Network Box
FOCUS

May 2021 Highlights

- **ItBR 202105**
  Market Share versus Vulnerability

- **Network Box HTML-5 Dashboard**

- **Network Box Media Coverage**
  - *RTHK Radio 3*
  - *CDOTrends*
  - *HPCC Hackpod Club*

24x7x365 Protection

Next Generation Managed Security

Unified Threat Management Plus (UTM+)

Award-Winning
Solutions and Services

Firewall, Intrusion Detection and Prevention (IDP), Virtual Private Networking (VPN), Anti-Malware, Anti-Spam, Anti-Spyware, 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 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, Secure Video Conferencing Gatekeeper, Quality of Service Control, Traffic Policing, Denial of Service Protection, Threshold Limiting, Hardware Fault Tolerance, clustering possible, Live Watch Real-Time Monitoring, Adobe PDF Report Generation, SSL (Secure Socket Layer) Virtual Private Networking, Anti-SPAM Pre-Scanning, bandwidth protection, Enhanced Image SPAM protection, including Optical Character Recognition technology, 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

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 high quality managed cybersecurity services, 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 in the USA, Europe, the Middle East, Asia, and Australasia; help 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 triple ISO 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 infection by trojans, viruses and other malware. Business risk and outgoing threats are alleviated by blocking leakage of valuable information and denying access to non-work related or infected web sites 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.

2021 Globee®
Cyber Security Global Excellence Awards

Network Box has won, in total, **13 Gold** and **3 Grand** awards published out of Silicon Valley.

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 infrastructure.

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.

Triple ISO Certified

Network Box HQ Security Operations Centre is triple ISO certified, by SGS of Switzerland. The certifications were renewed in February 2021, highlighting Network Box's continued commitment to excellence.

- **ISO 9001:2015**
- **ISO/IEC 20000:2011**
- **ISO/IEC 27001:2013**

Triple 100% **Tolly** Rating

Tolly Group, one of the world's most respected IT Testing Labs, certified Network Box with 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 triple 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 to stay 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, nor the resources to implement effectively. Network Box's Managed Security Services include:

24x7x365 Monitoring
Network Box analyses over 800 million statistical data packets each day, 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, on the other hand, provides **UTM+**, which has more enhanced features provided by even the most advanced UTMs and also 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 both internal and external threats, as well as additional features to manage your network

Incoming Threat Protection

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

Incoming Threat Protection

Outgoing Threat Protection

Additional Features

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 back up 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 available 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 business or branch office 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

PU↗ SH
PUSH TECHNOLOGY
WHY WAIT?

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*

* For real-time stats and figures:
http://response.network-box.com/services

PU↗ SH 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 they 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 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

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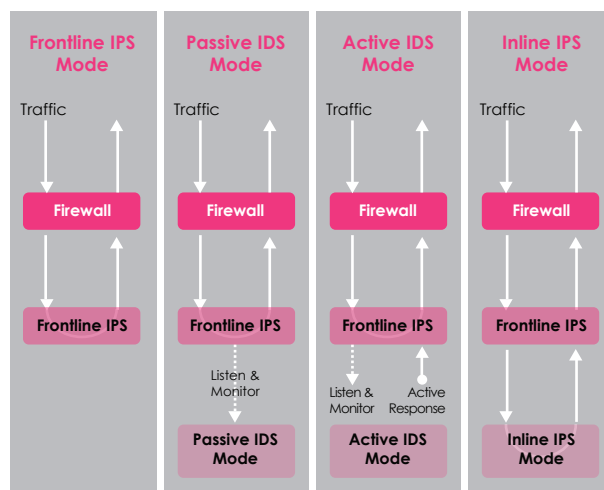
Proxy Firewall:
A set of secure proxies, integrated to the firewall, connection tracking and NAT systems, capable of high-level protection up to layer 7 Application Layer.

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, and the system can be preconfigured to actively block the threat.

There are four IDP modes offered by Network Box:

Frontline IPS Mode	Passive IDS Mode	Active IDS Mode	Inline IPS Mode
Traffic	Traffic	Traffic	Traffic
Firewall	Firewall	Firewall	Firewall
Frontline IPS	Frontline IPS	Frontline IPS	Frontline IPS
	Listen & Monitor	Listen & Monitor / Active Response	
	Passive IDS Mode	Active IDS Mode	Inline IPS Mode

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

* For real-time stats and figures:
http://response.network-box.com/protection

Incoming/ Outgoing
Email Protection

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

Multi-Layered
Anti-Spam

With support for SMTP, POP3 and IMAP email protocols, the Anti-Spam system scans and blocks spam and other malicious emails from entering your network. In addition to spam detection, the system also comprehensively scan emails for malware, intrusion, and company policy conformance.

25 Engines
30 million+ Spam Signatures*

99.73% Detection Accuracy**
0.01% 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 be also be customized to ensure more effective prevention.

Customizable rules and policies

Sophisticated pattern matching and content analysis

Scripting capabilities

*   http://response.network-box.com/protection
** http://response.network-box.com/services

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 terms of 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 57 productivity categories to identify and classify web content:

- Uncategorized
- 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
- Hacking
- Health & Medicine
- Hobbies & Recreation
- Hosting Sites
- Illegal Drugs
- Infrastructure
- Intimate Apparel & Swimwear
- Intolerance & Hate
- Jobs Search & Career Development
- Kids Sites

- Motor Vehicles
- News
- Peer-to-Peer
- Personal & 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 URL
- Tasteless & Offensive
- Travel
- 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

* For real-time stats and figures:
  http://response.network-box.com/protection

Brute Force Protection

The Anti-DDoS 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 engine mitigates Distributed Denial of Service (DDoS) attacks so that 'bad traffic' is kept at bay, while '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
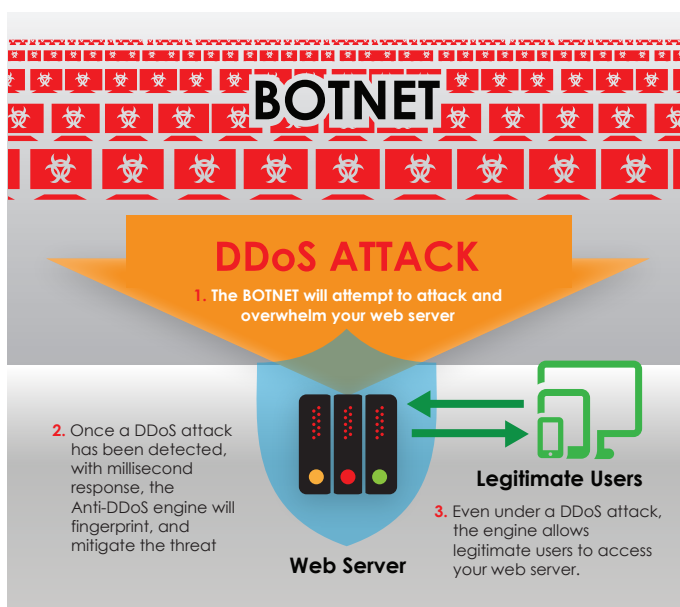
Slows down attacks by a factor of 1,000

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

BOTNET

DDoS ATTACK

1. The BOTNET will attempt to attack and overwhelm your web server

2. Once a DDoS attack has been detected, with millisecond response, the Anti-DDoS engine will fingerprint, and mitigate the threat

3. Even under a DDoS attack, the engine allows legitimate users to access your web server.

Legitimate Users

Web Server

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 database of rules, 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 a database of over 6,000 rules combined with a signature database, to identify several million threats

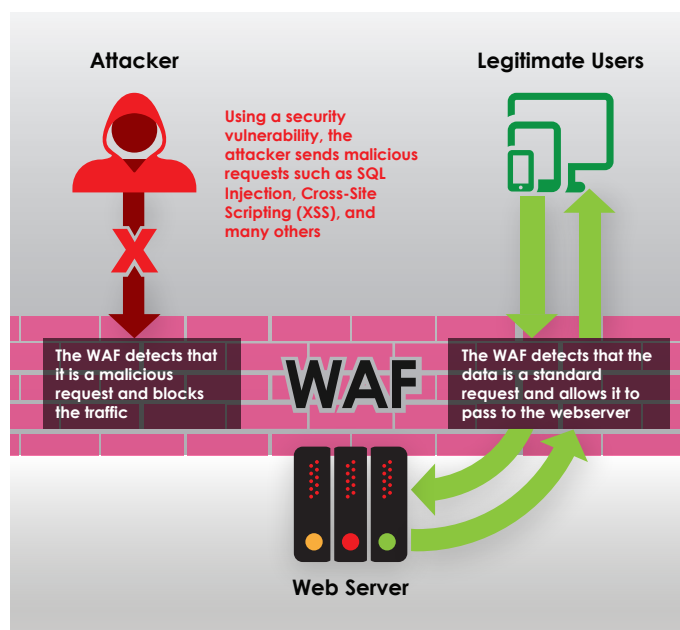Up to 15,000 fully analyzed transactions per second

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

Standard Applications:
Apache, IIS, Joomla, Drupal, Mediawiki, Wordpress, etc.

Custom Applications:
Specially developed, tailor-made software for a specific organization or specific user.

Attacker

Legitimate Users

Using a security vulnerability, the attacker sends malicious requests such as SQL Injection, Cross-Site Scripting (XSS), and many others

The WAF detects that it is a malicious request and blocks the traffic

WAF

The WAF detects that the data is a standard request and allows it to pass to the webserver

Web Server

Encrypted Secure

Data Exchange

Without a secured connection between your Internet endpoints, your communication and data can be intercepted and stolen by hackers.

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 home 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
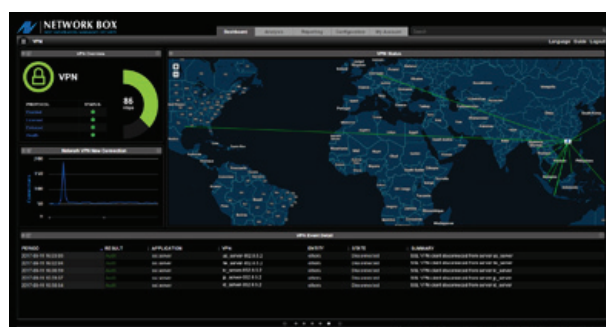
■ VPN Status Dashboard Screen

Enhanced
Policy Control

Application Scanning and Control 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 1,300+ 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 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
User will be able to 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, VOIP phones, into a single entity. Attributes such as MAC addresses, IP addresses, email addresses, are then tracked, as well as the network resources which they utilize. Comprehensive reporting and policy control facilities are then made available, based on the entity.

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 single holistic view of the activity of each of the entities 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.
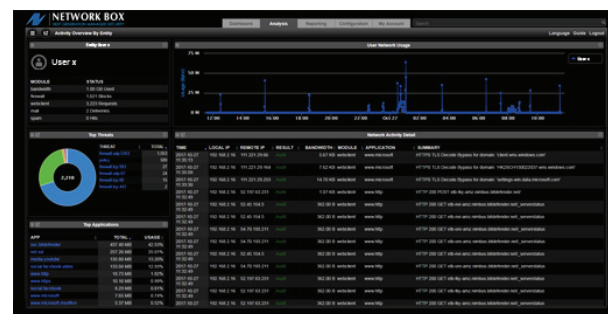

■ Entity Dashboard Screen

Internal 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 the LAN/DMZ areas of your network. Once identified, the engine can be configured to quarantine infected systems automatically. While other engines can detect access to malicious content, the engine explicitly scans outbound traffic to identify botnet access from your network.
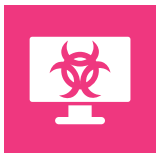
Identification and dynamic blacklisting of infected systems

Detection of outbound access to known botnet and malware sites

Highly-granular detection for highly-prolific malware (such as Palevo, Conficker, Zeus)

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 apply 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 and more; in both direct and STARTTLS modes.

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 index by standard search engines such as Google, Yahoo, or Bing. This is known as the **Surface Web**.

- The other 96% of the Internet, is made up of the **Deep Web**.

- Within the Deep Web, there is a subset of **Dark Nets**.

- It is the collection of these Dark Nets that make up the **Dark Web**.

Surface Web

The Deep Web

The Dark Web

Dark Net | Dark Net | Dark Net | Dark Net | Dark Net
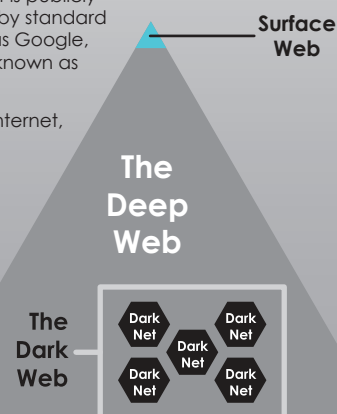
Cross Protocol Bridging

Using an automatic dual-stack interception mechanism combined with outgoing protocol translation, the IPv4 / IPv6 Bridging engine allows communication between both IP protocols.

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.

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

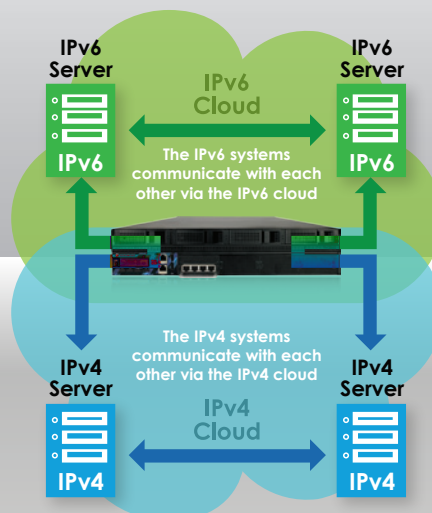- Dual-stack interception mechanism with outgoing protocol translation

- IPv6 Border Gateway Protocol offered as a service

True cross-protocol translation

The system is fully dual-stack, with all middleware services developed from the ground up to be IPv6 capable. Unlike other systems, Network Box does not merely just act as an IPv6 device on your network; the IPv4 / IPv6 Bridging engine assists you with migration to IPv6. Network Box also offers an IPv6 Border Gateway Protocol solution that can be installed along-side the IPv4 to IPv6 bridging service to allow you to connect your IPv6 network to the IPv6 internet.

The Network Box device recognizes both IPv4 and IPv6 protocols and acts as a bridge between the two IP clouds so that computers on IPv4 can access computers on IPv6 and vice versa.

IPv6 Server

IPv6 Cloud

IPv6 Server

IPv6

The IPv6 systems communicate with each other via the IPv6 cloud

IPv6

The IPv4 systems communicate with each other via the IPv4 cloud

IPv4 Server

IPv4 Cloud

IPv4 Server

IPv4

IPv4

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 outage 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.

4 Geographical regions: America, Europe, Asia and the Pacific

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, your internal network, or your 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.

Intuitive Graphic User Interface

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

KPI

The Network Box Reporting system has been enhanced to leverage the concept of Key Performance Indicators (KPIs). Each Network Box hardware appliance comes with predefined KPI weekly reports, which provides a weekly summary of events and actions within your network. Using the Network Box Dashboard, you can customize the reports for more granular control.

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 on how you want to monitor your network.

A highly customizable dashboard that gives 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 allows you to see what is happening in real-time, as well as what has been happening over any given time

Real-Time Portable Monitoring

The HTML-5 Dashboard is compatible with almost any modern large-screen mobile device. Thus, allowing you to continually monitor your network's status even when you are away from your workstation.

Customized Reports

By using the Dashboard, you can create customized reports on anything available in the system. These reports can either be generated on-the-fly for real-time instant reports or scheduled to be picked up or delivered periodically via email. Reports are available in Adobe PDF or CSV format.

Security Incident and Asset Monitoring

The Network Box SIEM+ system allows IT Managers to view all security incident 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.

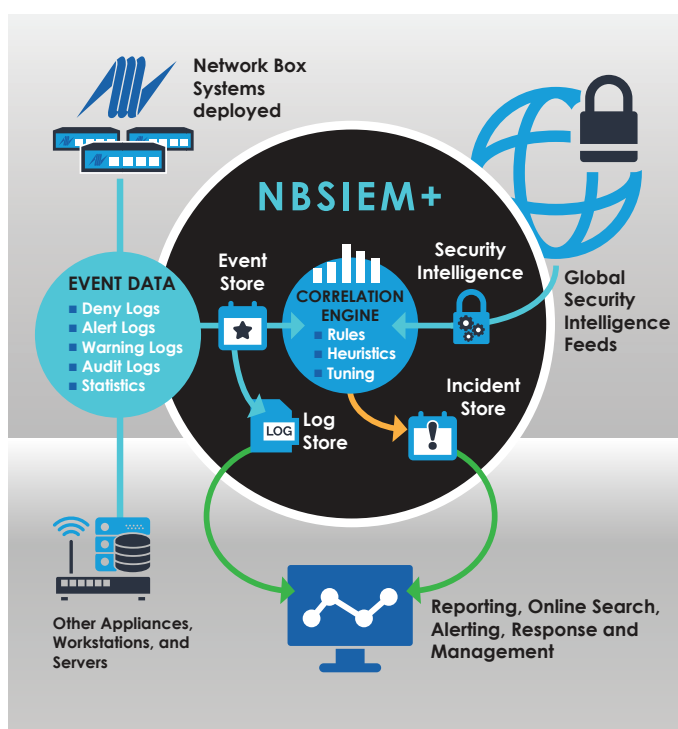Powerful on-line search facilities for events, incidents, assets and more

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 device and systems across their entire network.

Network Box Systems deployed

NBSIEM+

Security Intelligence

Global Security Intelligence Feeds

EVENT DATA
- Deny Logs
- Alert Logs
- Warning Logs
- Audit Logs
- Statistics

Event Store

CORRELATION ENGINE
- Rules
- Heuristics
- Tuning

Incident Store

LOG Log Store

Other Appliances, Workstations, and Servers

Reporting, Online Search, Alerting, Response and Management

MAY 2021

In the Boxing Ring
May 2021

This month, we are talking about **Market Share versus Vulnerability**. Looking at the statistics for malware detections, it is clear that Microsoft Windows is a huge target. Last year, around 83% of malware targeted Windows, with another 11% targeting browsers, leaving just a few percentages left for all the other platforms. But does that mean that Windows is inherently weaker and more vulnerable? In our featured article, we analyze the data and discuss this in detail.

LINK:
https://network-box.com/sites/default/files/files/ITBR-202105.pdf

Network Box
HTML-5 Dashboard

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

Additionally, the dashboard is compatible with almost any modern large-screen mobile device to provide real-time portable monitoring. Thus, allowing you to continually monitor your network's status even when you are away from your workstation.

Please use the link below to download the new Dashboard Admin Guide:
https://bit.ly/3aZ84MN

Network Box
Media Coverage

RTHK Radio 3
Backchat with Hugh Chiverton:
Rift between Apple and Facebook
LINK: https://bit.ly/3uhLZkb

CDOTrends
Herd Immunity from Computer Worms
LINK: https://bit.ly/3e9HtPc

HPCC Hackpod Club
Episode #8:
Funding in IT
LINK: https://bit.ly/2PHUmXc