



# In the Boxing Ring JAN 2025



## Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

### Welcome to the January 2025 edition of In the **Boxing Ring**

Happy New Year! This month, we are talking about **Pigeonholing**. As a species, we like to categorize things, as it is helpful to break things down and group things together - divide and conquer. However, sometimes, we take this too far and start pigeonholing unnecessarily. With cybersecurity, at the start, there were firewalls, then UTMs and NGFWs. Today, we have a plethora of buzzwords - SIEM, EDP, EDR, XDR, MSSP, MDR, SASE, PAAS, WAF, SOAR, SECaaS, SD-WAN, Edge Security, and dozens more small contenders. The bottom line is that this is all marketing fluff. On pages 2 to 3, we cut through all the buzz and hype, and highlight what is truly important in protecting you.

On page 4, we highlight the set of enhancements and fixes to be released in this month's Patch Tuesday for Network Box 5 and our cloud services.

In other news, Network Box Hong Kong participated in *Tradelink's Cyber Security 360* event, and the **Digital and Quality Development Forum** hosted by the *Internet Professional Association*. Additionally, Network Box's Michael Gazeley gave a cybersecurity seminar at the **Hong Kong Baptist University School of Business**. Finally, Network Box was the cover story of the latest issue of **Banking Today**.

**Mark Webb-Johnson**  
CTO, Network Box Corporation Ltd.  
January 2025

### Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with several social networks:



<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>

### In this month's issue:

#### Page 2 to 3 **Pigeonholing**

With so many acronyms and industry buzzwords to categorize security technologies, it can often leave one's head spinning. In our featured article, we ditch the pigeonholed marketing anti-competitive buzzwords and discuss what is required to protect you.

#### Page 4 **Network Box 5 Features**

The features and fixes to be released in this month's Patch Tuesday for Network Box 5 and our cloud services.

#### Page 5 **Network Box Highlights:**

- **Network Box Hong Kong:** Cybersecurity 360 Event
- **Network Box Hong Kong:** iProA Event
- **Network Box Hong Kong:** HKBU Cybersecurity Seminar
- **Network Box Media Coverage:** *Banking Today* (Issue 139 November-December 2024) **COVER STORY:** Hong Kong's Financial Cybersecurity Solutions at a Crossroads



## Dictionary

Definitions from Oxford Languages

### pigeonhole

*/ˈpiːdʒ(ɪ)nhoʊl/*

verb

gerund or present participle: **pigeonholing**

1. assign to a particular category, typically an overly restrictive one.

"I was pigeonholed as a 'youth writer'"

Similar: categorize    compartmentalize    classify    characterize    label    brand

# Pigeonholing

**Humans love to categorize things. It is in our DNA. From the dawn of time, we've been divided by race, gender, religion, tribe, and other attributes. Most commonly, 'them' and 'us.' Then, with the arrival of science came sophisticated categorization schemes such as Taxonomy and, ultimately, the pinnacle of sophistication, the Dewey Decimal Classification system for libraries. One can understand this. In a complex world, it is helpful to break things down. Group them together. Divide and conquer.**

But sometimes, particularly with commercial interests involved, we take things too far. Needlessly pigeonholing, often to differentiate or gain competitive advantage.

Let's look at firewalls. In the early days, the term 'firewall' was well understood as a piece of software capable of being configured to block specified network traffic. Like the firewall in a building able to block unwanted smoke/heat/fire, computer firewalls block unwanted traffic. Early firewalls would typically only be configurable based on IP address, but as time passed, other criteria were added (such as interface, UDP or TCP protocol port, ICMP request type, time of day, etc). Then came stateful firewalls that could track connections and block/permit at the start of a connection, not just on every single packet. But, no matter how sophisticated the configurable block types were, and whether stateful or stateless, these were all called 'firewalls.'



Then along came a new entrant to the market, with a feature to look inside the content of a connection, perform very rudimentary signature pattern matching, and block based on that. Others were doing something similar (combining anti-virus systems with firewalls), but the difference here is that marketing teams got involved and invented a new pigeonhole, 'Unified Threat Management' (or UTM). The marketing genius was that if you were using a 'firewall,' that was old technology, and you needed UTM to be truly secure. OK, one can just about accept that - with the understanding that UTM means combining more than one security feature or service into one single unified device.

Next, another new entrant arrived. This time, offering protocol identification (again with heuristics/signatures on the traffic), and a new term, 'Next Generation Firewall' (NGFW), was born. If you were running UTM, that was old technology, and you needed an NGFW to be truly secure.

**Are you seeing a pattern here?**

Now we have ended up with a plethora of buzzwords - SIEM, EDP, EDR, XDR, MSSP, MDR, SASE, PAAS, WAF, SOAR, SECaaS, SD-WAN, Edge Security, and dozens more small contenders. And that is just for the protection offerings. The threats themselves have morphed from 'viruses' to dozens of fine-grained and overlapping terms such as ransomware, rootkits, trojans, worms, droppers, zero-days, adware, phishing, keyloggers, and the all-encompassing 'malware.'

**Is your head spinning?**

The bottom line is that this is all marketing fluff. Ask the simple man in the street what he needs to be cyber-secure, and he will reply, 'a firewall', and he will not be too far from the truth.

We (the industry) know full well what is required to secure an organization, and it is a relatively straightforward three-step process:

1. Pick a framework (NIST, CIS, PCI DSS, ISO 27001/27002, CMMC, or any others).
2. Implement a technology platform that is compliant with that framework.
3. Monitor and manage the platform in a manner that complies with that framework.

Either do it yourself or outsource it to a managed security provider. But bear in mind that although much has changed in the past 25 years, much has stayed the same, and the fundamentals are still that 80% of attacks succeed because the technology to prevent them wasn't deployed, with the other 20% succeeding because of undetected failure or misconfiguration of the platform.

**So, in this new year, 2025, let's resolve to ditch the pigeonholed marketing anti-competitive buzzwords. We are calling our new platform Network Box X (so that you can substitute whatever latest buzzword you want for the 'X'). Let's all recognize that we need a cyber security platform to secure our organizations - and deploy, monitor, and manage it in a way compliant with a standardized security framework. It really is that simple.**

# Network Box

# 5

## NEXT GENERATION MANAGED SECURITY

On Tuesday, 7th January 2025, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOC's will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

## Network Box 5 Features January 2025

This quarter, for Network Box 5, these include:

- Minor fix to certificate authority error reporting
- Improvements to SOC systems for attribution of configuration change requests to matching tickets
- Improvements to Admin Portal Network interface Setup
- Updates to regional SOC IP address assignments
- Deprecate use of [networkbox@network-box.com](mailto:networkbox@network-box.com) email address
- Various improvements to SOC configuration and box maintenance systems

Regarding the deprecation of the [networkbox@network-box.com](mailto:networkbox@network-box.com) email address, we have used that address for some time now. However, with the evolving changes to email and the importance of email security features such as DKIM and SPF, it is becoming increasingly difficult to use our global @network-box.com domain in this way. Accordingly, this month, our regional SOC's will be migrating report emails to come from either their own domains or customer-specific email addresses. This should improve the reliability of report email delivery (particularly when the destination of the report is big email service providers such as Microsoft 365, GMAIL, etc).



In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

**Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.**

# Network Box HIGHLIGHTS



## Network Box Hong Kong iProA Event

Network Box Hong Kong participated in an event hosted by the **Internet Professional Association (iProA)**. The event, which took place at the Hong Kong Productivity Centre, was titled **“Digital and Quality Development Forum: Developing New Advantages, Creating the Future Together.”**



## Network Box Hong Kong Cybersecurity 360 Event

Network Box partnered with **Tradelink** for their **Cybersecurity 360** event, which took place at The Langham. During the event, Tradelink’s COO, Andrew Cheng, gave an outstanding presentation, analyzing the latest cybersecurity trends, demonstrating various cyberattacks, and providing practical strategies for companies to protect their digital assets. He also highlighted how Tradelink has leveraged Network Box’s Managed Cybersecurity Services for protection, business continuity, and KPI reporting, for over 20 years.



## Network Box Hong Kong HKBU Cybersecurity Seminar

Network Box’s Managing Director, Michael Gazeley, gave a cybersecurity talk at the **Hong Kong Baptist University School of Business** for their FinTech Masterclass.



### Newsletter Staff

**Mark Webb-Johnson**  
Editor

**Michael Gazeley**  
**Kevin Hla**  
Production Support

**Network Box HQ**  
**Network Box USA**  
Contributors

### Subscription

Network Box Corporation  
[nbhq@network-box.com](mailto:nbhq@network-box.com)  
or via mail at:

**Network Box Corporation**  
16th Floor, Metro Loft,  
38 Kwai Hei Street,  
Kwai Chung, Hong Kong.

**Tel: +852 2736-2083**  
**Fax: +852 2736-2778**

[www.network-box.com](http://www.network-box.com)



## Network Box Media Coverage



## Banking Today

Issue 139  
November-December 2024

**COVER STORY:**  
**Hong Kong's Financial  
Cybersecurity Solutions at a  
Crossroads**

LINK: <https://tinyurl.com/4xkpz6ts>