

# Multi-function security devices score over point solutions

**What is a Multi-function Security Device (MSD) and how can it benefit an organization?**

A typical security MSD combines the functionalities of a firewall, IDS, anti-virus into a single device. It offers benefits like ease of management, centralized policy creation, and lesser cost.

Integrated appliance solutions offer a wide range of security features that eliminate the cost of the operating system software, as well as payment for each individual security software package. The company also saves manpower and training costs for the IT team

In large enterprises with geographically distributed branch offices, an individual firewall, IDS, and anti-virus solution at each point of entry creates manageability problems. This is because the security manager will need manpower at each of the locations to manage these devices.

With the use of an MSD in a network can be centrally managed and centralized logging, reporting, and remote policy updates can be done by a central security team.



**What are the cost benefits, in particular of using an MSD?**

An integrated appliance-based solution offers a number of cost advantages over software point solutions.

Consider a typical company that

has deployed anti-virus, firewall, content-filtering, and IDS/IPS software on several servers. The company has to pay for each individual software package, its associated licenses, and the operating system licenses.

Integrated appliance solutions offer a wide range of security features that eliminate the cost of the operating

system software, as well as payment for each individual security software package. The company also saves manpower and training costs for the IT team.

**Will companies need to replace existing point solutions with a new multi-function device?**

Although it seems logical, both from a manageability and fiscal perspective, that companies would eventually replace all existing point solutions, enterprises are more likely to initially deploy a multi-function security appliance together with their existing security tools, perhaps fulfilling a specific function not currently being addressed.

However, more often than not, as the security appliance proves its usefulness and the need to purchase upgrades to existing software approaches, customers abandon the point software approach in favor of a

more sensible hardware-based appliance architecture and simply 'turn on' additional functionality.

**Are there any different types or categories of MSDs?**

The multi-function security device market is not homogeneous. There are actually three different categories of vendors of multi-function network appliances.

There are traditional software based firewall/anti-virus/IDS vendors currently aligning themselves with PC-based hardware manufacturers, calling their products integrated appliances with modular costing. There are hardware manufacturers who build ready-made appliances with security software pre-loaded on these appliances.

And there are high performance ASIC-based security appliances, ranging integrated firewall, VPN, IDS, AV and content filtering functions.

There are genuine technology limitations in hard disk-based system because of the latencies involved in reading from and writing to disk. For systems that offer deep packet inspection, data packets need to be assembled into their original messages and scanned for viruses and malicious content. The

computing overhead taxes PC-based architectures and significantly decreases network performance.

**What issue can the customer face from the use of an integrated device?**

Traditional software-based security vendors are quickly aligning with hardware manufacturers to port their existing software packages to those hardware platforms. These software solutions could be only anti-virus, anti-spam, or an IDS.

ASIC chips are integrated circuits that are built for a specific function. With ASIC hardware, much of the security functions and processing occurs in the ASIC chips, without impacting CPU or network performance

These vendors say that they provide the best-of-breed products on a single appliance. Although the argument seems persuasive on the surface, the biggest drawbacks are support and cost of ownership. Relationships are typically loose, between the companies that produce the security software and the

companies that develop and support the operating system.

The customer does not have any commitment from either party that he would get support in case he runs into problems. Typically customers are told that the 'other party' owns and has responsibility for answering the customer's support request.

**How can an ASIC-based integrated appliance architecture help?**

Typically, point security soft-

ware solutions are installed on top of commodity server hardware. The problem with this approach is that the software has to share the CPU or CPUs with operating system software and other applications, which may be running on the server. The server CPU then becomes the bottleneck.

ASIC chips are integrated circuits that are built for a specific function. With ASIC hardware, much of the security functions and processing occurs in the ASIC chips, without impacting CPU or network performance.

With increased processing bandwidth, the security appliance can incorporate more features like deep packet inspection, which re-assembles data packets and scans them for viruses and malicious content—a processor-intensive task that commodity hardware will find difficult to match. □

Soumitra Das Gupta can be reached at [soumitra@networkmagazineinside.com](mailto:soumitra@networkmagazineinside.com)

