以统一平台加强国防能力

核心优势：

- 从战略核心到战术边缘，无间断弹性保障
- 为非联网环境中的任务关键型应用提供一致的平台
- 以统一方法实现自主性与安全性

弥合从战略核心到战术边缘的弹性缺口

政府国防机构面临着一项关键挑战：在从战略核心到战术边缘的整个体系内，保持可靠的运维。受敏捷性、强大安全性和战略自主性等关键需求的驱动，国防领域正经历快速变革，从传统的集中式数据中心转向高度分散的任务就绪型架构。要实现决策优势，即让所有指挥官在所有领域都能比任何对手更快地感知、理解、决策并采取行动，这场深刻变革势在必行。

实现端到端运维弹性迫在眉睫

现代军事任务在庞大的混合云连续体中展开，涵盖私有隔离云、部署式微型数据中心以及无人机、士兵穿戴系统等坚固耐用的战术设备。这种架构是执行多域作战（MDO）的基础，其要求在空、陆、海、太空、网络及电磁波普等作战域实现资产的复杂集成与协同调度。

不过，作战域的拓展也催生了严重漏洞，并显著增加了技术复杂性。孤立的技术和不同的环境可能会破坏运维连续性，而网络安全威胁也在广阔的攻击面上成倍增加。对持续稳定连接的依赖已成为一个关键故障点。在对抗性环境中，边缘设备必须具备自主运行能力，仅通过可信的间歇性链路进行数据同步。核心挑战是在整个领域内实现真正的弹性。如果战术边缘无法独立运维，仅凭中央数据中心的主权控制将远远不够。

国防数字化转型面临的主要挑战

毋庸置疑，混合基础架构带来了出色的灵活性，但国防机构在其数字化转型之旅中仍面临着多项重大阻碍：

- **网络攻击：**国防机构最担忧的，是日益增长的复杂供应链和网络攻击威胁。例如，注入开源库的恶意代码可能会危及整个无人机或车辆编队。同样，中间人（MitM）攻击可能会篡改传输至战术设备的固件更新，从而破坏关键任务。
- **孤立的技术结构：**核心、云和边缘等不同环境往往采用互不兼容的技术堆栈。这种不兼容性迫使机构针对每次部署重新构建解决方案，进而导致碎片化。如此一来，作战人员与工程师必须学习使用 Amazon Web Service（AWS）、Microsoft Azure 和专用战术操作系统等多种平台，严重拖慢任务准备进度。
- **复杂性：**依赖手动流程必然会增加复杂性。例如，在核心和边缘位置之间来回传输数据需要自定义工作流，这会延长部署周期。与此同时，传统安全模型难以适应分布式架构，从而留下可供对手利用的关键漏洞。

红帽官方微博　红帽官方微信

采用统一方法

国防机构亟需一个统一的开放框架，以全面增强自主性与安全性。其目标是打造一个一致的平台，既能在私有云中运行关键应用，在边缘处理 AI 工作负载，还能在前线边缘设备上提供实时决策。真正的现代弹性，在于从核心到前线始终保持全面可靠的作战能力。

红帽如何提供助力

面对碎片化的数字战场，国防机构需要统一的基础架构和可信顾问，以确保从战略核心到战术边缘的弹性。红帽为此提供了至关重要的一致平台。凭借“一次部署，随处运行”的实践理念，红帽加快了作战任务准备进度，使工作人员能够在不同环境中使用熟悉的工具。除了提供一致的体验外，红帽解决方案的另一优势是基于开放标准而构建，其平台可避免对单一供应商的依赖，从而能够更好地与可扩展且灵活的解决方案集成。

军事级安全防护：红帽始终确保其核心平台（例如红帽® OpenShift®）遵守严格的合规性标准，以此实现军事级安全防护。依托红帽可信软件供应链，安全机制得以持续执行，从而提供全面且持续的安全防护方法。该方法集成了 DevSecOps 实践，可加强监管链，并验证软件是否符合机构在安全性、合规性、隐私性和透明度方面的标准。

保障主权：加密认证可验证固件和关键更新是否未经篡改，助力实现更广泛的保障主权目标。该流程可验证数字系统的完整性与可靠性，是红帽平台战略的核心组成部分，旨在验证软件供应链并降低恶意代码注入的风险。

非联网自动化：非联网自动化支持对前线设备进行补丁更新，并与客户已有的任何特定流程集成，而且无需任何互联网连接。红帽凭借红帽 Ansible® 自动化平台，助力实现现代国防所需的可靠自主运维。该平台可帮助管理在拒止、断连、间歇和低带宽（DDIL）条件下运维的设备，而无需依赖易受攻击的外部连接。这种自主性可以保护对已部署软件资产的大量长期投资，最大限度地降低与恶意代码注入相关的安全风险，并在无法获得外部支持时确保关键任务持续运行。

在战略核心层，红帽 OpenShift 等可靠解决方案提供可扩展的主权基础架构。在部署的边缘，精简 OpenShift 集群可以处理关键的智能和 AI 工作负载。在战术前线，轻量级红帽设备边缘解决方案可在坚固耐用的系统上实现超便携、非联网运维。

经验证的国防行业用例

多个国防机构已成功实施红帽解决方案，克服了关键的运维挑战并取得了重大进展：

欧洲空军战场行动优化：某欧洲空军在战场行动中，长期面临因网络中断导致任务受阻的问题。该空军 IT 部门通过在可移植边缘数据中心部署红帽 OpenShift，获得了本地 AI 处理能力，无论网络连接状态如何均能持续运维，同时大幅降低了带宽需求。

无人机系统空中软件更新：在另一项领先能力演示中，一家大型国防承包商展示了对无人机系统执行空中软件更新的能力。借助红帽设备边缘，该承包商在无人机执行任务期间成功部署了 AI 模型升级，在无需中断任务或停机的情况下，显著提升了实时目标识别能力。

国防机构基础架构和部署加速：某国防机构利用 Ansible 自动化平台和红帽 OpenShift 实现平台即服务（PaaS）流程自动化，显著提高了效率。该机构的基础架构部署周期从数周缩短至仅 24 小时，使其能够随时投入作战行动。与此同时，在严格遵守安全协议的前提下，其开发人员规模在一年内扩大近 4 倍。

开始使用

联系红帽，了解如何保护从核心到边缘的国防行动。

关于红帽

红帽通过一流的支持、培训和咨询服务，帮助客户跨环境实现标准化、开发云原生应用，并实现复杂环境的集成、自动化、安全防护和管理。

红帽官方微博

红帽官方微信

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

cn.redhat.com
#3134353_1225