In the Boxing Ring
2022年5月

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2022年5月份的 In the **Boxing Ring**

我最近重读了一本1989年出版的名为"布谷鸟的蛋"的书，作者是克利福德-斯托尔。它描述了一个计算机管理员试图追踪一个入侵学术和军事网络的德国间谍的过程。虽然是30多年前写的，但看到尽管在网络安全方面取得了进展，但实际变化如此之小令人震惊。80%的安全事件是由于缺乏保护而引起的，其余20%的安全事件是由于现有的保护措施没有正确配置或出现了问题，而故障没有被发现。Network Box就是为了解决这两个问题而成立的--用一个包含所有关键保护组件的UTM+产品，结合一个管理服务，以确保这些组件被配置、监测和安全地维护。

这个月，我们讨论Network Box的不同之处，比较我们与其他安全管理服务供应商和自我管理（又称DIY）的解决方案。这将在第2至3页概述。

为了配合我们的专题文章，Network Box发布了一个执行摘要视频，以强调我们的关键点，"你是否受到保护免受网络威胁？"在本月的全球安全头条新闻中，联想、松下、亚马逊网络服务、T-Mobile和超过800万的Cash app投资客户遇到了安全问题，可能会导致数据泄露。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
May 2022

保持联系

您可以通过电子邮件联系我们(cnnoc@network-box.cn)，或者上门拜访我们.您也可以通过社交网络跟我们保持联络

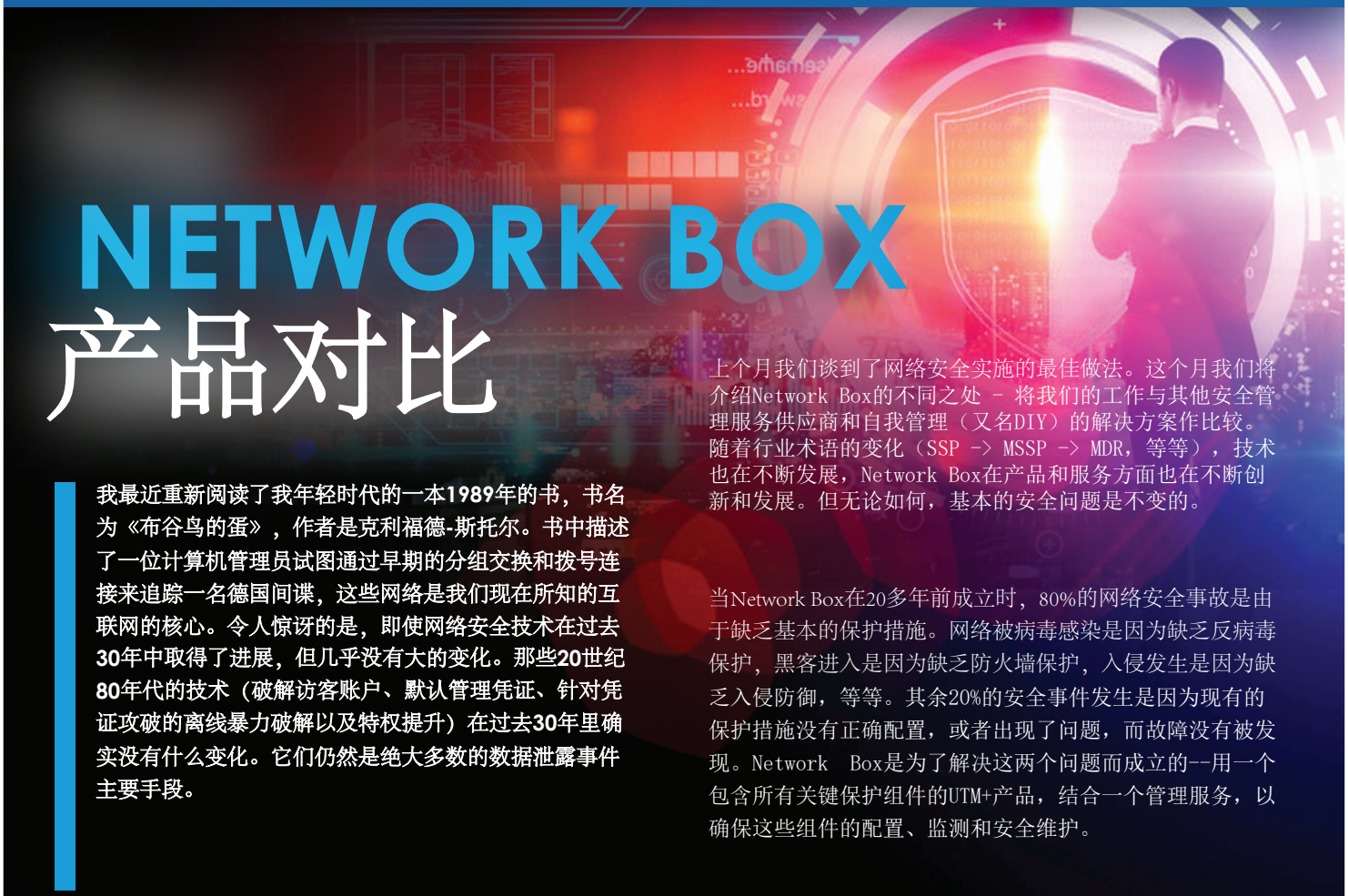
https://twitter.com/networkbox

https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

https://www.linkedin.com/company/network-box-corporation-limited/

https://www.youtube.com/user/NetworkBox

本月要闻:



NETWORK BOX
产品对比

我最近重新阅读了我年轻时代的一本1989年的书，书名为《布谷鸟的蛋》，作者是克利福德-斯托尔。书中描述了一位计算机管理员试图通过早期的分组交换和拨号连接来追踪一名德国间谍，这些网络是我们现在所知的互联网的核心。令人惊讶的是，即使网络安全技术在过去30年中取得了进展，但几乎没有大的变化。那些20世纪80年代的技术（破解访客账户、默认管理凭证、针对凭证攻破的离线暴力破解以及特权提升）在过去30年里确实没有什么变化。它们仍然是绝大多数的数据泄露事件主要手段。

上个月我们谈到了网络安全实施的最佳做法。这个月我们将介绍Network Box的不同之处 – 将我们的工作与其他安全管理服务供应商和自我管理（又名DIY）的解决方案作比较。随着行业术语的变化（SSP -> MSSP -> MDR，等等），技术也在不断发展，Network Box在产品和服务方面也在不断创新和发展。但无论如何，基本的安全问题是不变的。

当Network Box在20多年前成立时，80%的网络安全事故是由于缺乏基本的保护措施。网络被病毒感染是因为缺乏反病毒保护，黑客进入是因为缺乏防火墙保护，入侵发生是因为缺乏入侵防御，等等。其余20%的安全事件发生是因为现有的保护措施没有正确配置，或者出现了问题，而故障没有被发现。Network Box是为了解决这两个问题而成立的--用一个包含所有关键保护组件的UTM+产品，结合一个管理服务，以确保这些组件的配置、监测和安全维护。

指标	Network Box 解决方案	其他可管理的产品	自行管理产品
责任	■ 根据最佳实施建议和客户定制的政策，由一个供应商负责网络安全的实施。	■ 多个单位与多个外部供应商。 ■ 没有单一责任点。 ■ 供应商可能互相指责。	■ 多个外部供应商。 ■ 没有单一的责任点。 ■ 供应商可能互相指责。
部署选项	■ 服务可以部署在企业内部，云上，或作为多用户的SaaS。 ■ 单点统一的配置、报告和支持。	■ 取决于MSSP。 ■ 通常只有一个部署选项可用。	■ 虽然有可能是混合的（企业内部、云、多租户SaaS），但没有单一的接口。 ■ 技术支持可能是一个问题。
网络安全操作中心	■ 自主运营。 ■ 170个威胁情报合作伙伴。 ■ 微软认定的2019年威胁情报十大贡献者。	■ 取决于MSSP。 ■ 通常是通过与外部安全响应中心的合作。	■ 一般来说没有。 ■ 有时作为一项外部服务需要购买。 ■ 所有的威胁情报必须由IT人员自己采取行动。
配置	■ 统一配置。 ■ 完整的版本控制和审计跟踪。 ■ 在被管理的设备上和多个安全操作中心都有实时备份。	■ 取决于MSSP。 ■ 通常采用手动备份和有限的版本控制。	■ 手动备份和版本控制（如果有的话）。
服务	■ 24x7x365的安全监控。 ■ 根据需求提供硬件和配置支持的服务协议（从工作时间到24x7x365）。	■ 取决于MSSP。	■ 通常只有办公时间。 ■ 在夜间、周末和节假日提供有限的支持。

指标	Network Box 解决方案	其他可管理的产品	自行管理的产品
响应时间	■ 服务是根据单一的明确定义的服务等级协议提供的，并可以根据需要和目标升级。	■ 在提供服务的某些方面必须依赖外部设备供应商。 ■ 往往需要跨多个供应商的背对背服务协议。	■ 服务依赖于IT人员。 ■ 经常与其他使用有限资源的任务相冲突。
硬件响应	■ 在4个工作小时内更换硬件（视地区而定）。 ■ 替换件预先配置了当前的配置（自动同步），最大限度地减少了停机时间。	■ 硬件更换选项取决于个别MSSP和外部设备供应商。 ■ 替换通常需要从备份中手动配置和部署。	■ 通常只有办公时间。 ■ 在非工作时间、周末和节假日需要待命的工作人员。 ■ 替换的备件必须保存在现场或与外部供应商协调。 ■ 替换通常需要手动配置，并从备份中部署，导致长时间的停机。
网络安全技术	■ 一个统一的平台提供所有的关键技术，并对其进行配置、维护和全面的报告。 ■ 硬件和技术都是在一个封闭的安全循环中内部开发的。 ■ 由三重ISO认证和PCI兼容的Network Box SOC提供24x7x365支持。	■ 来自多个外部供应商的多个不同平台。 ■ 没有统一的配置、维护、备份或报告。	■ 来自多个外部供应商的多个不同平台。 ■ 没有统一的配置、维护、备份或报告。
安全更新	■ 通过专利的 PUSH技术。 ■ 24x7x365实时自动执行。 ■ 平均交付时间少于45秒。	■ 依赖于外部设备供应商，几乎无法控制。	■ 依赖于外部设备供应商，几乎无法控制。
更新部署	■ 24x7x365全面管理，有一个明确的更新周期。 ■ 与客户协调，以满足他们的要求。 ■ 所有补丁都在所有支持的硬件类型和配置上进行了预先测试。	■ 无法检查不同设备供应商类型和固件/软件版本之间的兼容性。 ■ 时间上取决于外部供应商。 ■ 不同步（不同供应商有不同的发布周期）。	■ 取决于IT人员的知识和工作时间。 ■ 补丁必须手动下载和安装。 ■ 无法检查不同设备供应商类型和固件/软件版本之间的兼容性。 ■ 时间取决于外部供应商，并且不同步。 ■ (不同的供应商有不同的发布周期）。
报告	■ 每周/定期的KPI报告 ■ 高度可配置的定制报告系统 ■ HTML-5仪表板 ■ 实时便携式监控 ■ 网页和App。	■ 取决于MSSP。 ■ 通常，每个服务提供商都有自己的报告系统和周期。 ■ 没有统一的报告。	■ 取决于所选择的产品。 ■ 通常，每个产品都有自己的报告系统和周期。 ■ 没有统一的报告。
业绩记录	■ 在我们自己的平台上提供管理安全服务20多年。 ■ 通过世界各地的十多个安全运营中心提供服务。 ■ 客户只有在我们很好地确保他们的系统安全的情况下才会继续订阅服务。	■ 取决于MSSP。	■ IT部门专注于帮助用户操作他们的计算机系统，而不是执行安全政策。 ■ 大多数IT部门的工作人员在网络安全主题方面实践经验或培训较少。

Network Box HIGHLIGHTS

Network Box 执行摘要视频: 您是否受到保护免受网络威胁?

在今天这个相互连接的世界里，网络安全至关重要。无论哪个行业，每个公司都需要有效的网络保护。然而，大多数公司都没有得到充分的保护，无法抵御黑客、病毒、蠕虫、勒索软件和不良内容，这些都使互联网成为严重的威胁。

这种情况下，依靠像Network Box这样的高质量网络安全管理服务提供商，可以使一切变得不同。不要成为互联网威胁受害者。将您的网络安全问题交给Network Box的专家，让您的组织今天就得到专业的保护。

链接:
https://mcdn.network-box.com/NB-Materials/NB-Network_Box_Overview.mp4

月刊主办	联系方式
Mark Webb-Johnson 主编 **Michael Gazeley** **Kevin Hla** 产品支持 **Network Box HQ** **Network Box USA** 贡献者	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

全球安全头条

CNN
超过800万Cash App投资的客户可能受到与前雇员有关的数据泄露的影响
链接: https://cnn.it/3ODVWmJ

The Hacker News
联想UEFI固件新漏洞影响数百万台笔记本电脑
链接: https://bit.ly/37PWCEV

CPO Magazine
松下承认6个月内遭受第二次网络攻击，康蒂勒索软件团伙声称对此负责
链接: https://bit.ly/3Lu5yOS

The Register
AWS的Log4j补丁在其自身的安全方面存在漏洞
链接: https://bit.ly/37KJHnT

The Hacker News
T-Mobile承认Lapsus$黑客获得了其内部工具和源代码的权限
链接: https://bit.ly/3vR39r1