In the Boxing Ring 2026年3月

Network Box 技术新闻

Mark Webb-Johnson *CTO, Network Box*

欢迎阅读2026年3月份的 In the **Boxing Ring**

本月，我们非常高兴地宣布，在我们的安全保障征程中取得了一项重要进展：我们的 Unified Threat Management Plus（UTM+）平台（由 NBRS-8 固件驱动）成功获得了 ISO/IEC 15408:2022 认证。

ISO/IEC 15408 在全球范围内被称为“通用准则”（Common Criteria），是评估 IT 产品安全特性的黄金标准。这一里程碑成果进一步彰显了我们对技术品质的坚定承诺——不仅追求卓越性能，更通过独立权威机构的验证，确保产品符合最严格的国际安全基准。

对于我们的客户和合作伙伴而言，这项认证再次提供了有力保障：我们解决方案的每一层架构，都是建立在信任、透明和经过验证的安全韧性基础之上。

第 2 至第 3 页将对此进行更为详细的说明。

在第 4 页，我们重点介绍了将于本月“周二补丁”（Patch Tuesday）发布的一系列增强功能与修复内容，适用于 Network Box 8和Network Box 5设备，以及我们的云服务平台。

此外，Network Box 发布了年度特别总结报告《Year in Focus 2025》，回顾了过去十二个月中的关键进展与重要里程碑。

同时，在本月的全球安全头条中，我们报道了新近发现的多项漏洞，这些漏洞影响到来自 Fortinet、SolarWinds、Deepseek、Claude AI、Palo Alto Networks 以及 Juniper Networks 等厂商的产品。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
March 2026

本月摘要：

ISO 15408 认证

强化产品安全与服务卓越性

Network Box 自豪地宣布，我们的 Unified Threat Management Plus（UTM+）平台（由 NBRS-8 固件驱动）已正式获得 ISO/IEC 15408:2022 认证。该标准即国际公认的《信息技术安全评估通用准则》（Common Criteria）。

此次认证标志着 Network Box 在持续推进网络安全保障方面取得了又一重要里程碑，同时也体现了我们为各类规模网络提供可验证、端到端安全防护的使命与承诺。

这一成就远不止是获得一枚“质量徽章”那么简单。它以可量化、且经过独立验证的方式，证明了 Network Box 的安全设备在产品设计、构建完整性以及安全功能方面，均符合严格的国际标准。

对于依赖 Network Box 保护其组织网络安全的 IT 管理员而言，这不仅增强了他们对托管服务的信任，也进一步巩固了对支撑这些服务的底层技术的信心。

ISO 15408 的意义

ISO/IEC 15408:2022（通常称为“通用准则”，Common Criteria）为 IT 产品安全功能的评估制定了全球基准标准。它不仅仅测试产品“是否可用”，更验证开发者所声明的安全特性是否经过严格文档化、正确实施，并接受独立评估。

成功通过评估，意味着产品不仅能够按预期执行关键安全功能，同时也表明其背后的组织在整个产品生命周期中采用了规范化、可重复、可审计的流程管理机制。对于像 Network Box UTM+ 这样的网络安全解决方案而言，这涵盖了所有关键安全层面：防火墙策略执行、入侵防御、恶意软件检测以及安全系统更新机制等。

通过获得 ISO 15408 认证，Network Box 为客户提供了更高程度的透明度，使客户能够了解我们的技术是如何设计、构建与管控的。这也在 Network Box 的托管安全服务与其所依赖的硬件和软件之间，形成了完整且闭环的安全保障体系。

构建在经认证的坚实基础之上

多年来，Network Box 一直维持着一套全面的 ISO 管理体系认证，每项认证均针对可靠性与信任体系的不同维度。这些认证包括：

- ISO（质量管理）：确保建立一致、以客户为中心的流程体系，推动产品与服务的持续改进。
- ISO/IEC 20000（IT 服务管理）：为可靠、规范且高效的服务交付提供结构化管理框架。
- ISO/IEC 27001（信息安全管理）：规范 Network Box 如何保护客户数据、实施访问控制，以及降低信息安全风险。
- ISO 31000（风险管理）：建立企业级方法体系，用于识别、评估和管理运营及安全风险。

此外，Network Box 还符合多项区域性及行业框架标准，包括 SSAE 18 SOC 2（美国）、SG CyberSafe（新加坡）、GB 42250-2022（中国）以及 PCI DSS（全球支付安全标准）。这些合规与认证共同构成了我们成熟且稳健的运营基础。

上述认证主要验证的是 Network Box 在安全管理与服务交付方面的体系能力，而 ISO 15408 则独特地聚焦于验证 Network Box 所交付的“产品本身”的安全性。二者相结合，形成了一个闭环的安全保障模型：由经过认证的流程运营经过认证的产品。

为什么产品认证对 IT 管理员至关重要

大多数 IT 管理员都明白，安全服务的可靠性最终取决于其背后的技术实力。管理体系类认证主要证明的是治理结构、政策制定以及流程管理方面的卓越性，但它们无法替代对“实际产品是否正确、可靠地实现安全功能”的直接验证。

ISO 15408 正是弥补这一空白的关键。它向管理员保证，经过评估的设备已依据明确的安全目标进行了系统化测试，例如防止未授权访问、保护数据完整性，以及在高负载或压力环境下确保系统可靠运行。这种保障使管理员在部署Network Box 的 UTM+ 或 NBRS-8 设备时能够确信，其安全基线不仅仅是厂商的声明，而是经过独立验证的事实。

在合规要求严格、风险监管高度敏感的环境中，该认证还能够简化采购与审计流程。客户可将 ISO 15408 认证证书作为公认的产品安全保障凭证，从而更高效地完成内部或监管合规要求的验证。

将信任从平台延伸至服务

此次获得认证的 UTM+ 平台体现了 Network Box 一体化安全架构的核心理念。通过将防火墙、入侵检测与防御以及内容过滤功能整合为统一的托管解决方案，UTM+ 为管理员提供了一个集中且协同的防御节点，用以应对不断演变的网络威胁。

在 ISO 15408 的评估过程中，产品架构、实现方法以及更新机制均接受了全面审查。该评估进一步强化了 Network Box 的设计原则：降低复杂度、保持透明性，并实施持续验证机制。结合托管服务层面的持续监督，这一体系确保客户不仅获得快速响应的防御能力，更拥有一个可验证、可持续的长期安全韧性基础。

对于 IT 管理员而言，这种信心意味着更少的不确定性、更清晰的审计路径，以及覆盖各个层面的更强防护能力——从机柜中的硬件设备，到持续监控网络流量的安全服务。

通过将 ISO 15408 纳入我们现有的认证体系，Network Box 进一步表明，我们对质量、安全与透明度的承诺贯穿于整体解决方案的每一个组成部分。这一里程碑不仅验证了我们当前解决方案的安全性与可靠性，也为未来托管安全领域的创新树立了更高的标准。

Network Box 5 and 8 新特性
2026年3月

2026年3月3日（星期二），Network Box 将发布本月的 周二补丁 “Patch Tuesday” 更新包，其中包含一系列功能增强与漏洞修复。各地区的 安全运营中心（SOC） 将在接下来的 14 天内分阶段 推出这些新功能。
本月针对 Network Box 5 与 8 版本 的更新内容包括：

NBRS-5

- **更智能的入侵防御** —— 在 IDS 与主动 IPS 模块中引入基于 HTTP Host 的绕过控制（bypass control），提供更精准且更灵活的防护能力。
- **更清晰的可视化洞察** —— 优化用户门户（User Portal）报表功能，实现更快速、更具价值的可视性展示。
- **更敏锐的传感能力** —— 增强 DNS Client GMS 传感器功能，提高检测能力与响应速度。
- **更完善的历史追踪** —— 配置历史报告现支持“上月”视图，便于审计与回溯。
- **更顺畅的邮件流转** —— 反垃圾邮件引擎在处理回环地址（loopback）及私有 IP 时跳过 RBL 检查，从而减少误报情况。

NBRS-8

- **WireGuard 功能增强** —— 提供对隧道运行的完整控制，并新增 “service restart wireguard” 命令，实现更便捷的 VPN 管理。
- **更可靠的 IP 处理机制** —— 修复配置变更后主 IP 分配问题，确保网络配置的一致性与稳定性。
- **更具韧性的代理机制** —— 在高负载场景下优化连接建立与关闭阶段的超时处理机制，提高稳定性。
- **默认采用更现代的安全标准** —— 集群同步连接现已默认启用 TLS 1.3，进一步提升加密强度。
- **更智能的邮件防护** —— 邮件扫描支持实时签名更新，实现更快速的威胁防护。
- **更强的 VPN 安全性** —— 优化 OpenVPN 默认加密套件配置，强化整体加密强度。
- **面向未来的硬件支持** —— 新增对即将发布的 E-1008i / 2008i 设备型号的支持。
- **扩展 API 能力** —— 新增对 NBSYNC 直连及集群同步协议的支持。

在大多数情况下，以上更改不会影响正在运行的服务或要求设备重启。然而，在某些情况下（取决于配置），可能需要设备重启。如果需要，您的本地SOC将与您联系安排此事。

如果您需要关于上述任何内容的更多信息，请联系您的本地SOC。他们将安排部署和联络。

Network Box HIGHLIGHTS

Network Box 年度回顾 2025

Network Box 荣幸推出 2025 年版《Year in Focus》——我们的年度回顾报告，全面呈现 2025 年的重要时刻、关键里程碑与创新成果。

这份年度总结汇集了塑造我们发展历程的核心亮点，展示了我们所取得的进展、克服的挑战，以及持续推动我们前行的突破性成果。

链接：
https://mcdn.network-box.com/focus/2025/Year_in_Focus-2025.pdf

月刊主办

Mark Webb-Johnson
主编

Michael Gazeley
Kevin Hla
产品支持

Network Box HQ
Network Box USA
贡献者

订阅

Network Box CNNOC
cnnoc@network-box.cn

或者上门到:
深圳市福田区深南大道
竹子林求是大厦西座
920

+86 (755) 3336 1581
www.network-box.cn

全球安全事件头条和漏洞情报

TechCrunch
Fortinet 防火墙遭恶意配置篡改
链接:
https://tinyurl.com/yc78pw54

The Hacker News
CISA 将被积极利用的 SolarWinds Web Help Desk 远程代码执行（RCE）漏洞纳入 KEV 漏洞目录
链接:
https://tinyurl.com/4paexb8z

GBHackers
黑客利用 DeepSeek 和 Claude AI 发动针对 FortiGate 设备的全球性攻击
链接:
https://tinyurl.com/5y99zfmb

Cyber Security News
Palo Alto Networks 防火墙漏洞可被攻击者利用，导致设备陷入反复重启循环
链接:
https://tinyurl.com/4w92d7s8

Bleeping Computer
Juniper Networks PTX 严重漏洞可导致路由器被完全接管
链接:
https://tinyurl.com/ywsf9tfc

翻译：James 校对: Jason