NETWORK BOX

NEXT GENERATION MANAGED SECURITY

www.network-box.com

Network Box FOCUS

October 2019 | Issue 83

Award Winning Protection

This month's highlights:

- **Network Box Hong Kong**
  Macquarie Group - Cybersecurity Awareness Week
- **Network Box Germany**
  Server-Eye Partner Day
- **Network Box Media Coverage**
  - *Financial Times*
  - *SCMP*
  - *SC Magazine*
  - *it-daily.net*

24 x7x365 **Protection**

Fast, Accurate **Performance**

Unified Threat Management Plus **(UTM+)**

Anti-Distributed Denial of Service Web Application Firewall Plus **(Anti-DDoS WAF+)**

Real-Time Cloud-Based **Defense System**

PUSH

Real-Time Security Updates

PUSH

Triple ISO

ISO 9001:2008
ISO/IEC 20000:2011
ISO/IEC 27001:2013

Triple Tolly

100% Extended WildList Malware detection over **HTTP**, **POP3** and **SMTP** protocols

IPv6

IPv6 Ready Core Phase-2 certified

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

Global
Cyber Security Services

Network Box is protecting over 1,700 key organizations and government departments around the world.

Cyber threats are a global issue, which is why Network Box has established Security Operations Centers (SOCs) around the world. With a global network of SOCs operating in the **USA**, **Europe**, the **Middle East**, **Asia** and **Australasia**; Network Box ensures customers right across the globe are protected and kept up-to-date against the very latest threats, 24 hours a day, 7 days a week, 365 days a year.

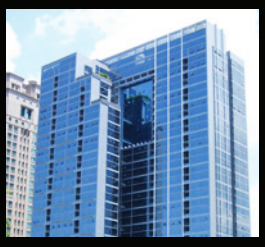
Global Security Network

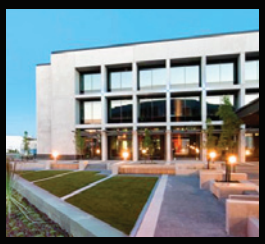
Global Threat Intelligence

24x7x365 Security Service

Clock-wise from top left: Network Box Germany, *Cologne;* Network Box Middle East, *Dubai;* Network Box Singapore, *Woodlands;* Network Box HQ; Network Box Indonesia, Jakarta; Network Box Taiwan, *Taichung;* Network Box Australasia, *Christchurch;* Network Box China, *Shenzhen;*








▲ Network Box USA Head Office, Houston, Texas

Certified **Performance**

Network Box is certified by independent international standard authorities.

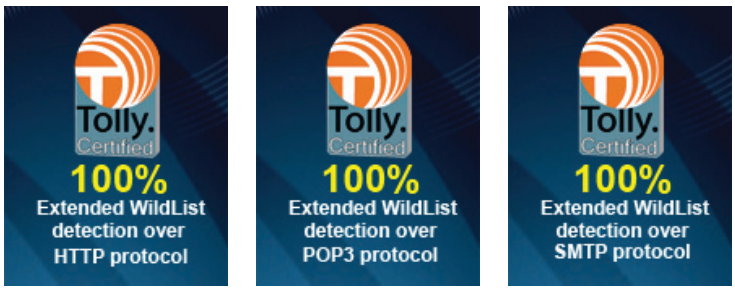
Triple ISO Certified

Network Box HQ Security Operations Centre is triple ISO certified, by SGS of Switzerland. The certifications were renewed in February 2019, highlighting Network Box's continued commitment to excellence.

- **ISO 9001:2008**
- **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.



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).

KV-S@feNet

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

CVE

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

Award Winning Technologies

Network Box has won more than 150 international industry, media and governmental awards.

Winner of multiple awards published out of Silicon Valley

Network Box's cutting-edge technologies have enabled the company to win **eight Gold** and **two Grand**, Silicon Valley Communications: Info Security Awards.

Best Enterprise Risk Management (ERM) Awards 2018

Gold Award

This prestigious award is given by the **Academy of Professional Certification (APC)**, to honour companies that demonstrate excellence and achievement in Enterprise Risk Management.

Gartner Recognition

Asia/Pacific Context:

Magic Quadrant for Global MSSPs

Analysts: Craig Lawson | Andrew Walls
Date: 02 July 2014

Summary

The adoption of managed security services in Asia/Pacific continues to grow, with most global vendors in the 2014 MSSP Magic Quadrant facing strong competition from regional MSSPs. Depth and breadth of services and language support vary widely, giving clients choice from many services and prices.

LINK: https://www.gartner.com/doc/2788117/asiapacific-context-magic-quadrant-global

Notable Vendors:

AT&T
BT Assure
Dell SecureWorks
e-Cop
HCL
HP
IBM
Network Box
NTT
Paladion
Symantec
Tata Communications
Telstra
Verizon
Wipro

FORRESTER®

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

The Forrester Wave
Emerging Managed Security Service Providers

FROST & SULLIVAN

"Strong credibility with customers, due to its many global operations centers, extensive experience, and continual research and development activities."

Frost & Sullivan
Unified Threat Management Market Report

"Network Box's Z-Scan Anti-Malware service uses hundreds of thousands of probes spread around the world on key network segments to detect advanced malware and other anomalies. The company also added more than a dozen anti-malware scanners and three IPS engines to examine packets."

David Strom
'The changing face of advanced malware detection'

Managed **Security Services**

Network Box's Managed Security Services, monitors, manages and mitigates cyber threats from your network 24x7x365, alleviating your security risk, and allowing you to concentrate on running your business.

It looks like a product **but it's acutally a service**

Cyber attacks are on-going, and to stay protected against these 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.

As part of Network Box's Managed Security Services, highly trained Network Box security engineers perform the never ending, yet vital, management of your cyber security, ensuring that you are protected against cyber threats 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. Futhermore, every Network Box system is constantly monitored to ensure it is running smoothly.

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

Mitigation: If a new cyber threat is detected, Network Box will automatically PUSH out and install security patches in real-time. Every Network Box system in the world is updated in an average time of less than 45 seconds.

Managed Service vs Self-Managed Product **Comparison Table**

Network Box Managed Security Services provide much more than Self-Managed Products.

	Managed Service	Self-Managed
Control	**Hosted**	Localized
Change Control	**Performed by trained security analysts to triple ISO standards**	Limited by product, time and skills
Service Levels	**Tailored to customer needs**	In-house limitation
Security Level	**Choice of security provision**	Limited to product and skill
Time	**Delegate the issues to the managed service provider**	Consumes considerable time and resources, especially when skills are limited
Updates	**One update of all services ensures compatibility**	Separate updates for each product with potential conflicts
Management	**From a single console**	From separate consoles
Knowledge of Threats/Risks	**Constantly refreshed and proactively applied**	Reactive

Real-time Monitoring · Threat Analysis · Bandwidth Management · Business Continuity · Change Control · Security Consulting

Unified Threat Management Plus **(UTM+)**

Cyber Security issues may arise if you do not have the right security solutions in place. Merely having a firewall with anti-virus software is not enough, you need comprehensive Unified Threat Management (UTM) protection.

What is **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 otherhand 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.

- Hybrid Firewall
- Intrusion Detection & Prevention
- Virtual Private Network
- Anti-Malware
- Zero-Day Protection
- Anti-Spam
- Data Leakage Prevention
- Anti-DDoS
- Web Application Firewall
- Infected LAN
- Content Filtering
- Application Scanning & Control
- Entity Management
- SSL Proxying
- IPv4 to IPv6 Bridging
- Cloud email & DNS Backup
- HTML-5 Dashboard
- PUSH Updates

Hybrid Firewall
18 Engines
Packet Filtering
Stateful Inspection
Proxy

Intrusion Prevention
3 Engines
16,027 Signatures*

Anti-Malware
16 Engines
12,464,026 Signatures*
Mobile Device Anti-Malware
Zero Day Protection

Anti-Spam
25 Engines
30,823,378 Signatures*
Zero Day Protection

Content Filtering
15 Engines
7,762,716 Signatures*
57 Categories

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

PUSH Real-Time Updates

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

Up-to-the-minute **Protection**

Standard security systems usually pull updates from a server once a day, or at best once an hour. In contrast, Network Box pushes out updates as soon as they become available.

- You do not need to know that there is an update waiting.
- You do not need to ensure that you have the rights to access the patch on the website.
- You do not have to download it and ensure the checksum is correct.
- You do not have to find time to install it.
- You do not have to repeat all these steps for each device.

Microsoft Active Protections Program **(MAPP)**

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

Microsoft

DID YOU KNOW?

In 2000, Network Box was PUSHING out **8** updates a day. Today, Network Box is PUSHing out **10,151** real-time signature updates a day.

Protection 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.

Stateful Inspection: monitors active connections to determine which network packets to allow through to the network.

Packet Filtering: blocks or allows packets through the network depending on the source/destination IP, protocols and ports.

Proxy Firewall: scans traffic at the layer 7 Application Layer.

Intrusion Detection and Prevention **(IDP)**

Tightly integrated with the firewall, the IDP system monitors and analyzes your network for signs of intrusion. If an intrusion attempt is detected, it is logged, and the system can be set to actively block the threat.

There are four IDP modes offered by Network Box:

Front-Line IPS: Inline with the data-stream, extremely light-weight, adds packet content inspection, rate limiting and traffic analysis, to the base firewall capabilities.

Passive IDS: Side-by-side with the data stream, alerting and logging of traffic only.

Active IDS: Side-by-side with the data stream, alerting and logging of traffic, and actively teardown connections once malicious traffic has been identified.

Inline IPS: Inline with the data-stream, alerting and logging of traffic, and able to drop traffic before the remote system even sees it.

Ruggedized Virtual Private Network Connections

The Network Box Virtual Private Network (VPN) engine secures internet connections between end points. In addition to providing graphical representation and control of the VPN, the engine has also been ruggedized to relieve connectivity issues.

Virtual Private Network **(VPN)**

The Network Box VPN engine secures out-of-office connections to ensure data remains secured and confidential during Internet exchange.

Network Box provides support for three core VPN technologies:

- PPTP
- IPSEC
- SSL VPN

All three VPN options are fully integrated to the firewall and provide excellent policy control, allowing different firewall policies to be applied to encrypted vs non-encrypted traffic, and to specific end-points. The VPNs are also inter-routable, so traffic can be translated between VPN technologies by a single Network Box appliance.

Furthermore, the VPN engine has been ruggedized to handle ISP connectivity issues, bridges non-standard compliant connections, and automates the approach for the most common connectivity issues.

Visual VPN

With the Network Box HTML-5 Dashboard, all the VPN types have been unified into a single unified frame-work, 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-5Q

The VPN-5Q is a fanless VPN device, designed to secure connections between Internet end points. It is light weight 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.

Z-SCAN

Zero-Day Anti-Malware

Z-Scan focuses on developing and releasing real time pattern matching updates to protect against emerging viruses with a best response time of **3 seconds** from a threat being detected.

Real-Time, Cloud-Based **Defence System**

DID YOU KNOW?

Network Box's anti-malware systems have offered protection for mobile devices since April 2011

Z-Scan operates by continually analysing all the threat information obtained in real time from more than **250,000** traps in the cloud, poised 24/7 for virus attacks to occur. With a best response time of **3 seconds**, Z-Scan performs up to **4,200** times faster than typical gateway anti-virus systems.

Multi-Layered **Anti-Malware**

In addition to Z-Scan, multi-layered Network Box anti-malware engine, M-Scan, provides an additional 15 anti-malware engines, including both **Kaspersky Labs** and **ClamAV**, to identify and prevent viruses, trojans, worms and other malicious software, from infecting your networked systems or networked smart devices.

Anti-Malware Systems **Comparison Chart**

	Z-Scan	M-Scan	Typical Anti-Virus
Engines Total	**1**	**15**	1
Current Signature Total	**250,000+**	**12,000,000+**	3,500 - 5,500,000
Malware Gathering	**Real Time**	**Real Time**	Batch Processing
Update Technology Used	**In-the-Cloud**	**PUSH**	PULL
Typical Signature Creation	**1 - 30 secs**	**10 - 120 mins**	3 - 12 hrs
Typical Signature Release	**2 - 3 secs**	**30 - 45 secs**	Hourly / Daily
Expected Best Response Time	**3 secs**	**10.5 mins**	3.5 hrs

Along with its anti-malware capabilities, Z-Scan's cloud-based infrastructure augments Network Box's anti-spam performance, by dealing with zero-day spam. This has helped Network Box achieve an industry-leading email detection accuracy of up to 98.83% in real world usage.

Incoming and Outgoing Mail **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**

The Network Box Anti-Spam engine is the most comprehensive and effective gateway anti-spam solution in the market today. It provides **25** anti-spam engines, and is backed by a database of over **30 million** signatures. The Network Box anti-spam email gateway achieves an industry-record detection rate of at least **97.99%** with almost zero false-positives.

Technologies Used:

- Co-operative Spam Checksums
- Signatures and Spam Scoring
- White Lists and Black Lists
- Real-Time IP and URL Black Lists
- URL to IP Mapping and Black Lists
- URL Categorization / Domain Age
- Bayesian Filtering
- Challenge / Response Systems

Data Leakage **Prevention** (DLP)

The Network Box DLP engine uses complex rules engines to scan and block outbound SMTP mail that may contain sensitive materials. This can include client info, account details, designs, commercial secrets, medical records as well document files, credit card numbers or social security numbers. The DLP rules and policies can be customized thus ensuring effective prevention.

Key Features:

- Customizable Rules and Policies
- Complex Pattern Matching
- Content Analysis
- Heuristics
- Boolean and Arithmetic Logic
- Optical Character Recognition (OCR)

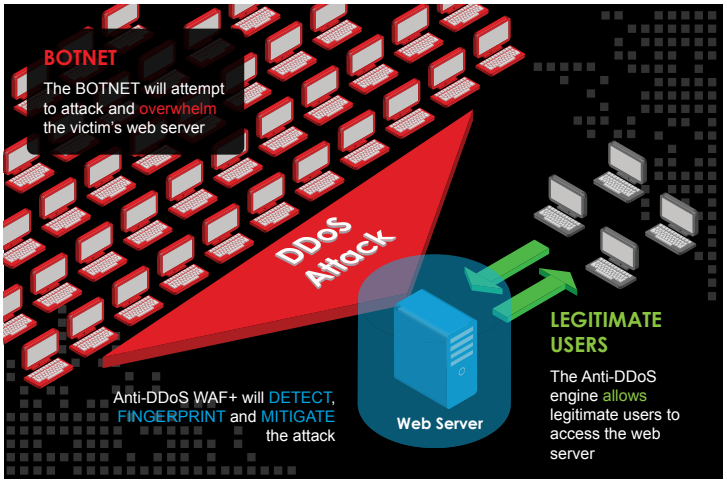
Assured **Business Continuity**

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

Anti-Distributed Denial of Service **(Anti-DDoS)**

The Network Box Anti-DDoS engine provides Distributed Denial of Service (DDoS) Attack mitigation, so that 'bad traffic' is kept at bay, while 'good traffic' is allowed through to secured web facing servers, defending business continuity during ongoing attacks. It uses real-time automated fingerprinting to identify and blacklist attacks. The engine takes milliseconds to respond to brute force attacks that typically come from thousands of sources.

The system keeps track of DDoS information on a per-source basis (which it periodically maintains and prunes), and imposes limits on reasonable behavior. Sources which exceed those limits are deemed to be DoS/DDoS attack sources and mitigated.



The Anti-DDoS engines offers DoS/DDoS mitigation facilities:

- 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

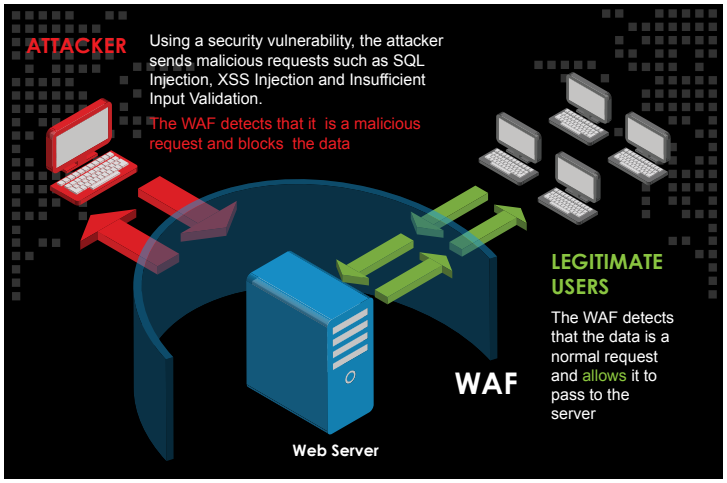
Next Generation **Protection**

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.

Web Application Firewall **(WAF)**

The WAF engine protects web servers against web application based attacks, including the OWASP Top 10 as standard. It also allows you to have a wide range of options for blocking and logging traffic as it passes through the WAF rules system. The rules system offers the possibility to define both positive and negative security models. Using PUSH Technology, the engine also allows for the real-time installation of emergency virtual patches at the gateway, to immediately detect and prevent any application or web server specific security issues.

The WAF engine uses a database of over **6,000** rules combined with anti-malware and IP signature databases to identify several million threats. The high performance rules engine is capable of millions of rule-checks per second, and up to **15,000** fully analyzed transactions per second.



WAF-Scan can offer protection for two application groups:

Standard Applications
Apache, IIS, Joomla, Drupal, Mediawiki, Wordpress

Custom Applications
Tailor made software that has been specially developed for a specific organization or specific user.

S-SCAN Web Content Filtering

S-Scan is designed to help organizations block users from accessing undesirable web content. With a detection rate of **98.7%** it offers excellent performance in terms of speed, coverage and web accuracy.

Fast, Accurate **Performance**

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

Comparison Table

Below is a comparison of the S-Scan *Extended* engine, and the SurfControl engine, over two empirical data sets: **Alexa100k-** the Top 100,000 websites, visited by global Internet users; and **NBCustDom-** the list of specific domains owned by Network Box customers.

Data Set	URLs	S-Scan *Extended*	SurfControl
Alexa100k	100,000	**98.7%**	73.9%
NBCustDom	270	**93.0%**	8.5%

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

Enhanced **Policy Control**

Application Scanning and Control looks at web traffic to identify the application and allows company policy control to be applied. Over **1,300** applications are supported.

Application Scanning **and Control**

DID YOU KNOW?

From a study of web traffic of Network Box customers, **58%** of Internet access is not work related.

While traditional firewalls block protocols, 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 identified, the system allows connections to be appropriately labelled for reporting and policy control.

Integrated to the SSL Proxy, even traffic inside encrypted SSL sessions can be identified and controlled.

The system can also promote traffic to be handled by protocol specific scanning modules to perform more detailed analysis such as anti-malware scanning.

Network Box's Application Scanning and Control engine supports over **1,300** applications such as Skype, Twitter, Facebook, YouTube, Spotify, WhatsApp, Reddit, etc; split over **15** categories and **20** tags.

15 Categories		
Collaboration	Messaging	Social Networking
Database	Network Monitoring	Streaming Media
File Transfer	Networking	Unknown
Games	Proxy	VPN and Tunnelling
Mail	Remote Access	Web Services

20 Tags		
Advertisements	Mobile	Video Conferencing
Encryption	Peer 2 Peer	Voice Conferencing
Facebook App	Phones Home	Excessive Bandwidth
Instant Messaging	Proxy	Potential Data Leak
Internet Search	Remote Control	Prone to Misuse
Logs Communication	Screen Sharing	Used by Malware
Media Share	Uses Stealth	-

Secured **Certificate Exchange**

DID YOU KNOW?

The average clickthrough rates for SSL warnings in Google Chrome and Mozilla Firefox are **73.4%** and **36.7%** respectively.

SSL Proxy provides identification, decryption, encryption, certificate validation and protection of SSL network traffic.

Secure Socket Layer (SSL) **Proxy**

SSL is a cryptographic protocol used to provide security to communications between two internet endpoints, such as a web browser and a web server.

SSL is vulnerable to attack through a number of vectors, ranging from user negligence, to administrator misconfiguration, to flaws in the protocol itself.

Network Box SSL Proxy is designed protect against these internal and external threats by decrypting secure connections on the way in, performing security analysis, then re-encrypting data on the way out.

Through security analysis of the SSL connection and the protocol data, the SSL Proxy can take responsibility for secure connections going through the gateway and apply organization-wide security policy on these secure communications.

The Network Box SSL Proxy has been developed with the ability to:

1. Move the choice of bypassing failed SSL server certificate validation away from the user, to the IT Manager. This prevents users from naively ignoring browser warnings and inadvertently connecting to potentially malicious sites.

2. Offload the decryption of secure connections onto the Network Box gateway device, which hosts an up-to-date SSL software stack. SSL connections over the internet, both incoming and outgoing, are upgraded to use as secure settings as possible, following the approach of highest common denominator security, rather than the lowest.

In addition, the Network Box SSL Proxy can pass the data from within the secure connections to the Web-Content or Application Control engines to perform scans for malicious content and apply administrator configured security policies. These actions are not possible to perform on SSL encrypted connections without the Network Box SSL Proxy.

Internal Threat **Protection**

The Network Box Infected LAN engine allows infected systems to be identified and isolated from your network.

Infected **LAN**

The Network Box Infected LAN engine helps pinpoint infected workstations, servers, and connected smart devices in the LAN/DMZ areas of your network, to be quarantined.

While other engines (such as anti-malware and content filtering) can detect access to malicious content, the Infected LAN engine scans outbound traffic to identfy botnet access from your network.

To stay up-to-date, the engine subscribes to a PUSH updated signature set of several thousand malicious URLs and IP addresses used by known botnet command and control centres.

- Detection of outbound access to known public botnet command and control servers.
- Detection of outbound access to known malware update sites.
- Highly-granular detection for highly-prolific malware (such as Palevo, Conficker, Zeus, etc.)
- Optional support for dynamically blacklisting infected workstations / servers / connected smart devices.

DID YOU KNOW?

Network Box can protect you from URLs and IP addresses containing: cryptowall, feodo, locky, palevo, teslacrypt, torlock, zeus, and other common botnets.

User and Device **Management**

The Entity Management system allows IT Managers to group all users' devices into a single entity and provide effective monitoring, management and protection.

Entity **Management**

Network Box's revolutionary Entity Management system completely redefines how users and machines are monitored and protected.

A user's devices (such as iPad, iPhone, Laptop, Desktop, VOIP Phone, etc) are all grouped into one single entity. The system tracks their attributes (such as MAC addresses, IP addresses, email addresses, etc), and the network resources which they utilize.

It 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, email, etc; 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 for helping IT Managers to monitor, manage and protect their users and networks.

Key **Features**

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 in your network.

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

DID YOU KNOW?

In developed countries, the average person owns 3.64 mobile/internet devices.

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.

IPv4 to IPv6 / IPv6 to IPv4 **Bridging**

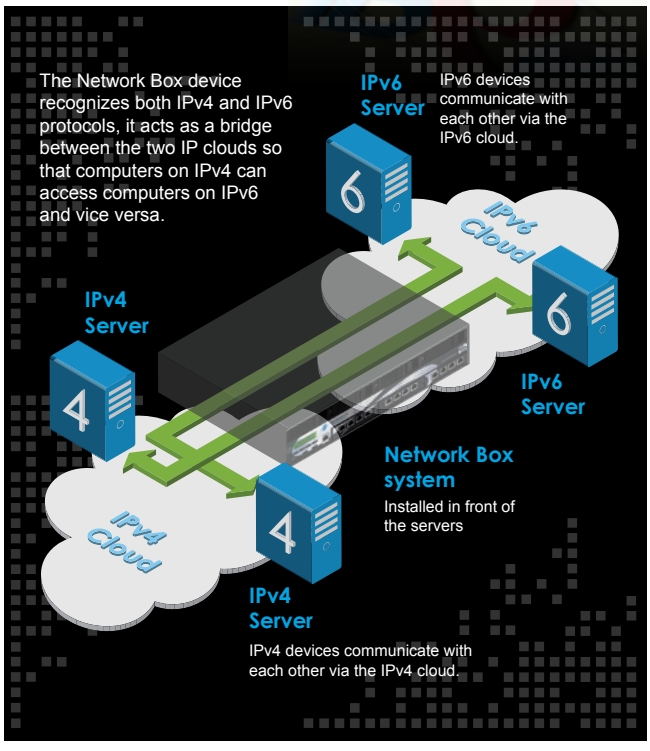
The Network Box IPv4 / IPv6 Bridging engine supports bi-directional translation between IPv4 and IPv6, allowing IPv4 clients to connect to IPv6 servers, and vice-versa. It is designed to help organizations with their migration to IPv6, while integrating naturally with any IPv4 network.

The system is fully dual-stack, with all middleware services developed from the ground up to be IPv6 capable. Network Box also offers an IPv6 Border Gateway Protocol solution that can be installed along-side the IPv4 to IPv6 bridging service to allow customers to connect their IPv6 network to the IPv6 internet.

As IPv4 addresses will soon become unavailable, organizations everywhere will soon be faced with the very real need to migrate over to IPv6.

DID YOU KNOW?

Network Box is the first, and so far only, Managed Security Service Provider to achieve IPv6 Ready Core Phase-2 Certification.



Secured In-the-Cloud Backups

With Network Box's global network of cloud backup servers, you are assured of business continuity and service reliability.

Cloud Mail Backup

Lost or bounced emails can affect business continuity. The Network Box Cloud Mail Backup system 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 problem has been resolved.

- Backup storage only if your email servers are overloaded and temporarily not accepting new connections/emails
- Once delivered, the emails will be removed and only logs (containing date, time, sender and recipient) will be retained
- **4 geographical locations:**
  Asia, America, Europe and the Pacific
  This allows you to 'lock-in' to a specific region so that your emails remain in your location

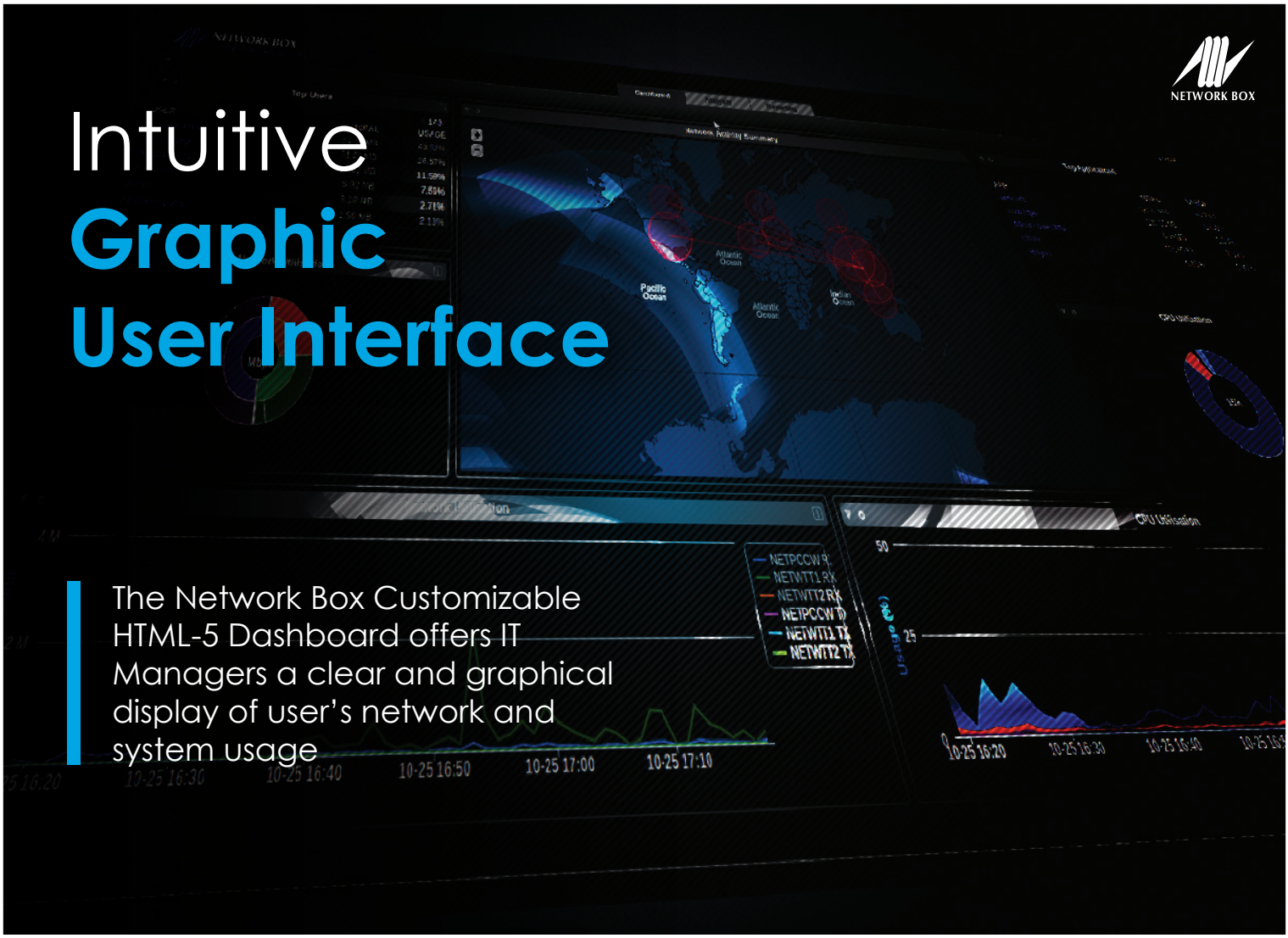
Cloud DNS Backup

The Domain Name System (DNS) is the 'telephone directory' of the Interenet responsible for converting names to IP addresses. Web and mail traffic can be severly affected if your DNS server suffers an outage. The Network Box Cloud DNS Backup system helps mitigate this, by allowing you to use Network Box's extensive network of DNS servers to provide backup in the cloud.

In addition 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 will be used 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 offers IT Managers a clear and graphical display of user's network and system usage

HTML-5 Customizable 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.

Real-Time Portable Monitoring

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

Adobe PDF Customized Reports

In addition to the real-time data capabilities, the system can automatically generate highly customizable Adobe PDF reports, and supports CSV formats.

Key Performance Indicators (KPIs)

The Network Box Monitoring and Reporting system, has been enhanced to leverage the concept of KPIs, and is able to show what has been happening both in real-time, as well as over any given period of time. Weekly KPI reports are automatically delivered to you.

Dark Web **Protection**

Whenever there is a data breach, user's personal data usually ends up on the **Dark Web**. There are currently billions of hacked credentials posted on the Dark Web, and the number is growing fast

Dark Web Monitoring **Service**

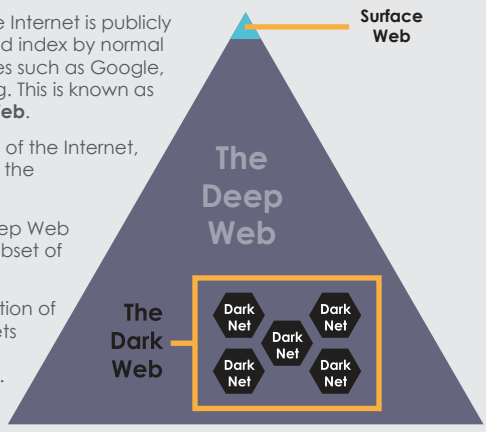
The Network Box Dark Web Monitoring system scans data breaches from the Dark Web, looking for your registered email addresses and domains. Reports are generated showing the breach details, such as breached email accounts and origin of breach. As a subscriptions service, monitoring is ongoing. When new data breaches are discovered, Network Box will re-scan and keep you informed as to changes since the last report.

In addition, the service includes **Cloud Reputation Monitoring**. This service continually monitors your registered IP ranges and domains against hundreds of public reputation lists, to ensure they are not blacklisted.

What is the Dark Web?

The Dark Web is the deliberately hidden part of the Internet, and is the natural habitat of hackers and cyber criminals. 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 normal 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 are a subset of **Dark Nets**.
- It is the collection of these Dark Nets that make up the **Dark Web**.



Hardware and Virtual **Appliance**

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

64-bit Hardware **Appliance**

A full range of Network Box models is available to support diverse performance and environmental requirements. These models are categorized into three groups: **S** for Small, **M** for Medium or **E** for Enterprise, and are designed to suit the typical workloads encountered in each organizational type. All units are 64-bit and designed to offer exceptional performance and reliability. The hardware is based on multi-core CPUs, and able to withstand extreme shock, vibration and temperature ranges.

The security software, services available and protection afforded are identical for all models. The difference between models are purely hardware features and performance.

Features	Details
Firewall	Proxy, Packet Filtering, Stateful Packet Inspection
IDS/IDP	3 Engines 16,000+ Signatures
VPN Types	IPSEC, PPTP, SSL
Anti-Spam	25 Engines 30.8million+ Signatures
Anti-Malware	16 Engines 11.2million+ Signatures
Content Filtering	15 Engines 7.7million+ Signatures
Anti-DDoS	Real-time automated finger-printing, millisecond response
IPv4 to IPv6 Bridging	Incoming/Outgoing Protocol Translation
PUSH Updates	Updates automatically delivered and installed in an average time of less than 45 sec.

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.

www.network-box.com

Network Box Focus

The latest Network Box news and updates

OCT 2019

Network Box Hong Kong

Macquarie Group - Cybersecurity Awareness Week

Network Box Hong Kong took part in Macquarie's Cybersecurity Awareness Week, conducting a seminar on the Dark Web, the dark side of the Internet. Various topics were covered, not least the threats posed by the Dark Web in terms of Identity Theft, Data Theft, and Credential Theft. In particular, credential theft, can lead to the serious compromise of workplace security, because approximately one third of people globally, use the same passwords for multiple accounts.

Network Box Germany Server-Eye Partner Day

Network Box Germany was at the Server-Eye Partner Day held in Saarbrücken, to talk about Managed Security Services and highlight key Network Box 5 security technologies.

Network Box Media Coverage

Financial Times
HKEX blames software bug for outage as website comes under attack
LINK: https://on.ft.com/2kKKgp6

SCMP
Beleaguered Hong Kong hit by double whammy as Fitch Ratings downgrades city and stock exchange hit by cyberattacks
LINK: https://bit.ly/2mJj62y

SC Magazine
Warner presses CBP on security best practices for third-party contractors
LINK: https://bit.ly/2lfaiAV

it-daily.net
Network Box Extends Its S-Series
LINK: https://bit.ly/2mCczqa