In the Boxing Ring

JAN 2020

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the January 2020 edition of In the **Boxing Ring**

Happy New Year. Network Box would like to extend our very best wishes to you for 2020. This year will be the 20th anniversary of Network Box providing Managed Security Services, and throughout all that time, we have always aimed to provide all the key security services in one device which is configured, maintained, and monitored to international security standards. We also regularly audit ourselves, employing external auditors to ensure that we meet those standards, including triple ISO certification and PCI conformance. Moving forward to the next decade, this month on pages 2 to 3, we be taking **a look ahead to the Network Box platform in 2020 and beyond**.

On page 4, we highlight the features and fixes to be released in this month's Patch Tuesday for Network Box 5. **Please note that from this month onwards we will switch to a quarterly Patch Tuesday cycle for Network Box 5.**

In this month's Media Coverage, Network Box was featured in the **South China Morning Post**, **The Standard**, and **funkschau**. Finally, to round-up another eventful year for Network Box, we have complied all the key events of the last twelve months in the 2019 edition of **Year in Focus**.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
January 2020

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:

A look ahead to the Network Box platform in 2020 and BEYOND

Network Box has always been the predator drone of Security Devices. Whilst our competitors try to rip the cockpit out of their products to add on remote control, Network Box has from day 1 been designed to be configured and maintained remotely by our Managed Security Service delivered through our global network of Security Operation Centres. Quite simply, we don't have a cockpit on our device, and nowhere for the 'pilot' to sit.

This year will be our 20th anniversary of providing Network Box managed security services, and the top three reasons for experiencing security issues still have not changed in all that time:

1. **Lack of protection (or of a particular component of protection).**

2. **Mis-configuration of the protection (or lack of maintenance of patches and signatures).**

3. **Failure to follow best security practices.**

Network Box has been specifically designed to address those top 3. We have always aimed to provide all the key security services in one device, expertly configured, maintained, and monitored, to international security standards. And we audit the hell out of ourselves, employing external testers to ensure that we meet those standards (including triple ISO certification and PCI conformance).

Migration to the Cloud

As we look at both how the security market is developing, as well as the upcoming threats we see on the horizon, it is clear that more and more customers are moving their data centres and applications to the cloud. Physical premises still exist, and that infrastructure still needs client-side protection, but the core organizational information is now mostly remotely stored (either in self-owned or multi-tenant applications), and mostly virtualized.

We call our product the 'Service Delivery Platform', and don't care whether the box is a hardware appliance, or a virtual device running in either the customer's own virtual infrastructure (VMWare, etc), or a multi-tenanted cloud. We support Rackspace, Azure, and Amazon's AWS public clouds. No matter how the device is deployed, or the model or size of appliance, we run the same firmware and offer the same set of security tools. The appliance is merely the platform we use to deliver our security services on.

A Centralized Cloud Portal

Our primary focus for the past year, and for the foreseeable future, is on our centralized multi-tenanted cloud portal called **NBSIEM+**. This replaces our ageing Box Office system to provide a single interface for customers, resellers / partners, and Security Operation Centres, to manage devices. NBSIEM+ allows us to provide a centralized view of all devices under management, in a single secure interface hosted in the cloud. Today, Box Office provides a hierarchal view of devices; and in the coming year, NBSIEM+ will provide the same for events, incidents, and reporting.

The overall direction we are headed for 2020 is the integration of Security Operation Centre management and maintenance functionality to the NBSIEM+ platform. This means:

- Functions typically performed from admin web portal will be able to be done from NBSIEM+ directly. Long-term, NBSIEM+ will be able to do all that admin web portal can do today, and so much more.

- As NBSIEM+ supports ownership hierarchies, configuration changes will be able to be applied across a selection of appliances. This will facilitate organization level policies, on a global, regional, and per-site basis - with or without SOC involvement.

- Similarly, reporting in NBSIEM+ will be based on the ownership hierarchy. Both real-time widgets, and periodic reports, will be able to be produced.

- Our reporting will be template based, with common templates for common compliance and management reports.

- The approach employed is that the request is made to NBSIEM+, and then NBSIEM+ decides whether to access the data locally (if available), or reach out over a secure cluster sync connection to the remote managed device to retrieve the data. For example, an event log may be stored locally (in NBSIEM+), or retrieved remotely.

- The long-term goal here is for a single interface (NBSIEM+) to all Network Box services (whether delivered in the cloud, or on-premises devices).

- And lastly, but not least, with NBSIEM+ we are moving to managing customer devices other than Network Box - retrieving the event logs, applying security intelligence, and generating incidents automatically.

Multi-Tenanted Cloud Services

We've already released several multi-tenanted cloud services including Cloud Reputation, Cloud Dark Web, Cloud Mail Backup, and Cloud DNS Backup. Upcoming new releases in 2020 will include:

- Cloud DNS Hosting (including integration to GMS availability for multiple Internet links and disaster recovery)
- Cloud Mail Scanning (including User Portal)
- Cloud Web Scanning (including User Portal)

These releases will be integrated to NBSIEM+ to allow for seamless management (no matter if the scanning is via muilti-tenanted cloud services, or a managed device).

The Box as a Content Classification and Policy Enforcement Engine

This all furthers our goal of the Network Box Service Delivery Platform (aka 'the box') behaving as a content classification and policy enforcement engine. It examines network traffic, classifies it, and then applies policy rules to that classification to deny/permit the traffic. The 'box' can be a physical device, a virtual device in a private or public cloud, or a multi-tenanted virtual cloud solution - all managed the same via NBSIEM+.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 7th January 2020, 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
January 2020

This month, for Network Box 5, these include:

- Fine tuning of defaults for some Global Monitoring System sensors
- Support for identification and display driver for new Box Model types
- Performance improvement in configuration and entity updating
- Extend support for Internet Explorer 8 (HTML5 javascript issue)
- Improve performance and reliability of health monitoring connections
- Support for AES192 cipher in phases 1 and 2 of IPSec VPNs
- Fix for utilization statistic storage after 1st January 2020

Revision to Patch Tuesday Policy for Network Box 5

Due to the stability of the Network Box 5 platform, and ability to remotely address most content classification and protection engines via our heuristic signatures and PUSH updates, with effect from January 2020 we will switch to a quarterly Patch Tuesday cycle for Network Box 5. The Patch Tuesdays will now fall on the first Tuesday of each quarter (1st Tuesday in January, April, July, October), rather than every month.

Essential security fixes will continue to be released out-of-cycle, if necessary.

Network Box
Security Response

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

**NEXT
GENERATION
MANAGED SECURITY**

NETWORK BOX

Network Box
Year in Focus 2019

2019 was another great year for Network Box. In addition to the many awards won, Network Box was listed as a **Microsoft Top Contributing Partners** in the *Microsoft Active Protections Program (MAPP)*. Network Box was also featured in numerous media outlets, and participated in various security events around the globe. Furthermore, the past year saw the launch of the **Network Box Dark Web Monitoring Service**, the **Network Box Spam Reporter** plug-in for *Microsoft Outlook*, and the **S-80i** hardware platform for the SME market.

As a special end-of-year summary, Network Box has complied all the key events of the last twelve months in the 2019 edition of Year in Focus.

LINK: https://network-box.com/sites/default/files/files/Year_in_Focus_2019.pdf

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
Media Coverage

SCMP
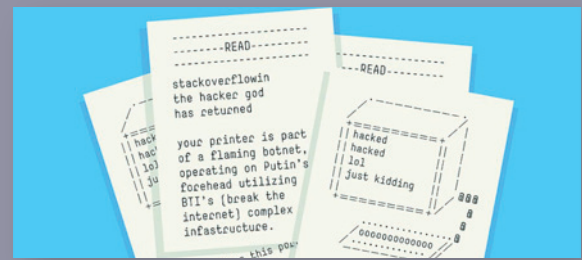**New year lucky draw crashes just minutes after registration opens**
LINK: https://bit.ly/2QiQKby

South China Morning Post

funkschau
**Hintertür Netzwerkdrucker
[Back door network printer]**
LINK: https://bit.ly/2MQGTrg

The Standard
Is your Start-up protected from hackers?