

NETASQ's IPS: KEY ADVANTAGES

Overview



Since its inception ten years ago, NETASQ has been recognized as one of the leading European network security providers with more than 45,000 appliances sold to date.

NETASQ works from a basic premise: no matter the size of an enterprise, the risk of attacks is exactly the same. NETASQ aspires therefore to provide the same complete, proactive solution for 0-day protection to all companies regardless

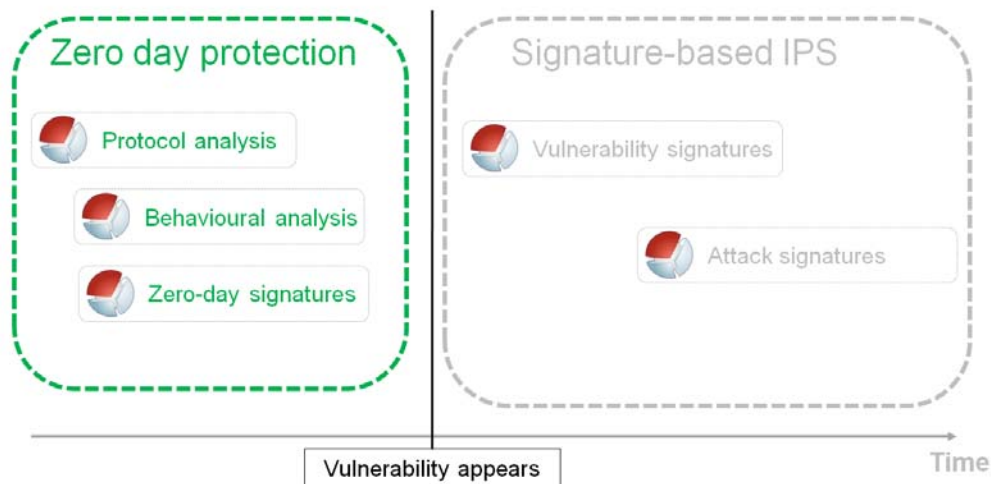
of their size.

Effective zero-day protection

NETASQ offers true “Zero-Day” protection security. The NETASQ engine (ASQ) is a unique technology in which all security features are part of the Operating System (kernel) at the network driver level. In addition to a traditional Firewall + attack signature features, traffic is automatically scanned upon arrival, combining 3 complementary technologies:

- ✓ **Protocol analysis** which combines deep understanding of the protocol, multiple security checks and traffic normalization
- ✓ **Behavioral analyses:** detection of abnormal behavior, such as scans, flood, covert channels, etc.
- ✓ **Zero-day protection contextual signatures:** over 30 signature databases. Each database is related to a specific protocol context.
- ✓ **Vulnerability & attacks contextual signatures:** These signatures are based on real-time security monitoring

The graph below shows which protections are true zero-day protections and which are based on security monitoring and require a quick and efficient reaction:

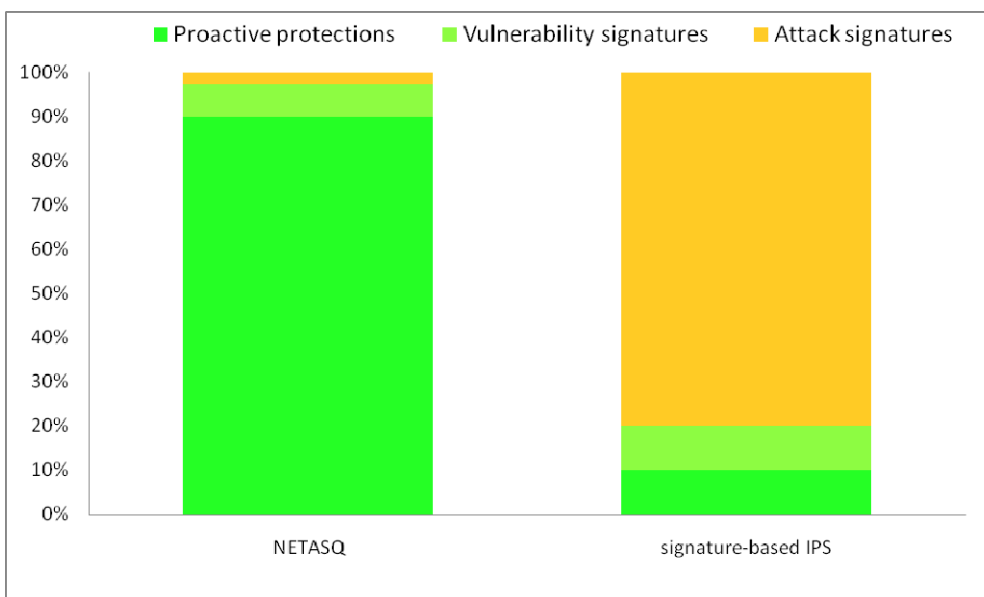


This combination of analysis methods favorably replaces thousands of traditional attack signatures.

Proactive protections vs attack signatures

When a new signature is required for each new variant of an attack, NETASQ’s zero-day protections respond proactively. The graph below displays an approximate distribution of the amount of attacks handled by each category of analysis.

The majority of the threats are proactively handled by NETASQ’s analysis



This means that the majority of new attacks are countered without the need to

create a new signature.

NETASQ's contextual signatures are highly-evolved versions of traditional signatures:

- ✓ Most of the signatures are zero-day protection signatures. One set of zero-day protection signatures such as SQL injection signatures **replace thousands of attack signatures**
- ✓ > 30 different databases based on protocol context drastically reduce the amount of signatures evaluated each time
- ✓ Thanks to the numerous protocol contexts, only a few sets of data are compared against a dedicated signature database
- ✓ Each signature database is compiled using the DAWG algorithm. This algorithm performs static analyses. **Performance is not directly linked to the number of signatures in a database.**

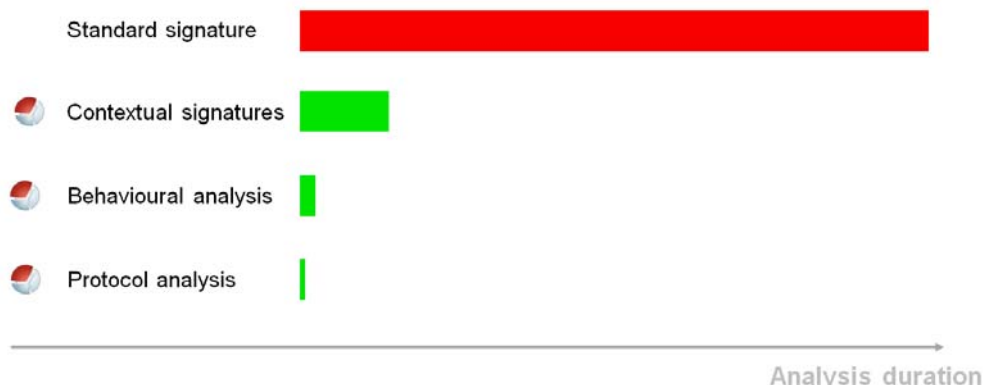
On top of that, NETASQ's IPS engine is also part of the NETASQ NGFW/UTM operating system. NETASQ's Stateful engine reassembles and monitors TCP/IP connections. It ensures that fragments do not overlap. It prevents traffic insertion and blocks attempts to guess the TCP sequence number. It has embedded protections against TCP reassembly DoS attacks.

Below is a non-exhaustive list of zero-day protections provided by NETASQ's IPS engine:

Zero-day protection	Dos and DDOS protections
✓ SQL injection prevention	✓ Intelligent connection management
✓ ICMP covert channel detection and blocking	✓ Configurable session purge that automatically adapts to traffic load
✓ XSS (cross-site scripting) prevention	✓ Protection against fragment reassembly attacks (rose attack)
✓ Multimedia traffic detection/blocking	✓ Flooding (ICMP/TCP/UDP)
✓ VoIP protections	✓ Attacks based on tiny IP fragments / MTU
✓ Several Buffer Overflow protections	✓ Several other TCP/IP-based DoS attacks

NETASQ continuously adds new protections to provide the best zero-day protection.

In terms of performance benefits, NETASQ's IPS technologies are far more efficient:



On an IPS based only on signatures, the number of signatures only reflects that a signature is needed to answer to each threat. **NETASQ's combination of technologies renders these metrics irrelevant because most of NETASQ's protections are proactive analyses.**

For example, below is a sample contextual signature of NETASQ's zero-day protection against SQL injections.

SQL injection prevention: suspicious SELECT statement in URL

Description: This alarm is raised when a suspicious combination of SQL known keywords is found in the URL.

Risk level: Moderate

Profiles	High	Medium	Low	Interrupt
Action	Block	Block	Block	Block
Level	Major	Minor	Minor	Major

References:

Available since: ASQ v3.2.0

Protection:

- Oracion Gallery SQL Injection and Cross Site Scripting Vulnerabilities
- Fluxus Hello "id" Parameter Remote SQL Injection Vulnerability
- Badnet "username" and "password" Remote SQL Injection Vulnerabilities
- Milnews "username" and "password" Remote SQL Injection Vulnerabilities
- Auth PHP "username" and "password" Remote SQL Injection Vulnerabilities
- PHP Director "username" Parameter Remote SQL Injection Vulnerability
- A Better Member-Based ASP Photo Gallery SQL Injection Vulnerability
- BusinessSpoker "id" Parameter Remote SQL Injection Vulnerability
- mlb.com Multiple Parameter Remote SQL Injection Vulnerabilities
- F-CMS "id" Parameter Handling Remote SQL Injection Vulnerability
- Cartoonize "url" Parameter Remote SQL Injection Vulnerability
- Emf FTP Data Processing Remote SQL Injection Vulnerability
- Fedora Security Update: Focus GLEP Multiple SQL Injection Vulnerabilities
- ClamAV "file" Parameter Remote SQL Injection Vulnerability
- GameSonic Remote SQL Injection and Local File Inclusion Vulnerabilities
- CompuLink CMS "id" Parameter Remote SQL Injection Vulnerability
- Max Blog "id" Parameter Handling Remote SQL Injection Vulnerability
- SHIP-NET "url" Parameter Remote SQL Injection Vulnerability
- Flash Message Deluxe for Joomla Remote SQL Injection Vulnerability
- ClickAuction "idEmail" Parameter Remote SQL Injection Vulnerability
- Google Gdata "url" Parameter Remote SQL Injection Vulnerability
- Yakuzen Online Software "url" Remote SQL Injection Vulnerability
- PHP-CMS "username" Parameter Remote SQL Injection Vulnerability

Equivalent to 1,540+ attack signatures (still counting)

Equivalent to 1,540+ attack signatures

Reference: <https://www.netasq.com/securitykb/us/9f26454f52554494.html>

Each set of NETASQ's contextual signatures may protect against hundreds/thousands of threats which would otherwise have required a dedicated signature for an IPS based on signatures only. NETASQ's IPS engine proactively protects against thousands of known and also future threats thanks to the combination of different analyses.

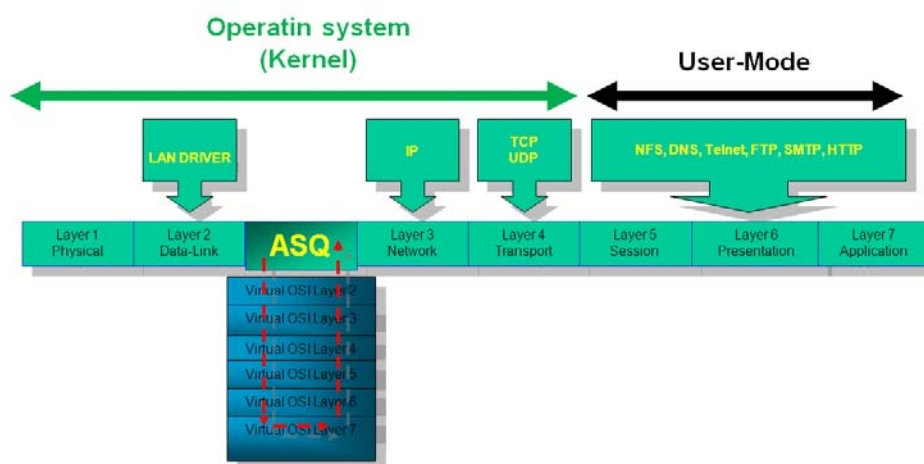
Highest IPS Performance

Since NETASQ's IDS/IPS engine is embedded in the Operating System, it is able to get exclusive access to all the resources (CPU and memory) on the appliance. While some architecture rely on dedicated chips for a specific task, thereby increasing the cost for only a part of the IPS inspection, NETASQ's engine intercepts traffic in real-time on the original network flow, at the hardware driver level. This dedicated allocation from hardware components enables the NETASQ IPS engine to get optimal resources for the complete analysis.

ASIC-based analyses are relevant for specific tasks such as IPsec encryption / decryption and NETASQ appliances use ASIC when appropriate. Network security is a fast-moving world where ASIC is not the most efficient answer.

The NETASQ IPS engine (ASQ) provides Layer 7 protection within the operating system. This saves a lot of resources:

- ✓ No context switching (OS <-> system)
- ✓ No duplicate data (OS memory <-> system memory)
- ✓ Traffic analysis: no proxy required (saves a lot of resources)



NETASQ's unique IPS architecture prevents performance bottlenecks which occur when only part of the required Intrusion Prevention has access to hardware-accelerated components.

Fight efficiently against false positives

NETASQ's IPS engine combines several technologies to attain a false positive rate that falls below 1/100,000 (0.001%).

The most false positive prone technology is signature-based detection. With the combination of several analyses, NETASQ's approach to Intrusion Prevention has proven to be efficient against false positives:

Automatic protocol detection ensures that the correct layer 7 analysis will be applied. A basic signature approach might incorrectly detect web attacks in word documents transmitted using the web or even via e-mail because of the lack of context around the signature evaluation (see below).

Protocol-based protections: Incorrect usage of signatures when protocol understanding is required increases the risk of false positives. For example, signature-based detection for buffer overflow has a high false positive risk. See this example of a Snort signature to detect FTP buffer overflow:

GEN:SID	1:341
Message	FTP EXPLOIT overflow
Rule	alert tcp \$EXTERNAL_NET any -> \$HOME_NET 21 (msg:"FTP EXPLOIT overflow"; flow:to_server,established; content:"XXXXXXXX" classtype:attempted-admin, sid:341, rev:6)

NETASQ's IPS engine uses thousands of protocol analyses when they are more relevant. This ensures a very low rate of false positives.

Several behavioral analyses replace in a more efficient way poorly-adapted signatures. For example, detecting every ICMP ping covert channel requires as many signatures as there are covert channel programs. The NETASQ IPS engine detects and effectively blocks these channels with a behavior-based analysis (check that ICMP ECHO payload = ICMP REPLY payload)

NETASQ's signatures rely on **protocol normalization** to effectively fight against evasion techniques and events at the application level. For example: http traffic is decoded (utf8, % encoding ...) and normalized before being inspected for attacks.

More than 30 different protocol contexts allow focusing threat searches on a target traffic portion (SIP request or answer, URL parameter, URL specific header, etc.). This has huge benefits compared to standard signature-based approaches.

Contextual signatures targeting vulnerabilities as opposed to most of the known signatures which focus on detecting known attacks (exploits). Signatures which focus on detecting vulnerabilities try to intercept an abnormal behavior. Without any context this might increase the risk of false positives: abnormal behavior for a protocol or a specific part of a protocol might be perfectly normal for another protocol and therefore trigger false alerts.

For this reason, a traditional signature-based approach focuses on attack detection. NETASQ's approach of using contextual signatures allows more effective vulnerability detection and saves the creation of thousands of attack signatures: since each attack signature adds a false positive risk, avoiding these unnecessary signatures drastically reduces the amount of false alerts (and has huge benefits in terms of performance).

Automated and targeted configuration profiles enable a fine-tuned configuration which prevents, for example, protection mechanisms on some company servers from triggering alarms when a user browses public websites.

Case study of the Kaminsky DNS vulnerability

The exploitation of this vulnerability allows passing off false DNS responses for valid responses (DNS spoofing). The attacks work on the basis of being able to guess the random elements (DNS ID and UDP port) necessary for creating a response in the right format.

	Signature-based IPS	NETASQ
Detection of attack behavior	<p style="text-align: center;">x</p> <p>No specific pattern can be found</p>	<p style="text-align: center;">✓</p> <p>"Targeted DNS spoofing attempt" alarm raised</p>
Allowing a single valid response	<p style="text-align: center;">x</p> <p>This requires a behavioral analysis and deep understanding of DNS protocol</p>	<p style="text-align: center;">✓</p> <p>The behavioral analysis only allows one response in the event of an attack.</p>

NETASQ's different behavioral analyses provide effective protection from the attack discovered by Mr Kaminsky.

NETASQ SEISMO: Real-Time Risk Management

Network protection is one of the foundations of high-level security. In addition to a Multifunction Firewall and proactive modes of protection, making the network as fireproof as possible is an everyday challenge. Risk management is driven by the compromise between risks and how much it costs to avoid them. One of the key risk factors is the lack of information on specific issues.

[Network overview](#)

- 87 vulnerabilities were detected on the monitored networks
- 19 of the vulnerabilities are critical
- 76 of the vulnerabilities are remote

Name	Family	Instance
Apache (Debian)	Web Server	1
Firefox	Web Client	9
FreeBSD	Operating System	1
HotBar HbInst	Malware	2
lighttpd	Web Server	1
Linux	Operating System	5
Microsoft Internet Explorer	Web Client	5
Microsoft Windows 2003	Operating System	1
OpenSSH	SSH	2
Postfix Server	Mail Server	1
Wget	Web Client	1

NETASQ Firewalls use real-time network information to assess the risk for each monitored user/computer. This unique engine, called SEISMO, is embedded in the operating system of NETASQ NGFW and Multifunction Firewalls (UTM). This brings a whole new range of information about existing applications and vulnerabilities.

In addition, the administrator is led to the solution that will decrease this risk and can get automatic reports about the evolution of the risk level for the company.

Name	Address	Users	Operating system	Vulnerabilities	Applications	Events
Estelle	172.30.103.11	Estelle	Linux	7	2	3
Dave	172.30.103.13	Dave	Microsoft Windows	0	1	0
Bob	172.30.103.20	Bob	Linux	18	1	1

Severity	Application name	Name
Critical	Firefox 2.0.0.1	Mozilla Firefox and SeaMonkey 'IMG' Tag Handling Remote Code Execution Vulnerability
Critical	Firefox 2.0.0.1	Mozilla Products Memory Corruption and Cross-site Request Forgery Issues
Critical	Firefox 2.0.0.1	Mozilla Firefox 'FirefoxURL' URI Handler Registration Code Execution Vulnerability
Critical	Firefox 2.0.0.1	Mozilla Firefox and Seamonkey Code Execution and Security Byblock Vulnerabilities
Critical	Firefox 2.0.0.1	Mozilla Firefox/SeaMonkey Code Execution and Information Disclosure

Detailed vulnerability view per host/user: vulnerability is, of course, documented

Conclusion

NETASQ offers exemplary “zero tolerance” reactivity to security problems. All the analyses that comprise the intrusion prevention system are automatically present and active from the moment the product is installed. As opposed to most competitors who added a software IPS module to a previous firewall solution, NETASQ’s technology was conceived from the beginning as an IPS upon which the firewall functionality was added. Moreover NETASQ is the only security vendor to embed natively real-time vulnerability detection and risk management.