世界中至关重要

目前越来越多的组织采用云、容器和微服务技术在数字世界中竞争，但安全仍然是首要关注的问题。事实上，50% 的企业高级 IT 主管将网络安全列为技术计划的三大优先事项[1]。与此同时，86% 的主管预计在 2021 年，他们组织的数字转型速度将会加快[1]。

这些新技术需要采用不同的安全方法，因为基于边界的传统方法在分布式环境中不起作用。此外，DevOps 和云原生方法帮助提高了开发速度和部署灵活性，因此在整个过程中应尽早考虑安全性。仅在开发周期结束时应用安全措施往往会导致交付延迟和保护等级降低。

采用 **DevSecOps** 方法和实践可以帮助您更好地保护您的应用环境和业务。

什么是 DevSecOps?

DevSecOps 是对 DevOps 协作文化的进一步扩展，旨在整个应用周期内集成安全性。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的责任，而不是由一个团队负责，在开发和部署流程结束时完成的一系列任务。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。

DevSecOps 的优势

提高安全性，降低风险。

在开发期间，而不是在生产时解决安全问题，以更好地保护您的应用，减少由于未能遵守政策而导致延迟或停止的部署次数。

更快解决安全问题。

应用现代安全实践和工具，鼓励展开协作，并集成自动化来加快版本发布周期，减少在生产期间修复安全问题所需的时间，并节省时间和资金。

提高合规性和可见度。

采用自动化流程和工具，降低人为错误的风险，提高可预测性和可重复性，以提升合规性并简化审核过程。

1 Flexera：“2021 技术支出状况报告”，2021 年 1 月。

DevSecOps 实施中的挑战

虽然 DevSecOps 方法具有很多优势，但多个因素会增加实施 DevSecOps 的难度。

- **安全格局不断变化。** 安全威胁和法规——包括业务、技术和地理要求，不断快速改变，使其难以跟上改变的步伐。
- **应用环境的复杂性。** 容器、微服务和云服务等共同构成复杂的大规模应用环境，而要理解所有这些不同技术之间的连接和安全含义颇具挑战性。
- **现有工具和流程效率低下。** 许多团队 开始时采用他们现有的工具和流程来执行 DevSecOps 计划，但后来发现随着时间发展，这种方法无法支持他们实现目标。
- **多种安全工具。** 为组织选择、测试和集成合适的安全工具且保持这种选择需要耗费许多时间，且需要不断的研究和努力。

成功实施 DevSecOps 要依赖文化、流程和技术

利用 DevSecOps 保护应用需要从三个领域做出调整和改变：文化、流程和技术。

文化

推动开发、运维和安全团队展开协作，为共同的目标努力。帮助每个团队了解在应用生命周期中构建安全性的原因和方法。

流程

标准化、记录和自动化流程和工作流，以提高整个应用生命周期的效率和安全性。

技术

将您用于应用开发、部署和运维的平台、工具和流程集成到单一内聚型系统中。

了解更多关于 DevSecOps 的基础知识

阅读**“为何您的 DevSecOps 实践会后继乏力” 博客文章**，详细了解为了成功实施 DevSecOps 需要做出的改变。阅读**“提高混合云安全性”电子书**，了解如何利用云原生安全方法来保护您的业务。

红帽的 DevSecOps 策略

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。这种组合让您能够实施综合性的 DevSecOps 解决方案，以提高应用的安全性，降低风险，提高性能，并使您的投资价值最大化。

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 解决方案提供了不错的基础。我们的合作伙伴通过创新、集成的产品扩展并增强这一基础，以在整个应用周期中实现安全性和自动化。最后，我们提供**培训和认证课程**、**交互实验室**、**咨询**和**托管服务**，帮助您成功实施 DevSecOps。

无论您处在 DevSecOps 之旅的什么阶段，我们都能为您服务。通过我们模块化、可扩展的解决方案和专家服务，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。

使用红帽产品构建开放的 DevSecOps 基础

Red Hat OpenShift

红帽 OpenShift® 是一款注重安全性的企业级混合云平台，包含多种内置 DevOps 工具和安全功能（默认启用）。该平台与合作伙伴和第三方安全工具和技术配合使用，以提高安全性和实现强大的 DevSecOps。阅读**红帽 OpenShift 安全指南**，了解如何在整个技术堆栈中解决安全问题。

免费试用

主要安全功能

- 安全增强型 Linux（SELinux）
- 安全环境限制（SCC）
- 身份和访问权限管理
- 数据加密
- 联邦信息处理标准（FIPS）模式

Red Hat Ansible Automation Platform

红帽 Ansible® 自动化平台是一个灵活、强大的平台，可以自动化和集成安全解决方案，并提供安全工具通用的语言。了解**自动化用例**。

Red Hat Enterprise Linux CoreOS

红帽企业 Linux® CoreOS 是一款轻量级、不可变的容器优化型操作系统，以注重安全性的红帽企业 Linux 为基础，在红帽 OpenShift 内使用。

Red Hat Quay

红帽 Quay 是一款分布式、高度可用的容器镜像仓库，可支持您构建、分布和部署容器。

Red Hat CodeReady Workspaces

红帽 CodeReady Workspaces 是一款工具，让开发人员能够在红帽 OpenShift 上运行的容器中编码、构建和测试。

Red Hat Advanced Cluster Security for Kubernetes

红帽 Kubernetes 高级集群安全防护提供保护容器安全的云原生架构，以在从构建到运行的过程中保护应用。

Red Hat Advanced Cluster Management for Kubernetes

红帽 Kubernetes 高级集群管理使用内置安全策略从单个控制台控制集群和应用。

利用经过认证的安全合作伙伴生态系统获得灵活性和可靠性

没有任何一家供应商能够提供全面实施高效的 DevSecOps 所需的所有功能。此外，每个组织都是不同的，需要采用独一无二的产品和技术组合来满足他们的需求。

红帽与**创新的、行业领先的安全合作伙伴合作**，提供基于经过认证的集成、容器镜像和**红帽 OpenShift Operator 的完整解决方案**。您始终可以选择最符合您需求的合作伙伴、产品和技术，且知道它们将可靠、稳定地彼此配合。我们还提供专家服务、支持和培训来支持这些解决方案，以帮助您成功实施 DevSecOps 文化、流程和工具。

红帽安全作伙伴生态系统的优势

选择

始终选择最符合组织需求的产品和供应商。

认证

构建您的解决方案，深知所有组件都已通过认证，彼此能够可靠配合使用。

专业实力

组合利用红帽和合作伙伴的 DevSecOps 专业实力和经验。

服务

寻求帮助，在您的组织中实施 DevSecOps 文化、流程和工具。

培训

学习最佳实践，获取采用 DevSecOps 方法所需的技能。

红帽漏洞扫描程序认证

红帽漏洞扫描程序认证最大程度降低漏洞扫描程序结果之间的差异。红帽与经过认证的安全合作伙伴合作，针对红帽发布的镜像和软件包提供更准确可靠的容器漏洞扫描结果。

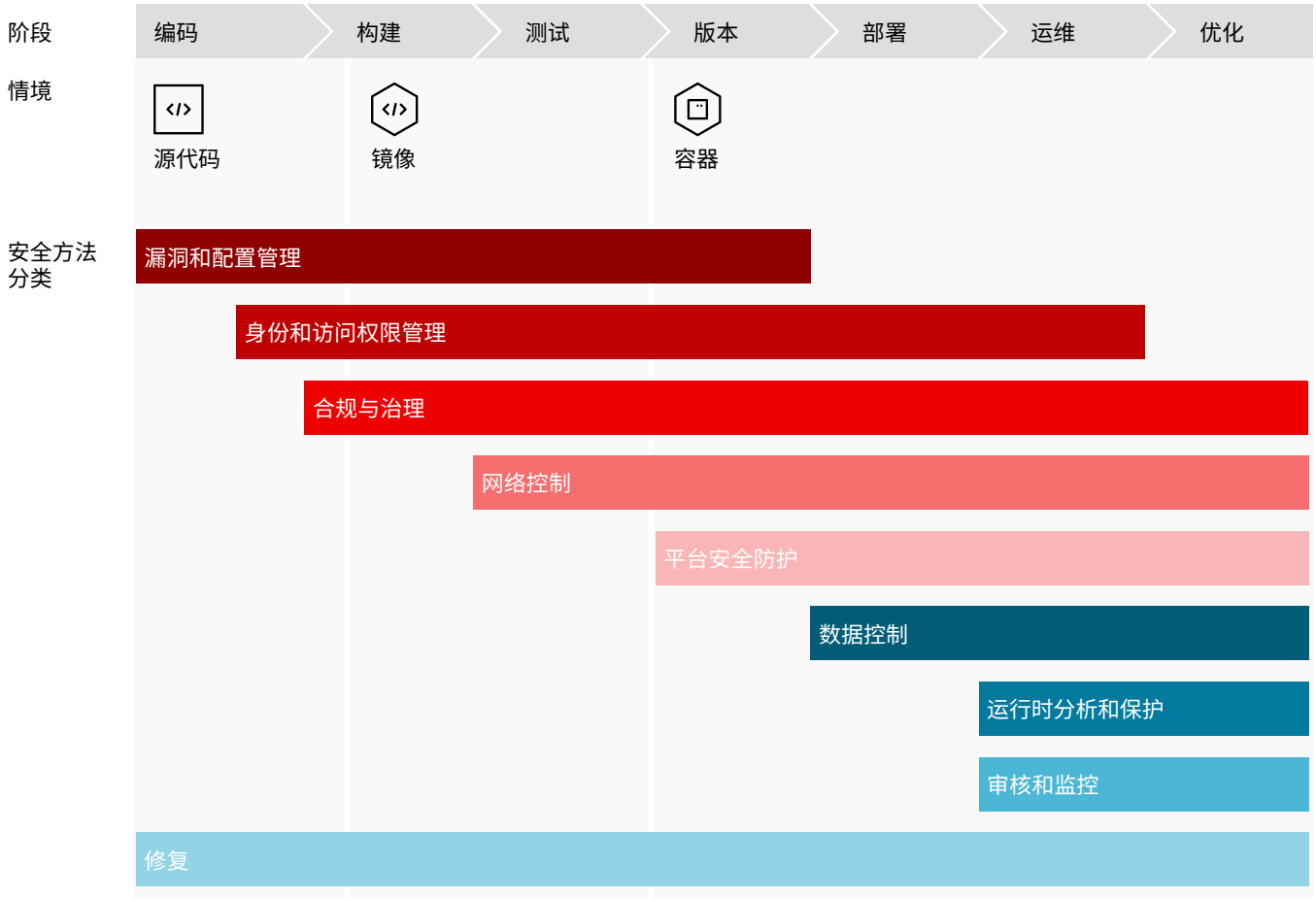
- 最大程度减少误报和其他差异。
- 为战略项目和计划腾出时间和预算。
- 实现更高的保证等级。
- 利用针对红帽发布的镜像的集中化数据，提高准确性。
- 简化漏洞管理。

查找经过认证的产品

创建完整的 DevSecOps 解决方案

红帽提供用于构建高度可扩展、综合性的 DevSecOps 解决方案的框架，这些解决方案可以满足整个应用生命期间对安全的要求。该框架是我们与我们的安全合作伙伴共同构建的，可以帮助您根据当前和预期需求在您的组织中实施 DevSecOps。

红帽 DevSecOps 框架将一整套按功能分类的安全工具和方法部署到整个应用开发生命周期。



阅读技术概述

选择符合需求的安全方法和产品

红帽 DevSecOps 框架将 34 个主要的安全方法划分为 9 类。红帽和经过认证的合作伙伴技术采用其中一种或多种方法来帮助您构建完整的 DevSecOps 解决方案，以满足您组织的需求，并适应未来的变化。

漏洞和配置管理

- 静态应用安全测试（SAST）
- 静态代码分析（SCA）
- 互动应用安全测试（IAST）
- 动态应用安全测试（DAST）
- 配置管理
- 镜像风险

身份和访问权限管理

- 身份验证
- 授权
- 秘密库
- 硬件安全模块（HSM）
- 出处

合规与治理

- 法规合规审核
- 合规控制和修复

网络控制

- 容器网络接口（CNI）插件
- 网络策略
- 流量控制
- 服务网格
- 虚拟化
- 软件包分析
- 应用编程接口（API）管理

平台安全

- 安全主机
- 容器平台
- 命名空间
- 隔离
- Kubernetes 和容器强化

数据控制

- 数据保护和加密

运行时分析和保护

- 许可控制器
- 应用行为分析
- 威胁防范

审核和监控

- 集群监控
- 安全信息和事件管理（SIEM）
- 取证

修复

- 安全编排、自动化和响应（SOAR）平台
- 自动分辨率

查找经过认证的合作伙伴

合作伙伴亮点

Sysdig

Sysdig 帮助组织采用以安全为重的 DevOps 技术，在云中可靠运行工作负载。Sysdig 用于监测和保护应用、工作负载和容器的产品帮助数百家公司更快交付云原生应用。

红帽和 Sysdig 携手合作，帮助企业快速采用云原生方法。 **Sysdig Secure DevOps 平台**、**Sysdig Secure** 和 **Sysdig Monitor** 与红帽 OpenShift 和**红帽 Kubernetes 高级集群管理**配合使用，为私有、混合和多云环境提供统一的安全、合规和监测。这些解决方案有助于确保构建管道的安全、检测和响应威胁、持续验证云态势和合规性，以及监控性能。基于开源堆栈构建，Sysdig 的云原生监测、安全防护和取证功能为您提供迁移至云所需的见解和控制，并帮助降低风险。

红帽和 Sysdig 解决方案帮助您：

- 直接在您的持续集成/持续部署（CI/CD）管道中扫描图像。
- 监测云级性能和可用性。
- 实现持续合规和运行时安全。
- 验证红帽 OpenShift 基础架构配置。
- 更轻松地排除故障和解决问题。

2020

红帽荣获公共部门年度星级合作伙伴称号[2]

管理安全风险。

识别和解决整个管道中的漏洞。利用自动化策略和控制，在运行时检测和阻止威胁。应对和调查事故，即使是在容器停用之后。

提高性能和可用性。

调查和保留数百万个指标。监测整个环境的运行状况和性能，以主动发现和解决问题。更轻松地排除集群、容器集和容器内的问题。

验证云的合规性。

按通用标准验证红帽 OpenShift 环境的合规性。通过详细的活动报告审核集群、节点和容器。在整个容器的生命周期实施文件完整性监测。

访问集成

*2 红帽博客：“**红帽表彰致力于实现开源创新的北美合作伙伴**”，2020 年 4 月 23 日。*

合作伙伴亮点

Synopsys

Synopsys 提供静态、软件组成和动态分析解决方案，以快速构建安全软件。Synopsys 结合行业领先的工具、服务和专业知识，帮助组织采用 DevSecOps 在整个软件开发生命周期优化安全性和质量。

红帽和 Synopsys 帮助您创建高质量、以安全为重的代码，以最大程度降低风险，同时尽可能提高速度和生产力。**Synopsys Black Duck 软件组成分析（SCA）**与红帽 OpenShift 集成， 以提高对容器的开源代码中的安全漏洞和策略违规的了解和控制。**Black Duck for OpenShift** 自动发现、扫描、监测和检查红帽 OpenShift 集群中的所有容器镜像，以识别容器构建的各个阶段中的开源安全和合规风险。该软件还可以帮助您确保不会急于将包含漏洞的容器投入生产，并快速解决会影响容器运行的新漏洞。

Black Duck for OpenShift 解决方案：

- 在每个容器镜像中提供所有第三方开源代码的完整列表，并用漏洞和策略元数据注释容器集。
- 在出现影响容器运行的新漏洞时立即提醒您，并识别哪些镜像和容器受到影响。
- 了解开源分叉和后端端口，并在适当的时候将漏洞标记为补丁，减少需要调查的漏洞数量。
- 与红帽 Kubernetes 高级集群管理**集成**，确保跨所有集群实现一致部署。

自动扫描容器镜像

持续监测开源代码

识别安全漏洞

“对于安全应用开发和部署的未来，Synopsys 和红帽拥有相似的愿景，双方携手合作，希望能帮助组织建立对其容器化应用的信任。”

Vatsal Sonecha
Synopsys 业务发展副总裁

访问集成

合作伙伴亮点

Palo Alto Networks

Palo Alto Networks 提供创新，以支持安全数字转型，即使变化的步伐加快也能从容应对。该公司提供一系列安全解决方案，帮助全球超过 60,000 名客户保障他们的业务。

红帽和 Palo Alto Networks 帮助您在整个开发生命周期中，利用云原生安全性和合规性来保护您的环境。 Palo Alto Networks 提供的 Prisma 云与红帽 OpenShift 配合，为您的部署提供综合云安全态势管理（CSPM）和云工作负载保护（CWP）。此解决方案为主机、容器和无服务器提供完整的生命周期安全性，以及对安全态势管理的可见性。

与红帽的合作始于

2017 年

关键功能和优势

漏洞管理

在应用生命周期的每个阶段，从开发到生产，嵌入安全性，并进行漏洞检测、理解和预防。

合规

轻松实现和维护互联网安全中心（CIS）基准、外部合规机制和自定义需求的合规性。

CI/CD 安全性

将安全性直接集成到持续集成（CI）流程中，以便在部署到生产环境之前及时发现并修复问题。

运行时防护

通过机器学习，为所有应用版本自动创建特权最少、基于允许列表的运行时模型，大规模应用安全性。

Web 应用和接口安全

保护公共和私有云环境免受第 7 层和开源 Web 应用安全项目（OWASP）10 大威胁。

访问控制

在与现有的身份、访问和秘密管理工具集成的同时，为工作负载和应用建立和监测访问控制。

访问集成

合作伙伴亮点

Cyberark

CyberArk 采用独特的安全优先方法来实施身份优先访问控制。该公司提供完整的解决方案，以跨企业、云和 DevOps 环境保护人员、应用、脚本和机器使用的密钥和凭据。

红帽和 CyberArk 携手合作，帮助您提升容器环境和自动化脚本的安全性。 企业级特权访问安全策略提供可见性、审核、实施和密钥管理，以降低业务风险。CyberArk DevSecOps 产品（包括 **Conjur 密钥管理器**和**凭据提供程序**）与红帽 OpenShift 和红帽 Ansible 自动化平台集成，为使用集中化平台的人员、应用、脚本和其他非人类身份保护、轮转、监测和管理特权凭据。通过组织中的单一控制点，您可以统一安全管理、减少安全漏洞、最小化攻击面并简化运维。

模块化架构允许您独立部署每个组件，以跨混合云、多云、容器化和 DevOps 环境自定义保护。强大的运行时身份验证和基于角色的访问控制确保只有授权的容器集和容器才能接收密钥。与红帽 Ansible 自动化平台集成，使得 playbook 能够访问托管密钥，并消除手动密钥输入和轮转需求。此集成还允许您自动执行修复任务，以应对检测到的安全事件。

统一安全性

根据您的策略，在基础设施中集中管理和保护密钥和特权访问凭据。

简化运维

允许开发人员和自动化工程师根据您的策略保护、管理和轮换他们使用的密钥和凭据。

提高一致性

始终保护访问管理控制台的应用、脚本和人员所使用的密钥和凭据。

观看网络研讨会

合作伙伴亮点

Tigera

Tigera 改变了公司保护、调查和排除 Kubernetes 网络和微服务通信故障的方式。

红帽和 Tigera 通过监测、分析和管理网络流量，帮助组织在 Kubernetes 环境中集成安全性。Tigera Calico Enterprise 通过红帽 OpenShift 验证，帮助您成功跨云环境运行、优化和保护关键的容器化应用。Kubernetes 原生架构将解决方案嵌入到您的应用环境中，以提供详细的安全控制，并提高网络和微服务层之间的可见性。此解决方案还与您现有的安全工具、环境和安全防护运维中心（SOC）集成，为现代工作负载提供额外的控制和功能。通过零信任网络、出口访问控制、流量可见性、威胁保护和防御，以及自动化合规性审查报告，跨开发、测试和生产环境提升应用安全性。

扩展您的安全防护功能

通过现有的防火墙、最低特权安全性和容器集间的流量加密来保护应用。

获取网络可见性

访问网络流，以调试连接、搜寻威胁和自动执行合规性报告。

确保合规性

监测应用的合规性，对于不合规的工作负载，提供实时提醒。

访问 operator

合作伙伴亮点

Aqua Security

Aqua Security 帮助客户创新，尽可能确保客户业务流畅运行。该公司在整个应用生命周期内提供威胁防护、监测和响应自动化，从环境的各个方面提高安全性。

红帽和 Aqua Security 帮助您在现场、混合和云基础设施中更安全地管理和扩展云原生工作负载。Aqua 云原生安全平台与红帽 OpenShift 集成，提供基于风险的漏洞管理、详细的运行时保护，以及综合性的基础设施保障和合规。该解决方案让开发、安全防护和运维团队能够更安全地交付应用，在运行时抵御威胁，并基于策略检查评估和修复基础设施配置。

关键功能和优势

支持 DevSecOps 方法

- 大规模分析红帽 OpenShift 注册表镜像的代码、配置和许可。
- 按风险确定漏洞处理的优先级。
- 通过与 CI/CD 管道集成，自动执行构建流程。

在运行时保护应用

- 在不中断应用的情况下，检测并自动消除未经授权的容器活动。
- 通过识别和阻止对标准镜像的未经授权的更改，强制保持容器的不可变性。

提高软件供应链的安全性

- 在受保护的预生产测试环境中运行和验证镜像。
- 识别静态扫描程序无法在部署前检测出来的高级恶意软件。

保持基础设施的合规性

- 扫描和验证数以百计的配置和控制策略，以符合最佳实践和互联网安全中心（CIS）基准。
- 通过基于开源策略代理（OPA）的声明性保障策略，执行基于角色的访问控制（RBAC）。

访问集成

准备开启您的 DevSecOps 之旅?

应用安全是数字业务必须满足的一项要求。采用 DevSecOps 方法可以帮助您更好地保护您的应用环境和业务。

红帽结合创新的技术基础、综合性的 DevSecOps 生态系统和深厚的专业知识，帮助您成功在整个组织内实施 DevSecOps。

- 从各种通过认证、行业领先的工具和技术中选择符合您的当前和未来需求的工具和技术。
- 通过专家培训资源，学习最佳实践，获取 DevSecOps 技能。
- 借助专业服务和咨询，加快部署速度。

关于利用红帽实施 DevSecOps 的更多信息，请访问：
redhat.com/zh/partners/devsecops

F29623_0721_KVM

Red Hat