红帽面向金融服务的安全性和合规性自动化

“各团队不但加快了自己的行动速度，还能更加高效地在整个公司范围展开合作，并投入更多时间进行创新。这方面的努力帮助我们兑现了承诺：为客户做正确的事。” [1]

James Hixon
高级总监，
云自动化与工程，
Ally Financial

简介

随着数字采用率的增加，相关基础架构也越来越复杂。尤其是金融服务行业，该行业历来厌恶风险，抗拒变革，受到技术和监管两方面的约束。金融服务公司需要自动化功能，用于部署应用，确保分布式架构一致且符合所需的安全要求。在采用 Windows 和 Linux® 操作系统、虚拟基础架构、公共云和私有云基础架构以及容器的环境中，很难管理不一致的补丁和配置。

随着这种混合环境的发展，风险也随着可见性和控制力的降低而增加，从而使手动安全性与合规性监控变得越来越困难。此外，开发、运维和安全团队之间的关系通常也很紧张，安全人员通常是最后知道配置更改和问题的人。

发现漏洞时，需要花时间来解决问题和自动修复，而遗留下来的问题会给组织带来麻烦。发现的漏洞也是一个挑战。最终应用修复程序时，组织需要详尽编写关于修复内容、修复时间和修复人员的文档。银行、支付提供商、保险公司以及其他金融服务公司也必须遵循安全标准，如支付卡行业数据安全标准（PCI DSS）和通用数据保护条例（GDPR），这些标准需要严格的跟踪、报告和文档说明以保持合规性。

通过自动化解决安全性与合规性问题

为解决安全性与合规性问题，金融服务提供商应专注于跨整个环境的数据驱动型 IT 和网络流程自动化。这一自动化包括：

- 操作系统（OS）
  - 软件包管理
  - 补丁管理
  - 操作系统在置备时将安全性强化到安全合规基准，以确保一致性和操作系统不变性
- 基础架构和安全即代码
  - 重复、共享和验证能力——并协助进行安全与合规审计
  - 组织中的每个人都可使用同一种脚本/编程语言，使其易于使用

红帽官方微博　红帽官方微信

1 *红帽成功案例。“Ally Financial 借助云平台和开发运维加速产品上市，”2019 年 5 月。*

- 系统置备
  - 与 IT 服务管理集成（ITSM）
  - 存储置备
- 工作流
  - 简化服务管理
- 通过 Day 2 security operations 实现持续的安全与监控
  - 补丁管理
  - 漏洞识别与管理（例如，健康检查）
  - 安全性的前瞻性治理、控制和合规性策略
  - 补救：修复生成与自动化

安全性与合规性自动化挑战

手动检查系统的安全性与合规性存在问题，原因有多个：

- 耗时且乏味
- 容易出现人为错误
- 操作不当和简单的配置更改缺少审计追踪信息
- 不可重复、不可共享或不可验证
- 由于更新日志信息不完整、不一致，很难通过审计
- 运维团队和安全团队之间沟通无效或没有沟通

金融产品和服务公司必须确定执行手动任务的地方、执行频率和自动化策略。应该专注于灵活的自动化技术以适应未来需求的变化。要在网络设备和服务上进行快速实施和扩展，选择合适的自动化技术至关重要。

红帽智能安全自动化

从加强安全的操作系统到自动化软件再到数十个供应商（AWS、Cisco、Juniper、VMware 等）的集成，红帽® 技术提供了端到端软件堆栈以支持自动化策略，可同时满足 IT 和网络自动化的需求。

无需红帽技术的整个堆栈，但将红帽产品结合使用时，安全性与合规性自动化的功能得到了增强。对于安全性与合规性自动化，将红帽企业 Linux、红帽 Ansible® 自动化平台、红帽卫星和红帽智能分析相结合后的功能尤其强大。

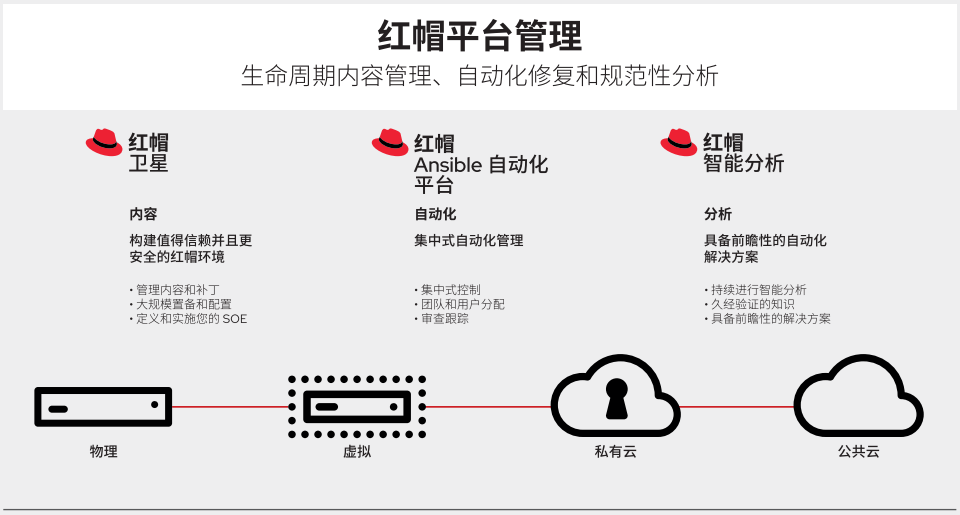


图 1. 结合使用红帽技术增强安全性与合规性

将这些红帽技术配合使用，可获得额外的安全性与合规性优势：

红帽企业 Linux

红帽企业 Linux 提供安全技术以抵抗漏洞、保护数据和满足法规要求。可利用经国家标准与技术研究所（NIST）认证的红帽扫描仪 OpenSCAP，在系统和容器内自动执行合规性和安全配置修复。该扫描仪的作用在于检查和修复漏洞和配置安全基线，包括：

- PCI DSS。
- 国防信息系统局（DISA）安全技术实施指南（STIG）。
- 刑事司法信息服务（CJIS）安全策略。
- 商业云服务（C2S）。
- 健康保险可携性与责任法案（HIPAA）。
- NIST 800-171。
- 操作系统保护配置文件（OSPP）v4.2。
- 红帽公司认证云提供商简介。

为了更好地满足混合计算的各种安全需求，红帽企业 Linux 提供增强的软件安全信息，通过将 OpenSCAP 与红帽 Ansible 自动化 平台集成，缓解风险。该集成支持应用预生成的红帽和支持的 Ansible Playbook 来修复系统以符合安全基线，从特定安全配置文件创建新的 Ansible Playbook，以及直接通过 OpenSCAP 扫描创建 Ansible Playbook。这些可用于在混合 IT 环境中更快速一致地实施补救。

红帽企业 Linux 系统角色也有助于实现自动化安全，利用一系列提供稳定一致配置接口的 Ansible 角色和模块来远程管理红帽企业 Linux 6.10 及更高版本。例如，安全增强型 Linux（SELinux）系统角色可用于跨红帽企业 Linux 系统正确一致地配置 SELinux。

通过实现常见管理任务自动化，更少的用户需要对主机的直接超级用户访问权限，从而减少了攻击面。通过使用 SELinux，可向自动化管理任务分配特定于该任务的特权，从而防止特权升级错误。

红帽 Ansible 自动化平台

红帽 Ansible 自动化平台包括红帽 Ansible Tower，是跨组织提供通用自动化平台的简单、强大、 无代理 IT 自动化技术，具有以下安全和合规优势：

- 可追溯性和可重复性，以确保合规
- 大幅减少花在重复任务上的时间
- 通过一致的基础架构管理方法，减少停机风险
- 通过自动化分析、检测和问题解决，将系统错误的风险降至最低
- 通过加快运用技术，加速上市时间
- 降低人为错误的风险
- 加速 IT 过程（通常从几天缩短为几分钟）
- 跨多供应商环境实现一致配置和管理
- 自动化部署、配置和配置生命周期管理，包括策略实施以及跨整个网络更新系统和防火墙
- 使用服务目录中的配置信息快速复制现场问题
- 能够使用表征状态转移应用编程接口（RESTful API）将 Ansible 自动化平台嵌入到现有安全工具和流程中
- 涵盖访问控制、凭证保管库、作业和工作流调度、源控制集成和图形化库存管理审计的高度可扩展自动化解决方案，可简化所有组件的表征并提供对所有自动化活动的可见性

Ansible 自动化平台包括专为与安全供应商和安全解决方案集成而创建的模块和角色，例如 Splunk（SIEM）、Snort（入侵检测和预防）和 Checkpoint（企业防火墙）。

红帽卫星

红帽卫星为 IT 部门提供有关环境中的红帽系统的信息，包括识别已过期和有已知漏洞的系统。组织使用红帽卫星进行订阅和内容管理、置备符合安全性的主机、配置管理和补丁管理。Ansible 自动化平台与红帽卫星配合使用，可自动部署和管理软件配置，在系统和应用的整个生命周期内对其进行端到端、自动化管理和控制，从而帮助维护安全性、合规性和审计跟踪。

红帽卫星：

- 定义并实施标准操作环境（SOE）。
- 使用 Ansible 自动化平台部署红帽企业 Linux 系统角色并为 SOE 安装红帽智能分析。
- 识别 SOE 偏移并使用 Ansible 自动化平台修复偏移问题。
- 通过智能分析识别安全性、性能、稳定性和可用性风险，然后动态生成 Ansible Playbook，直接从卫星执行进行风险修复。
- 通过卫星置备的系统可对 Ansible Tower 进行回调，对 playbook 进行置备后执行。
- 使用 Ansible 自动化平台导入并使用红帽企业 Linux 系统角色。
- 通过动态库存，Ansible Tower 使用卫星作为动态库存源。
- 可使用 Ansible 自动化平台从卫星内部署智能分析。

红帽智能分析

红帽智能分析随红帽卫星一起提供，也可单独作为红帽企业 Linux 附加组件。智能分析结果提供可行预测分析，与 Ansible Tower 集成时，智能分析可配置为自动生成 playbook 并执行修复 。Ansible Tower 使用智能分析 API 支持站点范围修复作业。智能分析检测和修复功能可集成到外部系统或脚本中，使运维团队能够将引导式修复扩展到整个企业。

Ansible Tower 可配置为连接到智能分析 API，从中检索信息。例如，Ansible Tower 可拉取红帽智能分析的客户门户版本中使用的 Ansible Playbook，这些 playbook 可直接从 Ansible Tower 启动，用于自动修复问题。

图 2. 红帽安全性和合规性自动化。

用例：自动化补丁管理

将红帽卫星、红帽智能分析和红帽 Ansible 自动化平台结合使用，可无缝检测红帽卫星管理的主机的风险，并使用红帽 Ansible 自动化平台 Playbook 修复发现的许多问题。可以创建可重复的修复计划，按计划行事，并向审计员提供报告信息。智能分析可配置为控制发送给卫星的信息类型，从而允许您查看传输的数据并进行管理。

1. 使用智能分析识别需要补丁的系统。
2. 为您要运行的 playbook 和在上面运行 playbook 的系统创建智能分析计划。
3. 安排执行智能分析计划或手动运行。
4. 按智能分析计划提供的信息采取行动。智能分析学习增加的每一条智能和数据，并变得更加智能。可以自动发现相关智能分析，主动推荐定制的后续行动，甚至实现任务自动化。
5. 提供通过执行智能分析计划而生成的整合审计跟踪信息，包括计划执行者、计划开始和结束时间，以及任务级别的执行情况。

综述

随着金融网络朝着可编程性方向发展，应用变得日益复杂，自动化对于管理 IT 和网络环境至关重要。红帽自动化和合规性解决方案可解决金融服务提供商所面对的、与 IT 和网络端到端自动化有关的问题。

无论是支持红帽卫星置备和配置符合安全性的系统，使用红帽智能分析数据主动解决安全问题，还是使用简单自动化部署、管理和升级云，红帽 Ansible 自动化平台都可以提供具有端到端自动化所需的公开 API 的通用自动化语言和操作层。对于具有整体安全性的设备特定和应用特定需求的组织，这种方法尤其适用。红帽 Ansible 自动化平台为整个红帽企业 Linux 环境提供自动化，包括发现环境信息，遵循组织策略，以及根据该策略制定配置更改。

所有红帽产品都与供应商无关，并可支持您的 IT 环境，无需替换关键的旧应用和流程，从而跨设备、平台和供应商提供安全任务和流程的集成与编排。内部资源可专注于创新，由红帽支持您的关键安全自动化，并简化服务管理。

后续步骤

- 为启动或扩展安全性和合规性自动化，红帽业务探讨分析您的环境是否能够自动化。红帽服务还提供更全面的安全性和可靠性工作流自动化产品，将红帽智能分析、红帽卫星和红帽 Ansible Tower 结合，确定现有差距或智能分析所识别可能有问题的配置。该产品提供一个可扩展框架，在该框架上，可使用和自定义智能分析提供的 playbook，还可使用和部署客户 playbook 以修复漏洞，以及在 IT 环境中提供审计跟踪。

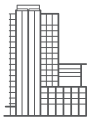
- 参加金融机构安全性与合规性网络研讨会，详细了解红帽安全管理技术如何能够帮助降低金融组织中的基础架构风险。

了解红帽解决方案详情

红帽卫星、红帽智能分析和红帽 Ansible 自动化平台跨红帽产品组合提供额外安全管理和控制，例如红帽 OpenShift® 客户端。

其他红帽技术提供专门解决主要安全与合规问题的功能。红帽认识到在当今瞬息万变的环境中，需要端到端安全性、合规性和审计编排，并提供管理和控制所需的平台和工具。

如有疑问或需要其他信息，请联系红帽代表或阅读有关金融服务自动化的更多信息。



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。

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
#F23392_0420