

# In the Boxing Ring

## 2024年7月

## Network Box 技术新闻

Mark Webb-Johnson CTO,  
Network Box

### 欢迎阅读2024年7月份的 In the Boxing Ring

本月，我们将讨论Network Box的引擎、签名和策略。对于我们的安全服务，Network Box一直有一个主要目标：不允许任何恶意内容通过。在第2至第3页，我们将讨论我们如何实现这一目标。

请注意，这将是今年这类通用文章的最后一期。从下个月开始，我们将介绍构成Network Box在2024年及以后的安全之道的四个关键组件：NBRS-8、终端保护、NBSIEM+和统一云管理。

在其他消息中，Network Box自豪地宣布公司荣获Business GoVirtual颁发的“年度科技公司 — 创新技术应用”卓越奖。

本月的技术重点是Network Box红队服务。您是否知道Network Box提供渗透测试和漏洞评估服务，以帮助您进行风险评估、审核或合规要求？

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

### 本月摘要:

#### 第2-3页

#### Network Box 引擎、签名和策略

本月，我们介绍了关于Network Box安全的三管齐下的方法：多引擎、策略执行以及广泛的签名、启发式技术和情报。

#### 第4页

#### Network Box 亮点:

- **Business GoVirtual科技大奖 2024:**  
年度科技公司 — 创新技术应用
- **Network Box 技术重点:**  
Network Box 红队服务

#### 即将推出...

从下个月开始，我们将介绍构成Network Box在2024年及以后安全方法的四个关键组件：

- NBRS-8
- 终端保护
- NBSIEM+ 增强功能
- 统一云管理



# Network Box

## 引擎、签名和策略

如今，保护组织的数字资产并不简单，比十年前复杂得多。我们不仅面临着新的各种威胁，而且我们的数据现在分布在物理、虚拟和SAAS系统上，通常跨越多个数据中心和服务提供商。

随着我们即将迎来成立25周年纪念日，Network Box一直以来对我们的安全服务有一个主要目标：不允许任何恶意内容通过。谚语“预防胜于治疗”在网络安全领域尤为正确。只有尽可能接近100%的效果，我们才能向各种规模的组织提供负担得起的安全保障。

那么，我们如何实现这个目标呢？  
通常通过一个三管齐下的方法：



## 1. 多引擎

Network Box产品通过多个引擎进行深度扫描、识别和网络流量分类。例如，我们的旗舰产品Network Box 5 (NBR5-5) 目前拥有18个防火墙引擎、3个入侵检测系统 (IDPS)、18个反恶意软件引擎、25个反垃圾邮件引擎和15个内容过滤引擎。每个引擎以不同方式检查流量，并共同提供最全面的安全性。

恶意流量必须通过每个独立引擎的检查。与大多数竞争对手的单引擎方法相比，这种多引擎方法在一个设备中提供了深度防御。

## 2. 广泛的签名、启发式技术和情报

引擎仅仅取决于背后的签名、启发式技术和威胁情报。Network Box安全情报的基础是我们的RepDB（声誉数据库）系统。这是一个包含有关IP地址、URL、文件校验和、电子邮件地址、域名等与网络流量相关的元数据的庞大情报收集。这些情报信息来自我们自己的情报数据、蜜罐、垃圾邮件陷阱、安全指标等，以及来自我们全球合作伙伴。

今天，RepDB存储着超过4700万个当前分类规则和另外1.58亿个历史分类规则，涵盖12种元数据和63个类别。除了RepDB，Network Box还从我们的安全合作伙伴那里生成保护签名、启发式技术和规则——所有这些都实时更新，并使用我们的专利PUSH技术在几秒钟内分发。NBR5-5目前拥有超过16,000个入侵检测系统规则、2400万以上的反恶意软件规则、3000万多的反垃圾邮件规则以及700万个内容过滤规则（不仅仅是简单的签名，还有能够捕捉许多威胁变体的启发式技术和智能规则）。

## 3. 策略执行

Network Box方法的最后一部分是策略执行。多个引擎、签名、启发式技术和情报的目标是准确分类网络流量。然后，由策略执行系统来执行严格的安全策略。这超越了竞争系统简单的“阻止和隔离任何被分类为恶意”的做法，因为我们提供一个复杂的基于规则的方法，不仅考虑分类，还考虑与该分类相关的元数据、网络流量连接的源和目的地。

重要的是，部署的安全策略既全面又有效，而Network Box安全运营中心负责与客户合作确保这一点。80%的安全事件可能是由于缺少保护技术，但剩下的20%是由于这些技术配置或维护不正确造成的。Network Box每周对所有客户网络进行外部视图扫描，结合季度安全策略审查来监控最佳实践的遵守情况。

最终，安全策略完全由客户决定；Network Box安全运营中心提供指导和监控服务。



通过结合我们的多个引擎、签名、启发式技术、威胁情报、策略执行系统和SOC支持，Network Box提供全面、有效的托管网络安全服务。

# Network Box HIGHLIGHTS



## Business GoVirtual 科技奖2024 卓越奖

Network Box很荣幸宣布，公司荣获由Business GoVirtual颁发的年度科技公司卓越奖——创新技术应用类别。该奖项表彰那些利用前沿技术开发创新产品或服务，并具有在不久的将来创造新机会或改变行业或日常生活潜力的科技公司。



### 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

Copyright © 2024 Network Box Corporation Ltd.

翻译: James



## Network Box 技术焦点

### 您知道吗...

### Network Box提供渗透测试和漏洞评估服务

虽然企业对“防御性安全”（如防火墙、终端保护、SIEM和MDM）的重要性了如指掌，但很少有企业会主动寻找黑客可能利用的漏洞。这就是为什么Network Box提供主动的进攻性安全服务，这是对您安全策略中重要的补充，可帮助您进行风险评估、审核或合规要求或事件响应。其中包括：

- 漏洞评估 — 低成本、大多数自动化进行、快速，但不基于风险。
- 渗透测试 / 红队行动 — 由专家手动完成，基于风险，结果质量更好，通常围绕威胁参与者的场景展开。
- 攻击模拟 — 使用MITRE ATT&CK数据对攻击技术和策略进行详细逐步分析，提供最高标准的结果。
- 事件响应 — 事故后补救、计算机取证、正式信息安全审计、信息安全培训和宣传。

请访问以下链接获取更多详细信息：

<https://network-box.com/networkbox-redteam>

