May 2023
Issue #126
network-box.com

Network Box FOCUS

24x7x365 Protection

Next Generation Managed Security

Unified Threat Management Plus (UTM+)

May 2023 Highlights

- **ItBR 202305**
  Configuration Review
- **Network Box Hong Kong**
  InnoEX 2023
- **Global Security Headlines**
  - Cisco XSS zero-day flaw
  - macOS Ransomware
  - Windows zero-day vulnerability
  - Intel CPUs

Award-Winning Solutions and Services

Firewall, Intrusion Detection and Prevention (IDP), Virtual Private Networking (VPN), Anti-Malware, Anti-Spam, SD-WAN, Web Proxy, Content Filtering, Data Loss Prevention (DLP), Company Policy Enforcement / Compliance, Real-Time updates with PUSH Technology, Secure 24 x 7 x 365 Monitoring, ISO 9001 / 20000 / 27001 / 31000 Certified Management, IPv6 Ready Core Phase-2 Certified, In-the-Cloud Protection, Comprehensive Adobe PDF Format Reporting, Mobile Protection, Anti-Distributed Denial of Service, Web Application Firewall, IPv4-IPv6 / IPv6-IPv4 Bridging, Multiple Internet Connections, High Availability / Load Balancing, Internet Acceleration, Secure VoIP (Voice over Internet Protocol) Gatekeeper, Quality of Service Control, Traffic Policing, Threshold Limiting, Hardware Fault Tolerance, clustering possible, Live Watch Real-Time Monitoring, SSL (Secure Socket Layer), Virtual Private Networking, Mail Portal System, End User email management including SPAM release and white / black listing, HTML-5 Dashboard, Secure Socket Layer (SSL) Proxy, Application Identification, Entity Management, Infected LAN, Cloud Mail Backup, Cloud DNS Backup, Dark Web Monitoring Service, Security Incident and Event Management, Mobile SIEM+, Cloud Domain and IP Reputation Service, Cloud SSL Reputation Services.

Cybersecurity for ALL

Today, every company is using the Internet to conduct their business. However, too many fail to realize that when they connect to the Internet, the world is linked back to them.

Merely having a Firewall is not enough in today's heightened cyber threat landscape.

Hackers, viruses, worms, ransomware, and phishing campaign, are just a few examples of what makes the Internet so dangerous. Because of this, relying on a high-quality managed cybersecurity services provider, like Network Box, can make all the difference.

With Network Box, your cybersecurity is assured.
Founded over two decades ago, Network Box is a leading global Managed Security Service Provider (MSSP), offering multi-award-winning cybersecurity services and technologies. A worldwide network of Security Operations Centres (SOCs) operating right across the globe, helps manage and protect your networks all year round.

At Network Box, we believe in providing our clients with the best security solution available and offer fully comprehensive protection for companies of all types and sizes. Indeed, many of the world's best-known companies, banks, hotels, and government departments have already been using Network Box to secure their computer networks.

■ Network Box HQ's ISO 9100 / 20000 / 27001 / 31000 certified Security Operations Centre

Award-Winning Technologies

Network Box continues to develop world-class security solutions that mitigate incoming threats from the Internet, such as intrusion attempts from hackers, zero-day threats, phishing emails/spam, DDoS attacks, and infections by trojans, viruses, and other malware. Business risk and outgoing threats are alleviated by blocking the leakage of valuable information and denying access to non-work related or infected websites and applications. Additional technologies including Entity Management, HTML-5 Dashboard, and KPI reporting, help with the management of your end-users and network.

These technologies have allowed Network Box to win more than 160 international industry, media, and governmental awards.

Industry Specialists

Independent security researchers and analysts have recognized Network Box.

Gartner

FORRESTER®

FROST & SULLIVAN

Gartner Recognition

Asia/Pacific Context: Magic Quadrant for Global MSSPs

Analysts:
Craig Lawson/Andrew Walls

Date:
02 July 2014

"Network Box's offering will appeal to companies that are looking for a managed UTM appliance with active support from professional security staff."

The Forrester Wave

Emerging Managed Security Service Providers

Managed security service providers (MSSPs) offer managed security services (MSS) that help manage and monitor the security posture of their customers' IT infrastructures.

Frost & Sullivan

Market Report: Increasingly Sophisticated Threat Landscape Drives the Uptake of Managed Security Services in APAC (February 2021)

Certified Performance

Independent international standard authorities have certified Network Box. Furthermore, Network Box has partnered with national and international associations, alliances, and standard bodies, across the world.

ISO Certified

Network Box HQ's Security Operations Centre has obtained 4 x ISO certifications, which are reviewed periodically to ensure Network Box's continued commitment to excellence.

- ISO 9001:2015
- ISO/IEC 20000-1:2018
- ISO/IEC 27001:2013
- ISO 31000:2018

Triple 100% Tolly Rating

Tolly Group, one of the world's most respected IT Testing Labs, certified Network Box with a triple **100%** detection rating against their Extended WildList Malware database.

Microsoft

Network Box is listed as a **Top 10 Contributing Partner** in the Microsoft Active Protections Program (MAPP).

PCI-DSS

Network Box HQ and HK Security Operations Centers have both achieved compliance with the latest **PCI DSS v3.2** standard.

SSAE 16

Network Box USA has attained **SSAE 16 SOC 2** attestation by the American Institute of Certified Public Accounts (AICPA).

CVE

Network Box is a **Common Vulnerabilities and Exposure** (CVE) output conformant partner on the MITRE website.

KV-S@feNet

Network Box Germany has been certified by **KV-S@feNet**, allowing for official integration with Germany's medical network.

24x7x365 Managed Cybersecurity Services

Network Box HQ's ISO certified Security Operations Centre monitors, manages, and mitigates cyber threats from your network 24x7x365.

The Network Box Approach

With Network Box, we do not just merely provide you with the hardware; we also fully manage your cybersecurity. As part of our services, once we install your device, our team of security engineers will remotely manage, monitor and protect your network from cyber threats 24 hours a day, seven days a week, 365 days a year. Thus, ensuring your network is continuously protected and allowing you to concentrate on running your business.

The uniqueness and what distinguishes Network Box from most other security vendors is our award-winning **Managed Security Services**. The Network Box Managed Security Services takes care of the never-ending, yet vital, management of your cybersecurity to protect you against the worst the Internet has to offer. And unlike other service providers offering managed services, we build our proprietary hardware and software and manage it ourselves. Nothing is outsourced, and no third parties are involved at any point, thus, ensuring a closed security loop.

It looks like a product, but it's actually a 24x7x365 cybersecurity service

Cyber-attacks are ongoing, and staying protected against these emerging threats requires a dedicated team of security engineers to continuously monitor and protect your network, which most businesses do not have the time or resources to implement effectively. **Network Box's Managed Security Services include:**

24x7x365 Monitoring
Network Box analyses over 800 million statistical data packets daily, collaborates with more than 70 security partners worldwide, and operates over 250,000 virtual honeypots deployed in the cloud. In addition, every Network Box system is continuously monitored to ensure it is running smoothly.

24x7x365 Management
Your security is remotely managed via a global network Network Box of Security Operations Centres (SOCs) spread across the world. The SOCs ensure that you are always protected against cyber threats.

24x7x365 Protection
If a new cyber threat is detected, Network Box will automatically PUSH out and install security patches in real-time. Using patented PUSH technology, every Network Box system in the world is updated in an average time of less than 45 seconds.

Unified Threat Management+ (UTM+)

The Network Box UTM+ provides a comprehensive suite of cybersecurity technologies to safeguard your network.

Network Box UTM+

Unified Threat Management (UTM) is a term that refers to an all-inclusive security solution that provides a comprehensive set of security functions and technologies within one single system.

However, not all UTMs are created equal. Most typical UTM offerings provide only the basics and do not give adequate protection from emerging cyber threats. Network Box, conversely, provides UTM+, which has more enhanced features provided by even the most advanced UTMs, and adds next-generation security technologies to provide fully comprehensive protection.

Cybersecurity issues arise because most businesses do not have the right solution in place. The Network Box UTM+ solution uses a multi-layered security approach to effectively safeguard your network from internal and external threats and additional features to manage your network.

Incoming Threat Protection | **Outgoing Threat Protection** | **Additional Features**

Incoming Threat Protection

- Hybrid Firewall
- Intrusion Detection and Prevention (IDP)
- Anti-Malware
- Zero-Day Anti-Malware (Z-Scan)
- Anti-Spam
- Web Application Firewall (WAF)
- Anti-DDoS WAF

Outgoing Threat Protection

- Virtual Private Network (VPN)
- Web Content Filtering (S-Scan)
- Data Leakage Prevention (DLP)
- Infected LAN
- SSL Proxying
- Application Scanning and Control

Additional Features

- PUSH Updates
- SD-WAN
- HTML-5 Dashboard
- Customized Reports / Key Performance Indicators (KPIs)
- Entity Management
- IPv4 to IPv6 Bridging
- Cloud email and DNS Backup
- Dark Web Monitoring Service
- Security Incident and Event Management (NBSIEM+)

And more...

Next-Generation Hardware

Virtual Hardware

In addition to the hardware units, Network Box can provide the same UTM+ Managed Security Services for your cloud / virtual environment, with a full range of virtual appliances.

S-M-E Hardware

A full range of Network Box models is available to suit your organizational needs. These models are designated **S** for Small, **M** for Medium, and **E** for Enterprise. Based on multi-core CPUs, all units are 64-bit and designed to offer exceptional performance and reliability. With high-grade chassis, the hardware units can withstand extreme shock, vibration, and temperature ranges.

Every unit has over 100 in-built sensors and is monitored 24x7x365 by the Network Box SOC to ensure the unit is running smoothly. Real-time backups of rules and settings of the hardware are also continuously performed. **Furthermore, the units have no backdoors and do not collect your private data.**

Security Features

The security software, services, and protection afforded are identical for all models. The differences between models are purely hardware features and performance. All models provide the following security functions:

Feature	Details
Firewall	Proxy, Packet Filtering, Stateful Packet Inspection
IDS/IDP	3 Engines / 16,000+ Signatures
VPN Types	IPSEC, PPTP, SSL
Anti-Spam	25 Engines / 30.8 million+ Signatures
Anti-Malware	18 Engines / 24.8 million+ Signatures
Content Filtering	15 Engines / 7.7 million+ Signatures
Anti-DDoS	Millisecond response to brute force attacks
IPv4 to IPv6 Bridging	Incoming/Outgoing Protocol Translation
PUSH Updates	Delivered and installed automatically in real-time

S for Small Businesses

Secures small businesses or branch offices with enterprise-quality protection.

M for Medium-Sized Organizations

Cutting-edge, high-performance hardware for medium-sized organizations.

E for Enterprises

Designed to protect enterprises, allowing for the highest performance possible.

True Real-Time Security Updates

Network Box's patented PUSH Technology proactively pushes out and installs security updates in an average time of less than 45 seconds.

Microsoft

Network Box is a Microsoft Active Protections Program (MAPP) partner. As a MAPP partner, Network Box has access to information on the latest zero-day threats and vulnerabilities. It provides virtual patching at the gateway before the public is even aware of any security issues.

PUSH Technology

Network Box's key technologies are all supported by patented PUSH Technology. Unlike standard security systems that usually pull updates from a server once a day, or at best once an hour, Network Box proactively PUSHes out and installs updates as soon as they become available.

Security updates are PUSHed out and installed in an average time of less than **45 seconds**

True real-time security updates

Network Box Security Response is currently pushing out security updates, on average, once every 8 seconds

PUSH vs PULL Comparison Table

The table below highlights the key advantages of Network Box's PUSH technology compared to PULL updates found with most other security solutions.

Detail	PUSH	PULL
Update Notification	You DO NOT need to know that there is an update waiting	The system will connect to the server at a scheduled time to check for updates
Access Privileges	You DO NOT need to ensure that you have the rights to access the patch on the website	You may need to have the rights to access the patch on the website
Downloads	You DO NOT have to download it nor ensure the checksum is correct	You may have to download it and ensure the checksum is correct manually
Time	You DO NOT have to find time to install it	You may have to find the time to install it
Installation	You DO NOT have to repeat all these steps for each device	You may have to repeat all these steps for each device

Fast and Early Protection from new threats

Virtual Patching deploys early patches at the gateway before attackers can exploit any vulnerabilities.

Virtual Patching

When a vulnerability is discovered or announced, a race starts between developing, testing, releasing, and installing the patches to fix it. Virtual Patching aims to quickly deploy early patches 'virtually' at your network gateway before formal patches can be released or installed, and before hackers can compromise your systems.

- Targets network traffic attempting to exploit a known security vulnerability
- Fast and effective protection before formal patches can be released and installed
- Augmented with global threat intelligence from 70+ security partners

The Network Box Approach

Virtual patches target network traffic attempting to exploit a known vulnerability. They often start with signatures to detect the vulnerability or exploit behaviors, and then actively interrupt the traffic and block it before it affects the target system. Virtual patches are often a short-term solution, to buy time before formal patches can be deployed. They are a quick solution to a complex problem, as they can usually be deployed without a reboot or service interruption.

The Network Box approach is to have many layers of protection. From frontline IPS, firewall, IDS/IPS, application proxies, protocol scanners, and hardened services. Virtual Patching technology is implemented at each of these layers - choosing the best approach for each particular vulnerability and deploying protection with multiple technologies to protect against different attack vectors.

Additionally, Network Box maintains partnerships with numerous security organizations and works with these to gather and share threat intelligence.

Cybersecurity at the Gateway

As your first line of defence, the Network Box Firewall and IDP engines protect your network against malicious threats and unauthorized access.

Hybrid Firewall

The Firewall, installed at the gateway, is your first line of defence against cyber attacks. Unlike most other firewalls, however, Network Box utilizes a Hybrid Firewall to effectively protect your servers and workstations from malicious probes and unauthorized access.

Packet Filtering Firewall:
Blocks or allows packets through the network depending on the source/destination IP, protocols, and ports. Suitable for basic protection with minimal overhead.

Stateful Packet Inspection Firewall:
Monitors active connections to determine which network packets to allow through to the network. Suitable for high performance and sophisticated rule sets.

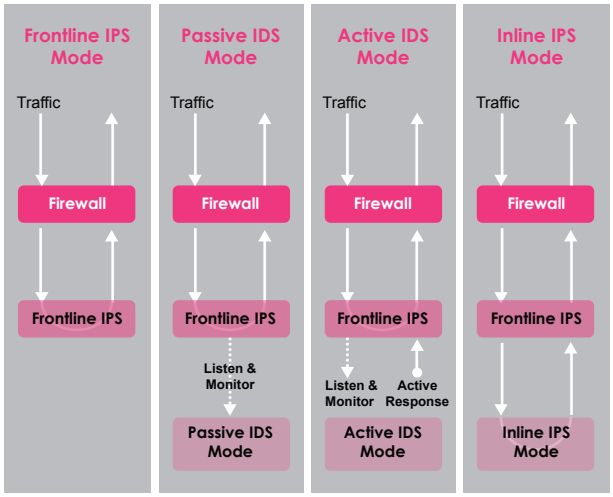
Proxy Firewall:
A set of secure proxies, integrated into the firewall, connection tracking and NAT systems, capable of high-level protection up to layer 7 Application Layer.

IDP

Intrusion Detection and Prevention

Tightly integrated with the Firewall, the Intrusion Detection and Prevention (IDP) system monitors and analyzes your network for signs of intrusion. If the system detects an intrusion attempt, it will log the incident. The system can be preconfigured to actively block the threat.

There are four IDP modes offered by Network Box:



Fast, Effective Malware Protection

Award-winning anti-malware technology that is probably the quickest and most comprehensive gateway solution in the market today.

Multi-Layered Anti-Malware

The Network Box Anti-Malware system provides 18 anti-malware engines, running over 24 million signatures, to identify and prevent viruses, trojans, worms, and other malicious software from infecting your networked systems or networked smart devices.

- 18 Engines
  24 million+ Malware Signatures
- Triple 100% Tolly Group detection rating against their Extended Wildlist Malware database over HTTP, SMTP, and POP3 protocols
- Anti-mobile malware protection

Z-Scan

Zero-Day Anti-Malware

Z-Scan is an in-the-cloud defence shield that protects against the latest zero-day threat. It operates by continually analyzing global threat intelligence obtained in real-time from virtual honeypots and security partners and releasing its own signatures to protect against emerging threats within seconds.

- Industry best response times of just **3 seconds**, which is up to 4,200 times faster than other typical anti-virus solutions
- 250,000+ virtual honeypots deployed in the cloud for threat intelligence gathering
- Augmented with global threat intelligence from 70+ security partners to extend the number and breadth of signatures available

Incoming/ Outgoing Email Protection

Multi-Layered Email Scanning and Data Leakage Prevention engines ensure that all SMTP traffic is protected and complies with company policies.

Anti-Spam and Email Protection

The Network Box mail scanning engines scans and blocks spam and other malicious emails from entering your network. In addition to spam detection, the system also comprehensively scans emails for malware, intrusion, and company policy compliance. Supports **SMTP**, **POP3**, and **IMAP** email protocols

- 25 Engines
  30 million+ Spam Signatures
- Industry-leading spam detection accuracy with a low false-positive rate
- Extremely configurable - individual engines can be enabled or disabled based on your requirements

DLP

Data Leakage Prevention

The Network Box DLP system scans and blocks outbound SMTP mail that may contain sensitive company data such as your client information, account details, commercial secrets, and document files. The DLP rules and policies can also be customized to ensure more effective prevention.

- Customizable rules and policies
- Sophisticated pattern matching and content analysis
- Scripting capabilities

Safe and Secure Web Browsing

S-Scan is designed to help organizations block users from accessing undesirable web content. With an industry-leading detection rate, it offers excellent performance in speed, coverage, and web accuracy.

S-Scan

Web Content Filtering

S-Scan uses high-performance signature-based technology, rather than a simple URL database, to identify web content more efficiently and effectively. Thus, specific categories of new undesirable websites can be identified almost immediately in real-time, without the need to update a URL database.

15 Engines
7.7 million+ Signatures

Uses high-performance signature-based technology

Real-Time identification and classification of web content

S-Scan uses 60 categories to identify and classify web content:

- Adult / Sexually Explicit
- Advertisements & Popups
- Alcohol & Tobacco
- Arts
- Blogs & Forums
- Business
- Chat
- Computing & Internet
- Criminal Activity
- Downloads
- Education
- Entertainment
- Fashion & Beauty
- Finance & Investment
- Food & Dining
- Gambling
- Games
- Government
- Malware
- Phishing
- Hacking
- Health & Medicine
- Hobbies & Recreation
- Hosting Sites
- Illegal Drugs
- Infected LAN Botnet Command and Control
- Infrastructure
- Intimate Apparel & Swimwear
- Intolerance & Hate
- Job Search & Career Development
- Kid's Sites
- Motor Vehicles
- News
- Peer-to-Peer
- Personals & Dating
- Philanthropic & Professional Orgs.
- Phishing & Fraud
- Photo Searches
- Politics
- Proxies & Translators
- Real Estate
- Reference
- Religion
- Ringtones / Mobile Phone Downloads
- Search Engines
- Sex Education
- Shopping
- Society & Culture
- Spam URLs
- Sports
- Spyware
- Streaming Media
- Suspicious URLs
- Tasteless & Offensive
- Travel
- Uncategorized
- Violence
- Virus / Malware Infected
- Weapons
- Web-based Email

However, the ultimate settings are entirely under your control. With S-Scan, it is also possible for you to:

- Turn all web content filtering off for your entire organization
- Only filter web content for specific user groups
- Only filter certain subsets of categories for all or specific user groups
- Filter certain web content during business hours, and turn off the content filtering during non-business hours

Brute Force Protection

The Anti-DDoS WAF engine uses real-time automated fingerprinting to identify and blacklist attacks, responding in milliseconds to brute force attacks while ensuring business continuity.

Anti-DDoS

Anti-Distributed Denial of Service

The Anti-DDoS WAF engine mitigates Distributed Denial of Service (DDoS) attacks to keep 'bad traffic' at bay. In contrast, 'good traffic' is allowed through to secured web-facing servers. By using real-time automated fingerprinting to identify and blacklist attacks, the engine takes milliseconds to respond to brute force/botnet attacks that typically come from thousands of sources.

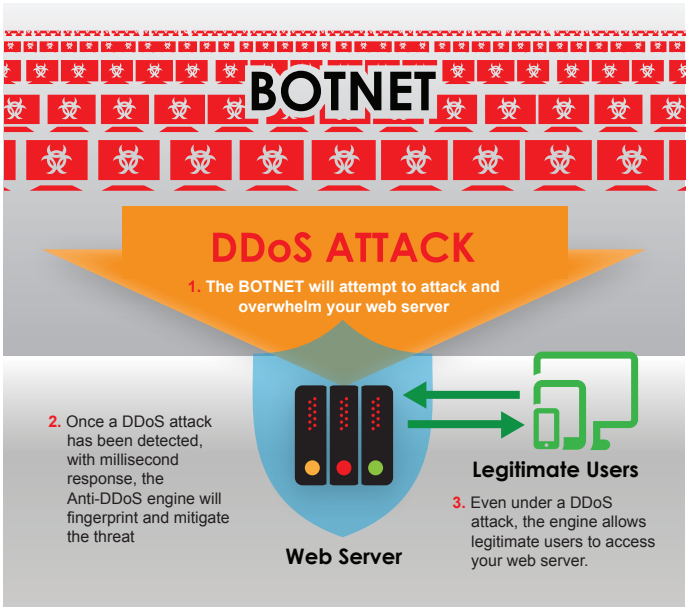
High-performance blocking - millions of data packets blocked per seconds

Slows down attacks by a factor of 1,000

Millisecond response to brute force attacks

The Anti-DDoS engine offers DoS / DDoS mitigation facilities for the following:

- Total connections limiting
- Total connection rate limiting
- Per-source connections limiting
- Per-source connection rate limiting
- Per-source-per-method rate limiting
- SYN cookies for SYN flood protection



Next-Generation Protection

With a database of over 6,000 rules combined with anti-malware and IP signature databases, the engine can identify and protect against several million types of threats.

WAF

Web Application Firewall

The WAF engine protects web servers against web application-based attacks, including the OWASP Top 10 as standard. The engine uses an extensive rules database combined with anti-malware and IDP signatures. Furthermore, the engine also allows for the real-time installation of emergency virtual patches at the gateway to detect and prevent any application or web server-specific security issues.

Real-time automated fingerprinting to identify and blacklist attacks

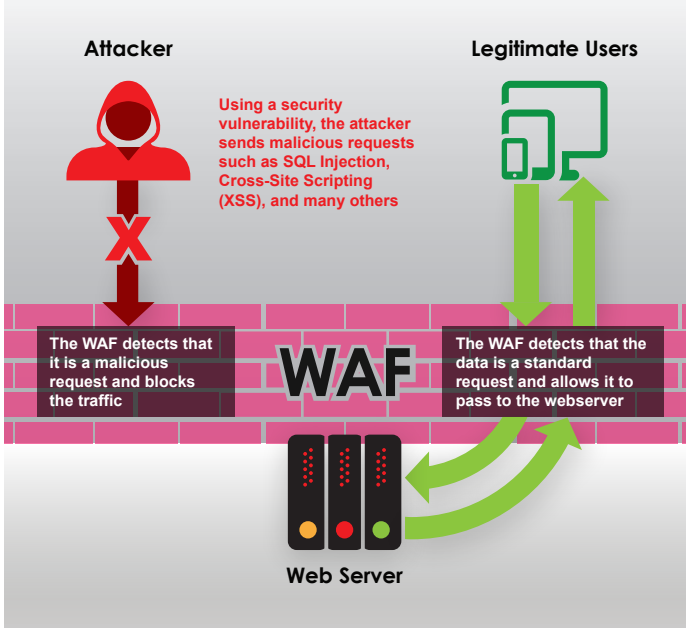
Uses an extensive combined database of rules signatures to identify several million threats

Up to 15,000 fully analyzed transactions per second

The Network Box WAF engine offers protection for two application groups:

Standard Applications:
Apache, IIS, Joomla, Drupal, MediaWiki, WordPress, etc.

Custom Applications:
Tailor-made software that has been specially developed for a specific organization or specific users/user groups.



Encrypted Secure Data Exchange

Without a secured connection between your Internet endpoints, hackers can intercept and steal your communication and data.

VPN-5Q

The VPN-5Q is a fanless VPN device designed to secure connections between Internet endpoints. It is lightweight and has a slim style design to fit any space-limited environment, making it an ideal and cost-efficient solution for homes or small branch offices.

Ruggedized VPN Virtual Private Network

The Virtual Private Network (VPN) engine secures connections between Internet endpoints to ensure data remains secured and confidential during Internet exchange. In addition to providing graphical representation and control of the VPN, the engine has been ruggedized to handle ISP and other fundamental connectivity issues.

Supported VPN Technologies:
PPTP, **IPSec**, **SSL-VPN**

Authenticated user sessions

Global Monitoring Sensor with a visual display of VPN links

Visual VPN

With the Network Box HTML-5 Dashboard, all the VPN types have been unified into a single unified framework for centralized status reporting and control.

- Configurability of VPN types
- Reporting on VPN availability
- Capability to start/stop/restart VPN tunnels
- New Global Monitoring Sensor for VPN links

- VPN Status Dashboard Screen

Enhanced Policy Control

The Application Scanning and Control engine analyzes web traffic to identify the application and allows company policy control to be applied.

Application Scanning and Control

While traditional firewalls block IP addresses and ports, the Network Box Application Scanning and Control engine analyzes web traffic at the data level to identify the application responsible for that traffic. Once the application has been identified, rules and policy control can be applied.

Supports over 1,900+ web applications

Customizable policy rules and granular control of applications

Encrypted SSL traffic can also be identified and controlled

Enhanced Policy Control

When the application has been identified by the engine, by using the rules system, different company policies can be applied to allow better control of the user's web access:

Time-Based Control

Allow users to access certain websites only during specific times of the day.

Example: Users can only access social media sites during non-working hours.

User-Level Control

Only specified users/user groups are allowed access to particular websites.

Example: The company's marketing department can access social media sites all day, but other user groups cannot access it/ can only access it during non-working hours.

Granular Control

Users can access certain websites but may have restrictions within the sites.

Example: Users can access Facebook but cannot use specific applications such as chat or games.

User and Device Management

The Entity Management system helps IT Managers to monitor, manage and protect end-users within their networks.

Entity Management

Entity Management allows you to group all your network users' devices, such as iPads, iPhones, laptops, desktops, and VOIP phones, into a single entity. Attributes such as MAC addresses, IP addresses, and email addresses are then tracked, as well as the network resources they utilize. Based on the entity, comprehensive reporting and policy control facilities are then made available.

All devices belonging to an individual end-user can be grouped into a single entity

Presents a single holistic view of the activity of each of the entities

Allows easier monitoring, management, and protection of your users and network

The Holistic Approach to Monitoring and Management

The revolutionary Entity Management engine completely redefines how users and devices are monitored and protected. The system presents a holistic view of the activity of each entity in your network. For example, calling up *'user X'* will show all firewall blocks, web accesses, network usage, and email; across the user's desktop, laptop, phone, tablet, and remote VPN.

The entity model itself is built and maintained by automated systems. It is an extremely efficient and effective technology to help you monitor, manage and protect your users and networks.

Entity Dashboard Screen

Report on your network and user activities

In addition to the automatic weekly reports, customized reports can be generated on the fly or scheduled to be delivered periodically.

Customized Reports

With Network Box, all actions and events are logged and audited to ISO standards. A central, unified logging system collects data throughout the system, which can generate reports. These reports are data-rich and contain information on time and time zone, information on host and origin, and are unlimited in scope.

Allows you to create instant real-time reports or reports covering a set time-frame

Available formats:
PDF, CSV

KPIs let you to see what is happening in real-time and what has happened over any given time-frame

Key Performance Indicators (KPIs)

The Network Box Reporting systems have been enhanced to leverage the concept of Key Performance Indicators (KPIs). Each Network Box hardware unit comes with predefined KPI weekly reports, which provide a weekly summary of events and actions within your network. Using the Network Box Dashboard, this can be customized for more granular control.

With KPIs, it is possible to make a comparison between any two defined periods. This facility is very useful to see if workloads are increasing over time, for example, to see how many more emails are being scanned by the system this week than in the same week last year.

Network Box KPIs includes:

- Network (INTERNET) utilization
- Network (LAN) utilization
- Network (DMZ) utilization
- Network (VPN) utilization
- DISK utilization
- CPU utilization
- Network Firewall connections denied
- Web Client requests made
- Web Client requests denied
- Web Client URL categories
- Web Client Threats
- emails received
- emails denied
- Outgoing emails sent
- Outgoing emails denied
- Incoming emails received
- Incoming emails denied
- email SPAM blocked
- email MALWARE blocked
- email POLICY blocked
- email DLP blocked
- VPN SSL site-to-site connections made
- VPN SSL client connections made to the server
- VPN SSL site-to-site percentage uptime
- VPN PPTP connections made
- VPN IPSEC connections made
- VPN IPSEC percentage uptime
- Frontline IPS attacks denied
- IPS attacks denied
- IDS attacks detected
- WORKLOAD utilization
- MEMORY utilization

and many more...

Outgoing Threat Protection

Safeguard your internal network from cyber threats with the Network Box Infected LAN and SSL Proxy engines.

Infected LAN

The Infected LAN engine helps pinpoint infected workstations, servers, and networked smart devices in your network's LAN/DMZ areas. While other engines can detect access to malicious content, the engine explicitly scans outbound traffic to identify botnet access from your network. Once identified, the engine can be configured to quarantine infected systems automatically.

- Identification and dynamic blacklisting of infected systems
- Detection of outbound access to known botnet and malware sites
- Highly-granular detection for highly-prolific malware

SSL Proxying

Secure Sockey Layer (SSL) is a cryptographic protocol used to secure communications between Internet endpoints, which can be vulnerable if not correctly configured. Through analysis of the SSL connection and the protocol data, the SSL Proxy takes the responsibility of securing connections going through the gateway and applies the company-wide security policy on these secured communications.

- Identification, decryption, encryption, certificate validation, and protection of SSL network traffic
- Denies end-users from bypassing failed SSL certificates
- An SSL proxy, supporting HTTPS, SMTPS, POP3S, and IMAP4S protocols in both direct and STARTTLS modes

Be connected regardless of connection types

Zero-touch provisioning technologies to help you connect to your different networks regardless of network configuration, environment, and connection type.

IPv6 Ready Core Phase-2 Certification

Network Box is the first provider of Managed Security Services to have had its proprietary managed security service delivery platform attain IPv6 Ready Core Phase-2 Certification.

SD-WAN

Sofware-Defined Wide Area Network

The Network Box SD-WAN optimizes network traffic and allows organizations to easily connect between head office and branch offices, data centres, and cloud services/applications, regardless of network environment and connection type. SD-WAN services are provided by on-premises Network Box devices, virtual cloud, and multi-tenanted SaaS services.

- Provides QoS and Security Technologies: Traffic Prioritisation, Traffic Shaping, and Traffic Policing; with UTM+ services
- Supports various network connection types and configurations: MPLS, Lease Line, Broadband, Hub-and-spoke, Mesh, Hybrid combinations, etc.
- Centralized administration of the SD-WAN, including configuration, link status monitoring, alerting, and reporting

IPv4 / IPv6 Bridging

The Network Box IPv4 / IPv6 Bridging engine supports bi-directional translation between IPv4 and IPv6 protocols, allowing IPv4 clients to connect to IPv6 servers and vice-versa. It is designed to help organizations with their migration to IPv6 while integrating naturally with any IPv4 network.

- Certified to IPv6 Ready Core Phase-2 Protocol standard
- Dual-stack interception mechanism with outgoing protocol translation
- IPv6 Border Gateway Protocol offered as a service

Assured Business Continuity

Network Box's global network of cloud backup servers assures your business continuity and service reliability.

In-the-Cloud Backups

The Network Box Cloud Email Backup and Cloud DNS Backup services help alleviate problems due to network outages and ISP-related connectivity issues. Thus, with Network Box's global network of cloud backup servers, you are assured of business continuity and service reliability.

3 Geographical regions:
America, Europe, and Asia

Backed-up emails are removed once they are delivered

Full control of which domains will use the cloud DNS backup service

Cloud Email Backup

Lost or bounced emails can affect business continuity. The Network Box Cloud Mail Backup service can alleviate this business risk by backing-up undeliverable incoming emails in the cloud. Thus, if there is a problem with your ISP, internal network, or email server, incoming emails will be stored in the cloud and delivered to you when the issue has been resolved.

- Backup storage only if your email servers are overloaded and temporarily not accepting new connections/emails
- Once delivered, the emails are removed, and the system will only retain the logs (containing date, time, sender, and recipient)

Cloud DNS Backup

Web and mail traffic can be severely affected if your DNS server suffers an outage. The Network Box Cloud DNS Backup service helps mitigate this by allowing you to use Network Box's extensive network of DNS servers to provide backup in the cloud. In addition to providing a security-hardened DNS solution, it is a faster and more reliable service than traditional ISP or in-house DNS servers would be able to offer.

- Full control over which of your domains will use the service
- Full control over which cloud backup servers to use for your domains
- Only the DNS records themselves, as well as statistical logs, will be stored on the Cloud DNS Backup servers.

Cloud Reputation Services

Ensure your domain names, public IP addresses, SSL servers, and SSL certificates are protected.

Cloud Domian/IP Reputation Service

This optional add-on service allows you to register your domain names and public IP address subnet ranges. The information is then entered into the Network Box Cloud Reputation Service database. From then onwards, Network Box will continually monitor the domains and IP addresses to ensure they are not blacklisted in public reputation lists.

- Full control over which domains / IP addresses will use the service
- Continuous monitoring against cloud reputation services and notification (via GMS ticketing) of any reputation issues found
- Augmented with the Network Box Reputation DataBase (RepDB) to ensure that you are not blacklisted

Cloud SSL Reputation Service

As more services adopt SSL encryption standards and the Public Key Infrastructure (PKI), managing the associated SSL certificates has increasingly become an issue for many organizations today. Expired certificates, browser warnings, and users unable to access your services can result from mismanagement. Certificate Authorities have also complicated the issue with their short validity certificates reliant on automated renewal. To address these issues, Network Box has the following:

Cloud SSL SERVER Reputation Service

The service lets you enter the connection details for your publicly accessible SSL servers and monitor the certificates those servers host. The service then checks certificate signing validating, Server Name, expiry date, and other attributes. Should any issues be found, a GMS Incident is raised to alert you. For upcoming certificate expiry, the system will, by default, warn 30 days before expiry and alert critical seven days before expiry.

Cloud SSL CERTIFICATE Reputation Service

The service is designed for non-public SSL services and their certificates. It is commonly used for private services or private self-signed CA certs used in a private PKI infrastructure. To use this service, you upload the certificate, and the system will automatically monitor it, similar to the Cloud SSL SERVER Reputation Service.

Dark Web Protection

There are currently several billion sets of hacked credentials already posted on the Dark Web. Because of this, it is crucial for you to check for postings of your information and passwords there regularly.

Dark Web Monitoring Service

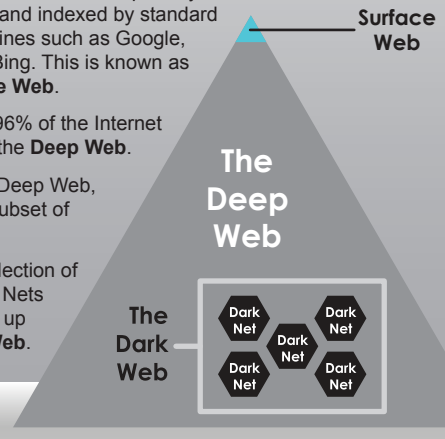
Whenever there is a data breach, the stolen personal information and data usually ends up on the Dark Web. The Dark Web Monitoring engine periodically scans data breaches from the Dark Web, looking for your registered email addresses and domains. As an ongoing subscription service, Network Box will inform you if your credentials have been discovered there.

- Regularly scans the Dark Web for postings of your registered domains and email addresses
- Ongoing monitoring and notification, with detailed reports of data breaches found on the Dark Web
- Optional monitoring services for the personal email accounts of key staff within your organization

What is the Dark Web?

The Dark Web is the deliberately hidden part of the Internet and is the natural habitat of hackers and cybercriminals. This 'dark side' can only be accessed with specialist knowledge and specific software tools such as TOR (The Onion Router), Riffle, Freenet, and I2P (Invisible Internet Project).

- Only 4% of the Internet is publicly accessible and indexed by standard search engines such as Google, Yahoo, or Bing. This is known as the **Surface Web**.
- The other 96% of the Internet comprises the **Deep Web**.
- Within the Deep Web, there is a subset of **Dark Nets**.
- It is the collection of these Dark Nets that makes up the **Dark Web**.



Intuitive Graphical User Interface

The Network Box Customizable HTML-5 Dashboard gives IT Managers a clear and graphical display of network status and system usage.

HTML-5 Dashboard

The Network Box HTML-5 Dashboard gives you real-time visual feedback of both cyber attacks and your network status. Made up of hundreds of different widgets, it is fully customizable, and the layout can be changed to give you complete control over how you want to monitor your network.

A highly customizable dashboard that provides an intuitive visual representation of your network status and cyber attacks

Instant real-time reports, or reports covering a set period, can be generated via the dashboard

KPIs let you see what is happening in real-time or what has happened over any given time-frame

Network Box Dashboard Screens

The layout of the dashboard can be customized to show different aspects of your network.

Main Overview

Top Mail Users Overview

Box Status

Network Activity

Real-Time Portable Monitoring

The Network Box Dashboard is compatible with almost any modern large-screen mobile device. This allows you to constantly monitor your network's status even when you are away from your workstation.

Security Incident and Asset Monitoring

The Network Box SIEM+ system allows IT Managers to view all security incidents and events for all devices within their network.

NBSIEM+

Security Incident and Event Management

Delivered as a hybrid cloud/on-premises or pure cloud-based solution, NBSIEM+ integrates all the security logs and incidents into one centralized system to provide an overview of the entire network and can apply Integrated Security Intelligence, Digital Forensics, and Security Incident Management.

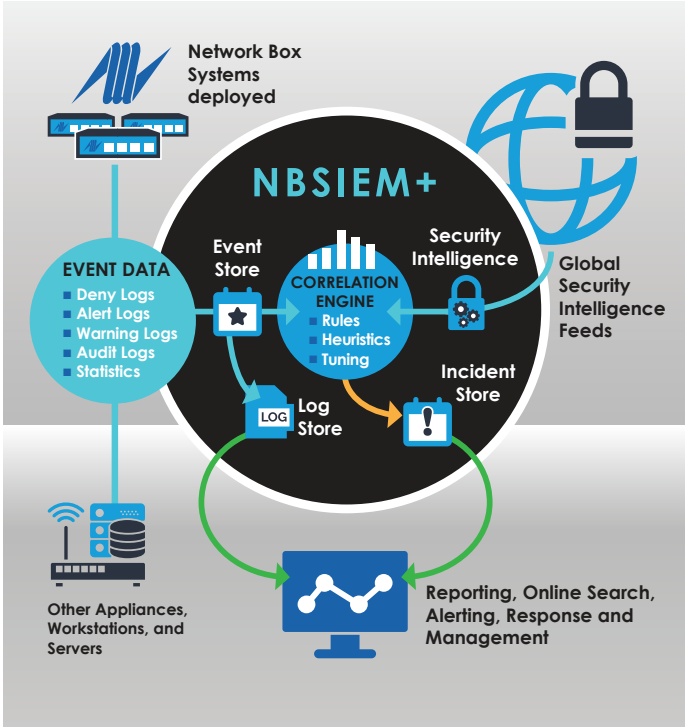
Powerful online search facilities for events, incidents, assets, and more

Real-time correlation of security incidents to provide a holistic view

Notification and alerts for critical security events

NBSIEM+ System Workflow

An advanced Correlation Engine is at the heart of the system. Designed to take a high-level overview of those individual data items and correlate them into actionable security incidents. Furthermore, a highly-intuitive graphical user interface/dashboard helps IT Managers identify real-time security incidents and events for all their devices and systems across their entire network.



NBSIEM+ Services at your fingertips

The FREE Network Box SIEM+ App is available on the Google Play Store and Apple iTunes App Store.

Mobile SIEM+ for Android

Mobile SIEM+ for iOS

Mobile SIEM+

Available for phones and tablets, for both Apple iOS and Android-based mobile devices, the Network Box SIEM+ App is designed to provide secure access to administer Network Box managed services.

In addition, the app provides access to the following:

- Security news stories
- Box Office ticketing system
- NBSIEM+ events
- Overview of managed assets

Provides access to the NBSIEM+ portal

Full access to the Box Office ticketing system

Support for both Android and iOS mobile platforms

Mobile SIEM+ Screens

Home Screen: Shows a timeline-based history of recent activities. Support and Incident ticket updates are shown alongside highlighted emerging security news stories. You can even use this system to distribute announcements to your own team with fine-grained privacy controls.

Support Screen: Provides full access to Box Office ticketing - including raising, reviewing, and updating support tickets.

Assets Screen: Provides an overview of your managed assets and their current status.

Incidents Screen: Provides access to Incidents (Global Monitoring System health, SIEM events, cloud services, or others).

Events Screen: Provides access to event logs if your devices are configured to submit events to NBSIEM+.

Services Screen: Provides access to your managed services including: physical, virtual, and multi-tenanted pure cloud.

Network Box *Focus*

The latest Network Box news and updates

network-box.com
Issue #126

MAY 2023

In the Boxing Ring
May 2023

This month, we are talking about **Configuration Reviews**. Most security frameworks include periodic configuration reviews as a core requirement. Whilst all configurations should adhere to the defined security policy at initial deployment, and all subsequent changes should have been made in accordance with that policy, this is often insufficient. As part of the general move towards Managed Detection and Response, Network Box SOCs have recently begun conducting formal configuration reviews. In our featured article, we discuss this in detail.

LINK: https://bit.ly/42vf8ZS

Network Box Hong Kong InnoEX 2023

Network Box Hong Kong was at the **InnoEX 2023** – Physical Fair, which took place at the HK Convention and Exhibition Centre. During the four-day expo, visitors were introduced to Network Box's award-winning security technologies and managed services. Additionally, Network Box Managing Director, Michael Gazeley, gave a talk titled: ***The top 10 cybersecurity facts you need to know***.

Global Security Headlines

Bleeping Computer
Cisco discloses XSS zero-day flaw in server management tool
LINK: https://bit.ly/3VdVAGY

Cyber Security News
First-Ever Ransomware Found to be Attacking macOS
LINK: https://bit.ly/41QUqDR

Bleeping Computer
Windows zero-day vulnerability exploited in ransomware attacks
LINK: https://bit.ly/44a20ek

Bleeping Computer
Intel CPUs vulnerable to new transient execution side-channel attack
LINK: https://bit.ly/3VbqXC5