

O'REILLY®
Report

重新定义操作系统选择

将 Linux 战略转化为竞争优势

Ned Bellavance 和 Chris Hayner

提供方：



将您的操作系统选择转化为 竞争优势

借助现代平台推动快速创新。了解红帽企业 Linux 如何提供敏捷性和控制力，以适应不断变化的需求。

探索更多



重新定义操作系统选择

将 Linux 战略转化为竞争优势

Ned Bellavance 和 Chris Hayner

O'REILLY®

重新定义操作系统选择

作者：Ned Bellavance 和 Chris Hayner

版权所有 © 2026 O'Reilly Media, Inc.保留所有权利。

由 O'Reilly Media, Inc. 出版，地址：141 Stony Circle, Suite 195, Santa Rosa, CA 95401。

O'Reilly 图书可用于教育、商业或促销推广用途。大部分书目亦提供在线版本（<http://oreilly.com>）。如需了解更多信息，请联系我们的企业/机构销售部门：800-998-9938 或 Corporate@oreilly.com。

策划编辑：Megan Laddusaw

封面设计师：Ellie Volckhausen

开发编辑：Gary O'Brien

内页设计师：David Futato

制作编辑：Jonathon Owen

内页插画师：Kate Dullea

文字编辑：Stephanie English

2026 年 2 月：第一版

第一版修订历史记录

2026 年 2 月 13 日：首次发布

O'Reilly 徽标是 O'Reilly Media, Inc. 的注册商标。“重新定义操作系统选择”这一标题、封面图片及相关商业外观均为 O'Reilly Media, Inc. 的商标。

本作品所表达的观点仅代表作者本人，不代表出版方的观点。虽然出版商和作者已尽最大努力确保本作品所含信息和说明的准确性，但出版商和作者对其中任何错误或遗漏概不负责，包括但不限于因使用或依赖本作品所导致的损害赔偿。使用本作品中所含信息和说明的风险，均由您自行承担。如果本作品所含或描述的任何代码示例或其他技术受开源许可或第三方知识产权约束，您有责任确保您的使用行为符合此类许可和/或权利的规定。

本作品是 O'Reilly 与红帽合作成果的一部分。查看我们的[编辑独立性声明](#)。

979-8-341-66786-0

[LSI]

目录

简介vii

1. 操作系统选择的战略转变 1

 重要主题和变化 1

 操作系统选择的重要性 2

 结论 7

2. 从问题到解决方案 9

 加速创新策略 9

 结论 13

3. 现代 Linux 平台15

 革新操作系统部署 16

 AI 辅助系统管理 17

 机群管理工具 18

 企业级安全防护 19

 扩展的硬件和软件支持与认证 19

 结论 20

4. 后续步骤21

 确定影响最大的压力因素 21

 将您的工作负载与能力需求进行匹配 22

 评估业务价值 22

 验证供应链安全性和长期可行性 22

 结论 22

简介

一直以来，企业组织在改变操作系统（OS）部署策略方面进展缓慢。企业通常会根据简单的技术要求和偏好来运行某一种操作系统，并且只有在绝对必要时才会运行多个操作系统。这种改变可能是由关键应用的技术要求所驱动，也可能是因操作系统即将终止支持而被迫升级。这使得企业组织普遍认为，操作系统选择是一个无需过多讨论的既定事实——更多是出于技术上的必要性。然而事实上，现代全球技术格局瞬息万变，这使得操作系统选择转变为一项战略要务。

如今，企业深陷于前所未有的变革洪流，仅凭过往经验已难以驾驭。短短数年间，容器化等技术使工作流变得更加灵活，应用部署工具集和策略发生了根本性变化，而 AI 和量子计算等技术更是彻底颠覆了以往的认知。当企业重新评估自身技术需求时，他们也必须调整操作系统选择策略，以应对当下更为动荡的局势。

本报告探讨了这一新战略要务背后的驱动因素。我们借鉴了包括调查和分析机构报告在内的实证研究，以确定现代 IT 企业组织面临的具体挑战。正如您将看到的，这一变化由一系列极具现代特征的战略因素所驱动。新的应用、硬件和平台不断涌现，这一切都是为了跟上不断加速的创新步伐。除了创新之外，企业组织还必须应对不确定的经济形势、复杂的现代网络安全威胁，以及数据主权和供应链验证等地缘政治问题。

我们将展示企业如何将操作系统选择从单纯的运营需求，重新定义为一种战略性的竞争优势。

操作系统选择的战略转变

现代 IT 环境提出多项要求，推动企业操作系统基础架构和应用部署策略发生重大根本性转变。在当今技术格局迅速演变的背景下，人们正在重新审视一成不变且未经审查的操作系统生态系统所带来的传统优势，例如简化管理和部署、减少培训需求等。企业组织逐渐认识到，僵化的操作系统偏好更多是负担而非优势；相较于维持现状，灵活性和快速提升能力显得更为重要。不考虑这一转型路径的企业，将面临被准备更充分、应变能力更强的竞争对手甩在身后的风险。此外，直接影响采购决策的地缘政治因素，使得不断变化的技术环境变得更加复杂。

重要主题和变化

目前，企业的操作系统选择决策受到几个主题的影响。这些并非孤立的趋势，而是相互关联的驱动力，它们正在重塑企业组织制定基础架构策略的方式。我们将在本报告后续部分中对这些主题逐一进行详细探讨。

创新加速：创新加速是操作系统选择决策的首要驱动因素。简而言之：AI、自动化、边缘和云计算、物联网及新型定制硬件发展速度极快，并非所有企业都能跟上步伐。随着技术以前所未有的速度演进，企业开始担忧技术债务问题。新兴技术过去需要数年才能达到生产就绪状态；如今，从创意构思到部署阶段，可能仅需数月。这正是促使企业寻找有助于提高竞争力的操作系统的主要驱动因素。

全球不确定性：近年来，全球供应链的不确定性持续加剧，这促使企业不再局限于本地环境，而是将目光投向提供所需工具、软件和服务的整个供应链体系。鉴于供应链中断的可能性始终存在，许多企业已将单一供应商关系（尤其是与外国供应商的关系）视为潜在风险。这些担忧使得供应商多元化既成为一种风险缓解措施，也成为一项战略要务。

经济压力：经济压力日益加剧，优化和投资回报率（ROI）成为关注焦点。投资回报率不仅体现在财务层面，技能短缺与预算限制同样令人担忧，这使得操作系统的选择变得更加复杂。在过去，一名管理员精通多种操作系统的情况非常罕见。对于企业来说，配备多名高级专家是不现实的，这也是单一操作系统环境成为默认选择的原因之一。因此，操作系统是否切实具备易用性，这成为一项首要考量因素。

安全问题：安全问题重新定义了基础架构要求。更多系统的部署速度比以往任何时候都快，这导致企业的攻击面急剧扩大。此外，在 AI 实施、现代网络威胁及监管合规性交织的新环境下，我们需要采取现代化的应对方法。

最后，AI 彻底颠覆了我们以往对计算机工作的所有认知。借助大语言模型（LLM），管理员或开发人员创建新应用的速度也达到了前所未有的水平。无论您是简单地连接到 LLM 进行提问、创建自己的聊天机器人，还是构建复杂的代理式 AI 工具，都需要一款最适合的操作系统。

操作系统选择的重要性

正如我们所见，在选择操作系统时需要考虑的因素比以往任何时候都多。若操作系统选择不当，可能会限制对关键 AI 功能的访问，影响性能，并使企业组织暴露于安全风险或供应链漏洞之中。相比之下，若能选择合适的操作系统，这将会成为进入这个快节奏、现代化且高效世界的跳板。经过深思熟虑的战略性操作系统选择，能够释放竞争优势和数字化灵活性，这两者对于希望把握新兴技术机遇的企业而言都至关重要。

现在，让我们更详细地探讨下各项选择因素。

创新加速

技术发展日新月异，这从根本上改变了围绕基础架构决策的标准模式。本节将探讨这些加速因素，以及企业如何据此调整其部署策略的制定方式。

更快的技术周期

正如麦肯锡发布的《2025 年技术趋势展望》报告中所述：“全球技术格局正经历重大转变，这主要得益于技术领域的快速创新。”¹简而言之，技术发展速度已达到前所未有的水平，并且还将持续加快。以云采用率为例。在许多情况下，企业起步缓慢，先在云端部署开发/测试环境，然后再历经数年逐步过渡到完整的生产工作负载。再来看看生成式 AI（GenAI）或代理式 AI，它们在短短数月内便从理论构想落地为企业级产品。

在传统的基础架构策略中，企业会沿用现有的操作系统选择，并设法让新技术在现有环境中运行。当今全球市场的发展速度实在太快，这种做法已不再现实。开发团队越来越多地尝试新平台，寻找能与最新技术完美契合的平台，而不是试图改造旧的基础架构以勉强维持运转。这正是推动操作系统实验的强大驱动力：如果当前操作系统无法满足开发人员和工程师的需求，他们便会开始寻找能够满足需求的操作系统。

有针对性的投资

新技术是操作系统审查和变更的首要驱动力。这反映了我们之前讨论的趋势：开发人员和管理员寻求最佳的基础架构，而非固守内部惯用的基础架构。但这并不意味着企业组织愿意投入无限的资源；他们强烈希望首次就将有限的资金投入到的地方。操作系统选择不仅关乎单台服务器的决策，它更是宏大平台架构的一部分，正因如此，这项投资决策的意义便愈发重大。

¹ 麦肯锡咨询公司，“McKinsey Technology Trends Outlook 2025”（《麦肯锡 2025 年技术趋势展望》），2025 年 7 月 22 日，<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech>。

这些投资旨在满足业务需求。技术发展日新月异，企业组织必须紧跟技术发展的步伐。例如，企业组织逐渐认识到，AI 能力需要专门的基础架构和开发工具作为支撑，而他们的标准操作系统可能难以胜任这项任务。为了满足 AI 工具的需求，企业不得不构建庞大的基于 GPU 的服务器集群。具备前瞻性思维的企业组织深知创新步伐之快，并积极调整他们的基础架构策略，以最大限度地释放潜能。企业希望能够以足够快的速度发展演进，从而自信地挖掘技术的最大价值，而非仅仅完成部署并寄望于一切顺利。

全球不确定性

全球不确定性已成为影响技术战略的一个重要因素。地缘政治紧张局势引发经济担忧，这对决策的影响比以往任何时候都更为显著。因此，企业不能仅从技术角度孤立地看待供应商，现在还必须结合地缘政治因素来评估自己的选择。企业组织对这些不确定性的担忧程度比以往任何时候都要高。²企业组织需要关注关税、法规以及出口管制。这些持续且充满不确定性的地缘政治紧张局势威胁着全球供应链，可能促使企业将其技术生态系统保留在本国境内。

关税和出口管制

关税问题及由此可能引发的汇率变动，正在改变企业对跨境采购的看法。如果市场出现剧烈波动，导致各国之间的汇率发生变化，那么一份长期合同在签署一年后，实际成本状况可能会截然不同。这是目前影响整个 IT 战略的关键问题。将经济维度纳入供应商选择的考量，这与以往关于 IT 采购决策的思维方式存在显著差异。

² 麦肯锡咨询公司，“Navigating the New Geopolitical Uncertainty”（应对新的地缘政治不确定性），2025 年 1 月 16 日，<https://www.mckinsey.com/capabilities/geopolitics/our-insights/navigating-the-new-geopolitical-uncertainty>。

数字主权

地缘政治压力不仅限于经济层面，各个国家/地区的监管要求各不相同，这改变了客户与供应商之间的合作模式与权责关系。这一点在云计算领域表现得最为明显，面对《通用数据保护条例》（GDPR）等法规带来的监管压力，企业要求采用“仅限于欧盟境内”的云服务，以确保数据留在欧盟境内。在此之前，相关争议已持续多年，导致许多企业开始积极寻找更符合其特定监管需求的云服务供应商。

经济不确定性

经济压力始终对 IT 领域存在影响。在快速变革与全球性压力的双重裹挟下，情况变得更加复杂。由于资金有限，且存在技能人才短缺的问题，这意味着即便企业有预算增设新的管理员岗位，也未必能找到合适的人选来填补空缺。

预算限制这一问题，使成本优化成为操作系统选择的首要考量因素。企业越来越关注投资回报率（ROI）和资金使用效率。重视成本优化，这无论从财务支出还是投资回报率的角度来看，都对操作系统的选择具有重要意义。

安全防护和数据泄露

多年来，IT 资产的安全性一直是人们关注的首要问题，Stack Overflow 发布的《2025 年开发人员调查》等调查结果明确显示，安全防护、漏洞分析和测试是开发人员最为关注的问题。“安全性与隐私问题”是开发人员放弃采用特定技术的首要原因。

供应链攻击

了解软件来源只是其中一个方面；企业越来越需要了解软件所依赖的各个组件来自何处。这本身就可能构成安全隐患，如果对某个主要软件产品至关重要的次要软件包遭到入侵，整个企业组织都将面临风险。最著名的例子可能是 2021 年的 SolarWinds 黑客攻击事件，由于 SolarWinds 供应链存在安全漏洞，无数 SolarWinds 客户遭遇数据泄露。然而，依赖项问题依然普遍存在。最近，JavaScript 注册表 npm 遭受了一次供应链攻击，导致一些本应安全的软件包被部署到用户设备上，用于挖掘加密货币。

事实证明，AI 既会带来安全风险，也会提高生产力，让业务运作变得更高效、更智能。过去几年间，基于 AI 的攻击呈爆发式增长，且未有减缓迹象。征信机构 Experian 近期发布的一份报告指出，AI 构成的威胁已足够严重，预计到 2026 年，它将取代人为失误，成为数据泄露的首要原因。³

对量子加密的担忧

过去几年，人们已经识别并研究了量子计算带来的新兴威胁。令人担忧的是，由于量子计算机采用完全不同的方法来解决传统加密问题，最终（可能在十年内，但这一时间框架存在争议），所有现有的加密算法都将在几秒钟内被破解。这将使所有采用“传统方式”加密的文件和数据存储完全暴露于风险之中。黑客们深知这一点，尽管目前他们还无法破解加密，但他们一直在尽可能多地下载数据。这种安全风险被称为“先收集，后解密”。

后量子密码学（PQC）是旨在抵御量子计算机强大算力威胁的下一代加密技术。这种密码学是计算机科学领域的一个新兴研究课题，目前并非所有操作系统都已采用该技术。采用 PQC 算法对技术进行加密，意味着黑客将无法实现“先收集、后解密”的图谋。

AI

AI 已成为推动众多技术采购决策的主导力量。这一趋势已显现多时，且势头似乎毫无减弱迹象。值得注意的是，AI 及相关技术正日益主导着操作系统的选择。

氛围编程

得益于 AI，操作系统的现代用例已然改变。如今，即使没有专业或技术背景的人，也能进行编程、数据分析和业务分析。举个例子，氛围编程就是一种基于 AI 的应用创建方法，用户无需成为程序员或应用开发人员即可使用。市场越来越青睐能够与支持此类行为的 AI 辅助开发工具协同运作的操作系统。

³ Experian, 2026 Data Breach Industry Forecast (《2026 年数据泄露行业预测》), 2025 年 12 月 5 日, <https://www.experian.com/thought-leadership/business/2026-data-breach-industry-forecast-report>.

硬件加速

此外，AI 仍然存在需要操作系统具备广泛能力的传统用例。执行推理、模型训练或托管基于大语言模型（LLM）的聊天机器人等任务时，操作系统必须能与 GPU 及其他自定义硬件高效交互。专用芯片可提供更快、更强大且更灵活的 AI 能力，这使得硬件兼容性成为一个关键的选择因素。AI 驱动的自动化和管理功能，将持续消耗操作系统可用的硬件资源。因此，操作系统与高级硬件交互的能力，将会对操作系统的选择产生影响。

结论

市场环境剧变，促使各企业组织重新评估其操作系统选择，这为探索新的可能性提供了战略性机遇。各企业组织逐渐意识到，这场全球性的动荡与创新浪潮，带来了前所未有的机遇。他们越来越主动地探索新机遇，而非固守那些可能已无法跟上时代变化的现有平台。将操作系统选择从“负担”转变为“机遇”，这代表着提升业务运营效率最重要的机遇之一。这意味着在变革的风暴中寻找最适合的工具，而非简单地沿用旧有的做法。

从问题到解决方案

在第 1 章中，我们确定了推动操作系统选择的几个关键因素：创新加速、全球不确定性、经济压力、安全问题以及 AI 需求。然而，认识到这些压力仅仅是一个开始。IT 主管面临的挑战在于如何有效应对这些压力，同时避免造成新的运营混乱或安全漏洞。成功的企业组织不仅会认识到这些问题，更会以富有成效且具有竞争力的方式做出回应。在本章中，我们将逐一探讨这些挑战，并讨论如何实现从问题到解决方案的跨越。

加速创新策略

加速创新已成为 IT 主管的驱动力。这不仅仅是为了跟上竞争对手的步伐：得益于“先发优势”等概念，行动最快的企业组织往往能获得最大的回报。这对操作系统选择策略具有重大影响，因为操作系统正是企业组织实现加速创新的基础。此类创新将引领企业驶入未知领域，因此务必要谨慎行事，并根据明确的需求和效益做出决策。加速创新并不意味着盲目做出改变。现代操作系统需要在支持实验的同时，保障安全性、性能表现与可靠性。

快速而审慎的实验

技术创新不断加速，催生出这样一种市场环境：传统的开发和评估方法已远远跟不上节奏。在应用开发领域，这种趋势已持续一段时间：从基于瀑布式方法的年度发布周期，到基于敏捷方法的软件开发和由 DevOps 驱动的持续交付，再到如今每天多次更新的超高速部署模式。整个技术领域也出现了同样的趋势，IT 主管意识到，他们必须顺势而为，方能保持领先。

创新速度如此之快，这就要求开发与测试周期迅速迭代，同时还要维持不会使企业面临风险的安全基线。为确保实验的有效性，需要成熟的沙盒环境，这些环境既要提供与生产环境类似的条件，又不会使企业数据（或托管应用的操作系统）置于风险之中。这是提供真实测试环境的最有效途径，可用于快速评估实际生产环境下的性能表现。

同样，应用也需要一条从测试到生产的快速、可靠路径。这应该是一个无缝衔接的过程，确保在测试中经过验证的应用能够在生产环境中稳定运行。这不仅仅关乎便利性，整个流程具备可靠性和可重复性，确保了后续升级与初始测试部署同样高效且安全。

鉴于此，在操作系统选择过程中保持审慎开放的心态，显然具有重要价值。在创新加速时代保持敏捷性，这无疑是一项明确的战略优势。操作系统最终会托管相关应用，而由于应用需求变化如此之快，企业组织需要确保操作系统能够跟上步伐。这种细致入微的方法已在 IDC 和麦肯锡等公司的研究与分析中得到印证。麦肯锡咨询公司于 2024 年 6 月指出：“事实上，并不存在放之四海皆准的方法。企业应当在追求创新的同时，兼顾维护稳健可靠的技术基础架构的需求。”¹

¹ 麦肯锡咨询公司，“Rethinking Conventional Wisdom: Future of Digital Tech Infrastructure”（重新审视传统观念：数字化技术基础架构的未来），2024 年 6 月 26 日，<https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/rethinking-conventional-wisdom-future-of-digital-tech-infrastructure>。

尽管如此，在选择工具和技术时仍需保持审慎的态度。为改变而改变，这本身就是一种风险。若在缺乏监管的情况下更改操作系统这类基础组件，只会徒增复杂性，却看不到明显的收益。支持此类变更的最有力证据，是那些能证明在提升企业组织能力具有明显优势的证据。这些优势必须能够被验证，而不能仅仅因为新操作系统是新的就盲目采用。就此而言，企业组织不仅要审视当前的能力，还需考量操作系统的未来潜力和稳定性。

安全至上的架构

技术创新步伐不断加速，这不仅仅惠及合法企业。网络安全威胁也在不断演变，如果企业组织未能确保自身安全，便极易遭受攻击。**CrowdStrike** 发布的《2025 年全球威胁报告》等市场研究明确显示，网络威胁的演变速度快于网络防御能力的提升速度。现代威胁形势复杂多变，这带来了前所未有且不断变化的挑战，而许多传统的安全框架和 IT 工具原本并非为应对这些挑战而设计。做好应对这些现代威胁的准备，现已成为一项战略要务。

在考虑实施新的操作系统时，务必要将这种安全架构纳入考量。未将安全性问题和验证环节纳入操作系统选择流程的企业组织，将面临双重风险：一是系统上托管的应用；二是系统本身的安全性与其可靠性。在撰写本文之时，这一问题尤为突出，因为操作系统供应商越来越多地在其操作系统中添加 AI 功能，并赋予这些功能巨大的访问权限，以便以自动化方式执行系统管理任务。

数据安全至关重要

这引出了一个核心要点：任何操作系统都需要提供一个能够让应用安全运行、数据安全存储的环境。企业必须确保运行的所有内容都能保持安全，无论是操作系统的内置组件还是操作系统托管的应用，皆如此。必须考虑以下三类数据的安全性：

静态数据

指存储起来以备将来使用的数据。

动态数据

指在不同系统之间，或在同一系统内的不同应用之间，以某种方式进行通信的数据。

使用中的数据

指计算平台正在积极处理的数据。

通常，静态数据和动态数据的安全性可通过加密来保障。而保护使用中的数据则更具挑战性。现代操作系统架构通过整合可信执行环境（TEE）来解决这一问题。这是系统中仅限高度可信软件运行且只能通过严格控制的机制进行访问的区域。在 TEE 内运行的任何内容，通常都无法从外部访问。这可以是基于硬件和软件的解决方案，覆盖范围通常不局限于一台服务器，并且需要保持最新的驱动程序和兼容性，以免丧失功能。具体实现方式因供应商而异，本报告中不做讨论，但确认应用能够在如此安全的环境中运行至关重要。

AI 工作负载需要的不仅仅是保护

尽管各类计算工作负载都需要满足前文所述的数据保护和数据主权保障要求，但 AI 工作负载还因另外两个原因而特别容易受到威胁：一是新颖性；二是数据密集性和计算复杂性。

AI 工作负载具有新颖性，这意味着生产环境中的工作负载尚未像标准工作负载那样经过全面测试。安全防护是一项协作性工作，整个市场对工作负载的测试和 QA 规模，远非任何单一供应商所能企及。这不仅适用于产品本身，也适用于产品的配置和使用方式。Tenable 在其 *《2025 年 Tenable 云安全风险报告》* 中指出，支持 AI 的云工作负载比其他工作负载更容易受到攻击。鉴于 AI 具有数据密集特性，再加上配置错误和漏洞长期存在，无论工作负载托管于何处，都要求我们在网络安全方面保持更高的警惕性。

企业组织在评估操作系统时，需要考虑 AI 相关风险。若未能做到这一点，将引入未知级别的风险，可能危及当前及未来的工作负载。

结论

要以审慎的态度来考量操作系统决策，需要从根本上改变企业组织评估技术的方式。本章所阐述的各项挑战，为通过做出正确选择来最大化竞争优势提供了必要的框架。在本报告的最后，我们将探讨一个涵盖所有这些决策的决策框架。目前，在操作系统部署方面亟需新的思维模式已不言而喻——现代挑战，当以现代解决方案应对。积极迎接挑战并进行战略性思考的企业组织，将能够更好地利用新技术，并最大限度地提高竞争优势。

现代 Linux 平台

现代企业在很大程度上已将服务器运维标准化为基于 Linux。这一点在过去至少十年的众多研究中得到了印证。举个例子，SQ Magazine 在 2025 年 8 月的报告中指出，61.4% 的大型企业至少有一项任务关键型工作负载在 Linux 上运行，78.3% 的面向互联网的 Web 服务器在 Linux 上运行。¹Linux 目前在市场上占据主导地位，这是长年累月持续增长的结果，且这一趋势毫无放缓迹象。

然而，在许多情况下，这些论述从未涉及具体的发行版，导致许多决策者误以为“所有 Linux 都一样”。事实并非如此。虽然所有 Linux 发行版都使用基本的 Linux 内核，但具体内核部署方式以及相关工具和应用生态系统可能存在天壤之别。

企业组织需要做的是，找到他们正在评估的操作系统的关键差异化因素。许多现代操作系统已具备先进功能，但不同操作系统对这些功能的处理方式各不相同，并且有些功能并非所有系统都支持。一些值得关注的、最具价值的功能包括：现代安全部署模式、集成 AI 的系统工具、机群管理工具、企业级安全防护，以及更广泛的支持服务与合作伙伴认证。此外，评估操作系统的各项能力时，还需结合未来将在该操作系统上运行的工作负载的需求来综合考量——这里所说的能力是指符合现代需求的顶尖能力。

¹ Robert A. Lee, “Linux Statistics 2025: Desktop, Server, Cloud & Community Trends” (《2025 年 Linux 统计数据：桌面、服务器、云及社区趋势》), SQ Magazine, 更新于 2025 年 11 月 18 日, <https://sqmagazine.co.uk/linux-statistics>.

革新操作系统部署

多年来，操作系统的部署方式并未发生太大变化。传统的部署方式通常是借助某种安装程序，将内核及其他工具分层部署到硬盘上，然后由用户安装应用。软件包管理的问世，堪称应用管理和系统管理领域的一次巨大飞跃，因为它意味着用户在每次安装或更新应用时，无需再从头开始编译代码。

现代 Linux 发行版应提供一种部署模式，使系统本质上成为不可变的容器，可根据需要进行替换。您可以下载新镜像，只需重新启动，即可升级（或降级）系统中需要更改的任何组件。这不仅提供了安全性与可靠性，还能确保机群中的所有系统均运行着预期版本的二进制文件和库。

您可以像管理应用容器（或镜像）一样管理所创建的镜像，但更加精细——可细化至二进制文件乃至操作系统内核本身。与之前基于软件包的更新模型相比，这是一项重大改进。虽然相较于从源代码编译，软件包已属更为优越的部署模式，但其自身也存在兼容性、软件包要求以及潜在版本冲突等问题。基于容器的模型消除了这些问题，因为一切都封装在镜像中。容器内所有组件的版本都将保持一致，这大大减轻了许多系统管理员对配置偏移的担忧。此外，镜像安装速度更快、操作更简单，只需下载、应用并重新启动镜像即可。

镜像还具备安全优势，因为它们是不可变的。这意味着恶意攻击者或恶意软件无法直接修改镜像，也无法替换镜像。由于这些镜像的管理方式与应用容器基本相同，您可以使用 Podman 等标准容器工具或许多其他常见的容器平台来查看镜像。已熟悉应用容器的管理员，面对这些工具自然驾轻就熟，因而能够快速且自信地部署操作系统镜像。

最后，您创建的镜像可在任何环境中使用。无论您是要部署到物理环境、虚拟化环境、云端还是边缘环境，皆可轻松实现。镜像在任何地方的部署和运行方式都是一致的。镜像也将更易于实现端到端的全生命周期管理。[图 3-1](#) 展示了一个镜像模式流程示例，该流程包含三个简单步骤：构建镜像、部署镜像以及部署后的镜像管理。

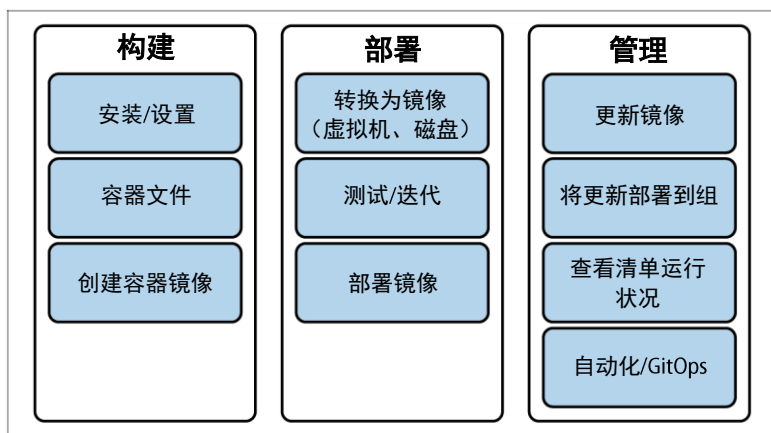


图3-1. 容器化（镜像模式）操作系统部署模式示例

AI 辅助系统管理

许多应用创建者开始将 AI 直接整合到系统管理工具中，例如终端模拟器（提供对命令行的访问权限）。这些工具非常有价值，因为借助这些工具，管理员无需打开浏览器窗口或单独的应用，即可向其选择的大语言模型（LLM）发起查询。接下来合乎逻辑的步骤是：操作系统制造商采取同样的做法，将 AI 直接整合到操作系统中。这样，无论最终用户选择哪种终端，都能从命令行调用 AI 助手。这一功能将极大地惠及各种级技能水平的管理员（尤其是初级管理员），他们可以直接在命令行中向 AI 助手提问，以便随时进行重新评估，并确保自己以正确的方式执行了正确操作。

与所有 AI 工具一样，使用命令行助手时应谨慎。为了获得准确的回答，您可能需要对向命令行助手提出的问题进行调整，尤其是当您要求助手生成代码（例如 shell 脚本）时。

如有疑虑，这些初级管理员最好向资深同事请教，确认 AI 助手给出的回答能否达到预期效果。

该工具的功能十分强大，远不止于理解基础 Bash 脚本——命令行助手可提供关于如何配置应用和服务，以及如何利用操作系统功能进行故障排除的实用提示。至关重要的是，这些助手不仅会针对 Linux 进行通用知识训练，还会针对特定发行版的细节及需

求和要求进行专项训练。在 AI 领域，这种微调已属常见做法：相较于通用大语言模型（LLM），一个仅基于正确类型的文档进行训练、旨在最大限度减少幻觉的定制模型，将使此类工具在内置工具集中脱颖而出，成为关键的差异化竞争优势。

对于诸如安全增强型 Linux（SELinux）和内置防火墙等工具而言，命令行助手将尤为有用。这些工具对系统运维至关重要，但它们十分复杂，且在多数情况下配置更改并不频繁。系统管理员会发现，借助命令行助手，配置这些工具将变得更快、更简单。此外，该 AI 工具将拥有大量经过审查的示例可供比对，从而能够很好地掌握最佳实践，并能指出即使是资深管理员也不易察觉的配置错误。

最后，命令行助手还可用于帮助理解所用工具的结构。例如，如果您想了解如何实施现代基于主机的防火墙，只需询问助手即可。它会根据您提交的内容，查询相关文档资源以获取最佳实践和示例，并生成通俗易懂的英语回答，用以补充说明配置或源代码更改，从而帮助您理解它所生成的建议及原因。

机群管理工具

我们刚才讨论的两款工具功能强大，能够极大地简化单个系统层面的系统管理工作。接下来的工具更进一步，可帮助用户主动管理整个已部署的 Linux 环境。此类工具将与操作系统制造商提供的所有产品建立深度连接，这意味着整个平台可从一个地方集中管理，从而使管理和审计工作变得更加轻松。理想情况下，该工具还应包含规划功能，可帮助企业组织了解他们已部署应用的生命周期，以及这些周期如何影响其环境中运行的系统。这些集成将支持在整个企业组织内实时进行安全防护和配置验证。

路线图功能将提供有关即将发布的应用和操作系统版本的详细信息，使企业组织能够根据预期的新功能来规划升级，而不是在这些新功能发布后被动应对。

机群管理工具还可用于确保系统处于最新状态。协调修补（无论是自动修补还是按计划修补，并确认是否成功）、功能/软件更新或部署，以及集中式配置管理，这些功能使得管理一千台服务器就像管理一台服务器一样简单。

企业级安全防护

一个在设计之初便将安全性纳入考量的操作系统，它所包含的安全优势应远不止前文所述的不可变镜像和配置管理。

在关于未来攻击的讨论中，最受关注的议题之一便是后量子密码学。正如我们在上一章中所讨论的，PQC 为企业组织提供了用于密钥、加密和数字签名的抗量子算法。这有助于确保数据和应用的未来安全性，也是在比较不同操作系统发行版时，值得关注的一项关键特性。

企业级操作系统平台还应提供一套强大的供应链安全防护功能。这不仅局限于操作系统本身，更是一项平台级战略，旨在为希望以 DevSecOps 方式进行部署的开发人员和企业组织赋能。最简单的示例是提供一个可信位置来托管已知安全的应用依赖项，但其作用远不止于此。一个理想的 DevSecOps 平台，应为开发团队提供覆盖所有应用及依赖项的端到端安全管道。

PQC 保护、面向管理员和开发人员的自动化安全防护工具以及主动式软件管理相结合，构建起一个与时俱进的分层防御体系，足以应对当今复杂多变的威胁形势。至关重要的是，这种安全性由企业组织使用的工具和操作系统提供，形成一个功能完备的平台级解决方案，而无需迫使企业组织依赖大量外部第三方安全投资。

扩展的硬件和软件支持与认证

尽管操作系统平台功能强大，但企业组织的正常运转仍离不开外部兼容性。这一点既适用于运行操作系统的硬件，也适用于将在运行系统中使用的第三方软件。

在当今时代，硬件兼容性领域的迭代速度非常快。AI 硬件的演进尤为迅猛，要求操作系统的驱动程序和兼容性必须同步跟进。确保所选发行版在这方面表现卓越至关重要，它应当能够提供最新的 AI 库、驱动程序、应用，以及针对 NVIDIA、Intel 和 AMD 等制造商的硬件优化。然而，除了这三大巨头外，操作系统制造商还需构建一个强大的第三方生态系统，能够以快速、安全且可靠的方式为终端用户提供最新功能。

结论

操作系统的安全防护体系、生态系统与功能集三者协同作用，共同应对本报告开头指出的挑战，即探索其他操作系统已成为一项战略要务。本章中所述的主要功能，无论是从功能上还是从可管理性上，皆可使操作系统从竞争对手中脱颖而出。这些技术进步与强大的合作伙伴计划相结合，构成了具有战略意义的关键差异化优势，在选择新的操作系统平台时不容忽视。

后续步骤

操作系统选择是企业组织的一项基础性决策，关系到竞争地位和内部基础架构管理。面对创新加速、全球不确定性、经济限制、现代安全需求以及 AI 带来的压力，企业组织需要一个专门构建的平台，从而以集成方式应对这些挑战。

对待这一选择，务必要慎之又慎。企业组织在制定关于未来操作系统和平台的决策时，应考虑以下四个关键评估步骤：

- 确定对您的企业组织影响最大的压力因素。
- 将您的工作负载与能力需求进行匹配。
- 评估对业务的整体价值。
- 验证供应链安全性和长期可行性。

确定影响最大的压力因素

企业组织会发现，不同团队面临的压力组合各不相同：AI 产品团队将优先考虑创新与硬件需求，而受严格监管行业则会更加关注安全性与合规能力。企业组织应根据当前及预期的未来重要程度，对各个压力领域（创新加速、全球不确定性、经济限制、安全需求和 AI）进行评级，并利用该评级列表针对未来的评估制定“必备”与“可选”清单。

将您的工作负载与能力需求进行匹配

推动任何需求形成的一个关键因素，在于对企业组织而言最为重要的工作负载。通过工作负载分析，可以明确您的企业组织是更适合针对特定工作负载进行优化，还是采用更广泛的标准化方法。这对于各种规模的企业组织都大有裨益，因为工作负载的数量和重要性不一定与公司规模相关。

评估业务价值

对工作负载进行分析后，企业组织就能清楚地了解服务器数量、员工数量（和技能水平）以及所管理的总工作负载量。这些数据将有助于评估操作系统许可、支持和基础架构需求等直接成本。它还有助于估算间接成本，例如内部专业知识水平、因意外限制导致的工作负载部署延迟，以及因基础架构缺乏灵活性而错失的商业机会。收集到这些数据后，企业便能做出更为明智的战略决策，从而提升运营效率并增强竞争优势。

验证供应链安全性和长期可行性

企业组织在做出操作系统或平台决策时，需要确保所选的操作系统或平台能够长期稳定运行。了解一家企业的历史固然重要，但同样重要的是了解该企业如何审查应用、合作伙伴组合的广度与深度，以及在监管合规性等关键领域和 AI 等先进功能方面的经验与能力。企业组织希望工作负载部署具有多年的生命周期；因此，确保该平台在当下及未来均能处理工作负载至关重要。

结论

在这一过程中取得成功的关键，在于认识到基础架构决策会催生依赖关系。今日所做出的选择，要么助力企业组织取得成功，要么限制企业组织的能力，使项目在未来数年内延迟受阻。如果企业组织能够以战略性眼光对待操作系统选择决策、明确需求并建立评估框架，将可积极追求创新、成功应对不确定性，并在当下及未来持续优化生产力和安全性。

作者简介

Ned Bellavance 是一位拥有超过二十年从业经验的 IT 专业人士和技术教育家。他曾担任过服务台操作员、系统管理员、云架构师和产品经理。近来，Ned 经营着自己的企业 “Ned in the Cloud LLC”，致力于为技术供应商开发课程、主持多档播客节目、撰写书籍，并创作原创内容。Ned 自 2017 年以来一直是微软最有价值专家（MVP），并自 2020 年起担任 HashiCorp 大使。他秉持三个核心原则：拥抱不适、做好失败的准备、心怀善意。

Chris Hayner 是一位经验丰富的 IT 专业人士，在操作系统、基础架构、云计算和网络安全领域拥有数十年的从业经验。他的职业生涯始于数据中心，曾管理过各种各样的系统，包括大型主机、AlphaServer 和白盒 x86 服务器。此后，他的工作范围逐步扩展，覆盖虚拟化、云技术，以及总体网络安全和 IT 战略领域。过去 15 年间，Chris 一直深耕于咨询领域，担任过业务专家（SME）、架构师和分析师。在这些岗位上，他协助数百家企业组织弥合业务目标与 IT 解决方案之间的鸿沟，进而推动创新并取得运营层面的成功。除了持有 CISSP 认证及众多供应商和行业证书外，Chris 还获得了天普大学的工商管理硕士（MBA）学位，这使他兼具专业技术知识与商业敏锐洞察力，形成了独树一帜的综合能力。