In the Boxing Ring JAN 2019

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

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

This month, on pages 2 to 3, we look at **Network Box Managed Security Services in 2019 and Beyond**. We are moving to an architecture where it does not matter where the device is located, whether it is physical or virtual, whether it is an individual device or a multi-tenanted cloud service, or even the manufacture of the device. Our aim is to seamlessly correlate event logs and security intelligence on a global basis; moving from single device events, to focus on incidents with global search capability.

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 won the Gold Award, at the **Best Enterprise Risk Management (ERM) Awards 2018**. In addition, Network Box Germany participated in **IT-Sicherheitstag NRW,** organized by the Chambers of Commerce and Industry of North Rhine-Westphalia. Furthermore, Network Box was interviewed by the **SCMP** regarding current cyber threat issues. And finally, the 2018 edition of **Year in Focus** is now available for download.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
January 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://plus.google.com/u/0/107446804085109324633

In this month's issue:

Network Box Security Services in 2019 and Beyond

As we start the new year, it seems an appropriate time to look at the architecture for Network Box security services in 2019 and beyond. We'll be looking at two areas: customer "premises" (either physical or virtual), and the Network Box Services cloud.

Customer "Premises"

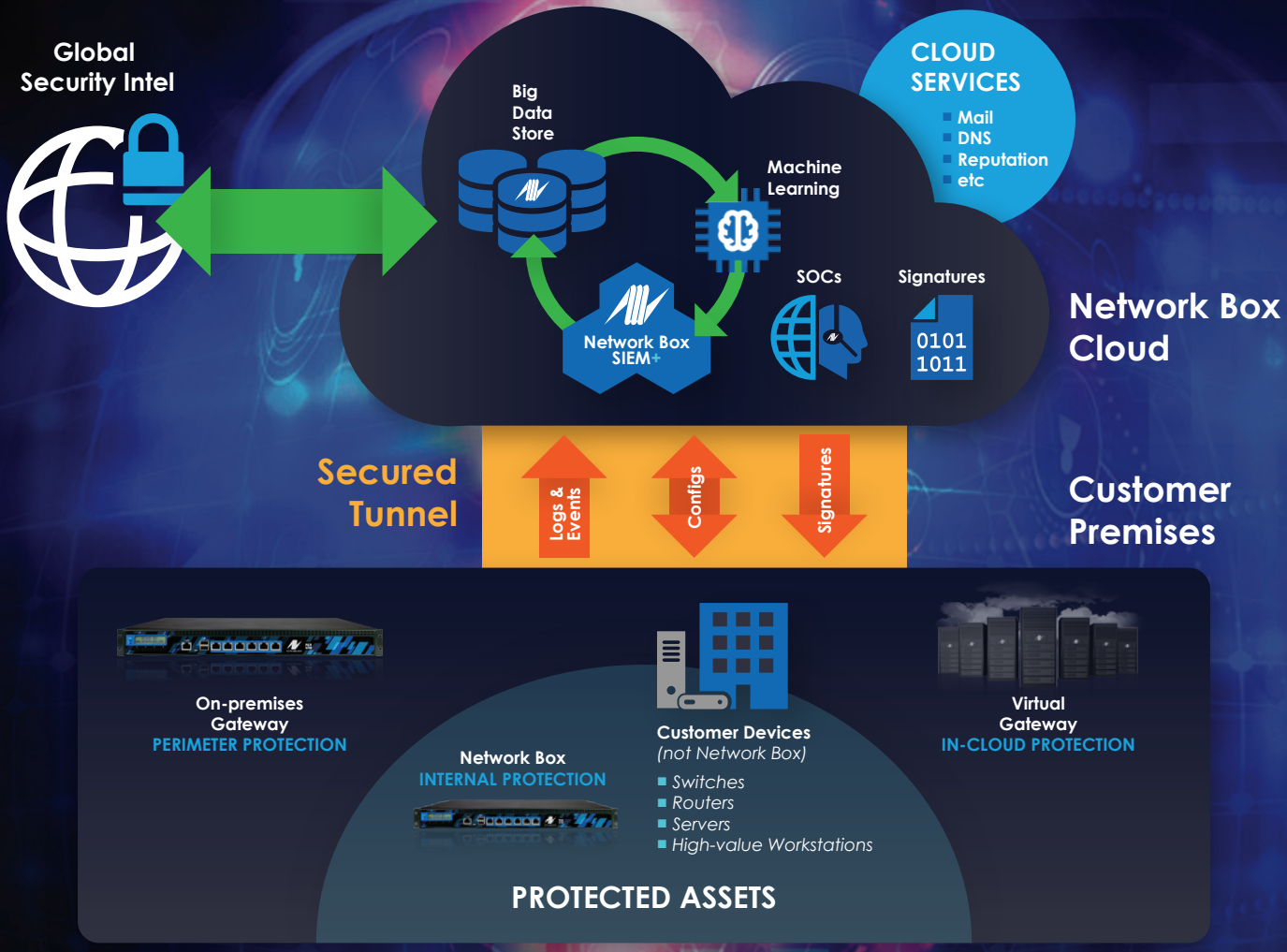
Customer premises can be either physical locations (offices, data centres, homes, etc), or virtual environments (such as local vmware clouds, or public clouds like Amazon, or Azure). Inside these premises are the protected assets - the devices and computers holding the data to be protected.

> Mobile devices introduce another layer of complexity to data protection. In general, Network Box recommends that mobile devices outside the customer premises be always protected, using VPN and proxy technology coupled with strong policy control. Unprotected mobile devices should be treated in the same way as visitors to your network - with extreme caution and care.

A Network Box device can only protect traffic that passes through it, and that has traditionally meant Network Box protection was placed at the gateway to the Internet (where visibility of the malicious traffic, and threat, was the greatest). However, with the proliferation of network links (such as VOIP, MPLS, VPNs, etc), we are seeing increasing demand for Network Box devices to be placed inside the customer network to fulfill IDS or IPS roles. We are also deploying Network Box systems internally as firewall and IPS devices; performing a network segmentation role.

Whether the Network Box device is a physical or virtual appliance, deployed at the perimeter or inside the network, is irrelevant to us; it is merely the Service Delivery Platform - the means by which we deliver our protection services.

Then we have the customer devices producing event information; routers, switches, servers, high value workstations, and other (not Network Box) security appliances. Starting in 2019, our **Network Box SIEM+** product can take event logs from these devices, and securely upload them to the cloud for event correlation, searching, and archiving.



Network Box Services Cloud

Since its launch, Network Box has provided security services based on regional SOCs managing Network Box appliances installed in customer premises. We have provided remote configuration synchronization, patented signature PUSH, global monitoring, and support services.

Still today, the vast majority of our customers' protected data is in customer premises (either physical or virtual), and Network Box appliances placed within those premises provides the best possible protection. However, we recognize that an increasing amount of data is being moved into public clouds. In recent years, we have extended our support to provide a number of cloud services (such as cloud mail backup, cloud DNS backup, and cloud reputation). We will continue to extend the cloud services we offer, as well as provide tight integration with other cloud service provider partners. Our role is to protect the data, no matter where it is stored or what networks it transits through; and the services we provide will continue to be designed to meet the demands of that role.

Over the past years, Network Box has invested heavily in the development of a multi-tenanted cloud framework to serve as the backbone for our future. Existing cloud services are being migrated into this new framework, and new services developed. This new framework is based on cloud level big data storage, horizontally scalable to billions of correlated indexed event records. Only by leveraging such cloud storage technology can we address the issues of correlating not just one customer's individual Network Box events, but across all Network Boxes and all other security devices that each customer has. We can also scale up to further correlate events across customer industries, and even globally.

The potential of such technology to solve today's security issues is impressive. Given a particular threat indicator, we can instantly know not just the history on one particular Network Box device, but can now correlate that threat across all devices belonging to that customer, comparing against other customers in the same industry, as well as globally. Using both machine learning and human security engineers in our Security Operation Centres, we are tackling the task of identifying the 'needle' of security incidents inside the 'haystack' that is millions of security events every second.

As Box Office migrates to become a component of **NBSIEM+**, fulfilling the asset tracking and support ticketing functions, we are directly connecting managed Network Box 5 devices to this system to allow for:

1. Synchronization of configuration sections across clusters of Network Boxes
2. Updating of configurations
3. Consolidated reporting

A single authorized change made to a configuration in **NBSIEM+** can instantly be replicated across a global cluster of devices.

By consolidating our SOC support systems and tightly integrating the remote Network Box devices themselves to our cloud based systems, we are moving to an architecture where it does not matter where the device is located, whether it is physical or virtual, whether it is an individual device or a multi-tenanted cloud service, or even the manufacture of the device. Using NBSIEM+, our regional data centres, and our cloud infrastructure, we aim to seamlessly correlate event logs and security intelligence on a global basis; moving from single device events, to focus on incidents with global search capability.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 8th January 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
January 2019

This month, for Network Box 5, these include:

- Enhancements to license status control
- Improvements to remote user authentication mechanisms for ldap, ntlm, and radius
- Improvements to local entity-based admin and user authentication
- Extended support for large report histories in admin portal
- Additional support for NBSIEM+ logging
- Enhanced support for NOC systems

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 wins Best Enterprise Risk Management Awards 2018

Network Box is extremely proud to announce that the company won the Gold Award, at the **Best Enterprise Risk Management (ERM) Awards 2018**. This highly prestigious award is given by the Academy of Professional Certification (APC), to honour companies, NGOs, and organizations, in any industry, that demonstrate excellence and achievement in Enterprise Risk Management, leading to ISO, and best practice world class standards.

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 Germany
IT-Sicherheitstag NRW

Network Box Germany participated at the **IT-Security Day NRW**, organized by the Chambers of Commerce and Industry of North Rhine-Westphalia, which took place in the Wuppertal Historical Town Hall.

Network Box Media Coverage

South China Morning Post

HSBC tightens e-wallet app security after PayMe breach allowed access to 20 accounts holding HK$100,000

LINK: https://bit.ly/2R2amCJ

Hong Kong police probe bomb-threat emails demanding US$20,000 in bitcoin

LINK: https://bit.ly/2F2zqU4

Network Box Year in *Focus* 2018

2018 was another great year for Network Box. In addition to the many awards that the company won, Network Box was featured in numerous media outlets, and participated in various security events. For more details, please refer to the 2018 edition of the **Year in *Focus***.

LINK: https://bit.ly/2F24mUa