In the Boxing Ring
JUL 2024

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

Welcome to the July 2024 edition of In the **Boxing Ring**

This month, we are talking about **Network Box Engines, Signatures, and Policies**. Network Box has always had one primary goal for our security services: ***nothing malicious can be allowed to get through***. On pages 2 to 3, we discuss how we meet that goal.

Please note that this will be the last of these general articles for this year. Starting next month, we will present the four key components that will form Network Box's approach to security for the rest of 2024 and beyond: **NBRS-8**, **Endpoint Protection**, **NBSIEM+**, and **Unified Cloud Management**.

In other news, Network Box is proud to announce that the company won the EXCELLENCE AWARD in **Tech Company of the Year — *Innovation Technology Application***, presented by *Business GoVirtual*. And in this month's Technology Focus, we are spotlighting **Network Box Red Team Services**. Did you know Network Box offers Penetration Testing and Vulnerability Assessment services to help you with Risk Assessment, Audit, or Compliance Requirements?

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

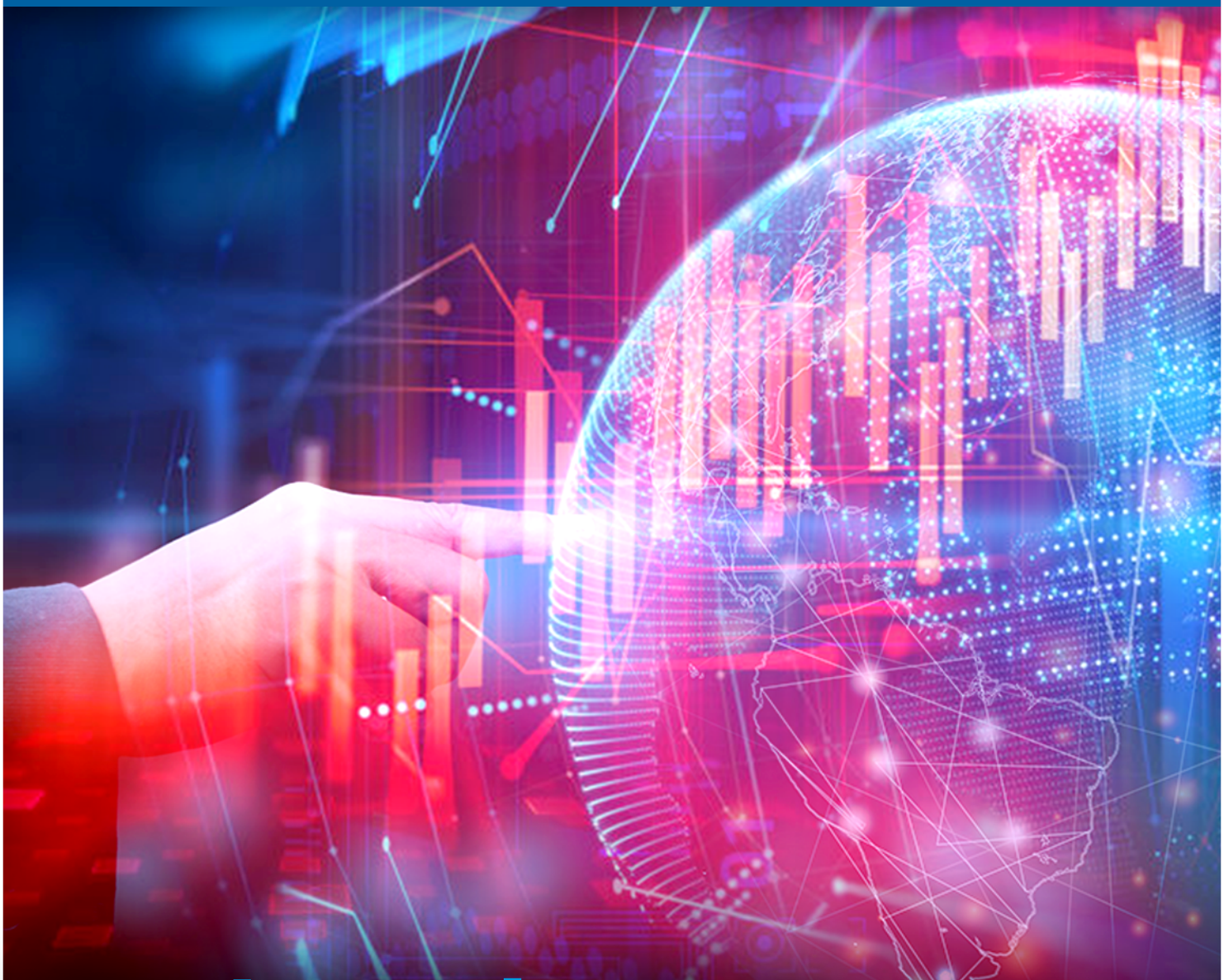
https://twitter.com/networkbox
https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse
https://www.linkedin.com/company/network-box-corporation-limited/
https://www.youtube.com/user/NetworkBox

In this month's issue:

Coming Soon...

Starting next month, we will present the four key components that will form Network Box's approach to security for the rest of 2024 and beyond:

- NBRS-8
- Endpoint Protection
- NBSIEM+ Enhancements
- Unified Cloud Management.



Network Box
Engines, Signatures, and Policies

Keeping an organization's digital assets secure nowadays is not at all simple and certainly much more complex than it was a decade ago. Not only are we faced with new and varied threats, but our data is now spread out over physical, virtual, and SAAS systems - often across multiple data centers and service providers.

With our 25th Anniversary fast approaching, Network Box has always had one primary goal for our security services: nothing malicious can be allowed to get through. The old saying that 'an ounce of prevention is worth more than a pound of cure' is so very true, and especially so when it comes to cybersecurity. Only by being as close to 100% effective as possible can we provide affordable security to organizations of all sizes.

So, how do we meet that goal?
Typically via a three-pronged approach:

1. Multiple Engines

Network Box products operate multiple engines to provide in-depth scanning, identification, and network traffic classification. For example, our flagship product, Network Box 5 (NBRS-5), currently has 18 firewall, 3 IDPS, 18 anti-malware, 25 anti-spam, and 15 content filtering engines. Each of those looks at traffic in a different way, and they all work together to provide the most comprehensive security available.

To pass through, malicious traffic would have to pass the checks of each independent engine. Compared to the single-engine approach of most competitors, this multiple-engine approach provides defense in depth in one single device.

2. Extensive Signatures, Heuristics, and Intelligence

Engines are only as good as the signatures, heuristics, and threat intelligence behind them. The foundation of Network Box security intelligence is our RepDB (Reputation Database) system. This is a massive collection of intelligence on IP addresses, URLs, File Checksums, Email addresses, Domains, and other such metadata associated with network traffic. This intelligence information is sourced from our own intelligence data, honeypots, spam traps, security metrics, etc., as well as from our partners worldwide.

Today, RepDB stores more than 47 million current and another 158 million historical classification rules covering 12 types of metadata and 63 categories. From our security partners, as well as RepDB, Network Box generates protection signatures, heuristics, and rules - all updated in real-time and distributed in seconds using our patented PUSH technology. NBRS-5 currently has more than 16,000 IDPS, 24+ million anti-malware, 30+ million anti-spam, and 7 million content filtering rules (not just simple signatures, but heuristics and smart rules capable of catching many threat variants).

3. Policy Enforcement

The final piece of the Network Box approach is policy enforcement. The goal of the multiple engines, signatures, heuristics, and intelligence, is to classify network traffic accurately. It is then up to the policy enforcement systems to enforce a robust security policy. This goes beyond the simple 'block and quarantine anything classified as malicious' of competing systems, as we offer a sophisticated rules-based approach taking into account not just the classification but also the metadata associated with that classification, the source, and destination, of the network traffic connection.

It is vital that the security policy deployed is both comprehensive and effective - and Network Box Security Operation Centres are tasked with working with customers to ensure that. 80% of security incidents may be caused by missing protection technology, but the remaining 20% result from that technology not being configured or maintained correctly. Network Box conducts weekly external view scans of all our customer networks, and combines that with quarterly security policy reviews to monitor adherence to best practices.

Ultimately, the security policy is entirely up to the customer to decide; with Network Box SOCs providing guidance and monitoring services.

By combining our multiple engines, signatures, heuristics, threat intelligence, policy enforcement systems, and SOC support, Network Box provides comprehensive and effective managed network security.

Network Box HIGHLIGHTS

Business GoVirtual Tech Awards 2024
Excellence Award

Network Box is proud to announce that the company won the EXCELLENCE AWARD in **Tech Company of the Year — *Innovation Technology Application***, presented by Business GoVirtual. The award recognizes tech companies that have harnessed the power of cutting-edge technologies to develop innovative products or services that possess the potential to create new opportunities or change industries or daily life in the near future.

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

Network Box Technology Focus

Did you know...
Network Box offers Penetration Testing and Vulnerability Assessment Services?

While businesses are well-versed in the importance of 'defensive security' such as firewalls, endpoint protection, SIEM, and MDM, it's less common for organizations to seek out vulnerabilities that hackers could exploit actively.This is why Network Box offers proactive OFFENSIVE SECURITY services, a crucial addition to your security strategy to help you with Risk Assessment, Audit or Compliance Requirements, or Incident Response.This includes:

- **Vulnerability Assessment** — low-cost, mostly automated, fast, but not risk-based.
- **Penetration Testing / Red Teaming** — done manually by experts, risk-based, better quality results, usually based around a scenario of a threat-actor.
- **Attack Simulation** — a detailed step-by-step analysis of attack techniques and tactics using MITRE ATT&CK data, providing the highest standard of results.
- **Incident Response** — post-incident remediation, computer forensics, formal information security audit, information security training and awareness.

For more details, please visit:
https://network-box.com/networkbox-redteam