# In the Boxing Ring
## NOV 2024

## Network Box Technical News
**from Mark Webb-Johnson**
*Chief Technology Officer, Network Box*

### Welcome to the November 2024 edition of In the **Boxing Ring**

This month, we are talking about **Unified Cloud Management** in Network Box 8. Cloud computing has revolutionized scalability and cost-effectiveness, but it has complicated security. Traditional data storage in DMZ servers required significant investments and posed challenges in scalability, costs, and management. Cloud computing, although improving accessibility and collaboration, introduced new security challenges by distributing data across multiple environments and requiring trust in SaaS providers. On pages 2 to 3, we discuss this in greater detail.

In other news, Network Box Singapore exhibited at the **Industrial Transformation Asia Pacific** at the Singapore EXPO. Additionally, Network Box Hong Kong participated in **Roubrick | Talks Tech.**, titled "AI Evolution and Security in Asia and Beyond." Finally, Network Box Managing Director Michael Gazeley was interviewed by the **SCMP** in the article "Hong Kong civil service restrictions on WhatsApp, WeChat needed in light of risks: experts."

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

## 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:

# Unified Cloud MANAGEMENT

**Gone are the days when our data was stored in servers in the DMZ and accessed via workstations on the LAN with a single point of entry/exit to the Internet. Over the years, we found that this infrastructure required substantial investment in hardware, maintenance, and personnel. This computing model presented challenges, including limitations to scalability, high upfront costs, and the need for constant management and upgrades.**

With the advent of high-speed Internet and advances in virtualization technology, cloud computing emerged as a revolutionary solution. Cloud computing allows data and applications to be hosted on remote servers managed by third-party providers. This shift of computing to the cloud improved scalability, reduced costs, and improved accessibility and collaboration capabilities (particularly in the era of COVID and work-from-home).

However, it also brought with it significant challenges related to information security. By distributing our data and applications across disparate data centres and services, we significantly complicated the security threat landscape we are now open to. We no longer have to protect one gateway - but now have to protect multiple environments, and in the case of SaaS, we have to trust the protections provided by our SaaS providers (which historically has not seen much success given that public data breaches now number in the tens of thousands).

## The XDR Solution

To address the security concerns, our industry started to look at consolidating all the security audit data from these disparate cloud and on-premises services into one framework. The current buzzword for this is Extended Detection and Response (XDR) - a unified security platform that integrates detection, investigation, and response capabilities across various domains, such as endpoints, networks, cloud environments, email, and data stores. By leveraging AI and automation, XDR provides a holistic approach to protect against advanced cyberat-tacks. It enhances visibility into cyberattack chains, streamlines security operations, and reduces response times. XDR platforms collect and correlate data from multiple sources, enabling faster and more effective threat detection and remediation. This comprehensive defence mechanism helps organizations improve their overall security posture and efficiently tackle sophisticated, multi-stage attacks.

## Network Box X (NBX)

**Whatever the current buzzword, this is precisely what Network Box X is designed to achieve.**

- With an optional NBX endpoint agent, we've extended security visibility to endpoint devices such as servers, desktops, and laptops (and, in cases such as Docker, to the individual sub-services running on those endpoints).
- We've introduced a new collector and rules engine component (called the NBX Server) capable of collect-ing logs not just from NBX endpoints, but also from cloud services and SaaS systems.
- We've upgraded our core operating system to NBRS-8, leveraging the latest security technologies, kernels, and user-space tools.
- And we've integrated all this into our multi-tenanted cloud-based NBSIEM+ platform to provide a single cloud-based holistic view.

### So, what differentiates NBX from other XDR systems?

The first key difference is the data storage. We separate this into three stages/types:

1. Raw event logs from endpoints, devices, and services are ingested into the NBX server, where they pass through a first-stage rules engine that determines whether they should be escalated to alerts.
2. Alerts raised by the NBX server are ingested into a second rules-based engine to determine if they should be reportable.
3. Reportable alerts of sufficient severity are escalated as incidents and handled by security engineers.

Typically, a single alert is raised for every 100 to 200 raw event logs, and an incident is raised for every 100 to 1,000 alerts. By allowing the NBX Server to be deployed either on-premises, physically, virtually, or in the cloud, Network Box X provides cost-effective, privacy-focused storage of raw events, alerts, and security incidents.

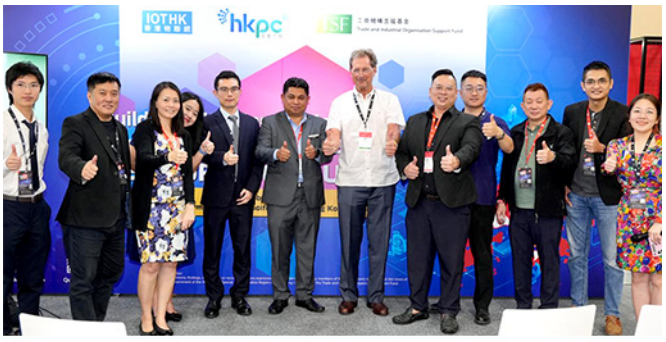
This provides Network Box X with a unique hybrid data access model where every service is offered client-server, and data storage is chosen to balance data protection, cost, performance, and security concerns. Our single cloud-based portal (NBSIEM+) can access this data and command response, whether the events are stored on endpoints, on a physical server, or in the cloud. By unifying the security events in this way, and allowing access from a single web-based/mobile platform, we simplify administration and allow incidents to be investigated and responded to globally.

**Cloud computing revolutionized scalability and cost-effectiveness but complicated security. While XDR solutions consolidate security audit data from various cloud and on-premises services into a unified framework, Network Box X (NBX) extends security visibility to endpoints, collects logs from cloud services and SaaS systems, and provides a hybrid data access model for cost-effective and privacy-focused storage of security events.**

# Network Box HIGHLIGHTS

## Network Box Singapore
### IOTHK Event

Network Box Singapore exhibited at Industrial Transformation Asia Pacific at the Singapore EXPO. Managed Cyber-Security Services, Dark Web Monitoring, Cloud SIEM+, Active Managed Detect Response End Point, Internet of Things Protection, Red Teaming, etc., Network Box provides everything required to protect your organization's computers, networks, programs, and data.




## Network Box Hong Kong
### Roubrick | Talks Tech

Network Box Managing Director Michael Gazeley participated in Roubrick | Talks Tech. Hosted by John Mulligan of Xontec.io, the title of the talk was "AI Evolution and Security in Asia and Beyond."

There is no denying that Artificial Intelligence is now very much part of our collective lives - so we better be ready to embrace it while protecting ourselves from it. As with Computers in general, the Internet, the Internet of Things, Robotics, and soon Quantum Computing, we all have little choice but to evolve with changing technology, or become irrelevant.

## Network Box Media Coverage

### SCMP

**Hong Kong civil service restrictions on WhatsApp, WeChat needed in light of risks: experts**

South China Morning Post

"Hong Kong is catching up to the rest of the world, by preventing the use of third-party apps, and in particular third-party apps from overseas. By prioritising Hong Kong's own cybersecurity systems, government departments can better protect sensitive information, ensure regulatory compliance, and maintain national security."

**LINK:** https://tinyurl.com/mtdxueyf

**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
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