



改善安全防护， 确保始终合规

利用稳健的开源 Linux 平台降低风险

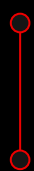
目录

1

Linux 是未来发展的基石

2

采用高效的安全性及合规性方法



2.1 Linux 环境中的漏洞识别和修复

2.2 Linux 环境中的合规性管理

3

最佳实践及推荐使用的工具

4

借助红帽提高安全性与合规性

5

成功案例：
英国气象局

6

准备好开始体验了吗？



Linux 是未来发展的基石



作为全球最受欢迎的操作系统之一，Linux® 为现代创新型 IT 提供了理想平台。该操作系统常用于数据中心和云计算环境中高可用、可靠且关键的工作负载，支持各种用例、目标系统和设备。每家主流公共云提供商均在其线上市场中提供多种 Linux 发行版。

即便如此，您所选择的 Linux 发行版和管理工具仍会极大地影响您的 IT 环境的效率、安全性和互操作性。本电子书汇总了与 Linux 环境的安全漏洞及合规性风险相关的关键考量因素和指南。

安全性与合规性是头等大事

管理 IT 安全性与合规性风险是所有企业组织都需要持续关注的问题。事实上，在过去两年中，23% 的企业组织都遭遇过重大网络安全攻击。¹ 而且，防止安全漏洞的成本很高。防止数据泄露的平均成本达到 445 万美元。²

行业和政府法规也在不断变化。保持合规性具有一定的挑战性，不合规会使防止数据泄露的成本平均提高 5%。²

避免无效安全防护带来的影响

速度对于降低泄露的风险和影响至关重要。

445 万美元

2023 年防止数据泄露的平均总成本（单位：美元）。²

277 天

2023 年发现并遏制数据泄露的平均用时。²

102 万美元

如果能在 200 天或更短时间内发现并遏制数据泄露，可减少的平均成本。²

¹ Nash Squared, “2023 年 Nash Squared 数字化领导力报告”，2023 年 11 月。

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

常见的安全性与合规性挑战

某些因素使安全漏洞与合规性的管理具有挑战性。

安全性与合规性环境不断变化

安全威胁变化迅速，因此，需要快速应对新的威胁以及不断变化的法规。

23%

的大小企业组织在过去两年中都遭遇过重大网络安全攻击。³

82%

2023 年，涉及存储在云环境或跨多个环境中的数据的泄露占 82%。⁴

云环境分散

地理位置和逻辑上分散的混合和多云环境可能会妨碍您全面了解 IT 基础架构，更难跨所有系统保持配置的一致性。

IT 环境庞大且复杂

大型基础架构通常包含多种安全性与合规性工具，导致风险管理变得复杂。

安全防护系统的复杂性使数据泄露成本增加

240,889 美元。⁴

与无需考虑远程办公因素相比，远程办公因素使防止数据泄露的平均成本增加

173,074 美元。⁴

员工有限以及远程办公指令

大多数企业组织都达不到手动管理安全性与合规性任务所需的员工人数，而远程办公又会增加保护企业组织数字资产的设备 and 接入点的负担。

3 Nash Squared, “2023 年 Nash Squared 数字化领导力报告”, 2023 年 11 月。

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

采用高效的 安全性与合规性管理方法

安全漏洞与合规性管理涉及通过监控和评估系统来确保系统符合安全和监管政策的要求。理想的安全漏洞与合规性管理方法可让您在整个环境中制定一致且可重复的流程，从而实现：



评估

识别不合规或易受攻击的系统。评估从基础架构到工作负载等环境的实际安全状态。了解众多安全防护建议中哪些真正适用于您的系统和环境。



确定优先级

按照工作量、影响和问题严重程度来安排修复措施。运用风险管理技术来确定每个问题的实际业务风险，并相应地制定修复措施计划。风险包括漏洞问题的可能性、漏洞的潜在严重程度以及修复问题的意义。修复开发和测试系统中的某个问题可能没有意义，但同样的问题如果出现在生产系统中，可能就是具有高优先级的问题。



修复

修复并重新配置需要快速采取行动的系統。实现配置和修复流程的自动化，以加快修复速度，确保跨系统的一致性并降低出现人为错误的风险。有效利用自动化工具有助于您快速修复问题，从而提高环境和业务的安全性。



报告

验证更改是否已应用并自动生成报告以简化审核流程。有效的报告可帮助您为高管、审核人员和技术团队提供正确的详细信息，以便其了解当前的安全风险和暴露情况。

这种方法还有助于您的企业组织为 **DevSecOps** 等快速发展的现代开发和管理技术做好准备。以下部分介绍了更高效地管理安全性与合规性风险需要考虑的重要因素以及可以采取的措施。

Linux 环境中的漏洞识别和修复

漏洞识别和修复是评估基础架构以发现并修复易受攻击系统的过程。这些漏洞可能是由新出现的威胁、补丁过时或缺失或系统配置错误造成的。修复措施通常包括修复、更新和重新配置系统以解决漏洞。

为何如此重要？

安全漏洞可能会导致代价高昂的数据泄露，进而导致客户的信任度下降以及公司声誉和收入受损。事实上，安全漏洞导致的业务损失占数据泄露平均成本的 29.2%。⁵

高效识别和修复漏洞所面临的挑战

大多数企业组织都缺乏大规模运维所需的一致安全防护策略。

- ▶ 员工数量有限会导致他们不堪重负，且他们可能不具备开发和执行全面的安全防护策略所需的技能。
- ▶ 通用的安全漏洞扫描工具会生成大量的潜在漏洞列表，但并非所有漏洞均适用于您的环境，因此，员工需要花费大量时间来调查漏洞并采取修复措施。
- ▶ 手动识别、修复和跟踪流程会减慢运维速度，且已知漏洞通常并未得到修复。
- ▶ 临时的修复方法会导致应用的补丁不一致，还会导致潜在的安全风险增加。

关键的安全管理工具功能

要提高效率，您必须在导致数据泄露之前快速识别并修复系统漏洞。寻找具有以下功能的统一安全管理工具：



分析系统以识别您的整个环境中系统和实例在操作系统和工作负载级别的风险。



自动修复已识别的风险，以提高 IT 和安全防护团队的速度、准确性和效率。



结合供应商的专业知识为其产品提供修复指导，您可以采取一些简单的措施来降低风险。



定期访问操作系统和应用供应商提供的有关已知漏洞和安全风险的最新数据。



以适当的详细程度为不同的受众**生成有关潜在风险、修复措施和审核的报告**。

Linux 环境中的合规性管理

合规性管理是确保系统持续符合企业政策、行业标准和适用法规的过程。它通过对基础架构进行评估来识别由于法规、政策或标准发生变化、配置错误或其他原因而不合规的系统。

为何如此重要？

除了安全漏洞以外，不合规还可能会导致罚款、业务损失以及失去认证。不合规会导致数据泄露的平均成本增加。⁶

高效管理合规性所面临的挑战

许多企业组织通过手动操作和自定义脚本来管理合规性，这些流程太慢且可扩展性有限，无法满足快速发展的现代开发和运维的需求。

- ▶ 大量通用标准和基线使得难以理解与环境的相关性以及带来的影响。
- ▶ 手动流程会减慢合规性监控、修复和审核操作的速度，导致员工时间利用效率低下、策略应用不一致且合规性问题的风险增加。
- ▶ 许多企业组织都是使用不同的工具来管理安全性与合规性，导致运维效率较低，且难以制定一致的自定义策略。

关键合规性管理工具功能

要提高效率，您需要指定并应用情境化策略，保持系统合规性，并快速生成和管理审核报告。寻找具有以下功能的统一合规性管理工具：



使用分析以省时高效的方式一致地识别合规性风险。



自动修复不合规系统。



可全面了解整个环境的合规态势。



根据您的审核要求和受众需求**自动生成合规性报告**。



提供专家建议和情境化指导，以修复整个环境中的不合规系统。

最佳实践及 推荐使用的工具

定期分析系统

日常监控可以帮助您在漏洞和合规性风险导致业务运营中断或数据泄露之前进行识别。确保使用操作系统和应用供应商提供的最新安全数据以提高分析的准确性。根据您的环境和运维定制安全策略，以生成更准确的合规性结果。

在

200 天

或更短时间内发现并阻止数据泄露可显著降低其造成的损失。⁷

经常修复并对补丁进行测试

使系统保持最新状态可提高安全性、可靠性、性能及合规性。定期应用补丁以预防一般意义上的重要问题。尽快针对关键漏洞和缺陷应用补丁。将修复的系统重新投入生产环境之前，对其进行验收测试。

高效的管理工具可将系统修复速度提高

56%。⁸

实现部署自动化

随着基础架构规模和复杂性的扩大，手动管理变得越来越困难。可利用自动化来简化监控、加快修复、提高一致性并确保定期生成报告。

安全防护自动化和人工智能 (AI) 可将防止数据泄露的成本降低

39.3%。⁷

⁷ IBM Security, “2023 年数据泄露成本报告”, 2023 年。

⁸ IDC 白皮书 (由红帽赞助), “红帽卫星帮助企业组织利用自动化工具优化基础架构”, 文档编号: US46109220, 2021 年 8 月。

连接您的工具并使您的流程保持一致

分散的环境通常包含每个平台所用的不同管理工具。通过应用编程接口（API）集成这些工具，并使用您偏好的接口在其他工具中执行任务。使用较少的接口来简化运维，更详细地了解环境中所有系统的安全性和合规性状态。使整个环境中的流程保持一致，以提高一致性和可靠性。

高度复杂的安全防护系统会使数据泄露的平均成本增加

31.6%⁹

采用一致且持续的安全防护策略

高效的安全防护需要一种能够整合人员、流程和技术的方法。持续安全防护策略依赖于反馈和调整，以支持现代开发技术、DevSecOps 和数字化业务需求。采用多层次深度防御安全防护方法可充分利用环境中每一层的功能，包括操作系统、容器平台、自动化工具、软件即服务（SaaS）资产和云服务。

采用 DevSecOps 方法可将数据泄露的平均成本降低

38.4%⁹



理想的安全性与合规性工具应包含几项关键特性和功能。

主动分析

了解您的安全性与合规性态势是加以改善的第一步。自动执行分析的工具可确保定期对系统进行监控，并针对一些问题发出提醒，无需员工花费太多时间和精力。

划分响应的优先级

提供规范性修复步骤的工具无需您研究如何操作，可节省时间并降低出错的风险。根据潜在影响和受影响的系统划分操作的优先级有助于您充分利用时间有限的修复窗口期。

可定制的结果

某些漏洞和合规性检查可能并不适用于某些系统的用途、配置或工作负载。理想的工具可指定业务场景，从而减少误报，管理风险，并呈现真实的安全性与合规性状态。

直观的报告

通过工具生成有关哪些系统已修复、哪些系统需要修复以及哪些系统不符合安全防护策略的清晰直观报告，提高可审核性，有助于您更好地了解环境状态。

统一的界面

工具不仅能管理环境中的单一组件或层，还能简化安全防护运维，以便您更好地了解安全性与合规性态势。统一的安全工具还可为扫描和修复指南提供更多背景信息。



可指导行动的洞察

工具为您的环境提供的定制信息有助于您更快识别存在哪些潜在的安全漏洞和合规性问题、哪些系统受到了影响以及潜在影响。这些工具还有助于您制定计划并确定修复措施的优先级。



借助红帽提高安全性 与合规性

红帽采用全面的安全性及合规性风险管理方法，可提高您的整个 IT 环境（从裸机和虚拟化服务器到私有云、公共云和混合云基础架构再到边缘部署）的速度、可扩展性和稳定性。通过整合人员、流程和技术，红帽® 平台可帮助您高效运维、推动创新并提高员工满意度。

该战略的核心是**红帽企业 Linux**。红帽企业 Linux 可为现代 IT 和企业混合云部署奠定一致且智能的运维基础，为您的企业带来无与伦比的优势。通过实现跨基础架构的一致性，无论身在何处，您都能使用相同的工具来部署应用、工作负载和服务。

安全性是红帽企业 Linux 架构和生命周期的一个关键组成部分。多层漏洞防御系统通过可重复的自动化安全防护措施来降低您暴露于漏洞之下的风险。作为红帽企业 Linux 订阅的一部分，关键的安全升级和实时补丁有助于您使环境保持最新状态并提高安全性。

66

改用红帽企业 Linux 后，**发现并调查错误和漏洞的速度要快于**以前使用的 Linux 发行版。¹⁰

Yuki Miyamoto

Square Enix Co., Ltd. IT 基础架构/在线业务基础架构系统信息技术部

红帽管理工具与红帽企业 Linux 的集成可提供高效管理安全漏洞风险和合规性所需的功能。



可配置的工具和基线能够减少误报，让您准确了解基础架构的状态。



自动化功能可提高配置和修复的准确性，同时减少人为错误。



可定制的视图可在恰当的时间快速向合适的受众提供正确的信息。



自动进行主动修复可帮助您更快解决问题，无需再联系支持部门。



内容广泛的资源库可全天候提供详尽且具有针对性的信息。



本地和软件即服务（SaaS）选项可让您根据自己的偏好部署工具。



API 可将您的现有和偏好的安全防护、合规性和管理工具与接口相连接。



漏洞和恶意软件检测功能可扫描系统以查找常见漏洞和暴露（CVE）及恶意软件签名。



资源优化功能可帮助您利用计算、内存和性能方面的指标调整公共云部署的规模。

利用集成的工具

红帽管理工具基于多年的 Linux 开发和支持经验。它们通过协同工作来简化 IT 管理，节省您的团队的时间和精力，并使您的环境更加安全、优化和可靠。



分析、观察和管理红帽系统

红帽智能分析以服务的形式随附于红帽企业 Linux 中，可持续分析平台和应用，以预测风险、推荐操作并跟踪成本，从而帮助您更好地管理混合云环境。借助智能分析，您可以监控 IT 效率、稳定性和性能，管理安全性与合规性风险，以及跟踪和优化跨云的支出。

26% 解决安全事件的速度提升幅度¹¹

24% IT 安全防护团队的效率提升幅度¹¹

76% 计划外停机时间减少幅度¹¹



实现系统管理的简化和自动化

红帽卫星是一款基础架构管理解决方案，可在物理、虚拟、云或边缘环境等任何位置置备和维护红帽企业 Linux 系统。红帽卫星可大规模简化置备、修复及其他重复性系统管理任务，以提高运维效率，同时保持系统安全性、可用性和策略合规性。

56% 修复操作的效率提升幅度¹²

56% IT 基础架构的效率提升幅度¹²

28% 运维总成本降低幅度¹²

¹¹ IDC 商业价值速览（由红帽赞助），“红帽智能分析的商业价值”，文档编号：US51795124。2024 年 2 月。

¹² IDC 白皮书（由红帽赞助），“红帽卫星帮助企业组织利用自动化工具优化基础架构”，文档编号：US46109220。2021 年 8 月。

成功案例

英国气象局

英国气象局是英国的国家气象服务机构，每天为世界各地的人们提供与天气和气候相关的服务。为了建立全面的服务器管理方法，英国气象局采用红帽智能分析来作为对红帽卫星的补充。在红帽大客户技术经理的支持下，英国气象局显著提高了对其服务器环境的了解程度。

英国气象局首先在几台存在已知问题的机器上对智能分析进行测试。问题立即被呈现出来，IT 团队决定扩大部署范围。该团队按照内部更改管理流程使用红帽卫星，简化了在整个环境中安装智能分析的过程。

借助智能分析，团队可以更轻松地确定任务的优先级，查看是否存在某些问题，了解哪些系统受到了影响以及问题的严重程度。它还通过识别和修复配置问题帮助英国气象局使其服务器资产达到所需的标准。

英国气象局计划继续使用智能分析和红帽卫星来管理其整体环境，并以更积极主动的方式改善其安全态势。

66

红帽智能分析可为我们提供自上而下的概览，使我们能够采用**更全面的方法来管理我们的资产**。红帽卫星能很好地发现单台机器上的问题，红帽智能分析的优势则在于将整个环境的共性问题联系起来，而不是逐台机器地处理。

—
Chris Wilkinson
高级系统工程师
英国气象局

准备好开始体验了吗？

您的企业依赖于您的 IT 基础架构和应用。采用高效的安全漏洞和合规性风险管理方法和工具有助于对您的企业组织进行保护。

红帽为注重安全的运维和创新提供了值得信赖的 Linux 平台以及所需的集成管理工具和服务。



利用红帽智能分析来分析风险

- ▶ [了解智能分析](#)
- ▶ [了解分析师对红帽智能分析的评价](#)

利用红帽卫星大规模管理系统

- ▶ [了解红帽卫星](#)
- ▶ [了解分析师对红帽卫星的评价](#)