增强混合

云安全性

利用基本的云原生安全注意事项来保护您的业务

/选择开放，自在成长

Red Hat

作者：Lucy Huh Kerner，红帽安全部门全球战略与宣传总监

目录

第 1 章

部署安全至上的混合云

云采用的应用和普及规模不断扩大。如今，65% 的组织表示他们是高度依赖云技术的用户，72% 的企业拥有混合云战略。[1]

混合云是一种 IT 架构，能在两个或更多互联但独立的环境之间进行某种程度的工作负载移植、编排和管理，这些环境包括裸机、虚拟化、私有云和公共云环境。借助混合云架构，您可以在任何互联环境中运行工作负载，在这些环境之间相互移动和使用资源。

企业采用混合云环境来：

- 连接来自不同供应商的基础架构、平台、应用和工具。
- 提高效率和可扩展性。
- 降低成本。
- 提升敏捷性。
- 优化数据放置。

[1] Flexera，“2023 年云状态报告”，2023 年 3 月。

无论您处于混合云之旅的哪个阶段，安全性都是重中之重，79% 的企业将云安全性视为一项挑战。[1]混合云安全漏洞通常是由于资源监督和控制的缺失造成的，包括未经批准的公共云使用、资源缺乏可见性、变更控制不足、配置管理不善、访问控制无效以及人为错误等等。未经授权的用户可以利用这些漏洞来访问敏感数据和内部资源，由此产生高昂的代价。

2023 年，全球数据泄露的平均成本达到 **445 万**美元的新高，其中业务损失占了 **29.2%**。[2]

51%

的公司表示他们计划增加安全投资，以应对数据泄露问题。[2]

[1] Flexera，“2023 年云状态报告”，2023 年 3 月。
[2] IBM Security，“2023 年数据泄露成本报告”，2023 年。

2023 年，数据泄露事件中涉及的每条记录的平均成本和遏制泄露问题所需的时间都有所增加。[2]通过调整方法来应对本地和云架构之间的差异，您可以部署安全至上的混合云，帮助克服这些日益严峻的挑战。本电子书讨论了实现混合云安全性的新方法和注意事项。

277 天

2023 年识别和遏制数据泄露的平均用时。[2]

$ 102 万美元

如果能在 200 天或更短时间内识别并遏制数据泄露，可以节省的成本金额。

[2] IBM Security，“2023 年数据泄露成本报告”，2023 年。

第 2 章

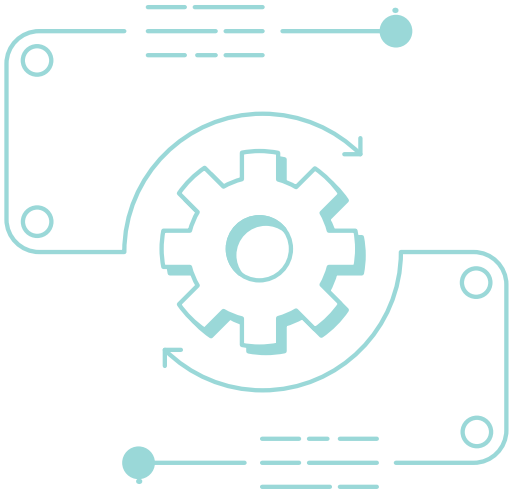
安全防护是一个过程，而不是一种产品

有效的安全防护需要一种能够整合人员、流程和技术的全面方法。仅仅部署以安全为中心的产品和工具并不足以保护您的基础架构、云或业务。还应考虑安全策略和流程，以最大限度地利用产品的功能并降低风险。

随着技术、威胁和需求的发展，这些策略和流程可随着时间的推移进行调整。混合云环境要求您改变安全方法，并且由于它们没有既定的边界，传统的安全方法不起作用。

集中式身份管理和访问控制是以云为中心的安全方法的关键。它运用最小特权原则，仅向用户提供他们需要的访问权限。这种方法需要审核每个用户的当前访问权限，然后对他们进行重新评估，以确定适当的访问级别。

混合云安全性还要求多层次深度防御安全防护策略能够结合环境中每一层的功能，包括操作系统、容器平台和自动化工具。



操作系统

寻找可帮助您满足安全合规性要求、实施物理安全防护、提高网络安全性、控制用户访问、隔离进程和提高数据安全性的内置工具。例如 OpenSCAP、USBGuard、安全增强型 Linux®（SELinux）、身份管理和网络绑定磁盘加密。

容器平台

使用平台和 Kubernetes 中的内置功能来提高容器安全性。例如容器集安全策略、网络流量控制、集群入口和出口控制、基于角色的访问控制（RBAC）、集成证书管理和网络微分段。

自动化工具

选择企业中每个人（包括开发、IT 运维、安全和合规团队）都可以轻松学习和使用的自动化语言与平台。寻求访问控制、日志记录和审核功能。

重新审视现有的安全流程和工具也很重要。确保您正在使用所有可用功能，并确定是否可以修改或重新配置任何设置以提供更好的保护，或者是否需要新的流程和工具。

1. 创建当前 IT 资产和工具的清单。
2. 记录现有的安全和网络架构、网络安全政策、工作流程以及技能和人才缺口。
3. 建立威胁模型并确定您对网络安全漏洞的风险容忍度和缓解策略。
4. 评估您的架构、策略和流程，以确定需要改进的领域。
5. 评估当前的工具和资产，确定它们是否可以支持更新后的策略和流程。记录并计划如何解决安全漏洞。

以下部分讨论了混合云安全性的关键注意事项，并提供了加强防护的提示。

第 3 章

安全注意事项 1

从坚实的基础着手

为什么这很重要?

如果您的工作负载分布在多个环境中，或者环境中使用了未经审查的开源技术，那么确定漏洞所在的位置可能很困难。此外，如果没有坚实的安全基础，使用多层安全保护措施就很难降低风险。直接使用来自上游社区的开源软件可能会让您面临安全风险和供应链攻击，这些攻击会利用第三方服务和软件的弱点来损害最终目标。这些攻击有多种形式，包括劫持软件更新和将恶意代码注入合法软件。过去 3 年中，软件供应链攻击事件的年均增长率达到了 742%。[3]因此，建立一个统一、稳定、安全至上的基础对保护您的业务至关重要。

建议和最佳实践

通过使用来自可信企业开源供应商的开源软件来减少软件供应链安全风险，这些供应商可在其软件的整个生命周期中提供企业支持，例如红帽。企业开源供应商使用可靠的软件供应链安全流程来开发软件，其中包括代表客户管理开源软件。这可以确保客户使用的开源软件是值得信赖、有弹性且安全的。

此外，在具有内置安全功能的平台上运行关键应用也很重要。这将为客户可靠地运行关键应用提供基础安全保护，包括用于降低风险以及实施安全性和合规性自动化的多层安全功能。

通过采用具有弹性、可信赖且在稳定性和安全性方面经过强化的操作系统（如红帽®企业 Linux®），优先构建面向应用和流程且安全至上的基础。这提供了一个稳定的基础，您可以在此基础上可靠地扩展关键应用、维护安全合规性，并在裸机、虚拟环境、容器及各类云环境之间一致地部署各种新兴技术。

[3] Sonatype，“第 9 次软件供应链状况年度报告”，2023 年。

红帽企业 Linux 是许多红帽产品组合的基础，鉴于其提供的内置安全功能，它也是许多企业信赖的操作系统。

借助红帽企业 Linux，您可以：

通过实时内核修补等内置安全功能来降低数据泄露或系统暴露的风险。这样，您就可以在无需重新启动或中断运行时的情况下应用安全补丁。此外，其他内置安全功能还包括：应用白名单，是指将一些获得批准的应用或可执行文件列在清单中，只有这些应用或文件才能由指定用户在系统上运行；SELinux，用于对文件、进程、用户、应用等应用细粒度级别的控制。

使用网络绑定磁盘加密等内置安全功能实现大规模的数据保护自动化，并随着时间的推移加以维护，通过该功能，您无需管理加密密钥即可自动解锁加密系统。此外，使用全系统加密策略，您可以专注于数据安全工作，并确保系统范围内一致且可自定义的加密设置的合规性，以满足特定于站点的策略需求等内容。

满足合规性要求并精简审核过程。红帽企业 Linux 内置了 OpenSCAP 合规性扫描和修复功能，可在本地系统上执行配置和漏洞扫描，以验证是否符合各种行业安全标准。

有了红帽企业 Linux 提供的基础安全方法，在其上运行的**红帽 OpenShift** 等分层产品即可为容器和 Kubernetes 提供深度防御。红帽将安全功能向上扩展到 Kubernetes 组件。 同样，凭借其内置的安全功能，**红帽 Ansible 自动化平台**允许企业大规模地实现安全性和合规性自动化。

战术步骤

开始实施混合云安全策略时，请采取以下措施：

切换为商用版本

将直接来自上游开源项目的开源软件迁移到受信任的商用版本。这些版本经过测试和验证，可降低错误和安全漏洞的风险。它们可能还包括企业支持，可以快速提供安全补丁并提供有关配置软件安全性的指导。通过采用来自可信企业开源供应商的开源软件，您可以确保他们的软件是使用可靠的软件供应链安全流程开发的，并在其软件的整个生命周期中提供企业支持。所有这些确保了企业在使用开源软件的同时，能够最大限度地降低安全风险。

选择具有内置安全功能的平台

选择具有内置安全功能的平台（例如操作系统、容器应用平台和自动化平台）非常重要。这将为客户可靠地运行关键应用提供基础安全保护，包括用于降低风险以及大规模实施安全性和合规性自动化的多层安全功能。

在整个技术堆栈中实现安全性

为安全性奠定基础后，请确保在该基础上运行的分层技术既能继承安全优势，又能协同工作以实现多层安全性。

第 4 章

安全注意事项 2

借助 DevSecOps 实现可信赖的软件供应链

为什么这很重要？

2023 年，12% 的数据泄露事件源自软件供应链攻击。[2]直接使用来自上游社区未经审查的开源软件可能会让您面临安全漏洞和供应链攻击，这些攻击会利用第三方服务和软件的弱点来损害最终目标。这些攻击有多种形式，包括劫持软件更新和将恶意代码注入合法软件。

由于在应用开发和基础架构部署中，安全防护变成了事后补救措施，因此分割式安全方法往往会导致安全漏洞和重复工作。随着开发速度和部署灵活性的提高，在整个流程中考虑安全性变得更加重要。

建议和最佳实践

为了在软件供应链中采用安全至上的方法，首先要培养 DevSecOps 思维模式。在 DevSecOps 思维模式中，应用开发人员、IT 运维团队和安全团队协同工作，在软件开发生命周期（SDLC）和基础架构生命周期中实现软件供应链安全，构建跨混合云的企业级强化开源基础。

[2] IBM Security，“2023 年数据泄露成本报告”，2023 年。

从初始设计一直到集成、测试、部署和软件交付，DevSecOps 可自动实现软件开发生命周期内每个阶段的安全性集成。

采用 DevSecOps 流程的好处包括：

- 帮助 IT 和安全团队应对人员、流程和技术方面的挑战。
- 可提高效率、一致性、可重复性和协作性。
- 有助于减少人为错误，最终降低风险。

有了 DevSecOps，安全性就成为需要全程关注的共担责任。安全、开发和运维团队的员工携手合作，共享可见性、反馈、经验教训和见解，而不是让一个独立的、不相干的团队单独负责设置安全策略。这种方法允许从开始开发应用和部署基础架构时就构建安全流程，以增强保护。

为企业构建新软件功能的企业级应用开发人员需要大幅提升安全态势并减少认知负荷。安全性需要在整个 SDLC 中实现：在代码阶段，通过集成的应用安全检查来发现 SDLC 早期的问题并减少长时间停机；在构建阶段，通过使用安全至上的持续集成和持续交付（CI/CD）工作流来保护构建系统；在部署阶段和运行阶段，使用黄金路径模板、漏洞分析、工件签名、认证、来源、策略实施点和软件物料清单（SBOM）来确保安全性。

还需要创建一个策略，以确保您的团队使用的开源技术来自可靠的来源，能够以自动化方式不断修补，并在配置时考虑到安全防护措施。此外，您应该鼓励使用在整个生命周期都能提供企业支持的企业级开源产品。

通过使用企业级开源产品（例如红帽提供的产品），您可以利用红帽在保护其产品的开源软件供应链方面超过 30 年的经验。此外，企业需要相应的解决方案来帮助他们部署、管理和保护 Kubernetes 集群，还需要统一的方式来大规模构建、部署应用并对其进行现代化改造。

红帽 OpenShift 平台 Plus 是一个统一的平台，包括红帽 OpenShift、红帽 Kubernetes 高级集群安全防护、红帽 Kubernetes 高级集群管理、红帽 Quay 和红帽 OpenShift 数据基础。该平台可帮助企业在 Kubernetes 中大规模地安全构建、部署容器化应用并对其进行现代化改造。提供多集群安全性、合规性、应用和数据管理，以确保 整个软件供应链的一致性。

战术步骤

在实施 DevSecOps 和软件供应链安全改进方法时，请尝试以下措施：

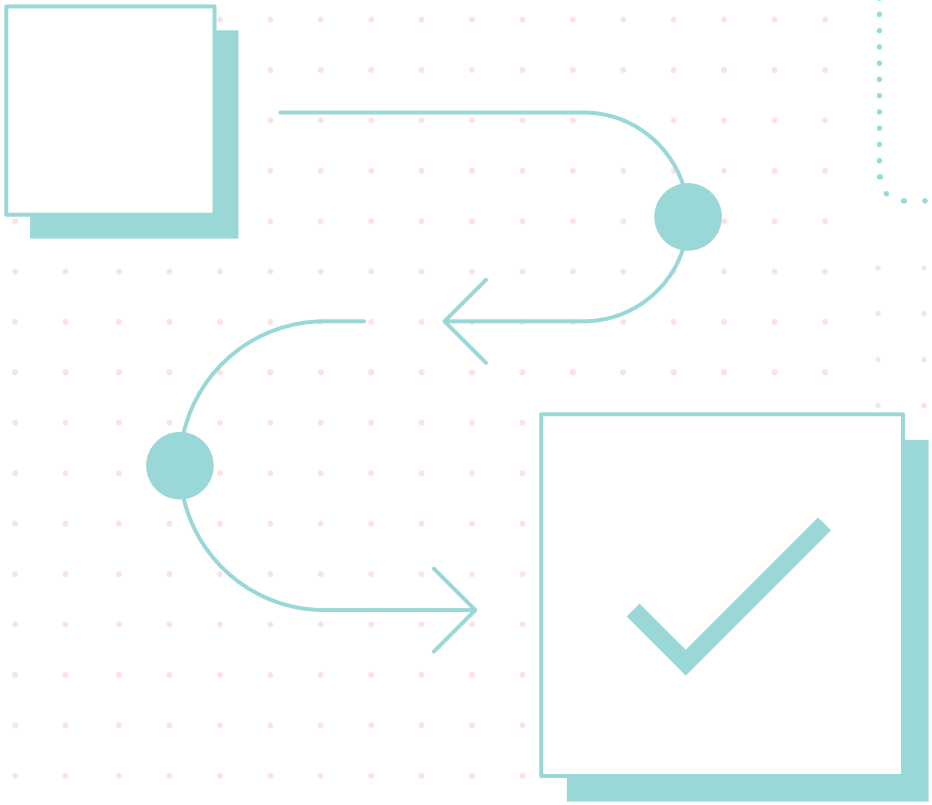
从小规模着手，逐步扩展。
选择一个项目开始。鼓励实验和迭代、持续改进以微调和优化流程。庆祝成功并向企业内的其他人展示已证明的价值。

协商设定明确的目标和时间表。
透明度至关重要。确保每个参与者都理解并同意项目的目标和时间表。

对员工进行交叉培训。
建立有关安全性、基础架构和开发的学习路径，定期更新并供所有团队成员随时使用。

组建安全工作组。
建立一个集成的跨学科团队来定义安全用例和策略。向他人学习。利用借鉴其他企业的知识经验。

借助统一的应用平台，实现整个 SDLC 中的安全性。
安全性需要在整个 SDLC 中实现：在代码阶段，通过集成的应用安全检查来发现 SDLC 早期的问题并减少长时间停机；在构建阶段，通过使用安全至上的持续集成和持续交付（CI/CD）工作流来保护构建系统；在部署阶段和运行阶段，使用黄金路径模板、漏洞分析、工件签名、认证、来源、策略实施点和软件物料清单（SBOM）来确保安全性。



第 5 章

安全注意事项 3

使用自动化和管理来保护您的混合云

为什么这很重要?

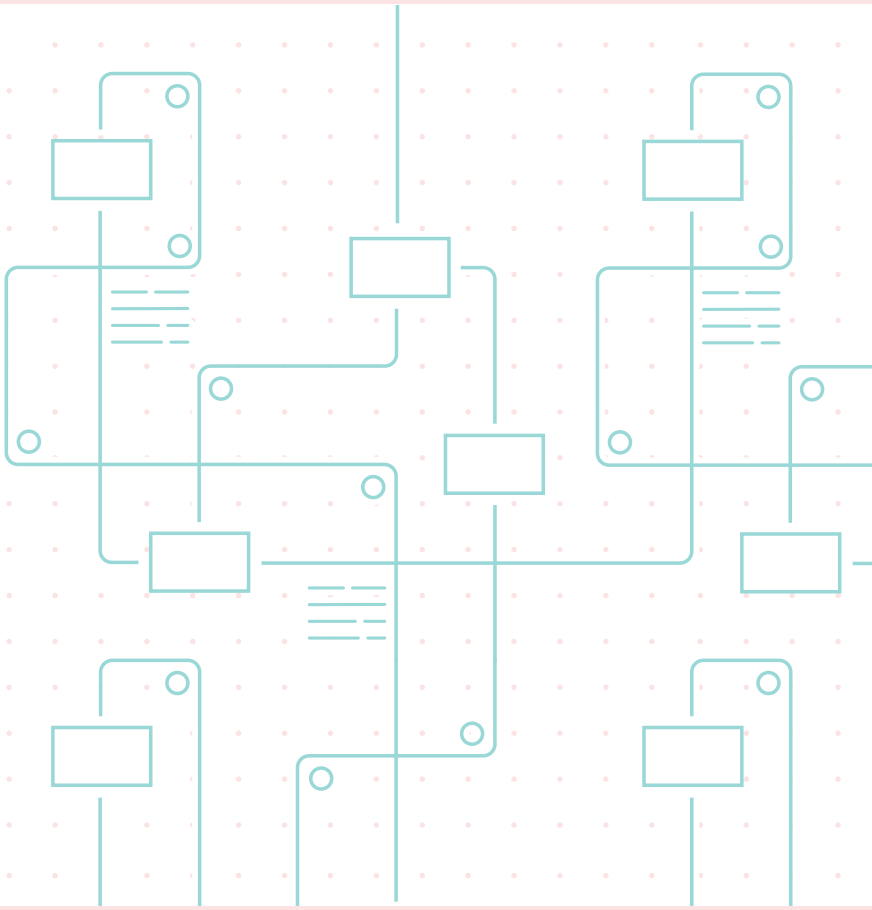
错误配置和不充分的变更控制是对安全性的最大威胁。[4]错误配置可能使系统容易受到攻击。变更控制对于了解谁修改了配置、何时修改以及在整个系统生命周期中更改了哪些内容至关重要。

自动化、管理和 AI 可帮助您简化日常运维，并从一开始就将安全防护集成到流程、应用和基础架构中。在整个企业中使用自动化和管理策略有助于减少人为错误，还能提供速度、一致性、可重复性以及验证和审核能力。此外，集中式自动化和管理策略可帮助企业从一开始就将安全性集成到应用开发和 IT 运维当中并贯穿整个生命周期，从而提高安全性和合规性。这让他们能够成功实施 DevSecOps。事实上，将广泛的自动化、管理和 AI 整合到安全流程中可以将数据泄露的平均成本平均降低 39.3%，但只有 28% 的企业这么做了。[2]

[2] IBM Security，“2023 年数据泄露成本报告”，2023 年。
[4] 云安全联盟，“云计算的主要威胁：Pandemic 11 深入分析”，2023 年 10 月。

建议和最佳实践

在企业范围内实施自动化和管理策略，以跟上动态安全性、风险和合规性需求的步伐。通过为混合云采用一致的自动化和管理策略，您可以获得更高的敏捷性、可重复性、一致性和简化的审核过程。



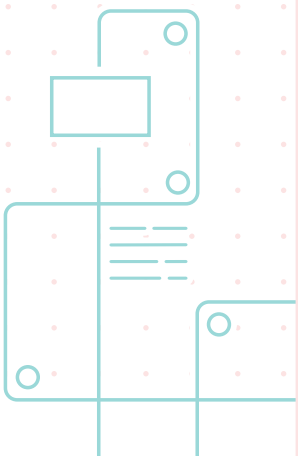
统一的自动化和管理策略可以降低整个企业中错误配置和人为错误的风险。自动化和管理可简化并提高基础架构管理、应用开发和安全运维的一致性，以改进保护、合规性和变更控制。这样，您就可以：

根据预先批准的策略始终如一地配置资源，并在其生命周期内以可重复的方式主动维护资源。

快速识别需要修补或重新配置的系统。

根据定义的基线，以一致的方式跨大量系统简化修补过程或更改系统设置。

通过自动记录的操作日志简化审核和故障排除。



通过对自动化平台和流程进行身份管理和访问控制，您可以确保只有经过授权的人员才能执行自动化任务。选择企业中每个人都可以使用的自动化平台。选择一个实现了通用、易于学习的自动化语言的平台可以改善：

- **可见性。**每个人都可以理解每个自动化任务的作用。
- **可重复性。** 可访问的平台和语言允许所有获得批准的员工有效且高效地使用自动化功能。
- **协作。** 自动化任务可在整个企业内共享，允许其他团队利用已完成的工作，避免重复工作。
- **审核。**多名员工可以验证自动化任务并查看日志以进行审核。

企业依靠 IT 自动化来管理日益复杂的运维环境、应用、安全运维和混合云环境中的安全性。**红帽 Ansible 自动化平台**是一个端到端的自动化平台，可提供一致的企业框架，在帮助您大规模构建和运维 IT 自动化的同时，自始至终优先考虑安全性。它有助于改善效率、提高生产力、帮助控制风险和费用、允许团队以可重复的方式在整个企业内实现安全性和合规一致性的自动化，还可以提供经过认证的自动化内容，在红帽全天候的企业支持下，以协调一致的方式应对威胁。

红帽 Ansible 自动化平台可帮助企业管理自动化安全流程，提供从自动化配置管理到自动修补和修复的所有功能，以防范恶意攻击。此外，红帽 Ansible 自动化平台使用来自 CyberArk、IBM 和 Palo Alto Networks 等众多经认证合作伙伴的内容，可充当安全解决方案的集成点，帮助用户自动化各种外部安全技术的管理和集成。

战术步骤

尝试这些操作以开始实施安全自动化。

从单个项目开始。
不要试图马上实现全面自动化。从一组数量有限的任务开始。

选择重复性任务。
自动执行重复性任务，包括配置管理、软件包和补丁管理、安全漏洞识别和修复以及策略实施。

衡量、调整和重复。
以迭代方式部署自动化、衡量结果并进行相应调整。

通过使用可扩展的端到端企业自动化平台来规划扩张。
确保所有自动化过程都是可验证、可审核且可共享的，以便企业内的其他人可以利用这些优势并使用端到端企业自动化平台进行扩展。

第 6 章

准备好开始了吗?

混合云安全性是所有企业的共同责任。无论您处于混合云之旅的哪个阶段，红帽都可以帮助您部署安全至上的混合云。

凭借集成的内置安全功能，红帽的生产级开源软件产品组合可为您提供克服当前和未来安全性与合规性挑战的工具和平台。红帽还提供企业级支持、实践培训和专家服务，帮助您更高效、更安全地构建和运维混合云环境。

了解红帽的混合云安全防护心法

请参阅这些资源，了解有关红帽跨混合云实现安全性和合规性方法的更多信息。

- 混合云安全性概述
- 混合云安全性评估
- 保护混合云环境的方法
- 提升混合云的安全性

Lucy Huh Kerner 是红帽安全部门全球战略与宣传总监
Lucy Huh Kerner 负责引领安全思想领导力，以及红帽公司和全球整个红帽产品组合的安全技术和市场进入战略。此外，她还帮助创建安全相关技术内容，并提供给现场、客户、合作伙伴、分析师和媒体，还在众多活动（包括安全会议）中发表演讲。Lucy 拥有超过 20 年的软件和硬件开发工程师、解决方案架构师和全球安全战略分析师的专业经验，工作曾涉及安全防护的方方面面。

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