Managed Virtual Network Security

NETWORK BOX

NEXT GENERATION MANAGED SECURITY

VIRTUALIZATION *and security concerns*

Today, more and more organizations are moving their IT infrastructure to the cloud. Higher efficiency and lower total cost from this, have enabled them to leverage their resources better and respond to the needs of their business.

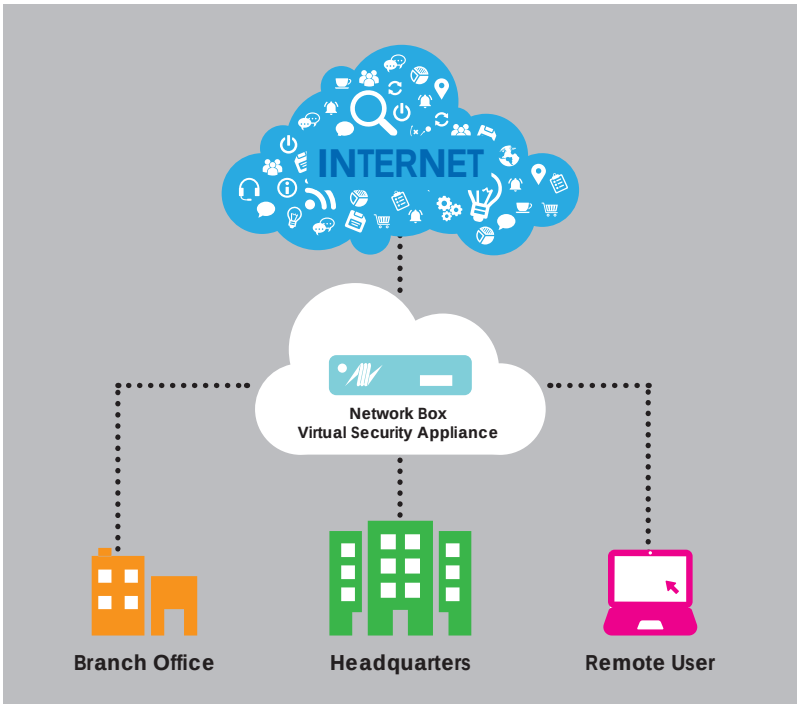
With this migration, however, security of their virtual environment becomes an issue. Virtualization presents new and challenges on security, and require a virtualized security solution specifically designed for virtual environments.

Network Box provides comprehensive solution to secure and protect your virtual environment.

Security for your cloud can be complex, Network Box makes it simple

Network Box offers multi-award winning cyber security for virtualized environments, with our range of virtual security appliance which can be deployed to your network as UTMs or WAFs (Web Application Firewalls).

Our virtual security appliances scan all incoming and outgoing traffic and protects your virtual network from both **incoming** threats from the Internet (e.g. intrusion attempts, zero-day threats, infection by trojans, viruses and other malware, spam, denial of service, etc), and **outgoing** threats from your business (e.g. by blocking leakage of important information, denying access to non-work related or undesirable web sites and applications, etc).



It may look like a product, but it is actually a service

The difference between Network Box and other virtual security appliance providers, is that Network Box offers fully managed cyber security service. Meaning, once our virtual security appliance has been installed in your virtual environment, we remotely monitor, manage and protect your network 24 hours a day, 7 days a week, 365 days a year, via our 16 SOCs (Security Operations Centres) spread across the globe.

Network Box analyses over 800 million statistical data packets each day, cooperate with more than 70 security partners, and operate over 250,000 virtual honey-pots deployed in the cloud. So if there is a new threat detected, we can automatically PUSH out and install security patches in an average time of less than 45 seconds.

Easy deployment and peace of mind

As part of our managed security services, Network Box will configure and deploy your virtual security appliance in your virtual environment, for you.

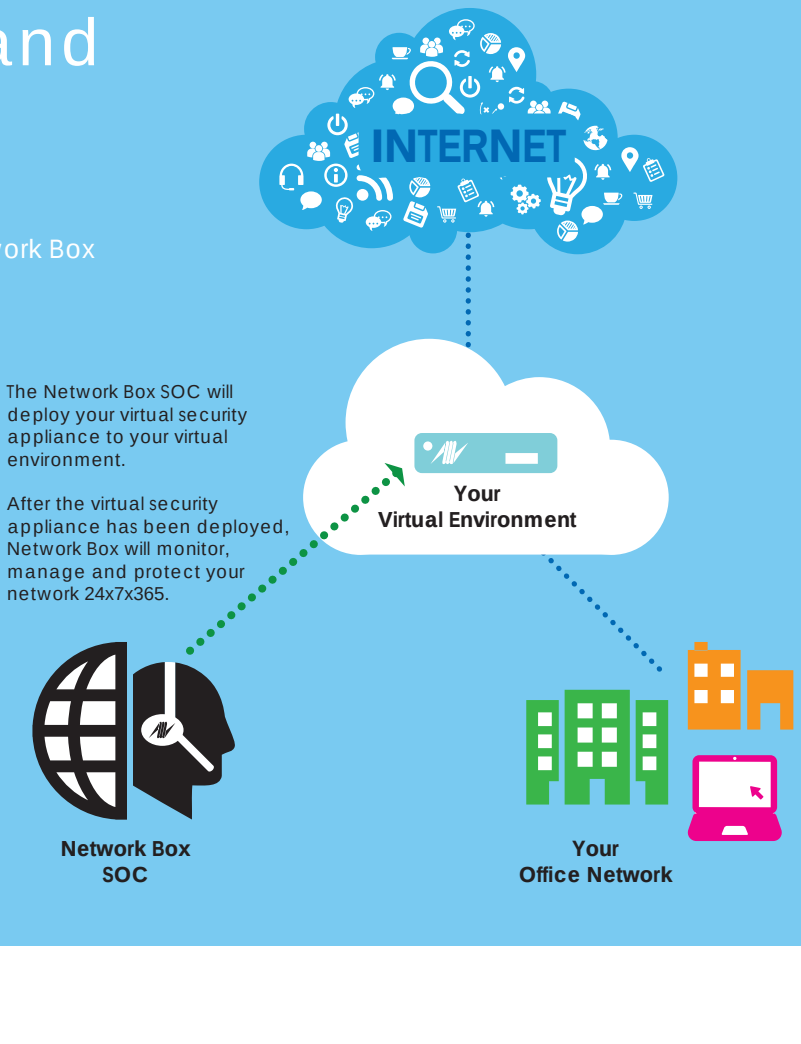
Four easy steps:

1. Consultation
Network Box will discuss your network settings, your company policy rules, and security configurations.

2. Deployment
Network Box will provision your virtual security appliance and deploy the image disk to your virtual environment.

3. Configuration
Once the virtual security appliance has been deployed, the SOC will remotely configure it.

4. Activation
When configuration is completed, your virtual security appliance is ready to use.



Merely having a firewall with anti-virus software is not enough to protect you

Cyber security issues arise because most businesses do not have the right protection in place. Network Box's all-in-one virtual security appliance protects you from all internal and external security threats with multi-award winning security technologies:

PUSH Technology
- Updates are PUSHed out and installed in an average time of less than 45 seconds
- Automated process, the customer does not need to manually download and install the updates
- Currently, Network Box is PUSHing out 15,567 updates a day

Hybrid Firewall
- Proxy Firewall, maintains transparency between requester and server
- Packet-Filtering, suitable for basic protection with minimal overhead
- Stateful Packet Inspection, suitable for high performance and sophisticated rule sets

Intrusion Detection and Prevention (IDP)
- 3 Engines; 16,011 Signatures
- Scans network traffic at the application level, and seamlessly blocks malicious behaviour with zero latency
- Two Modes: *Active* (blocks network traffic)
  Passive (logs intrusion attempts)

Virtual Private Network (VPN)
- Authenticated user sessions
- Allows different firewall policies to be applied to encrypted vs non-encrypted traffic and to specific end-points
- Supports 3 core VPN Technologies: PPTP, IPSEC, SSL VPN

Data Leakage Protection (DLP)
- Customizable rules and policies
- Complex pattern matching and Content analysis
- Optical Character Recognition (OCR)

Anti-Spam
- 25 Engines; 30,741,316 Signatures
- 98.75% Spam Detection Accuracy, with 0.01% False-Positive Rate
- Anti-Spam technologies: Co-operative Spam Checksums, Signatures and Spam Scoring, Real-Time IP and URL Blacklists, Mail Portal, URL Categorization, Bayesian Filtering, OCR

Anti-Malware
- 16 Engines; 11,146,829 Signatures
- Triple 100% Tolly Group detection rating against their Extended Wildlist Malware database over HTTP, SMTP and POP3 protocols
- Email malware protection
- Mobile malware protection

Zero-Day Threat Protection
- Industry best response times of just 3 seconds
- Performs 4,200 times faster than other typical gateway anti-malware systems
- 250,000+ virtual honey pots already deployed
- In-the-cloud Update Technology

Web Content Filtering
- 15 Engines; 7,762,716 Signatures
- Uses high performance signature based technology, rather than a simple URL database
- Detection rate of 98.7% for the Top 100,00 websites

Application Identification and Scanning
- Customizable policy rules for enhanced control of Internet access
- Supports:
  1,390 applications, 15 categories, 20 tags
- SSL encrypted traffic can also be identified and controlled

Secure Socket Layer (SSL) Proxying
- Identification, decryption, encryption, certificate validation and protection of SSL network traffic
- Uses lowest denominator of security internally, but highest common denominator externally
- Denies end-users from bypassing failed SSL certificates

Anti-Distributed Denial of Service (Anti-DDoS) Protection
- Real-Time Automated fingerprinting
- Slows down attacks by a factor of up to 1,000
- Millisecond response to brute force attacks

Web Application Firewall (WAF)
- 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
- Supports standard and custom applications

Entity Management
- Allows IT Managers to monitor, manage, and protect, their users and networks
- All users' devices can be grouped into individual entities
- Presents a single holistic view of the activity, of each of the entities in the network

IPv4 to IPv6 Bridging
- Certified to globally recognized IPv6 Ready Core Phase 2 standard
- Automatic dual-stack switching mechanism combined with protocol translation
- Offers IPv6 Border Gateway Protocol services for customers

Network Monitoring and Reporting
- HTML-5 Customizable Dashboard
- Customized Reports: Adobe PDF, CSV and other formats
- Real-time portable monitoring

NETWORK BOX

NEXT GENERATION MANAGED SECURITY

www.network-box.com

facebook Network Box | LinkedIn Network Box | YouTube NetworkBox