In the Boxing Ring OCT 2024

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

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

This month, we are talking about **Endpoint Protection**. Network Box has protected organizations against network security threats for over two decades, focusing primarily on the perimeter. While this approach has been effective and economical, Network Box will be launching our endpoint security offering to expand our service scope and offerings. **Network Box X** extends our managed security services from the perimeter gateway to the endpoints and SAAS cloud services. On pages 2 to 4, we discuss this further and highlight its key features.

On page 5, we highlight the enhancements and fixes for Network Box 5 and our cloud services that will be released in this month's Patch Tuesday.

In other news, Network Box Hong Kong participated in a cybersecurity event organized in partnership with the *Hong Kong Security Association.* Additionally, Network Box China was at the **2024 China Cybersecurity Week**. And in this month's Technology Focus, we highlight the Network Box **Cloud Email Backup** and **Cloud DNS Backup** services.

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

Endpoint PROTECTION

In Network Box 8

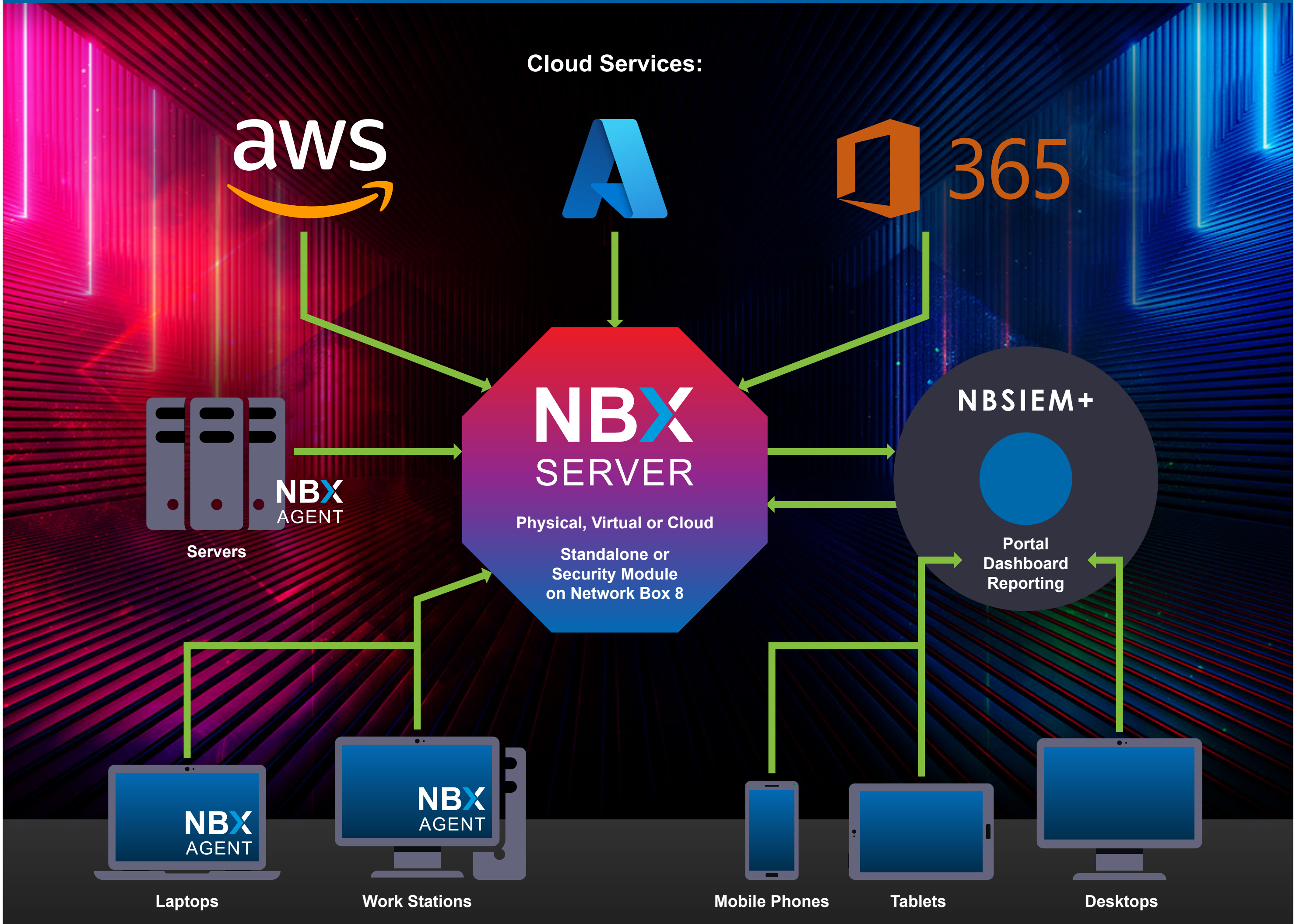
For more than 20 years, Network Box has been protecting organizations of all sizes against network security threats, focusing primarily on the perimeter — the junction of the organization's network with the hacker's playground known as 'The Internet'.

This was simply because that was where most attacks originated from or exfiltrated data went. So long as the traffic passes through the Network Box appliance at the perimeter gateway, it can be protected (both inbound and outbound). As virtual systems gained popularity, Network Box expanded its services to offer both virtual and cloud-based devices (in addition to the existing physical boxes we've always offered).

Time and time again, our approach of delivering Managed Security Services via our perimeter Service Delivery Platform (aka 'The Box') has proved both effective and economical - scaling from the smallest offices to enterprises with thousands of users. 80% of computer security issues result from missing protection components; the remaining 20% are from misconfiguration or undetected failures, proving the effectiveness of a Managed Security Service delivering the security components combined with professionally configured, monitored, and maintained protection.

Then, a few years ago, Network Box expanded our offering with NBSIEM+. This allowed us to manage our Network Box devices and take event logs from other networking equipment (routers, switches, firewalls, etc.), analyze them with our security rules engines, and consolidate reporting and incident response into one easy-to-use cloud-based portal. Today, NBSIEM+ handles more than 400 million security events a day (more than 4,600 each second) from thousands of devices around the globe.

As powerful as NBSIEM+ is and (when combined with Network Box appliances at the perimeter) as good a view of the network it provides— when it comes to servers, workstations, and laptops, SIEM technology is limited. Events logs tell only a part of the story. We must bring security technology to the endpoints to get a fuller picture. That is why this year, Network Box will be launching our endpoint security offering, which we are calling **Network Box X**.



Endpoint Security Architecture

Network Box will deliver endpoint protection under our **Network Box X** framework, which is a core part of Network Box 8. This consists of three major components:

1. For Microsoft Windows, Apple OSX, or modern Linux endpoints (laptops, workstations, servers), a small user-space program called NBX AGENT will be deployed on each endpoint.
2. An NBRS-8 Security Module called NBX SERVER will be deployed as an additional security module on existing Network Box 8 (NBRS-8) appliances or as a separate virtual, physical, or cloud-based server (for larger deployments). This server collects events from NBX AGENT running on the endpoints but can also directly pull events from cloud services such as Office 365, Azure, AWS, and others. The events are stored locally on the server itself and processed by a rules engine running several thousand security rules and heuristics.
3. NBSIEM+ receives security alerts (events of sufficient severity to warrant escalation) from NBX SERVER, which are integrated into the existing NBSIEM+ framework for incident response. In addition, a full cloud web portal is provided for monitoring and endpoint investigations of incidents.

This way, costs are optimized by keeping the event logs close to the endpoints and minimizing privacy issues such as GDPR. Only events requiring escalation are forwarded to NBSIEM+ (while still providing NBSIEM+ users full remote access to the original events if necessary for investigation).

Utilizing the best open source technology, combined with commercial engines, intelligence feeds, and threat protection, Network Box X extends Network Box protection from the gateway down to the endpoint and up to your SAAS cloud infrastructures.

NETWORK BOX X

Network Box X Features

We can divide the feature set of Network Box X into three sections. Let's look at some of the core features that make up each.

1. Endpoint Security

Event Collection: Running on Windows, OSX, and modern Linux endpoints, the NBX AGENT collects statistics, inventory, security events, and other such information and forwards it to the NBX SERVER for storage and processing.

Configuration Policy: The configuration policy of each endpoint is continuously assessed against best practice security standards (based on Center for Internet Security {CIS} security benchmarks), as well as locally defined policies, and reported on.

Malware Detection: In addition to integrating with common endpoint anti-malware engines, NBX offers behavior-based malware detection using a combination of file integrity monitoring, registry monitoring, and security events.

File Integrity: NBX can continuously monitor directories, files, and the Windows registry for changes. It accomplishes this using file metadata and content checksums.

Active Response: As well as alerting to issues, NBX allows the server to command an active response to a detected threat—usually in response to a specific rule or heuristic being triggered. Various active response actions are supported, including blocking specific source IP addresses, users, or network segments.

2. Cloud Security

Event Collection: In addition to receiving events from endpoints running NBX AGENT, the NBX SERVER can also directly pull events from SAAS cloud services such as Office 365, Azure, AWS, and others.

Platform Integration: Beyond events, NBX SERVER has deep platform integration for specific services within AWS, Azure, Google Cloud, Github, and others.

Cloud Endpoints: The NBX AGENT can be deployed on virtualized machines within cloud environments (typically running Windows or Linux) to provide deeper insight and control of these cloud-based endpoints.

Container Security: When installed on an endpoint running Docker or Kubernetes, the NBX AGENT can monitor individual container events and health.

CSPM: Cloud Service Posture Management (CSPM) is the continuous assessment and monitoring of cloud systems. NBX uses CSPM to look for misconfiguration, vulnerabilities, and potential threats.

3. Threat Investigation

Threat Hunting: As a platform unifying XDR and SIEM, collecting event logs from the myriad of networking devices within the organization and across the clouds, NBX provides a single centralized view for analyzing and responding to all that data. Using NBX's threat intelligence, an incident can be followed across the network to determine and limit its impact.

Event Log Analysis: All Event Logs in NBSIEM+, regardless of source, are unified into one simple format. Powerful analysis tools are provided to drill down and look for correlations between events or their metadata.

Vulnerability Detection: The NBX AGENT collects inventory details from each endpoint, including software repositories, applications installed, and their versions. The NBX SERVER then compares this against known vulnerabilities and reports accordingly.

Incident Response: Fully integrated into the NBSIEM+ incident response system, NBX provides configurable rules for escalation to NBSIEM+ and, within NBSIEM+, further rules for incident response.

Compliance: Combining results from all the services within NBX, events are highlighted with each related industry security standard. In this way, we can assist with reporting on compliance against PCI DSS, GDPR, HIPAA, NIST 800-53, and TSC standards.

> **To be released towards the end of 2024, Network Box X extends our Managed Security Services from the perimeter gateway to the endpoints and SAAS cloud services, all delivered through our cloud-based NBSIEM+ portal. In a typical deployment scenario, NBX AGENT will be deployed on all the endpoints, and cloud services (such as AWS, 365, etc) will be configured in NBX SERVER. Thus, the events from NBX, combined with the data already in NBSIEM+ (from Network Box appliances, routers, switches, and other firewalls), can be viewed and reported on from one cloud-based web portal. With such a deployment, you can drill down to inspect individual endpoints, no matter where they are - showing regulatory compliance, software inventory, vulnerabilities, hardware configuration, registry entries, running process, etc. All without leaving the comfort of your desktop or mobile phone.**

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 1st October 2024, 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

October 2024

This quarter, for Network Box 5, these include:

- First phase deprecation of the networkbox@network-box.com email address used for report emails
- Improvements to GMS suppression functionality
- Period update to IP geolocation accuracy
- Various improvements to SOC configuration and box maintenance systems

Regarding the deprecation of the networkbox@network-box.com email address, we have used that address for some time now. However, with the evolving changes to email and the importance of email security features such as DKIM and SPF, it is becoming increasingly difficult to use our global @network-box.com domain in this way. Accordingly, this month, our regional SOCs will be migrating report emails to come from either their own domains or customer-specific email addresses. This should improve the reliability of report email delivery (particularly when the destination of the report is big email service providers such as Microsoft 365, GMAIL, etc).

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 Hong Kong
Cybersecurity Seminar

Network Box Hong Kong participated in a cybersecurity seminar titled, "Securing Tomorrow: Unified Approaches to IOT Vulnerabilities, Access Management, and AI Surveillance," organized in partnership with the Hong Kong Security Association.

During the event, Managing Director Michael Gazeley highlighted the latest cyber threats to IoT devices, delved into various vulnerabilities and attack vectors, and offered practical prevention strategies.

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:

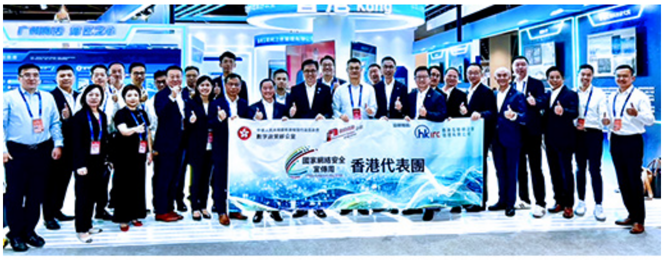
Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong.

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com

Network Box China
2024 China Cybersecurity Week

Network Box China's Director, Anthony Or, was part of the HKSAR Digital Policy Office delegation at the **2024 China Cybersecurity Week**, which took place in Nansha, Guangzhou. The delegation participated in multiple events at the cybersecurity technology summit to promote and strengthen public awareness of cybersecurity.



Network Box Technology Focus

Did you know...

Network Box can help alleviate problems due to network outages and ISP-related connectivity issues with free in-the-cloud backup services.

Cloud Mail Backup - alleviates the business risk of lost or bounced emails by backing up undeliverable incoming emails in the cloud and delivering them to you when the issue has been resolved.

Cloud DNS Backup - allows you to use Network Box's extensive network of DNS servers to provide backup in the cloud.

LINK: https://network-box.com/cloudbackups