NETWORK BOX
NEXT
GENERATION
MANAGED SECURITY

www.network-box.com

In the Boxing Ring AUG 2019

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the August 2019 edition of In the **Boxing Ring**

This month, we are talking about **The Network Box Difference**. Quite often we are asked to explain the difference between the Network Box Managed Security Services, and our (mostly Do-It-Yourself) competitors. Perhaps the clearest demonstration is how close the relationship to our customers is; we are there to help resolve problems and diagnose networking issues, and not just some voice in a distant call centre. Our service renewal and customer loyalty rates are the highest in the industry, but what exactly is the difference? Why is Network Box security so effective? On pages 2-3 we answer these questions, and highlight the Network Box approach to security.

On page 4, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

In other news, Network Box is proud to announce that the company is listed as a *Top Contributing Partner* in the **Microsoft Active Protections Program (MAPP)**. In this month's media coverage, Network Box Hong Kong was interviewed by **E-Zone Magazine** and **JobMarket Magazine**; Network Box USA was featured in **SC Magazine** and **infosecurity Magazine**; and **it-daily.net** interviewed Network Box Germany.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2019

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 us by 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:

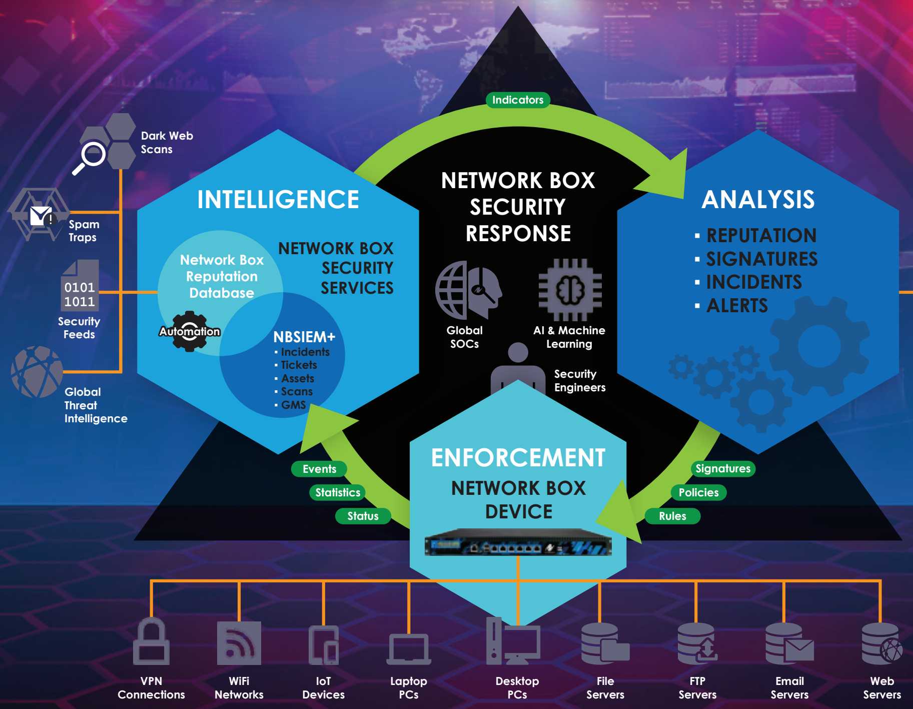
The Network Box Difference

Quite often we are asked to explain the difference between the Network Box Managed Security Services, and our (mostly Do-It-Yourself) competitors. Perhaps the clearest demonstration is how close the relationship to our customers is; we are there to help resolve problems and diagnose networking issues, and not just some voice in a distant call centre. Our service renewal and customer loyalty rates are the highest in the industry, but what exactly is the difference? Why is Network Box security so effective?

When Network Box was formed, we looked at and addressed the fundamental statistics:

- 80% of organisations were hacked, exploited, or infected because they did not have adequate protection. They got a virus because they did not have anti-virus technology. They got an intrusion because they did not have Intrusion Prevention Systems. So we put all the core protection technologies in one single appliance device.
- The remaining 20% had problems because the protection they had was either not configured correctly, or not maintained. Virus signatures had stopped updating. Protection systems were not updated to address the latest threats. So, we launched the first managed security service to look after our own devices, expertly installing, configuring, and maintaining our devices protecting customer networks.

Since then, over the past 20 years we have amassed an enormous amount of intelligence. We have grown and learned. We have extended the protection capabilities of our devices, expanded the protection and policy engines, and improved the quality, quantity, and rate of protection signature and heuristics delivery; using our patented PUSH technology, but also embracing new cloud delivery mechanisms.



But what makes Network Box different?

In a word (or two): Security Response. We have developed Network Box Security Services into a feedback loop; joining Intelligence, Analysis, and Enforcement into a single holistic real-time framework, for the protection of customer networks.

Intelligence

At the heart of Network Box Security Response is a big data scale database called RepDB (Reputation Database). Here we store network indicators (IP addresses, email addresses, URLs, fingerprints, hashes, etc) and classify them. This forms a database of Intelligence information classifying and storing the history for hundreds of millions of network indicators. We update this database with feeds from partners, as well as global threat intelligence, spam traps, honeypots, and the dark web; in total more than a hundred different sources of information.

We also receive data feed flows from end-user devices under management, and these include things like statistics (how many times a particular signature fired, for example), events (a malware block, for example), and status.

All this information is fed into NBSIEM+, and made available to security engineers in our Security Operation Centres, as well as customer administrators.

Analysis

Threat indicators from RepDB then flow into our big data analysis engines to produce reputations, signatures, incidents, and alerts. Most of the work here is automated, using heuristics, AI machine learning, and other behavioral based systems. For example, one system we have is called OUTBREAK - it compares the last three minutes of activity on the Internet again the preceding 57 minutes, to track the behavior of individual threats and vectors. Machine Learning systems look at patterns of events to isolate the needle that is targeted attack behavior from the haystack that is the Internet Background Radiation of scanning, probing, and other such nuisance.

Enforcement

Signatures, Policies, and Rules, flow from the Analysis stage into the enforcement engines running on Network Box devices both on customer premises as well as in the cloud. Here these signatures are used to classify network flows and objects, for policy enforcement, and statistics are kept to record the effectiveness of the enforcement protection.

In this way, a feedback loop is formed. Statistics and Events from the enforcement devices flow into Intelligence gathering engines that combine with partner and global feeds to build up a huge Intelligence database (called RepDB). Indicators from there flow into the Analysis engines where heuristics, AI, and Machine Learning systems produce Reputation scores, signatures, incidents, and alerts. These flow into the enforcement engines on customer devices to improve the categorization systems and enable effective policy enforcement. Feedback loop round trip times through all three systems (Intelligence, Analysis, and Enforcement) are typically of the order of less than a minute (and mere seconds in some cases).

All the above is overseen by the staff at Network Box Security Response, as well as local Security Operation Centres and customer administrators.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 6th August 2019, 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.

Network Box 5 Features

August 2019

This month, for Network Box 5, these include:

- Introduce support for DHE and EC cryptography in cluster sync connections
- Improvements to logging display for imap4 client holistic records
- Improvements to search results and performance, when searching by threat ID
- Enhancements to NBSIEM+ log concentrator, to improve performance and reliability in cases of poor Internet connectivity
- Improvements to KPI reporting, In cases where large reports are being produced
- Fix to duplicate email alerts for configurations containing multiple alert recipients
- Further support for optional 4G modem options
- Improvements to kernel routing with IPSec passthrough VPN tunnels

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 listed as a Microsoft Top Contributing Partners in the Microsoft Active Protections Program (MAPP)

Network Box is listed as a *Top Contributing Partner* in the **Microsoft Active Protections Program** (**MAPP**). This listing is in recognition of Network Box's Security Operations Centre, and Research & Development teams' hard work to making a significant contribution to global cyber-security, by Microsoft.

LINK: https://bit.ly/31snP7Z

> MAPP provides security and protection to customers through cooperation and collaboration with industry leading partners. This bi-directional sharing program of threat and vulnerability data has proven instrumental to help prevent broad attacks and quickly resolve security vulnerabilities in Microsoft products and services.

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 Hong Kong E-ZONE Magazine

Network Box's Managing Director, Michael Gazeley, was interviewed by E-ZONE Magazine about today's increasingly dangerous cyber-threat landscape, and potential critical issues as we head towards 2020.

Network Box Media Coverage

SC Magazine

Why is election security a partisan issue?

LINK: https://bit.ly/2ODRbhW

infosecurity Magazine

Silicon Valley Issues Election Security Report

LINK: https://bit.ly/2GLjDIs

it-daily.net

New phishing simulation from Network Box

LINK: https://bit.ly/31he4t1

JobMarket Magazine

More Enterprises are strengthening their cybersecurity due to increased cyber-attacks

LINK: https://bit.ly/2OFssKd