Red Hat

改善安全防护，确保始终合规

利用开源 Linux 平台降低风险

目录

3 第1章：
Linux 是未来发展的基石

4 第 2 章：
采用高效的安全防护与合规性方法

5 第 3 章：
Linux 环境中的漏洞识别和修复

6 第 4 章：
Linux 环境中的合规性管理

7 第 5 章：
最佳实践和工具推荐

8 第 6 章：
在红帽的帮助下提升安全性与合规性

9 第 7 章：
充分利用集成工具

10 第 8 章：
Zoom 携手红帽打造可靠的企业系统

11 从您的数据中获取更多价值

近期的基准测试结果揭示了安全防护措施无效所引发的典型后果：[1]

- **440 万美元**——2025 年数据泄露的平均总成本为 440 万美元。
- **241 天**——2025 年识别和遏制数据泄露的平均用时为 241 天。
- **97%**——报告 AI 相关安全防护事件的企业组织中，有 97% 的企业组织缺乏适当的 AI 访问控制措施。

第 1 章

Linux 是未来发展的基石

作为最受欢迎的操作系统（OS）之一，Linux® 为现代 IT 架构提供了理想平台。它是数据中心和云计算环境中高可用、可靠和关键工作负载的标准，支持各种用例、目标系统和设备。许多主要公共云提供商都在其市场中提供多种 Linux 发行版。

即便如此，企业组织选择的特定 Linux 发行版和管理工具会极大地影响其 IT 环境的效率、安全性和互操作性。本电子书提供了有效的安全管理方法、关键的集成工具功能和建议，以及有关在 Linux 环境中管理安全漏洞及合规性风险的指导。

AI 带来新问题

如何管理 IT 安全性与合规性，这是许多企业组织持续面临的挑战。“在全球范围内，五分之一的企业组织在过去两年内经历过重大网络事件。这些事件代价高昂，全球数据泄露的平均成本高达 444 万美元。”[1]AI 兴起带来了新的威胁，并使安全形势变得更加复杂。具体而言，员工绕过 IT 监管，擅自使用未经批准的 AI 工具（即“影子 AI”），将会带来新的重大威胁。“涉及影子 AI 的泄露事件使[总]成本平均增加 67 万美元，[较标准泄露成本]高出 15%。”[1]

避免安全防护措施无效带来的后果

速度对于降低泄露风险和影响至关重要。企业识别潜在威胁的速度越快，对财务和运营造成的影响就越小。近期的基准测试结果揭示了安全防护措施无效所引发的典型后果：[1]

- **440 万美元**——2025 年数据泄露的平均总成本为 440 万美元。
- **241 天**——2025 年识别和遏制数据泄露的平均用时为 241 天。
- **97%**——报告 AI 相关安全防护事件的企业组织中，有 97% 的企业组织缺乏适当的 AI 访问控制措施。

三大常见安全防护挑战

多项因素使现代安全漏洞与合规性管理变得更为复杂：[1]

安全防护与合规形势不断变化

团队不仅要管理设备，还要努力管好获得批准的 AI 模型，同时防范影子 AI 工具的攻击。

- **20%** 的数据泄露由涉及影子 AI 的安全事件造成。

当数据存储在多个环境中时，保护难度将会显著增加。与存储在单一环境中的数据相比，这种复杂性使得安全团队更难以识别和遏制数据泄露。

- **30%** 的泄露现涉及存储在多个环境中的数据。

1 *IBM Security。“2025 年数据泄露成本报告”，2025 年。*

复杂性带来的额外代价

大型基础架构通常包含多种安全防护与合规性工具，这可能会使风险管理工作变得更加复杂。

- 涉及多个环境的数据泄露事件如今最为普遍，代价也最高，平均每次事件的成本为 **505 万美元**，这一数字略高于仅发生在本地环境中的数据泄露事件。

人员配置方面的挑战

大多数企业组织都缺乏足够的人员来手动管理安全防护与合规性任务。此外，随着远程办公的兴起，保护设备以及通向企业数字资产的各个接入点的负担也随之增加。

- **63%** 的企业缺乏管理 AI 所需的治理策略，主要是因为没有足够的人员来制定和实施这些策略。

第 2 章

采用高效的安全防护与合规性管理方法

安全防护与合规性管理是一项以风险为导向的持续性工作。它有助于企业组织增强安全态势，同时在日益复杂的环境中满足监管和业务要求。借助现代方法，团队能够在整个 IT 资产（本地、云和混合基础架构）中建立一致、可重复且可审计的实践，从而能够：

评估

持续识别不合规或存在漏洞的系统。评估企业组织整个环境（从基础架构到工作负载）的安全状态，以确定哪些安全公告真正适用于特定系统。

确定优先级

在经过验证的自动化和 AI 驱动的工具的支持下，根据风险、影响和运营工作来确定修复工作的优先级。运用风险管理技术，理解每个问题对业务的影响，并相应地规划修复工作。例如，开发系统上的漏洞可能风险极低，而生产工作负载上的相同问题则需要立即处理。

修复

快速修补并重新配置系统。自动化修复流程，这可确保各系统间的一致性，并降低人为错误的风险。如果能有效应用自动化工具，可加快修复速度，从而保护企业及其数据。

报告

持续验证是否已应用更改，并自动生成报告，以简化审计流程。清晰且契合角色的报告，可为高管、审计人员和技术团队提供适当级别的洞察力，帮助他们了解当前安全态势及长期风险敞口。通过将持

续验证与可审计的自动化报告相结合，企业组织能够超越被动应对式安全防护实践，支持 DevSecOps 等现代运营模式，在这种模式下，速度、一致性和治理三者必须同时兼顾。

Square Enix 简化了在线游戏基础架构的管理

“改用红帽企业 Linux 后，我们可以比以前使用 Linux 发行版时，更快地发现和调查错误及漏洞。”

Yuki Miyamoto
Square Enix Co., Ltd. 信息技术部 IT 基础架构/业务在线基础架构系统

注意：本文所包含的信息在采访时为最新信息。

第 3 章

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。这些漏洞可能由新兴威胁、补丁过时或缺失，或是系统配置错误引起。修复措施通常包括修补、更新和重新配置系统，以消除潜在风险。

为什么漏洞识别至关重要？

安全漏洞可能会导致代价高昂的数据泄露事件，从而损害客户信任、公司声誉及收入。事实上，“攻击者以客户个人身份信息（PII）为目标的攻击数量，远远超出针对其他类型数据的攻击。此类数据在被盗或遭泄露的数据类型中位居首位，占比高达 53%。”[1]由于此类数据在身份盗用和欺诈方面具有很高的价值，它仍是攻击者最想窃取的数据类型。

高效识别和修复漏洞所面临的挑战

大多数企业组织缺乏一致的安全防护策略来支持大规模运营，而 AI 工具和工作负载的快速、无序采用，进一步扩大了这一差距。主要障碍包括：

- 技能和资源缺口：随着 AI 环境不断扩展，人员数量有限且不堪重负，而且可能缺乏制定和执行全面安全防护策略所需的技能。
- 警报疲劳：通用安全扫描工具会生成大量潜在漏洞列表。由于其中许多漏洞并不适用于特定环境，员工必须耗费更多时间去排查相关风险。
- 手动操作瓶颈：手动识别、修复和跟踪流程，这会拖慢运营速度，并导致已知漏洞长期得不到修复。
- 修复不一致：临时性的修复方法会导致补丁应用不一致，并增加整个基础架构中出现安全漏洞的风险。

安全管理工具的主要功能

为了提高效率，企业组织必须能够在系统漏洞导致数据泄露之前，迅速识别并解决这些漏洞。在评估统一安全管理工具时，请关注以下关键功能：

- **系统分析：**识别任何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：**帮助 IT 和安全团队更快、更准确、更高效地识别风险。
- **整合供应商专业知识：**可针对他们的产品提供修复指导，确保修复方案经过验证。

- **定期访问最新数据：**从企业组织的操作系统及应用提供商处，获取有关已知漏洞和安全风险的最新数据。
- **生成符合审计要求的报告：**为高管、审计人员和技术团队提供适当的详细信息。

阅读这份 PeerSpot 报告[2]，了解如何利用红帽®卫星解决方案改善基础架构管理和安全性，即便是顶尖 IT 部门也能从中受益。

第 4 章

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。该过程涉及对基础架构进行评估，以识别因法规和政策变化、配置错误或其他内部标准而导致不合规的系统。

为什么合规性管理至关重要？

除了增加安全漏洞的风险外，不遵守适用的法规，还可能导致巨额罚款、企业声誉受损以及丧失必要的认证。若未能满足监管合规要求，将会使数据泄露的平均成本增加 173,692 美元。[1]

高效管理合规性所面临的挑战

许多企业组织依赖手动操作和自定义脚本，这些方法在快节奏的技术开发和业务运营背景下，不仅效率低下，且规模有限。具体挑战如下：

- 通用标准和基线众多，难以确定哪些要求与特定环境相关。
- 手动流程会拖慢合规性监控、修复和审计工作，导致人员效率低下、策略执行不一致，并进一步增加出现合规问题的风险。
- 用于安全防护与合规性管理的工具不统一，这可能会导致运维效率降低，且难以制定一致的自定义策略。

合规性管理工具的主要功能

为了提高效率，企业组织需要定义和应用上下文策略，以维护系统完整性并在更短的时间内生成符合审计要求的报告。在评估统一的合规性管理工具时，应寻找具有以下功能的工具：

- **利用分析功能**，以省时高效的方式持续识别合规风险。
- **自动修复**不合规的系统。
- **提供完整视图**，帮助了解跨多个环境的当前合规态势。

2 *PeerSpot 报告。“红帽卫星提高安全性和基础架构管理效率的七种方式”，2024 年 4 月 24 日。*

Zoom 携手红帽打造可靠的企业系统

“我们每周都必须对环境中的每个系统进行安全扫描。这些扫描程序会列出操作系统上软件包中存在的漏洞。每当出现这种情况，我们都能立即访问红帽网站，获取关于漏洞的完整说明，这有助于我们判断自身是否受到影响。任何其他 Linux 发行版均无法做到这一点。如果没有红帽的支持，运营一个生产级的政府环境将很快变成一场噩梦，因为我们每月都得自己完成所有这些研究工作。”

Ryan Kimbrell
Zoom
高级云运维工程师

- **可生成自动化合规报告**，满足审计要求和受众需求。
- **提供专家建议**和有针对性的指导，助力跨多个环境修复不合规的系统。

下一章将探讨在动态企业环境中更有效地管理安全防护与合规性风险的最佳实践。

第 5 章
最佳实践和工具推荐

定期分析系统

通过日常监控，企业组织能够在漏洞与合规风险导致业务运营中断或数据泄露之前，及时发现它们。使用来自操作系统和应用供应商的最新安全防护数据来提高分析准确性，并针对特定环境制定自定义安全防护策略。

- 对于列入 CISA 已知被利用漏洞（KEV）目录的漏洞，攻击者开始大规模利用这些漏洞的中位时间仅为 **5 天**。[3]

经常修补并全面测试

确保系统处于最新状态，这有助于提高安全性、可靠性、性能及合规性。常规补丁应定期应用，而关键错误和缺陷则需要立即处理。在将修补后的系统重新投入生产环境之前，对它们进行验收测试。

部署自动化和经批准的 AI 工具

随着企业组织的基础架构规模不断扩大，手动管理变得越来越困难。使用自动化和 AI 驱动的工具，以简化监控、加速修复，并确保报告的一致性。

- 与未使用 AI 和自动化解决方案的企业组织相比，使用这些解决方案的安全团队，数据泄露处理时间缩短了多达 80 天，且平均数据泄露成本降低了 **190 万美元**。[1]

连接工具并统一流程

通过应用编程接口（API）集成不同的平台管理工具，以保持跨分布式环境的可见性。通过减少接口数量，可简化运营流程，并确保更加一致和可靠的安全态势。

- 安全系统具有复杂性，使数据泄露成本平均增加 **207,914 美元**。[1]

采用一致且持续的安全防护策略

要想实现有效的安全防护，需要一种能够整合人员、流程和技术的全面方法。深度防御策略通过在所

3 *Verizon Business。“2025 年数据泄露调查报告”，2025 年。*

有层级（包括操作系统、容器平台、自动化和 AI 工具、软件即服务（SaaS）解决方案以及云服务）应用安全控制措施，从而最大限度地提升防护能力。

- **63% 的企业组织**缺乏正式的 AI 治理策略，这直接导致了更高的数据泄露成本。[1]

随时了解企业组织在安全防护与合规态势方面的需求，这是改进的第一步。理想的安全防护与合规性工具，应包含以下几项关键特性和功能：

- **主动分析：**能够提供主动式、自动化分析的工具，可确保系统得到定期监控，并在出现问题时发出警报，而无需持续的人工监督。
- **按优先级响应：**工具应提供规范的修复步骤，并根据潜在影响确定操作的优先级，从而使团队能够充分利用有限的修补窗口。
- **可定制的结果：**为减少误报，应寻找允许企业组织 IT 主管定义业务上下文的工具，确保检查仅针对相关系统和工作负载。部分漏洞与合规性检查可能不适用于某些系统，因为这些系统具有特定的配置、用途或工作负载。
- **直观的报告：**能够为不同受众生成清晰、直观的补丁状态与政策合规性报告的工具，可提高可审计性并促进利益相关方达成共识。
- **统一的界面：**能够管理 IT 环境多个层面的工具，可简化安全防护运维，并且有助于更好地了解当前的安全防护与合规性态势。实现工具统一，这还可为扫描和修复指导提供更丰富的上下文信息。
- **切实可行的分析洞见：**可提供针对 IT 环境量身定制信息的工具，有助于快速识别受影响的系统以及漏洞的潜在影响，从而帮助企业组织确定修复措施的优先级并制定修复计划。

第 6 章

在红帽的帮助下提升安全性与合规性

红帽采用全面的、具有前瞻性的方法来管理安全防护与合规性风险，从裸机和虚拟化服务器到私有云、公共云、混合云和边缘部署，全面提升整个 IT 环境的速度、可扩展性与稳定性。通过协调人员、流程和技术，红帽® 平台助力企业组织提高运营效率、推动创新，并提升员工满意度。

这一战略的核心是红帽企业 Linux，它为现代 IT 提供持续稳定、智能化的运营基础。这种跨基础架构的一致性，使 IT 团队无论在任何位置，都能使用相同的工具来部署应用、工作负载和服务。

安全防护是红帽企业 Linux 架构和生命周期的重要组成部分。多层数据泄露防御体系利用自动化、可重复的安全控制措施来降低漏洞暴露风险，而关键安全升级与实时补丁（包含在红帽企业 Linux 订阅中）则有助于确保 IT 环境受到妥善保护，而不会造成停机。

Zoom 如何满足 FedRAMP 和 DoD 的要求

“合规说到底就是纪律。而红帽恰恰拥有我们所需的纪律性……”

John Keese
Zoom
技术合规主管

“改用红帽企业 Linux 后，我们可以比以前使用 Linux 发行版时，更快地发现和调查错误及漏洞。” [4]

Yuki Miyamoto
Square Enix Co., Ltd.
技术部
IT 基础架构/业务在线基础架构系统

集成的管理工具和 AI 赋能的智能分析使红帽企业 Linux 的能力得到进一步增强，让用户能够全面了解整个混合环境，从而有效管理安全防护与合规性。企业组织可从以下方面获益：

- **减少警报疲劳：**利用可配置的工具和基线减少误报，从而准确呈现 IT 基础架构的当前状态。
- **主动修复：**通过自动化提高配置和修补的准确性，减少人为错误，无需联系技术团队。
- **全面的可见性：**使用漏洞和恶意软件检测功能，扫描系统中的通用漏洞披露（CVE）和恶意软件签名，同时通过可自定义视图，以恰当的速度在恰当的时间将正确数据传递给目标受众。
- **简化集成：**利用本地部署和软件即服务（SaaS）部署选项，结合 API，确保红帽企业 Linux 能与现有安全、合规及管理工具和接口顺畅连接。这种简化的集成由庞大的资源库提供支持，该库全天候提供有针对性的详细信息。
- **资源优化功能：**帮助企业组织的 IT 团队根据计算、内存和性能指标，选择合适的公共云部署规模。
- **预先防御机制：**借助经美国国家标准与技术研究院（NIST）认证的抗量子算法和机密计算[5]，为应对未来量子计算机的威胁做好准备，确保敏感数据在使用过程中受到保护。

阅读什么是机密计算?

第 7 章

充分利用集成工具

红帽管理工具基于多年的 Linux 开发和支持经验。这些红帽工具协同工作，可简化 IT 管理，为 IT 团队节省宝贵的时间，同时确保整个环境始终安全至上、经过优化且稳定可靠。

分析、观察和管理红帽系统

红帽提供值得信赖的 Linux 平台，以及安全至上的运营与创新所需的集成管理工具和服务。

4 *红帽案例研究。“Square Enix 简化了在线游戏基础架构的管理”，2023 年 5 月 17 日。*
5 *红帽概述。“什么是机密计算?”2025 年 10 月 22 日。*

- **红帽 Lightspeed：**红帽 Lightspeed（以前称为“红帽智能分析“）包含在订阅中并作为服务提供，它可以持续分析平台和应用，以预测风险、推荐操作并跟踪成本。它使企业组织能够监控 IT 效率、稳定性和性能，同时管理混合云环境中的安全防护与合规性风险。

进一步了解红帽 Lightspeed

简化并自动化系统管理

采用有效的自动化管理方法和工具，这对于保护企业组织安全至关重要。

- **红帽卫星：**该平台提供具有数字主权和自主管理能力的红帽企业 Linux 管理方案。该管理工具可以在几分钟内完成红帽企业 Linux 系统的配置与部署，通过在隔离环境中进行内容和补丁管理来扩展红帽安全至上的供应链，并持续监控合规性。借助集成式分析功能，IT 安全团队能够预先识别问题并获取修复建议，同时支持大规模自动化修复。

进一步了解红帽卫星

第 8 章

Zoom 携手红帽打造可靠的企业系统[6]

Zoom Video Communications, Inc.（Zoom）是一家全球化的通信技术公司，自 2011 年以来一直致力于创新。该公司最初以视频通信解决方案起家，后来不断发展壮大，提供更多产品与服务，例如 Zoom for Government。为了遵守联邦风险与授权管理计划（FedRAMP）和美国国防部（DoD）严格的安全要求，Zoom 采用红帽企业 Linux 来运营其平台。该公司还依靠红帽 Ansible® 自动化平台和红帽卫星来实现基础架构自动化，以保障合规功能并管理部署。

Zoom for Government 依靠红帽企业 Linux 及其他红帽工具来确保常规裁决流程顺利进行，几乎每一步都有红帽参与。Zoom 数据中心运营主管 Zak Peirce 对采用红帽解决方案毫不犹豫。Peirce 表示：“我一直是红帽的忠实用户。若要运行一个稳固的企业系统，我会选择红帽作为我的企业平台。”

Peirce 接着分享了他为何认为整个生态系统如此有用。“我知道，当我更新 IdM 后，它能与我的红帽系统兼容。我还知道，当我更新系统安全服务守护进程（SSSD）代理后，它也能正常运行。此外，能够使用红帽卫星来托管这些软件包，使系统保持最新状态，并管理安装到系统中的具体软件包，这有助于我测试系统，并确保开发阶段和生产阶段保持一致。所有这一切都有助于我们顺利开展运营工作。”

在与美国政府合作时，红帽网站上的资源（包括通用漏洞披露（CVE）数据库和红帽安全公告（RHSA）具有不可估量的价值。

6 *红帽案例研究。“Zoom for Government 通过红帽平台增强安全性”，2023 年 3 月 10 日。*

“我们每周都必须对环境中的每个系统进行安全扫描。这些扫描程序会列出操作系统上软件包中存在的漏洞。每当出现这种情况，我们都能立即访问红帽网站，获取关于漏洞的完整说明，这有助于我们判断自身是否受到影响。任何其他 Linux 发行版均无法做到这一点。如果没有红帽的支持，运营一个生产级的政府环境将很快变成一场噩梦，因为我们每月都得自己完成所有这些研究工作。”

Ryan Kimbrell,
Zoom 高级云运维工程师

从您的数据中获取更多价值

企业依赖于其 IT 基础架构和应用的稳定性和可靠性。采取积极主动的方法来管理安全漏洞及合规风险，这是保护企业组织资产的最有效途径。

红帽提供值得信赖的 Linux 平台，以及安全至上的大规模运营所需的集成管理工具和服务。

利用红帽 Lightspeed 分析企业组织风险

- 进一步了解红帽 Lightspeed
- 阅读这份红帽概述[7]，了解红帽 Lightspeed 如何帮助简化合规性和漏洞管理

利用红帽卫星实现大规模管理

进一步了解红帽卫星

进一步了解红帽卫星的商业价值[8]

---

7 *红帽概述。“借助红帽 Lightspeed 简化 Linux 管理”，2025 年 5 月 2 日。*

8 *IDC 商业价值白皮书，由红帽赞助。“红帽卫星的商业价值”，2024 年 7 月。*

关于红帽

Red Hat 是領先全球的企業開放原始碼軟體解決方案供應商，透過在社群上集思廣益，提供效能卓越且可靠的 Linux、混合雲、容器及 Kubernetes 技術。Red Hat 致力協助客戶開發雲端原生應用程式，整合既有與全新 IT 應用程式，自動處理並管理複雜的環境。Red Hat 是深受《財星》世界 500 強公司信賴的顧問，能提供獲獎肯定的支援、訓練及諮詢服務，為各項產業帶來開放創新的優勢。Red Hat 作為全球企業、合作夥伴與社群的聯繫中樞，致力協助組織成長與轉型，迎接數位時代的未來。

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
#US52390824_0426

版权所有 © 2026 Red Hat, LLC。红帽、红帽 logo 和 Ansible 均为红帽或其子公司在美国和其他国家/地区的商标或注册商标。Linux® 是 Linus Torvalds 在美国和其他国家/地区的注册商标。