In the Boxing Ring
JUL 2025

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

Welcome to the July 2025 edition of In the **Boxing Ring**

This month, Network Box Managing Director Michael Gazeley discusses **Critical Cyber Vulnerabilities Threatening Physical Security**. In an era where door readers, CCTV cameras, intercoms, and even turnstiles all operate on IP networks, a single cyber breach can instantly become a brick-and-mortar disaster. Exploited software flaws can blind security cameras, unlock doors or expose sensitive footage, turning digital weaknesses into physical vulnerabilities. The days of treating IT and physical security as separate silos are over. Today's perimeter demands a unified defence.

On pages 2 to 3, we discuss the most pressing cyber-driven threats to physical security and show how organisations can shore up every link in the chain.

In other news, Network Box Hong Kong participated in **Business GoVirtual AI+ 2025**, which took place at the HK Convention and Exhibition Centre. Also, this month, we will release our **Patch Tuesday** set of enhancements and fixes for our Network Box platform.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
July 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://x.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:

Critical Cyber Vulnerabilities Threatening Physical Security

by Michael Gazeley
Managing Director
Network Box Corporation Limited

In an era when door readers, CCTV cameras, intercoms, and even turnstiles, operate on IP networks, a cybersecurity failure can instantly become a brick-and-mortar problem. Treating physical security and IT as separate silos is no longer an option for modern organisations.

Unpatched IoT and OT devices

Most video cameras, smart locks, and environmental sensors, rely on embedded operating systems that rarely receive routine updates. A recent industry survey revealed that 57% of organisations cite outdated IT and OT infrastructure as a top challenge. Attackers exploit known vulnerabilities to hijack cameras—effectively blinding facilities—and pivot laterally into corporate networks. Left unpatched, these always-on endpoints offer a direct path from the internet to server rooms, storerooms, and warehouses.

Cloud misconfiguration

Cloud-managed access-control and video-management systems promise scalability, yet simple configuration errors (such as open storage buckets or over-privileged administrator accounts) put stored footage, credential data, and archive records at risk. As 43% of organisations now integrate cloud services into their physical-security programme, cloud missteps represent a leading breach vector. A single misplaced access-control list can expose live video feeds and reveal personal data to unauthorised viewers.

Weak identity and access management

Physical-security consoles and back-end platforms often ship with default credentials or hard-coded login pairs. In a hybrid-IT environment where IT and security teams collaborate more than ever, failing to enforce multi-factor authentication and strict role-based permissions, means any compromised user can unlock doors, disable alarms, or erase critical incident logs.

Supply-chain and third-party risks

Manufacturers of cameras and access-control devices, frequently rely on common software libraries, development toolkits, and third-party modules. A tainted firmware update can embed backdoors across hundreds of sites before anyone notices. Without rigorous vendor-attestation processes, organisations expose their perimeters to upstream compromise.

Insider threats and configuration drift

Security operators may open firewall ports to troubleshoot a malfunctioning card-reader device, then forget to close them. Over time, these ad hoc exceptions accumulate—often without documentation—leaving hidden entry points that attackers or rogue employees can exploit to sabotage operations or conceal theft.

Mitigation recommendations

To address these challenges, organisations must adopt a unified cyber-physical security strategy covering all network-attached assets and devices. Patch management and secure-configuration review remain critical. Cloud settings should be codified using infrastructure-as-code and standardised templates to reduce error. Identity controls must enforce zero-trust principles, with robust multi-factor authentication and granular permissions. Ongoing vendor risk assessments and regular user training, help manage supply-chain and insider exposures. Finally, continuous monitoring and automated drift detection, ensure that unauthorised changes to network or security policies are identified and remediated, before they can cause harm.

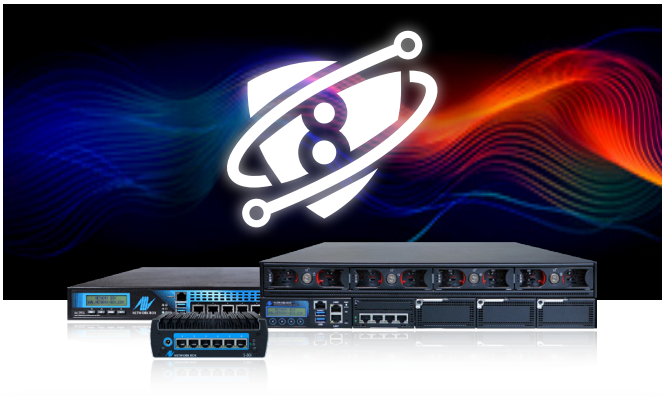
By following these recommendations and closing both cyber and physical gaps, organisations can safeguard people, property and reputation.

Network Box HIGHLIGHTS

Network Box 8 Features
July 2025

On Tuesday, 1st July 2025, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days. This quarter, for Network Box 8, these include:

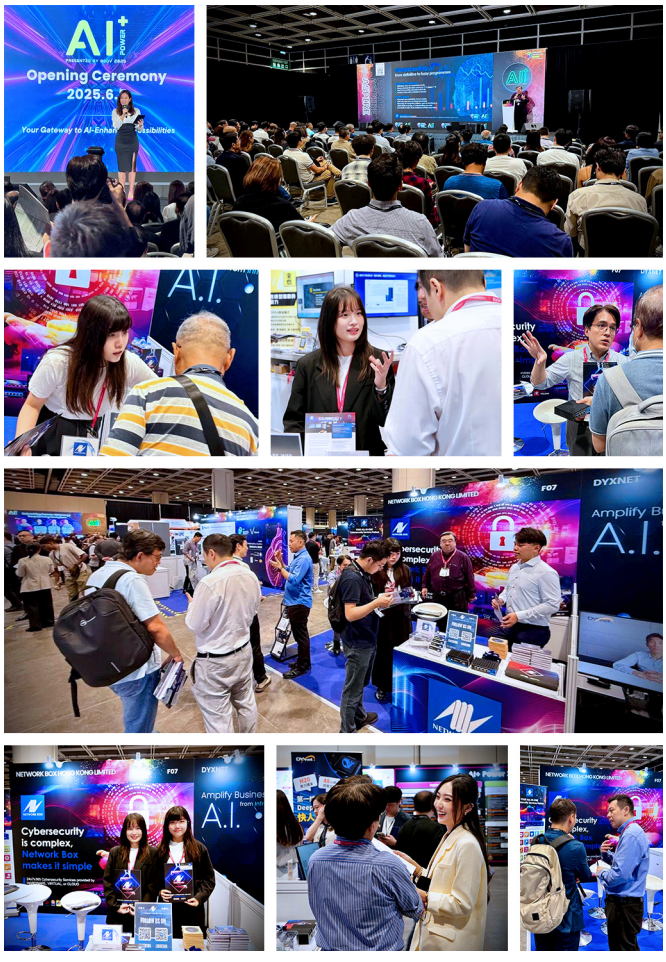
- Fix to LCD memory display on M and E series models
- Improvements to database watchdog monitor
- Enhanced support for new AES-GCM ciphers in SSL-VPNs
- Enhancements to active-backup mode in network interface bonding
- Provide support for configurable system-wide cryptographic policies (legacy, FIPS, etc)
- Improved validation in syslog target configurations
- Minor fixes to SSL-VPN server scripting



Network Box Hong Kong
Business GoVirtual AI+ 2025

Network Box Hong Kong was at the **Business GoVirtual AI+ 2025** Expo & Conference, which took place at the HK Convention and Exhibition Centre. Several thousand delegates from various countries converged to explore innovations in cybersecurity, AI-driven applications, infrastructure and platforms, blockchain with AI integration, and other related topics.

Network Box Managing Director Michael Gazely gave a keynote talk titled **"AI-Powered Disruption: How AI Is Transforming Cyber-Security"**. He then joined a high-profile panel moderated by WTIA (HK Wireless Technology Industry Association) to debate the future and evolving landscape of AI.



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