# In the Boxing Ring
## DEC 2024

# Network Box 技术新闻

**Mark Webb-Johnson**
*CTO, Network Box*

## 欢迎阅读2024年12月的 In the **Boxing Ring**

本月，为庆祝公司成立 25 周年，Network Box 推出了 Network Box 8 平台。在过去的二十五年里，Network Box 在周界保护方面表现出色，无论是办公室、数据中心还是云网络，现在我们很高兴推出 Network Box 8。我们在增强顶级技术的同时，还将保护范围向下扩展到端点，向上扩展到云，所有这一切都以隐私为中心。在第 2 页至第 4 页，我们将重点介绍其主要功能以及对这一新平台的期待。

另外，为纪念 Network Box 8 的发布，2024 年 12 月 3 日在米拉酒店宴会厅举行了发布会。此次活动也标志着 Network Box 成立 25 周年。此外，Network Box 董事总经理 Michael Gazeley 还在《南华早报》和《CDO Trends》上发表了文章，分享了他对最新网络威胁形势的看法。

**Mark Webb-Johnson**
*CTO, Network Box Corporation Ltd.*
December 2024

## 本月摘要:

**第2到4页**
**Network Box 8 - 概述**
在我们的专题文章中，我们详细讨论了 Network Box 8 的三个核心组件：
- **NBRS-8**: 平台操作系统
- **NB-X**: 终端和XDR
- **NBSIEM+**: 统一云管理

**第5页**
**Network Box 亮点:**
- **Network Box 8 发布会**
- **Network Box 媒体报道**
  ***SCMP:*** 专家称香港公务员有必要限制*WhatsApp*、微信以应对风险
  ***CDO Trends:*** 人类防火墙：网络安全为何仍需人为干预

# NETWORK BOX 8

**2024 年 12 月 3 日星期二，在庆祝公司成立 25 周年之际，Network Box 推出了 Network Box 8 平台。在此，我们总结了此次活动、推出的内容以及对新平台的期待。**

网络安全形势不断变化，但 80/20 法则依然存在：80% 的攻击因保护缺失而得逞，20% 的攻击因配置错误或监控不力而失败。因此，Network Box 在 25 年前推出了全面的 UTM 平台，并提供托管服务，以确保 100% 的保护。

将军事战争中的 “洋葱生存力 ”概念应用于 Network Box 的网络安全战略，这一点非常吸引人：

- 避免被发现： 使用外部扫描和最佳实践。
- 避免被检测到： 采用 IPS、前线防御和蜜罐。
- 避免被获取： 使用代理和混淆技术。
- 避免受中招：将先进的反恶意软件集成到防火墙中
- 避免被入侵： 实施内部控制，隔离黑客。


但是，如果发生攻击，为了限制损失，我们要确保快速识别受影响的系统、迅速关闭程序并进行有效清理，以阻止横向扩散。

更简单地说，遵循最佳做法隐藏自己，使用保护措施避免中招，如果中招，找出中招的原因，并在其扩散之前采取应对措施。

# NETWORK BOX

一直以来，Network Box 在生存性洋葱的上三分之二部分表现出色，现在我们很高兴推出 Network Box 8。我们在增强顶级技术的同时，还将保护范围向下扩展到端点，向上扩展到云，所有这些都以隐私为中心。我们将为您提供保护数据和网络安全的工具和服务。

让我们探讨一下 Network Box 8 的三个核心组成部分

- **NBRS-8**: 我们的操作系统
- **NB-X**: 终端和XDR
- **NBSIEM+**: 统一管理

## NBRS-8

没有人喜欢部署重大的软件更新。用户会面临服务中断和兼容性问题，而服务提供商则要应对艰巨的部署任务。Network Box 采取了不同的渐进式更新路线。我们坚持在产品的整个生命周期内，提供更小、更频繁的更新。对我们来说，长期支持意味着 10 年或更长的时间。自 NBRS-5 推出以来，我们已经推出了 100 多个固件更新和 2,000 多个软件包更新 - 这还不包括多年来数十万次的 PUSH 更新。

由于要管理分布在世界各地的众多网络，我们的目标是尽量减少重大的平台升级，只在有重大硬件支持、新威胁或必要的结构变化时才进行升级。尽管更新了数百万行代码和 10,000 多个软件包，但我们很高兴地宣布，NBRS-5 和 NBRS-8 仍然完全兼容并可互操作。它们可以在网络上并肩运行，由任一版本的 SOC 进行管理，甚至可以在高可用性模式下一起运行。这可确保顺利、无忧的迁移和支持体验。

NBRS-8 有大量新功能。支持 TLS 1.3（包括后量子加密）。Wireguard VPN（在 SSL、IPSEC 和 GRE 之外）。我们运行的是最新的稳定内核，甚至包括无需重启即可实时修补内核的功能。

今天，我们将向各地区安全运营中心发布 NBRS-8 预发布版本。新的部署将于 2025 年初启动，NBRS-5 客户的升级预计将于 2025 年第二季度开始。NBRS-8 兼容当前所有 Network Box 硬件，但在决定升级或更换时，请考虑硬件的使用年限。有关详细信息，请联系您当地的 SOC。

## Network Box X (NB-X)

25 年来，无论是办公室、数据中心还是云网络，Network Box 都在周界保护方面表现出色。但是，随着新的云服务、软件即服务和远程工作安排的不断发展，我们面临着新的挑战。

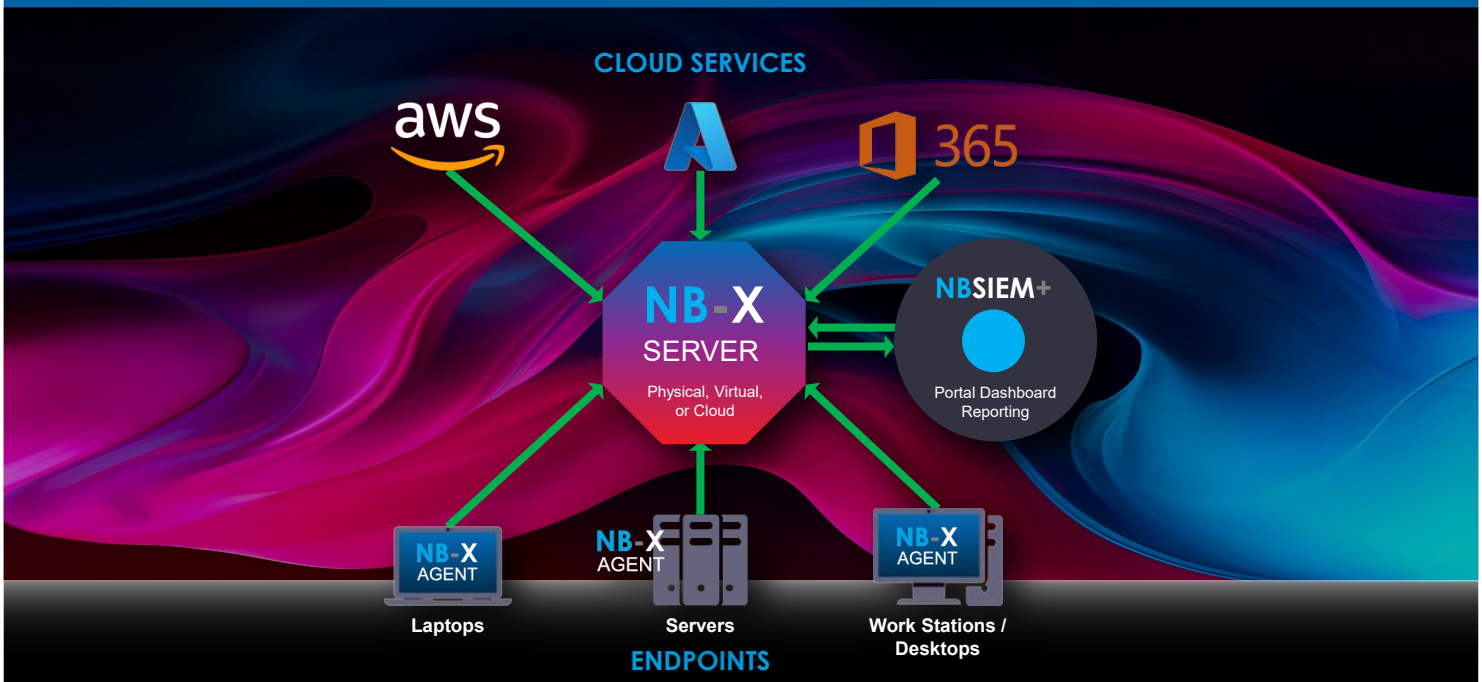
NB-X 将我们的保护范围向下扩展到笔记本电脑和服务器等端点，向外扩展到 Microsoft 365 和 Amazon AWS 等云服务。我们为不断变化的数字环境提供保护。

NB-X 通过每个设备上的轻量级代理将端点保护与 XDR 结合在一起。该代理可处理事件日志收集、遥测、主机入侵检测、可靠性评估、文件完整性监控、主动响应等。NB-X 服务器将这些代理连接起来，并集成了无代理云服务，将安全性集中在一处。我们可以将其部署在内部、专用设备或云中。

所有这些都由浏览器或移动应用程序上的NBSIEM+仪表板进行管理和控制。

通常，对于发生的每个事件，都会生成数百万个事件日志。将所有这些数据传输到云端可能成本高昂，并有不遵守 GDPR等法规的风险。这就是NB-X使用混合数据模型的原因。原始安全事件根据个人要求在本地或云中进行处理、规范化和存储。应用实时安全规则，并提出潜在问题的警报并转发给NBSIEM+进行进一步分析和事件处理。这种方法可以进行经济高效、隐私优先的事件预处。然后，NBSIEM+使用高级启发式和机器学习进一步处理可疑活动。

有了Network Box 8的混合架构，您的数据存储在哪里并不重要——本地、虚拟机、云、NBSIEM+或外部数据库。NBSIEM+提供所有数据的统一视图，确保无缝的安全管理。




NB-X 具有多种功能，重点关注 Survivability Onion 的最内层，以检测端点上的可疑活动。实时警报： 快速识别和评估安全问题。文件完整性监控可跟踪更改，并使用进程、文件或 YARA 规则查找破坏迹象。能够要求 NB-X 显示运行特定软件包的所有端点、运行特定进程的端点或与目标 IP 地址打开连接的端点，这真是不可思议。这项技术不仅适用于事件取证，也适用于一般的日常 IT 管理任务。NB-X 可以让您实时全面地了解端点、端点上正在运行的内容以及端点正在进行的操作。同样重要的是，NB-X 支持主动保护--根据 PCI DSS、GDPR、HIPAA、NIST、TSC 和 CIS 基准等合规框架进行分析和报告。识别错误配置、未经授权的应用程序并执行漏洞扫描。NB-X 甚至将可视性扩展到 Docker 和 Kubernetes 的容器安全，以及对 Office 365、Amazon AWS 等的 XDR 云支持。

NB-X将于本月开始首次试行部署，我们预计在2025年第一季度初全面可用。

## NBSIEM+和统一云管理

自 NBSIEM+ 推出以来，我们每周处理的数千种资产的事件数量已接近 40 亿次。其中Windows系统居首位，但我们也在利用来自Fortinet、Ubiquiti、思科、苹果、惠普、华硕等公司的数据。随着 NB-X 端点和 XDR 的集成，这些数字只会上升。

NBSIEM+ 凭借其基于云的横向扩展性和快速数据搜索能力而大放异彩。我们的目标是让它取代 Box Office、Admin Portal 和 User Portal，成为跨物理设备、虚拟设备和多租户云的所有 Network Box 服务的统一仪表板。它响应迅速，可通过门户网站或 iOS 和 Android 移动应用程序访问。NBSIEM+ 的一个突出特点是它是 100% REST API 驱动的，API 规范公开可用，并已被合作伙伴用于工单务和资产管理集成。

Network Box 8 扩展了 NBSIEM+，增加了新功能，提高了性能，减少了延迟。我们整合了管理门户，可通过网络或移动应用程序访问，基于云的用户门户选项即将推出。NBSIEM+ 现在可以无缝管理 NBRS-5 和 NBRS-8，使用混合数据模型在任何地方存储数据，同时符合 GDPR 和隐私要求。

新的灵活标签系统补充了现有的所有权层级，允许自定义报告层级。这为我们新的云报告系统提供了动力，可从这些自定义层级中的Box、资产和服务生成报告。

Network Box 8 NBSIEM+ 目前正在进行最终测试，并将于本月发布测试版。我们的目标是在一月份全面发布。展望未来，NBSIEM+ 将成为 Network Box 服务的管理员和用户的单一统一界面。

我们希望您能了解 **Network Box 8** 如何将我们屡获殊荣的外围保护系统扩展到端点和云。在此过程中，我们始终专注于保护客户设备和数据的核心使命。

网络安全领域充斥着大量炒作和流行语，往往忽略了真正的日常问题。在 **Network Box**，我们的效率由您（我们的客户、分销商和经销商）来衡量。只有保证您的安全，我们才能取得成功；这是我们的首要任务。作为 **CTO**，我向您承诺，为各种规模的企业提供有效的保护仍然是我们的指导原则。

# Network Box HIGHLIGHTS

## Network Box 8 | 发布会

为了纪念 **Network Box 8** 的发布，2024 年 12 月 3 日在 Mira 酒店宴会厅举行了一场发布会。此次活动也标志着 Network Box 成立 25 周年。感谢所有参加这一里程碑式活动的人。


NETWORK BOX

**月刊主办**

**Mark Webb-Johnson**
编辑

**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

### Network Box 媒体报道

**SCMP**
专家：鉴于风险，香港公务员需要对 *WhatsApp* 和微信加以限制

**LINK:** https://tinyurl.com/4fbmeedp

**CDO Trends**
人类防火墙：网络安全为何仍需人为干预

**LINK:** https://tinyurl.com/5myb8ths


翻译：Jason