In the Boxing Ring JUN 2023

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the June 2023 edition of In the **Boxing Ring**

This month, we are pleased to announce the Network Box **Managed Zero-Trust End-Point Security** solution is now available to customers and has been released globally. To coincide with the release, we thought illustrating some example deployment case studies might be helpful. Thus, on pages 2 to 3, we present three case studies demonstrating different deployment approaches.

In other news, Network Box regional offices participated in various events, workshops, and seminars. Network Box Germany participated in ComTeam Roadshow events, Network Box USA was at the Channel Partners Conference, and Network Box Hong Kong hosted a cybersecurity seminar. And in this month's global security headlines, there were security issues with ChatGPT, Microsoft Azure, Cisco, WordPress, Toyota, Suzuki, and Barracuda Networks.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
June 2023

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:

Managed Zero-Trust End-Point Security

With the Network Box managed Zero-Trust End-Point Security solution now available and released globally, we thought showing some example deployment case studies might be helpful. This month, we present three case studies illustrating different deployment approaches for whitelisting technology.

Case 1 - The Reactive

The user here has a network of approximately fifty workstations, laptops, and servers. All run traditional antivirus technology. A salesman took his laptop out of the office and got infected with some trojan malware while on a business trip. Upon returning to the office, a ransomware application was downloaded and executed by remote hackers - encrypting his laptop and files on several network shares. The network admins have already disconnected and isolated what they could but are concerned that with the trojan application in place - hackers have remote access to the network for lateral spread. Taking everything offline, forensic imaging, and one-by-one cleaning things up would take an estimated 7 to 10 days, with associated business impact costs.

In cooperation with Network Box SOC, the following actions are taken:

- All suspected infected machines are taken offline and rebooted into safe mode. Zero-trust End-point security is installed from USB, and machines rebooted into a group-based application control policy only permitting a very limited set of pre-trusted applications to be run (primarily Microsoft and some business-critical applications). At this point, these machines are safely brought back online, used as normal, and critical data is extracted.
- A Network Box device is placed at the Internet perimeter to replace the simple firewall there before (with zero outbound policy), and effective policy rules are put in place to control both inbound and outbound traffic. Infected LAN, IDS, and IPS engines are enabled to monitor and control outbound traffic.

With the hackers locked out of the network and the infected machines back under control, the business impact is limited, and ransomware-encrypted files can be restored from backups.

Case 2 - The Cautious

Here, we have a large network of several hundred workstations, laptops, and servers. Traditional antivirus technology is run on these machines, and the network is protected at the perimeter by a Network Box. The owners and administrators are concerned that an end-user will make a mistake and click on something they shouldn't - potentially bringing down the entire network.

We identify key high-risk workstations and servers, including:

- Internet-accessible servers running web, email, and collaboration software
- Accounts workstations
- Key decision-maker workstations (including high-level executives, the financial controller, etc.)
- Out-of-the-office laptops

Zero-Trust End-Point Security is deployed to all those high-risk machines and runs in monitoring mode for two weeks. During that time, Network Box SOC staff monitor the applications being run and whitelist as necessary. Some potentially unwanted applications are identified, and Network Box SOC staff work with the admins to address these on a case-by-case basis. Towards the end of the two weeks, the number of alerts raised for unrecognized applications falls to zero, and the machines moved to enforcing mode (blocking the execution of untrusted applications).

The approach here is not perfect, and particular care needs to be taken regarding network shares accessible by end-points not protected by zero-trust (as ransomware infections on those end-points could encrypt files on the network shares). Security can never be 100%, and there is always a balance between convenience, cost, and security; such a risk-based approach attempts to address that balance trade-off.

Case 3 - The Prepper

This is a relatively small network. A financial services firm with a small number of highly paid staff offering consultancy services. Key decision-makers are concerned that a ransomware attack, or network intrusion, could leak sensitive customer data (particularly given that most staff use laptops that spend time outside the office network protection).

Zero-Trust End-Point Security is deployed to all workstations, laptops, and the network server, in monitoring mode. Over a period of two to three weeks, Network Box SOC staff monitor the applications being run, whitelisting as necessary, until the machines can be moved to enforcing mode (blocking the execution of all untrusted applications).

During the deployment and subsequent months, several unwanted and potentially dangerous applications are blocked from running on the network. Network Box SOC staff alert the office manager for follow-up with the end user. The key decision-makers are impressed with the reports they can obtain showing which applications are being run by which users at what times.

Conclusions

Moving from a blacklisting (antivirus) to whitelisting (zero-trust) approach requires a shift in mindset. Each approach has its advantages and disadvantages, best summarized as:

Whitelisting vs Blacklisting Pros and Cons

Metric	Whitelisting	Blacklisting
Effectiveness against known malware	100%	Close to 100%
Effectiveness against emerging malware	100%	Perhaps 90% to 95%
False positives	Updates, and new installs	Few
Maintenance of the list	Admin or SOC managed	Vendor
Blocking action	On execution	On download / scan
Visibility of applications used	Full reporting	Typically none
Policy control of applications used	Full control	Typically none

You can see that the biggest drawback of the whitelisting approach is that it requires end-user / admin maintenance of the whitelist. At the same time, the most significant differentiator (apart from anti-malware effectiveness) is the improved reporting and control over which applications are permitted to be run on the network. By simply not trusting (or adding to the whitelist) unauthorized (as opposed to malicious) applications, effective policy control can be implemented. Whitelisting gives the end-user full control and reporting on which applications are actually being run on their end-point devices.

The Network Box approach solves the end-user administrative burden problem of maintaining the whitelist by moving that function to Network Box SOC engineers and our managed service. We offer self-managed, SOC-managed, as well as hybrid combinations. In other words, we offer all of the advantages of zero-trust with none of the drawbacks.

Network Box HIGHLIGHTS

Network Box Global
Events, Workshops, and Seminars

It was a busy month for Network Box regional offices. Network Box Germany participated in various ComTeam Roadshow events, which took place in Hamburg, Gelsenkirchen, and Darmstadt. Network Box USA was at the Channel Partners Conference in Las Vegas. And Network Box Hong Kong hosted a cybersecurity seminar to discuss Network Box service offerings: Cloud SIEM+, Mobile SIEM+, Cloud UTM+, Continuous Security Scanning, Penetration Testing, and Network Box's 24x7x365 SOC Management.



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

Global Security Headlines

Security Intelligence
ChatGPT Confirms Data Breach, Raising Security Concerns
LINK: https://bit.ly/3qlpGgs

Dark Reading
Microsoft Patches Serious Azure Cloud Security Flaws
LINK: https://bit.ly/43eWR3R

Bleeping Computer
Cisco warns of critical switch bugs with public exploit code
LINK: https://bit.ly/43DgS3E

The Hacker News
New Vulnerability in Popular WordPress Plugin Exposes Over 2 Million Sites to Cyberattacks
LINK: https://bit.ly/3oGe07v

Dark Reading
Toyota Discloses Decade-Long Data Leak Exposing 2.15M Customers' Data
LINK: https://bit.ly/43f11Zx

BitDefender
Suzuki motorcycle plant shut down by cyber attack
LINK: https://bit.ly/3qfivWV

The Hacker News
Hackers Exploit Barracuda Email Security Gateway 0-Day Flaw for 7 Months
LINK: https://bit.ly/43zp0SN