



SECURITY
WITHOUT COMPROMISE

A PERFECT STORM

More than ever before, our economic success depends on the secure capture, management and transfer of digital information. Yet with approximately 580M web-based attacks recorded in 2010 alone and discreet new malware samples appearing, on average, every two seconds, the task of securing that information is becoming one of the greatest challenges facing IT professionals today.

When NETASQ was founded in 1998, the threat landscape was markedly different. At that time, attacks were sporadic and often the work of teenage hackers more concerned with personal notoriety than financial gain. A major part of NETASQ's success since then, results from the insight that these isolated clouds of cyber-vandalism were in fact the precursors to a gathering storm – a storm which would launch an escalating arms race between the security industry on one side and the increasingly sophisticated and well funded resources of organised crime on the other.

VISION

NETASQ's founding vision was to realise that winning this arms race would require technology capable of intelligent, real-time, deep analysis of the traffic flow. Only with such an approach would it be possible to pre-empt new attacks before they appeared in the wild – what we now refer to as zero-day protection.

The key to realising this vision was the development of a highly efficient attack prevention engine, which today forms the basis of our intrusion prevention capabilities. The next inspiration was to embed this engine directly into a hardened BSD-based operating system, thus reducing the load on the processor and maximising data throughput. Upon this, was built an extensible framework of higher level security functions, allowing integration of best of breed antivirus, web filtering and all the other technology now included in the category of unified threat management. Finally, to avoid compromising this superior performance, optimised hardware and virtual appliances were developed to create a range of solutions capable of scaling to the needs of organisations both large and small.

UNIFIED THREAT MANAGEMENT

Unified Threat Management and Next Generation Firewall solutions have evolved to address the fundamental need of IT managers to maximise both security and its return on investment. The proven answer to this challenge is to consolidate multiple technologies in a single all-in-one solution.

Such consolidation can potentially reduce both capital as well as operating expenses, as the number of devices and their associated management overhead are reduced. However, unless certain factors are taken into consideration, such solutions may also represent an unacceptable compromise.

All too many UTM solutions, while performing acceptably as firewalls, struggle to maintain adequate performance when other critical protection such as intrusion prevention or antivirus is enabled.

As network traffic increases to meet the growing demands of the business, so the performance of these solutions degrades further and IT managers resort to disabling essential layers of security. Another area where many traditional solutions currently fall short, is that of control. According to IDC, more than 40% of security breaches arise from errors in firewall configuration, and so with the additional functions of UTM, this problem may be compounded.

NETASQ - UNIFIED THREAT MANAGEMENT WITHOUT COMPROMISE

NETASQ UTM solutions come with all critical levels of protection enabled by default and due to their unique architecture, deliver this protection without compromising performance, security, or control. With the industry's most intuitive web-based management console and step by step wizards, administrators are guided intelligently through the configuration process while real-time alerts reduce the likelihood of mistakes as well as the time and cost of deployment. By hiding unnecessary complexity, the chances of leaving a security hole through misconfiguration are drastically reduced and the resulting level of protection increased.

DEFENSE-GRADE CERTIFICATIONS

This non-compromising combination of performance, protection and control has been recognized not only by a multitude of business customers worldwide, but also by major government and defense organizations. As a result, NETASQ is currently the only provider of UTM appliances to achieve the following certifications for its products:



NATO secrecy accredited VPN and Firewall Mailguard to the level of NATO Restricted.

<http://www.ia.nato.int/niapc/Search/netasq>



EU RESTRICTED Certification

<http://www.consilium.europa.eu/showpage.aspx?id=1892&lang=en>



EAL4+ certification (Common Criteria v 3.1)

http://www.commoncriteriaportal.org/files/epfiles/anssi_2009-30en.pdf

This unparalleled suite of certifications guarantees that NETASQ solutions, having met the most rigorous specifications of military, defense and governmental agencies, are among the most reliable, secure and effective UTM appliances on the market.

SERVICE AND SUPPORT

At NETASQ, we realize that no solution is complete without a comprehensive range of services, training and support to back it up, and through our network of over 750 channel partners across 40 countries, we have earned a solid reputation for quality and consistency of services.

Our NETASQ Certified Partners are the entry point for first level, local language support. This expanding community of Expert Certified Partners and Certified Support Centers have direct access to our own qualified engineers ensuring fast and effective support and services across Europe and much of the rest of the world. In addition to this, local language training courses are provided via an extensive network of NETASQ Certified Training Centers.

NETASQ NETWORK SECURITY

Our solutions give our customers assurance that a security threat will never jeopardize their activity. We enable business continuity and contribute to their success as they can focus 100% of their effort on growing their business. As computing threats grow more prevalent, dangerous and diverse we continue to develop innovative solutions to protect our customers' data, their communications and their network.

U-SERIES

NETASQ is best known for designing and building the NETASQ UTM (Unified Threat Management) range of "all-in-one" Network Security appliances that combine multiple security features in one device.

Key features include intrusion prevention, firewall, antivirus, antispymware, antispam, content filtering, VPN access and NETASQ Vulnerability Manager for improved real-time vulnerability detection and risk management.

YOUR BENEFITS

NETASQ believes that all organizations, no matter what their size, face the same threats. NETASQ includes as standard a wide range of features and tools which ensure our solutions are tailored specifically to meet your needs.

SME, large enterprises, geographically distributed organizations and MSSPs can all benefit from our real time, Zero-Day prevention network security solutions. Every NETASQ appliance includes protection against malware (virus, spam, phishing) and content and URL filtering.

In addition, our products support inter-site communication via IPSec VPN tunnels. We also include clientless access to network resources for remote users via SSL VPNs, as well as professional tools to configure and monitor our appliances and for log and event analysis.

THE ALL-IN-ONE FUNCTIONALITY OF NETASQ'S SOLUTION IS A MAJOR BENEFIT TO OUR CUSTOMERS.

— WEST LOTHIAN COUNCIL
ENGLAND

NG-SERIES

NG1000-A and NG5000-A are designed to meet the needs of large organizations.

Both the NG1000-A and the NG5000-A have been designed to protect high traffic e-commerce servers and dynamic university networks or as an IPS probe. They are equally suitable for secure high-speed Internet access and to protect critical data centers.

NETASQ's powerful administrative tools give you a single overview of the company's entire security policy, even when it covers many different sites. You can easily set up and monitor all your user access points and VPN interconnects.



Intrusion Prevention System (IPS)

NETASQ's combination of technologies allows you to choose the most appropriate protection for each threat, rather than being totally dependent upon signatures. The result is optimum security levels which meet all your needs. Every NETASQ firewall comes with IPS as standard.

Key factors include capabilities for optimizing detection, the ability to anticipate future attacks and of equal importance, is the ability to avoid the risk of false positive alerts.

VIRTUAL APPLIANCES

The benefits provided by virtualization are clear: cost reduction, resource optimization and easier service deployment and management, in addition to faster data recovery.

VIRTUAL APPLIANCES FOR SMB

Virtualization enables multiple services, many with different trust levels, to run on the same physical platform. This is a practice that requires powerful solutions to secure traffic flowing between each of the virtual machines.

As it is not possible to place a traditional firewall within a virtual network, the best way to monitor communication in a virtual environment is to deploy a virtual security appliance.

VIRTUAL APPLIANCES FOR ENTERPRISE

Many enterprises adopt virtualization as a means to consolidate their major data centers. It is crucial for them to ensure that new virtual architectures do not suffer any degradation in the level of protection afforded to them.

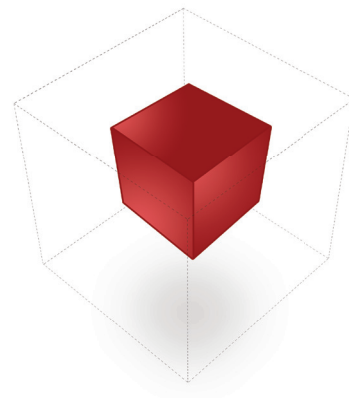
Enterprises adopt virtualization both to bring consistency to their IT infrastructure and to profit from a technology, which brings about a huge TCO reduction, enhanced system exploitation and manageability, load balancing, server portability and immediate recovery.

Enterprises need to maintain the same quality of security for virtual environments hosting their business critical applications and information, as previously granted within physical networks.

VIRTUAL APPLIANCES FOR SERVERS

To compete on today's market, organizations deploy more and more web and application services supporting 24x7 business operations. The level of investment for this uncontrolled growth being no longer acceptable, IT managers see in virtualization a viable means to highly reduce the costs of their server infrastructure.

From a security perspective though, virtualization is not a synonym for benefits. By fully overthrowing the traditional physical separation in different trust zones for back-end and front-end servers, virtualization is a two-edged sword. In the strive towards simpler, more consistent and agile hardware utilization, businesses often neglect, that virtual assets are exactly as vulnerable as their physical counterparts.



NETASQ MFILTRO

Time wasted and lost messages have become a norm for companies. In fact, spam and viruses can wipe out productivity. How much time do you waste everyday deleting spam from your inbox? Too much! Yet there is a solution.

THE BEST SPAM DETECTION RATE

MFILTRO has the best spam detection rate. The winning technologies embedded in the appliances make the MFILTRO range the most effective spam predator on the market.

GAIN PRODUCTIVITY NOW

MFILTRO improves security for your employees and restores their productivity by protecting your mail server. 80% of emails are spam (2008 figure)

With MFILTRO, you will be able to evaluate your employees' productivity gain. The spam spread will be hold back and you will be in a position to assess the savings your company has made in time and resources.

E-mail will become again what it always should have been: an efficient communication tool.

PLUG AND PROTECT

Thanks to a step by step configuration, you will enjoy effective protection on your mail infrastructure.

OPT FOR SIMPLICITY AND SECURITY

With the help of a simple and intuitive interface, your users will be able to easily create their own white lists of authorized senders.

Because every e-mail matters, MFILTRO allows every user to access and monitor his message quarantine. Your users will receive the daily report on spams detected by MFILTRO.

**THIS APPLIANCE IS TRULY AIRTIGHT,
NOTHING CAN GET THROUGH.**

— SHORR KAN IT ENGINEERING SRL
ITALY



Each year, spam can cause a company with 50 employees a cost of over 19,000€

With an average of 50 e-mails per day per employee, 80% of which are spams, it can take up to 14 hours and 26 minutes per year and per employee, simply to delete unwanted messages. Considering annual wages of 40K€, the overall cost is over 15K€ to which must be added 4k€ to cover indirect costs (such as bandwidth/storage/IT intervention)

NETASQ SERVICES

NETASQ's wide range of robust services sets standards of excellence and guarantees high levels of customer satisfaction. Some of these services are delivered by our trusted partners who are present in over 40 countries.

MAINTENANCE

NETASQ's comprehensive hardware and software maintenance programs deliver proactive protection, with maintenance packs that include exchange programs, extended warranties and an Active Update service to keep you one step ahead of the daily onslaught of new threats.

In addition you'll receive access to:

- The very latest major and minor software releases
- Intrusion Prevention Engine contextual signature updates
- Updates to dynamic URL lists

On top of this you'll benefit from:

- Access to our support centre via your partner
- A contract offering warranty and equipment exchange options with return times dependent on the maintenance pack selected

CONSULTANCY

Also available is a wide range of tailored consulting services developed by NETASQ experts to complement those of our trusted partners and integrators.

Professional Services as well as Technical Account Management address the specific needs of some of our most demanding customer environments.

SUPPORT

All NETASQ sales partners are fully trained and certified to enable them to provide direct, local language support, wherever you are in the world.

TRAINING

The NETASQ Institute provides training to its partners on an on-going basis to ensure they are fully qualified to support all NETASQ security products.

**FOR MORE THAN THREE YEARS
NOW, WE HAVE VALUED NETASQ'S
PROACTIVITY BOTH ON UPDATES AND
ON AFTER-SALES SERVICE.**

— CENTRE HOSPITALIER DE VALENCIENNES
FRANCE

End user training programmes are delivered by NETASQ Approved Certified Training Centers (NCTCs). There are numerous NCTCs across Europe and throughout the world guaranteeing that one will be conveniently located for you.

NETASQ has put in place a rigorous certification process to ensure that its training solutions are delivered to the highest standards of quality and professionalism.

NETASQ approved Training Center No. 31.59.05307.59

Active Update

Defending your network against attack is a daily struggle. Failure to invest in a solution which provides real-time protection puts your network security at risk and may cost your organization dearly. NETASQ understands these issues and our INITIAL and PRIVILEGE maintenance contracts offer you real-time protection in key areas:

- Updates for contextual signatures for the NETASQ intrusion prevention engine
- Updates for URL filter databases (Optenet as an option)
- Availability of major and minor software updates
- Availability of antivirus signatures (Kaspersky as an option)
- Updates for NETASQ Vulnerability Manager (as an option)
- Automatic updates for RBL servers and Whitelist

About NETASQ

With over 75,000 unified threat management firewalls deployed to business, government and defence organisations of all sizes, NETASQ delivers solutions of unrivalled performance, protection and control and the most comprehensive EU and NATO certifications of any firewall.

For further information: www.netasq.com

FRANCE Paris +33 1 46 21 82 30 france@netasq.com	BENELUX & NORDICS Breda +31 76 8883022 benelux@netasq.com	IBERICA Madrid +34 91 761 21 76 iberia@netasq.com	ITALIA Milano +39 02 7253 7249 italia@netasq.com	UK London +44 207 092 6682 uk@netasq.com	DACH München +49 89 20 300 6320 dach@netasq.com	MIDDLE EAST & AFRICA +971 50 5573 746 INTERNATIONAL international@netasq.com
---	--	--	---	---	--	---
