NETWORK BOX | NEXT GENERATION MANAGED SECURITY

www.network-box.com

In the Boxing Ring MAY 2022

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the May 2022 edition of In the **Boxing Ring**

I recently re-read a 1989 book titled "The Cuckoo's Egg" by Clifford Stoll. It describes a computer administrator's attempts to track a German spy hacking academic and military networks. Although written over 30 years ago, it is shocking to see that so little has changed despite the progress made with cybersecurity. 80% of security incidents are caused by a fundamental lack of protection, and the remaining 20% of security incidents occur because the existing protection is either not configured correctly or has a problem, and the failure wasn't detected. Network Box was formed to address those two issues - with a UTM+ product containing all the key protection components, combined with a managed service to ensure that those components are configured, monitored, and maintained securely.

This month, we discuss the **Network Box Difference**, comparing what we do against other Managed Security Service Providers and self-managed (aka DIY) solutions. This is outlined on pages 2 to 3.

In keeping with our featured article, Network Box has published an executive summary video to highlight our key points, **'Are you protected from cyber threats?'** In this month's Global Security Headlines, security issues were encountered by **Lenovo**, **Panasonic**, **Amazon Web Services**, **T-mobile**, and more than 8 million **Cash App** investing customers potentially impacted by a data breach.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
May 2022

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

The NETWORK BOX Difference

I recently re-read a 1989 book from my youth titled "The Cuckoo's Egg" by Clifford Stoll. It describes a computer administrator's attempts to track a German spy using the early packet switching and dial-up connections to rifle through the early connected academic and military networks that were the core of what we now know of as The Internet. It is amazing to see that despite the progress made in the past 30 years, so little has changed. Those 1980's techniques (breaching guest accounts, trying default administrative credentials, offline brute force attacks against credential breaches, and privilege escalation) have really not changed much in the past three decades. Still, they account for the vast majority of data breaches.

Last month we talked about Security Best Practices. This month we present what makes Network Box different - comparing what we do against other Managed Security Service Providers and self-managed (aka DIY) solutions. As the terminology changes (SSP -> MSSP -> MDR, etc.), the technology evolves, as Network Box has shown with our continued innovation and evolution of our product and service offerings. Regardless, the fundamental security issues remain the same.

When Network Box was founded more than 20 years ago, 80% of security incidents were caused by a fundamental lack of protection. Networks got virus infections because of a lack of anti-virus protection, hackers got in because of a lack of firewall protection, and intrusions occurred because of a lack of intrusion prevention, and so on. The remaining 20% of security incidents occurred because the existing protection was either not configured correctly or had a problem, and the failure wasn't detected. Network Box was formed to address those two issues - with a UTM+ product containing all the key protection components, combined with a managed service to ensure that those components are configured, monitored, and maintained securely.

Metric	Network Box Solution	Other Managed Products	Self Managed Products
Responsibility	■ A single organization responsible for network security implementation, based on best practice recommendations and customer-defined policy.	■ Multiple organizations with multiple external vendors. ■ No single point of responsibility. ■ Vendors may blame each other.	■ Multiple external vendors. ■ No single point of responsibility. ■ Vendors may blame each other.
Deployment Options	■ Services can be deployed on-premises, in the cloud, or as multi-tenanted SaaS. ■ A single point of unified configuration, reporting, and support.	■ Dependent on individual MSSP. ■ Typically only one deployment option is available.	■ While hybrid (on-premises, cloud, multi-tenanted SaaS) is possible, there is no single interface. ■ Support can be challenging.
Security Response Centre	■ Self-operated. ■ 170 threat intelligence partners. ■ Recognized by Microsoft as a **Top 10 Contributor** to their threat intelligence in 2019.	■ Dependent on individual MSSP. ■ Typically through partnerships with external security response centres.	■ Generally none. ■ Sometimes subscribed to as an external service. ■ All threat intelligence must be acted on by IT staff themselves.
Configuration	■ Unified configuration. ■ Full version control and audit trail. ■ Real-time backed up both on the managed device and at multiple security operation centres.	■ Dependent on individual MSSP. ■ Typically with manual backups and limited version control.	■ Manual backups and version control (if any).
Service Times	■ 24x7x365 security monitoring. ■ SLAs for hardware and configuration support is available according to requirements (from working hours through to 24x7x365).	■ Dependent on individual MSSP.	■ Typically office hours only. ■ Limited support during nights, weekends, and holidays.

Metric	Network Box Solution	Other Managed Products	Self Managed Products
Response Times	■ Services are delivered according to a single clearly defined SLA with escalation thresholds and targets.	■ Must depend on external equipment suppliers for some aspects of service delivery. ■ Back-to-back SLAs across multiple vendors are often required.	■ Services are dependent on IT staff. ■ Often conflicting with other tasks using limited resources.
Hardware Response	■ Hardware replacement within 4 business hours (depending on territory). ■ Replacement pre-configured with current configuration (automatically synchronized), minimizing down-time.	■ Hardware replacement options are dependent on individual MSSP and external equipment suppliers. ■ Replacement typically needs to be manually configured and deployed from backups.	■ Typically office hours only. ■ Requires on-call staff during non-business hours, weekends, and holidays. ■ Replacement spares must be kept on-site or co-ordinated with external vendors. ■ Replacement typically needs to be manually configured and deployed from backups, leading to long down-times.
Security Technologies	■ One unified platform offering all key technologies, configured, maintained, and reported on holistically. ■ Hardware and technologies are developed in-house within a closed security loop. ■ Supported 24x7x365 by a triple ISO certified and PCI compliant Network Box SOC.	■ Multiple different platforms from multiple external vendors. ■ No unified configuration, maintenance, backup, or reporting capability.	■ Multiple different platforms from multiple external vendors. ■ No unified configuration, maintenance, backup, or reporting capability.
Security Updates	■ Delivered via patented PUSH Technology. ■ Automatically performed in real-time 24x7x365. ■ Average delivery time of less than 45 seconds.	■ Dependent on external equipment vendor, with little control.	■ Dependent on external equipment vendor, with little control.
Patch Deployment	■ Fully managed 24x7x365 with a single clear release cycle. ■ Co-ordinated with customers to match their requirements. ■ All patches are pre-tested across all supported hardware types and configurations.	■ Inability to check compatibility across different equipment vendor types and firmware/software versions. ■ Timing is dependent on external vendors. ■ Not synchronized (different vendors have different release cycles).	■ Dependent on IT staff knowledge and working hours. ■ Patches must be downloaded and installed manually. ■ Inability to check compatibility across different equipment vendor types and firmware/software versions. ■ Timing is dependent on external vendors and not synchronized (different vendors have different release cycles).
Reporting	■ Weekly / Periodic KPI reports ■ Highly configurable customized reporting system ■ HTML-5 Dashboard ■ Real-time portable monitoring ■ Web and mobile apps.	■ Dependent on individual MSSP. ■ Typically each service provider has its own reporting system and cycle. ■ No unified approach.	■ Dependent on the products chosen. ■ Typically each product has its own reporting system and cycle. ■ No unified approach.
Track Record	■ 20+ years of delivering managed security services on our own platform. ■ Services are provided via more than a dozen Security Operation Centres worldwide. ■ Measured by our success, customers only renew services if we do a good job ensuring their systems are secure.	■ Dependent on individual MSSP.	■ IT departments are focused on helping their users operate their computer systems, not enforcing security policies. ■ Most IT department staff have little practical experience or training in cybersecurity topics.

NETWORK BOX
NEXT
GENERATION
MANAGED SECURITY

www.network-box.com

Network Box HIGHLIGHTS

Network Box Executive Summary Video: Are you protected from Cyber Threats?

In today's hyper-connected world, cyber-security is critical. Regardless of which industry it operates in, every company needs effective cyber-protection. Yet, most are not adequately protected from hackers, viruses, worms, ransomware, and undesirable content, that make the Internet a serious threat.

This is where relying on a high-quality managed cyber-security service provider like Network Box can make all the difference. Don't be a victim. Outsource your security to dedicated experts at Network Box, and get your organization professionally protected today.

LINK:
https://mcdn.network-box.com/NB-Materials/NB-Network_Box_Overview.mp4

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

CNN

More than 8 million Cash App Investing customers potentially impacted by data breach linked to former employee

LINK: https://cnn.it/3ODVWmJ

The Hacker News

New Lenovo UEFI Firmware Vulnerabilities Affect Millions of Laptops

LINK: https://bit.ly/37PWCEV

CPO Magazine

Panasonic Admits Suffering a Second Cyber Attack in 6 Months with Conti Ransomware Gang Claiming Responsibility

LINK: https://bit.ly/3Lu5yOS

The Register

AWS's Log4j patches blew holes in its own security

LINK: https://bit.ly/37KJHnT

The Hacker News

T-Mobile Admits Lapsus$ Hackers Gained Access to its Internal Tools and Source Code

LINK: https://bit.ly/3vR39r1